NetIQ Identity Manager

Einrichtungshandbuch Bei Linux

Februar 2018

NetIQ

Rechtliche Hinweise

Inhalt

Info zu diesem Handbuch und zur Bibliothek

Das *Einrichtungshandbuch* bietet Anweisungen zum Installieren von NetIQ Identity Manager (Identity Manager). In diesem Handbuch wird die Installation 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 Identity Manager-Bibliothek finden Sie auf der Website der Identity Manager-Dokumentation.

Info zu NetIQ Corporation

NetIQ ist ein globaler Hersteller von Unternehmenssoftware. Unser Fokus liegt auf drei besonderen Herausforderungen, die Sie in Ihrer Umgebung meistern müssen: Änderungen, Komplexität und Risiken. Unser Ziel ist es, Sie dabei zu unterstützen.

Unser Standpunkt

Sich an Änderungen anzupassen und Komplexität und Risiken zu beherrschen ist nichts Neues

Unter den verschiedenen Herausforderungen, denen Sie gegenüberstehen, beeinflussen diese drei Punkte sicherlich am meisten Ihre Möglichkeiten, Ihre physischen, virtuellen und Cloud-Umgebungen sicher zu messen, zu überwachen und zu verwalten.

Kritische Geschäftsservices schneller und besser bereitstellen

Wir sind davon überzeugt, dass IT-Organisationen über eine möglichst umfassende Kontrolle verfügen müssen, um eine zeitgerechte und kostenwirksame Servicebereitstellung zu ermöglichen. Der von Änderungen und Komplexität ausgehende, kontinuierliche Druck steigt ständig, weil sich die Unternehmen ständig ändern und die erforderlichen Technologien zur Verwaltung der Änderungen immer komplexer werden.

Unsere Philosophie

Intelligente Lösungen entwickeln, nicht einfach Software

Damit Sie jederzeit die Kontrolle behalten, informieren wir uns zunächst über sämtliche Aspekte der Szenarien, in denen IT-Unternehmen wie Ihres tagtäglich arbeiten. Nur so können wir praxistaugliche, intelligente IT-Lösungen entwickeln, die nachweisbar messbare Ergebnisse liefern. Und das ist für uns wesentlich bereichernder, als einfach eine Software zu verkaufen.

Ihr Erfolg ist unsere Leidenschaft

Ihr Erfolg ist der Wegweiser für unser Geschäft. Wir wissen, dass Sie IT-Lösungen von der Produktkonzeption bis hin zur Bereitstellung suchen, die richtig funktionieren und nahtlos mit Ihren vorhandenen Investitionen integriert werden können. Sie benötigen fortlaufenden Support, Schulungen nach der Bereitstellung und jemanden, mit dem Sie unkompliziert arbeiten können. Ihr Erfolg ist auch unser Erfolg.

Unsere Lösungen

- Identitäts- und Zugriffsregelung
- Zugriffsverwaltung
- Sicherheitsverwaltung
- System- und Anwendungsverwaltung

- Workload-Management
- Serviceverwaltung

Anfragen an die Verkaufsunterstützung

Bei Fragen zu Produkten, Preisen und Funktionen wenden Sie sich an Ihren Händler vor Ort. Wenn dies nicht möglich ist, wenden Sie sich an unser Verkaufsunterstützungsteam.

Weltweit:	www.netiq.com/about_netiq/officelocations.asp
Vereinigte Staaten und Kanada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Kontakt zum technischen Support

Bei spezifischen Produktproblemen, wenden Sie sich an unseren technischen Support.

Weltweit:	www.netiq.com/support/contactinfo.asp
Nord- und Südamerika:	1-713-418-5555
Europa, Naher Osten und Afrika:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Kontakt zum Dokumentationssupport

Wir möchten Ihnen stets eine nützliche, aussagekräftige Dokumentation an die Hand geben. Die Dokumentation für dieses Produkt steht auf der NetIQ-Website im HTML- und PDF-Format zur Verfügung. Für den Zugriff auf diese Dokumentationsseite ist keine Anmeldung erforderlich. Wenn Sie uns einen Verbesserungsvorschlag in Bezug auf die Dokumentation mitteilen möchten, klicken Sie auf die Schaltfläche **comment on this topic** (Kommentar zum Thema abgeben) unten auf jeder Seite der HTML-Version unserer Dokumentation auf der Netiq-Dokumentationswebseite. Sie können Verbesserungsvorschläge auch per Email an Documentation-Feedback@netiq.com senden. Wir freuen uns auf Ihre Rückmeldung.

Kontakt zur Online-Benutzer-Community

NetIQ Communities, die NetIQ-Online-Community, ist ein Netzwerk zur Zusammenarbeit mit anderen NetIQ-Benutzern und -Experten. NetIQ Communities bietet Ihnen aktuelle Informationen, nützliche Links zu hilfreichen Ressourcen und Kontakt zu NetIQ-Experten, damit Sie über die Voraussetzungen verfügen, um alles aus den IT-Investitionen herauszuholen, auf die Sie sich verlassen. Weitere Informationen finden Sie im Internet unter community.netiq.com.

Einführung

Mit NetIQ Identity Manager errichten Sie ein intelligentes Rahmenwerk für das Identitätsmanagement Ihres Unternehmens – sowohl innerhalb der Firewall als auch in der Cloud. Identity Manager zentralisiert die Verwaltung des Benutzerzugriffs und sorgt dafür, dass jeder Benutzer genau eine Identität besitzt – von den physischen und virtuellen Netzwerken bis hin zur Cloud.

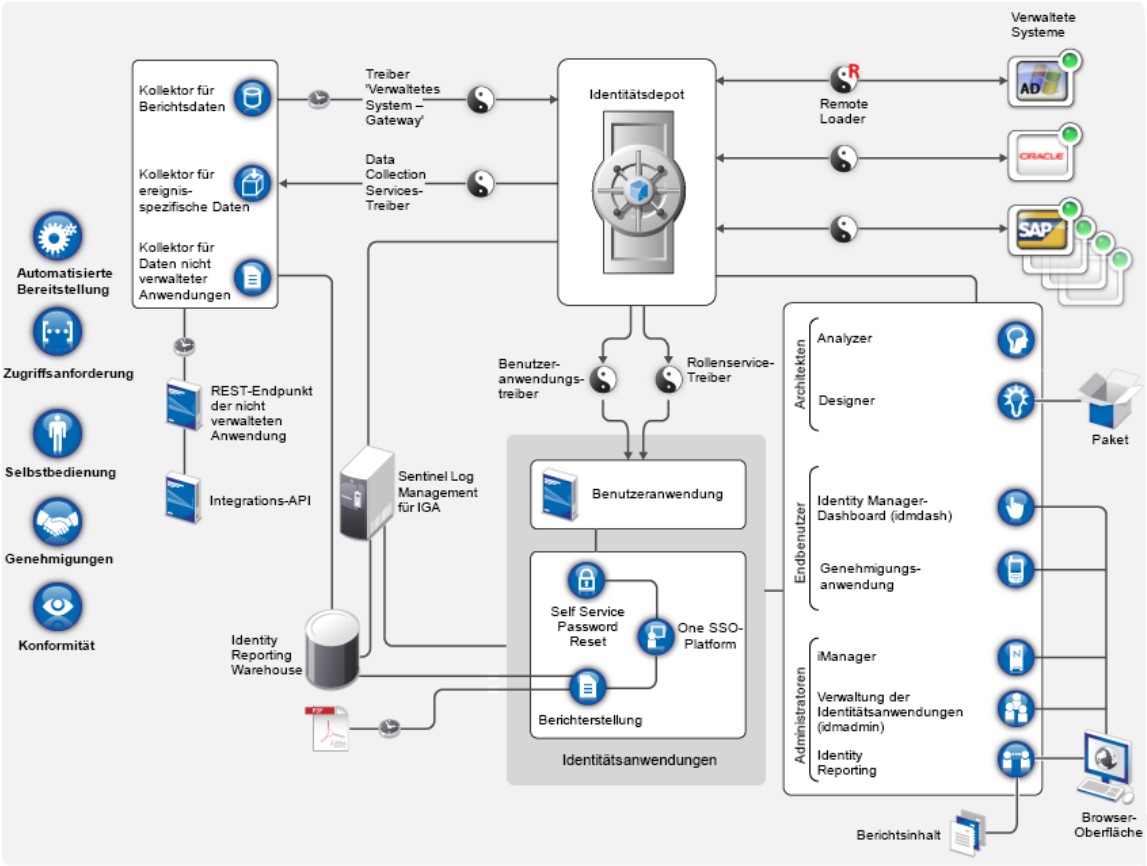
Im Allgemeinen lassen sich die Komponenten von Identity Manager in die folgenden Bereiche gliedern:

- Identity Manager-Umgebung erstellen und pflegen. Weitere Informationen finden Sie unter Kapitel 2, „Erstellen und Pflegen der Identity Manager-Umgebung“, auf Seite 19.
- Identity Manager-Umgebung überwachen (z. B. Benutzerbereitstellungsaktivititäten prüfen und Berichte über diese Aktivitäten erstellen). Auf diese Weise können Sie die Konformität mit den Geschäfts-, IT- und Unternehmensrichtlinien nachweisen. Weitere Informationen finden Sie unter Kapitel 3, „Verwalten von Daten in der Identity Manager-Umgebung“, auf Seite 21.
- Benutzerbereitstellungsaktivitäten überwachen, z. B. Rollen, Beglaubigungen und Self-Service für bestimmte Benutzer. Weitere Informationen finden Sie unter Kapitel 4, „Bereitstellen von Benutzern für den sicheren Zugriff“, auf Seite 25.

In diesem Abschnitt werden die Identity Manager-Komponenten für diese Aktivitäten vorgestellt. Auf der Grundlage dieser Angaben können Sie beginnen, die Installation des Produkts zu planen. Einen Überblick über die Zusammenhänge zwischen diesen Komponenten finden Sie in Kapitel 1, „Übersicht der Komponenten von Identity Manager“, auf Seite 17.

1 Übersicht der Komponenten von Identity Manager

Identity Manager sorgt dafür, dass jeder Benutzer mit genau einer Identität aus Ihren physischen und virtuellen Netzwerken in der Cloud auftritt. Das folgende Diagramm zeigt die höchste Ebene der Komponenten, die die Funktionen von Identity Manager unterstützen. Bestimmte Komponenten können auf demselben Server installiert werden, je nach Größe der Identitätsmanagement-Lösung. Einige andere Komponenten, beispielsweise die Identitätsberichterstellung, bieten jedoch eine browserbasierte Benutzeroberfläche, auf die Benutzer über eine Arbeitsstation oder eine mobile Plattform zugreifen.



In Identity Manager versteht man unter einem **verwalteten System** (auch **verbundenes System** oder **Anwendung** genannt) ein System, ein Verzeichnis, eine Datenbank oder ein Betriebssystem, dessen/deren Identitätsinformationen Sie verwalten möchten. Verbundene Systeme sind beispielsweise die PeopleSoft-Anwendung oder ein LDAP-Verzeichnis. Ein **Treiber**, wie etwa der Data Collection Services Driver, sorgt für die Verbindung zwischen einem verwalteten System und dem Identitätsdepot. Er ermöglicht darüber hinaus die Datensynchronisierung und Datenfreigabe zwischen Systemen. Identity Manager speichert Treiber und Bibilotheksobjekte in einem besonderen Container (einem **Treibersatz**).

2 Erstellen und Pflegen der Identity Manager-Umgebung

In den meisten Unternehmen erfolgt die Entwicklung und das Staging von Identity Manager in separaten Umgebungen, bis die Anwendung schließlich in der Produktionsumgebung bereitgestellt wird. Mit den folgenden Identity Manager-Komponenten können Sie die Identity Manager-Umgebung aufbauen und pflegen:

- Abschnitt 2.1, „Designer für Identity Manager“, auf Seite 19
- Abschnitt 2.2, „Analyzer für Identity Manager“, auf Seite 19
- Abschnitt 2.3, „iManager“, auf Seite 20

Diese Komponenten tragen außerdem dazu bei, Identity Manager an die veränderlichen Anforderungen Ihres Unternehmens anzupassen, wodurch Sie die Unternehmenskontinuität wahren und die Produktivität der Benutzer unternehmensweit steigern.

2.1 Designer für Identity Manager

Designer für Identity Manager (Designer) hilft beim Konzipieren, Testen, Dokumentieren und Bereitstellen von Identity Manager-Lösungen in einer Netzwerk- oder Testumgebung. Sie können das 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 Identity Manager-Lösung werden grafisch dargestellt, und ihre Zusammenarbeit wird überwacht.
- Ändern und testen Sie Ihre 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.

Weitere Informationen zur Verwendung von Designer finden Sie im *NetIQ Designer for Identity Manager Administration Guide* (Administrationshandbuch zu Designer für Identity Manager).

2.2 Analyzer für Identity Manager

Analyzer für 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.

Weitere Informationen zur Verwendung von Analyzer finden Sie im *NetIQ Analyzer for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer für Identity Manager).

2.3 iManager

Das browsergestützte Werkzeug **NetIQ iManager** fungiert als zentraler Administrationspunkt für zahlreiche Novell- und NetIQ-Produkte (z. B. Identity Manager). Sobald Sie die Identity Manager-Plugins für iManager installiert haben, können Sie Identity Manager verwalten und Echtzeitinformationen zum Zustand und Status Ihres Identity Manager-Systems erhalten.

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

Weitere Informationen zu iManager finden Sie im *NetIQ iManager-Administrationshandbuch*.

3 Verwalten von Daten in der Identity Manager-Umgebung

Identity Manager erzwingt einheitliche Zugriffskontrollen in physischen und virtuellen Netzwerken sowie in Cloud-Netzwerken, wobei die Konformität in dynamischen Berichten nachgewiesen wird. Identity Manager synchronisiert im Wesentlichen alle Arten von Daten, die in der verbundenen Anwendung oder im Identitätsdepot gespeichert sind. Die folgenden Komponenten der Identity Manager-Lösung sind für die Synchronisierung (auch Passwortsynchronisierung) zuständig:

- Identitätsdepot
- Identity Manager-Engine
- Identity Manager Remote Loader
- Fan-out-Agent
- Identitätsberichterstellung
- Identity Manager-Treiber
- Verbundene Systeme

3.1 Erläuterungen zur Datensynchronisierung

Mit Identity Manager können Sie Informationen über eine Vielzahl an verbundenen Systemen hinweg synchronisieren, transformieren und verteilen, z. B. Daten aus SAP, PeopleSoft, Microsoft SharePoint, Lotus Notes, Microsoft Exchange, Microsoft Active Directory, NetIQ eDirectory und LDAP-Verzeichnissen. Mit Identity Manager können Sie die folgenden Aufgaben durchführen:

- Datenfluss zwischen den verbundenen Systemen steuern.
- Festlegen, welche Daten gemeinsam genutzt werden, welches System als autorisierte Quelle für bestimmte Daten fungiert und wie die Daten gemäß den Anforderungen anderer Systeme interpretiert und transformiert werden müssen.
- Passwörter zwischen Systemen synchronisieren. Wenn ein Benutzer beispielsweise sein Passwort in Active Directory ändert, kann Identity Manager diese Änderung an Lotus Notes und Linux weitergeben.
- Neue Benutzerkonten in Verzeichnissen (z. B. Active Directory), Systemen (z. B. PeopleSoft und Lotus Notes) und unter Betriebssystemen (z. B. UNIX und Linux) erstellen und vorhandene Konten entfernen. Wenn Sie beispielsweise einen neuen Mitarbeiter zu Ihrem SAP-Personalsystem hinzufügen, kann Identity Manager automatisch ein neues Benutzerkonto in Active Directory, ein neues Konto in Lotus Notes und ein neues Konto in einem Linux NIS-Kontenverwaltungssystem erstellen.

3.2 Erläuterungen zu Revision, Berichterstellung und Konformität

Ohne Identity Manager kann die Bereitstellung für Benutzer ein mühsamer, zeitaufwändiger und kostenintensiver Vorgang sein. Sie müssen überprüfen, ob die Bereitstellungsaktivitäten gemäß den Richtlinien, Anforderungen und Vorschriften Ihres Unternehmens erfolgt sind. Haben die richtigen

Mitarbeiter Zugriff auf die richtigen Ressourcen? Ist gewährleistet, dass Unbefugte nicht auf diese Ressourcen zugreifen können? Hat der neue Mitarbeiter Zugriff auf das Netzwerk, seine Emails und die weiteren für seine Arbeit erforderlichen Systeme? Wurde der Zugriff für den Mitarbeiter, der die Firma letzte Woche verlassen hat, gesperrt?

Mit Identity Manager haben Sie die Gewissheit, dass alle Benutzerbereitstellungsaktivitäten - vorangegangene und aktuelle - verfolgt und zu Revisionszwecken protokolliert werden. Aus diesem Identitätsinformations-Warehouse können Sie jederzeit alle Informationen abrufen, die für die Einhaltung der für Ihre Organisation geltenden geschäftlichen Regeln und Richtlinien erforderlich sind.

Identity Manager enthält vordefinierte Berichte für Identitätsinformations-Warehouse-Abfragen zur Sicherstellung der Einhaltung von Geschäfts-, IT- und Firmenrichtlinien. Sie können auch benutzerdefinierte Berichte erstellen, falls die vordefinierten Berichte für Ihre Anforderungen nicht geeignet sind.

3.3 Erläuterungen zu den Komponenten für die Synchronisation der Identitätsdaten

3.3.1 Identitätsdepot

Das **Identitätsdepot** enthält alle Informationen, die für Identity Manager erforderlich sind. Das Identitätsdepot dient als Metaverzeichnis der Daten, die zwischen den verbundenen Systemen synchronisiert werden sollen. Zum Beispiel werden Daten, die von einem PeopleSoft-System nach Lotus Notes synchronisiert werden, zuerst zum Identitätsdepot hinzugefügt, bevor sie an das Lotus Notes-System gesendet werden. Im Identitätsdepot werden außerdem besondere Informationen für Identity Manager gespeichert, z. B. Treiberkonfigurationen, Parameter und Richtlinien.

Das Identitätsdepot nutzt eine NetIQ-eDirectory-Datenbank. Weitere Informationen zur Verwendung von eDirectory finden Sie im NetIQ eDirectory -Administrationshandbuch.

3.3.2 Identity Manager-Engine

Die Identity **Manager-Engine** verarbeitet die Datenänderungen, die im Identitätsdepot oder in einer verbundenen Anwendung vorgenommen werden. Bei Ereignissen, die im Identitätsdepot auftreten, verarbeitet die Engine die Änderungen und sendet über den Treiber Befehle an die Anwendung. Bei Ereignissen, die in der Anwendung auftreten, empfängt die Engine die Änderungen vom Treiber, verarbeitet diese und sendet Befehle an das Identitätsdepot. Die Identity Manager-Engine ist über **Treiber** mit den Anwendungen verbunden. Ein Treiber hat zwei grundlegende Aufgaben: Er meldet Datenänderungen (Ereignissen) in der Anwendung an die Identity Manager-Engine und führt

Datenänderungen (Befehle) aus, die von der Identity Manager-Engine an die Anwendung gesendet werden. Die Treiber müssen auf demselben Server wie die verbundene Anwendung installiert werden.

Die Identity Manager-Engine wurde bislang auch als Metaverzeichnis-Engine bezeichnet. Der Server, auf dem die Identity Manager-Engine ausgeführt wird, wird als **Identity Manager-Server** bezeichnet. Je nach Serverauslastung können Sie mehrere Identity Manager-Server in Ihrer Umgebung betreiben.

3.3.3 Remote Loader

Der **Identity Manager Remote Loader** lädt die Treiber, die auf den Remote-Servern installiert sind, und kommuniziert an deren Stelle mit der Identity Manager-Engine. Wenn die Anwendung auf demselben Server wie die Identity Manager-Engine ausgeführt wird, können Sie den Treiber auf diesem Server installieren. Wird die Anwendung dagegen nicht auf demselben Server wie die Identity Manager-Engine ausgeführt, müssen Sie den Treiber auf dem Anwendungsserver installieren.

Weitere Informationen zum Remote Loader finden Sie in Abschnitt 8.4.2, „Erläuterungen zum Remote Loader“, auf Seite 69.

3.3.4 Identitätsberichterstellung

Das **Identitätsinformations-Warehouse** in Identity Manager bildet ein intelligentes Repository mit Angaben zum aktuellen und gewünschten Status des Identitätsdepots und der verwalteten Systeme in Ihrer Organisation. Mit dem Identitätsinformations-Warehouse erhalten Sie einen Gesamtüberblick über alle Geschäftsberechtigungen, und es wird ersichtlich, welche Autorisierungen und Berechtigungen den Identitäten in Ihrer Organisation in der Vergangenheit und Gegenwart erteilt wurden.

Beim Abfragen dieses Identitätsinformations-Warehouse erhalten Sie alle Informationen, die für die Einhaltung der für Ihre Organisation geltenden geschäftlichen Regeln und Richtlinien erforderlich sind. Somit haben Sie die Gewissheit, dass Sie für die Einhaltung selbst anspruchsvollster GRC-Richtlinien gerüstet sind.

Für die Infrastruktur des Identitätsinformations-Warehouse sind die folgenden Komponenten erforderlich:

- „Identitätsberichterstellung für Identity Manager“, auf Seite 23
- „Datenerfassungsdienst“, auf Seite 24
- „Treiber „Verwaltetes System – Gateway““, auf Seite 24

Identitätsberichterstellung für Identity Manager

Das Identity Information Warehouse speichert die Daten in der SIEM-Datenbank von Sentinel Log Management für Identity Governance and Administration (IGA). Mit der **Identitätsberichterstellung** in Identity Manager können Sie die Identity Manager-Lösung prüfen und Berichte dazu erstellen. Die Berichte können Ihnen dabei helfen, die Einhaltung etwaiger für Ihre Branche geltender Vorschriften zu gewährleisten. Mithilfe von vordefinierten Berichten können Sie die Konformität mit den Geschäfts-, IT- und Unternehmensrichtlinien nachweisen. Sie können auch benutzerdefinierte Berichte erstellen, falls die vordefinierten Berichte für Ihre Anforderungen nicht geeignet sind. Mit der Identitätsberichterstellung können Sie Berichte generieren, die unternehmenskritische Informationen zu verschiedenen Aspekten Ihrer Identity Manager-Konfiguration liefern, z. B. Informationen, die zu Identitätsdepots und zu den verbundenen Systemen erfasst wurden. 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 zur Identitätsberichterstellung finden Sie im *Administrator Guide to NetIQ Identity Reporting* (Administratorhandbuch für die NetIQ-Identitätsberichterstellung).

Datenerfassungsdienst

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:

- **Berichtsdatenkollektor:** 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 Kollektor ruft zum Abrufen der Daten den Treiber „Verwaltetes System – Gateway“ auf.
- **Ereignisgesteuerter Datenkollektor:** Verwendet ein Push-Modell zum Sammeln von Ereignisdaten, die vom Datenerfassungsdiensttreiber erfasst wurden.
- **Datenkollektor 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.

Treiber „Verwaltetes System – Gateway“

Der **MCS-Treiber** („Verwaltetes System – Gateway“) fragt die folgenden Arten von Informationen für die verwalteten Systeme aus dem Identitätsdepot ab:

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

4 Bereitstellen von Benutzern für den sicheren Zugriff

Identity Manager zentralisiert die Zugriffsverwaltung und sorgt dafür, dass jeder Benutzer genau eine Identität besitzt – von den physischen und virtuellen Netzwerken bis hin zur Cloud.Oft hängt es außerdem von der Rolle eines Mitarbeiters in einer Organisation ab, auf welche Ressourcen er Zugriff benötigt. Zum Beispiel benötigen die Anwälte einer Kanzlei vermutlich auf andere Ressourcen Zugriff als die Anwaltsgehilfen.

Mit Identity Manager können Sie die Bereitstellung für Benutzer abhängig von deren Rolle innerhalb der Organisation durchführen. Definieren Sie Rollen und nehmen Sie Zuweisungen entsprechend den Anforderungen Ihrer Organisation vor. Wenn einem Benutzer eine Rolle zugewiesen wird, stellt Identity Manager für den Benutzer den Zugriff auf die Ressourcen bereit, die der Rolle zugeordnet sind. Benutzer mit mehreren Rollen erhalten den Zugriff auf alle Ressourcen, die mit diesen Rollen verknüpft sind.

Bei Bedarf können die Benutzer bei bestimmten Ereignisse in Ihrer Organisation automatisch den verschiedenen Rollen zugeordnet werden. Beispielsweise können Sie einen neuen Benutzer mit der Berufsbezeichnung „Anwalt“ in die SAP-Personaldatenbank aufnehmen lassen. Wenn für das Hinzufügen eines Benutzers zu einer Rolle eine Genehmigung erforderlich ist, können Sie Workflows einrichten, mit deren Hilfe Rollenanforderungen an die entsprechenden Genehmiger weitergeleitet werden. Sie können Benutzer auch manuell zu Rollen hinzufügen.

Es kann vorkommen, dass bestimmte Rollen nicht derselben Person zugewiesen werden dürfen, da die Rollen im Widerspruch zueinander stehen. Identity Manager bietet die Möglichkeit zur Funktionstrennung, mit deren Hilfe Sie verhindern können, dass Benutzern widersprüchliche Rollen zugewiesen werden, sofern nicht ein Mitarbeiter Ihrer Organisation eine Ausnahme für den Konflikt macht.

Die Identity Manager-Lösung bietet die folgenden Komponenten für die Bereitstellung von Benutzern:

- Identity Manager-Dashboard
- Verwaltung der Identitätsanwendungen
- Benutzeranwendung

Das Dashboard bietet einen einzigen Zugriffspunkt für alle Benutzer und Administratoren von Identity Manager. Es ermöglicht den Zugriff auf alle Funktionen der Katalogadministrator- und Benutzeranwendung. Ab Identity Manager 4.6 werden die Identity Manager-Startseite und das Bereitstellungs-Dashboard durch das Dashboard ersetzt.

4.1 Erläuterungen zum Beglaubigungsprozess in Identity Manager

Mit Identity Manager können Sie die Richtigkeit der Rollenzuweisungen durch einen Beglaubigungsprozess validieren. Falsche Rollenzuweisungen können die Einhaltung von Unternehmensvorschriften und behördlichen Bestimmungen gefährden. Mithilfe des Beglaubigungsprozesses zertifizieren die verantwortlichen Mitarbeiter innerhalb Ihrer Organisation die den Rollen zugewiesenen Daten:

- **Benutzerprofilbeglaubigung:** Ausgewählte Benutzer bestätigen ihre eigenen Profilinformationen (Vorname, Nachname, Stellenbezeichnung, Abteilung, Email-Adresse usw.) und korrigieren falsche Angaben. Die Richtigkeit der Profilinformationen ist für korrekte Rollenzuweisungen ausschlaggebend.
- **Funktionstrennungsverletzungsbeglaubigung:** Verantwortliche Mitarbeiter prüfen einen Funktionstrennungsverletzungsbericht und bestätigen die Richtigkeit des Berichts. In dem Bericht sind alle Ausnahmen aufgeführt, die es erlauben, einem Benutzer widersprüchliche Rollen zuzuweisen.
- **Rollenzuweisungsbeglaubigung:** Verantwortliche Mitarbeiter prüfen einen Bericht, in dem ausgewählte Rollen zusammen mit den Benutzern, Gruppen und Rollen aufgeführt sind, die den einzelnen Rollen zugewiesen sind. Die verantwortlichen Mitarbeiter müssen dann die Korrektheit der Informationen bestätigen.
- **Benutzerzuweisungsbeglaubigung:** Verantwortliche Mitarbeiter prüfen einen Bericht, in dem ausgewählte Benutzer zusammen mit den Rollen aufgeführt sind, denen sie zugewiesen sind. Die verantwortlichen Mitarbeiter müssen dann die Korrektheit der Informationen bestätigen.

Diese Beglaubigungsberichte sollen Ihnen in erster Linie dabei helfen, sicherzustellen, dass die Rollenzuweisungen korrekt sind und dass es gültige Gründe für das Zulassen von Ausnahmen für widersprüchliche Funktionen gibt.

4.2 Erläuterungen zum Self-Service-Prozess in Identity Manager

Die Identitäten bilden die Grundlage, auf der Identity Manager den Zugriff auf die Systeme, Anwendungen und Datenbanken autorisiert. Die eindeutigen Kennungen und die Rollen der einzelnen Benutzer sind mit bestimmten Zugriffsrechten auf Identitätsdaten verbunden. Benutzer, die als Vorgesetzte benannt sind, können beispielsweise auf die Gehaltsinformationen ihrer direkten Untergebenen zugreifen, nicht jedoch auf die Daten anderer Mitarbeiter in ihrem Unternehmen. Mit Identity Manager können Sie administrative Aufgaben an die Mitarbeiter delegieren, die dafür zuständig sein sollten. Zum Beispiel können Sie einzelnen Benutzern Folgendes ermöglichen:

- Das Verwalten ihrer persönlichen Daten im Unternehmensverzeichnis. Statt sich an Sie zu wenden, um eine Handynummer ändern zu lassen, können die Benutzer diese an einer Stelle ändern und die Änderung an alle Systeme weitergeben, die Sie über Identity Manager synchronisiert haben.

- Das Ändern ihrer Passwörter, das Einrichten eines Tipps für vergessene Passwörter sowie das Einrichten von Sicherheitsabfragen und -antworten für vergessene Passwörter. Statt Sie zu bitten, ein vergessenes Passwort zurückzusetzen, können die Benutzer dies selbst tun, nachdem sie einen Tipp erhalten oder eine Sicherheitsabfrage beantwortet haben.
- Das Anfordern von Zugriff auf Ressourcen wie Datenbanken, Systeme und Verzeichnisse. Die Benutzer müssen sich nicht mehr an Sie wenden, um den Zugriff auf eine Anwendung zu erhalten, sondern sie können die entsprechende Anwendung aus einer Liste von verfügbaren Ressourcen auswählen.

Zusätzlich zur Selbstbedienung für einzelne Benutzer bietet Identity Manager eine Selbstbedienungsverwaltung für Funktionen (Verwaltung, Helpdesk usw.) an, die für die Unterstützung, die Überwachung und die Genehmigung von Benutzeranforderungen verantwortlich sind. Robert fordert beispielsweise über die Self-Service-Funktion in Identity Manager den Zugriff auf die Dokumente an, die er für seine Arbeit benötigt. Diese Anforderung wird über die Self-Service-Funktion an Roberts Vorgesetzten und an den Leiter der Finanzabteilung weitergeleitet, die dann die Anforderung genehmigen können. Der eingerichtete Genehmigungsworkflow ermöglicht Robert, seine Anforderung zu initiieren und ihren Fortschritt zu überwachen, und Roberts Vorgesetztem und dem Leiter der Finanzabteilung, auf seine Anforderung zu antworten. Wenn die Anforderung von Roberts Vorgesetztem und dem Leiter der Finanzabteilung genehmigt wird, veranlasst dies die Bereitstellung der Active Directory-Rechte, mit denen Robert auf die Finanzdokumente zugreifen und diese Dokumente einsehen kann.

Identity Manager bietet außerdem Workflow-Funktionen, die dafür sorgen, dass bei Ihren Bereitstellungsprozessen die richtigen Ressourcengenehmiger einbezogen werden. Nehmen Sie beispielsweise an, dass Robert, für den bereits ein Active Directory-Konto eingerichtet wurde, über Active Directory auf Finanzberichte zugreifen muss. Dies muss von Roberts unmittelbarem Vorgesetzten sowie vom Leiter der Finanzabteilung genehmigt werden. Hierzu können Sie einen Genehmigungsworkflow einrichten, der Roberts Anforderung zunächst an seinen Vorgesetzten und (sobald dieser die Genehmigung erteilt hat) an den Leiter der Finanzabteilung weiterleitet. Wenn der Leiter der Finanzabteilung seine Genehmigung erteilt hat, wird die automatische Bereitstellung der von Robert zum Zugriff und zur Ansicht der Finanzdokumente benötigten Active Directory-Rechte veranlasst.

Workflows können automatisch ausgelöst werden, sobald ein bestimmtes Ereignis eintritt (z. B. wenn ein neuer Benutzer zum Personalsystem hinzugefügt wird), oder auch manuell über eine Benutzeranforderung. Sie können sicherstellen, dass Genehmigungen rechtzeitig erteilt werden, indem Sie Vertretungsgenehmiger und Genehmigungsteams einrichten.

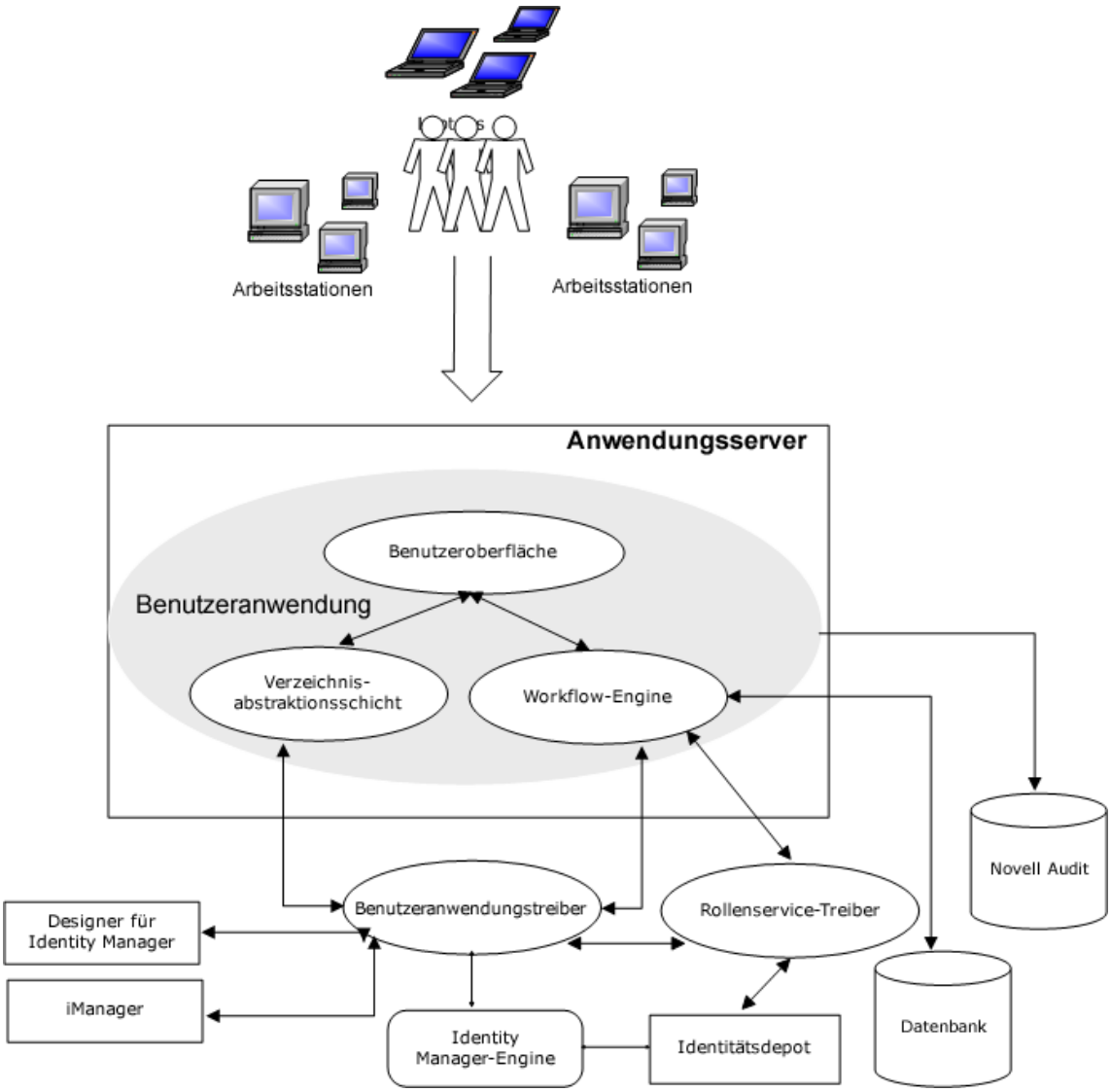
4.3 Erläuterungen zu den Komponenten für die Verwaltung der Benutzerbereitstellung

In diesem Abschnitt werden die folgenden Komponenten erläutert:

4.3.1 Benutzeranwendung und rollenbasiertes Bereitstellungsmodul

Die **Benutzeranwendung** in Identity Manager ermöglicht Ihren Benutzern und Unternehmensadministratoren den Zugriff auf die Informationen, Ressourcen und Funktionen von Identity Manager. In der browsergestützten Benutzeranwendung erledigen die Benutzer verschiedene Identitäts-Self-Service-Aufgaben und Rollenbereitstellungsaufgaben. Die Benutzer können Passwörter und Identitätsdaten verwalten, Bereitstellungs- und Rollenzuweisungsanforderungen auslösen und überwachen, den Genehmigungsprozess für Bereitstellungsanforderungen lenken und Beglaubigungsberichte überprüfen.

Die Benutzeranwendung beruht auf dem Zusammenspiel verschiedener unabhängiger Komponenten.



Die Benutzeranwendung wird im Rahmenwerk des **rollenbasierten Bereitstellungsmoduls** (RBPM) ausgeführt. Dieses Rahmenwerk umfasst die Workflow-Engine, die das Routing von Anforderungen durch den entsprechenden Genehmigungsprozess steuert. Für diese Komponenten sind die folgenden Treiber erforderlich:

Benutzeranwendungstreiber

Speichert Konfigurationsinformationen und benachrichtigt die Benutzeranwendung 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

Verwaltet alle Rollen- und Ressourcenzuweisungen. Der Treiber startet Workflows für Funktionszuweisungsanforderungen, die eine Genehmigung erfordern, und verwaltet indirekte Rollenzuweisungen nach Gruppen- und Containermitgliedschaften. Außerdem kann der Treiber die Berechtigungen für Benutzer gemäß ihren Rollenmitgliedschaften erteilen und widerrufen. Abgeschlossene Anforderungen werden ebenfalls bereinigt.

Die Benutzer können über die unterstützten Webbrowser auf die Benutzeranwendung zugreifen. Weitere Informationen zur Benutzeranwendung und zu RBPM finden Sie im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

4.3.2 Verwaltung der Identitätsanwendungen

Mit der Benutzeroberfläche **Verwaltung der Identitätsanwendungen** können Sie die folgenden Aufgaben mit einer entsprechenden Administratorrolle verwalten:

- Erstellen und Verwalten von Rollen, Ressourcen und ihren Zuweisungen
- Festlegen der Funktionstrennungsbeschränkungen zum Vermeiden von Überschneidungen zwischen zwei verschiedenen Rollen im System
- Konfigurieren der Benutzerfunktion zum Genehmigen von Berechtigungsanforderungen per Email
- Konfigurieren der Standardeinstellungen Ihrer Identitätsanwendungskomponenten wie Rollen, Ressourcen und Delegierung

Administratoren können wahlweise auf einem Computer oder einem Tablet über einen unterstützten Webbrowser auf die Administrationsseite zugreifen. Weitere Informationen finden Sie in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen).

4.3.3 Identity Manager-Dashboard

Das **Identity Manager-Dashboard** (das Dashboard) umfasst eine personalisierte Ansicht der Berechtigungen, Aufgaben und Anforderungen der einzelnen Benutzer. Dadurch konzentrieren sich Benutzer auf die folgenden grundlegenden Funktionsbereiche:

Ich brauche etwas.

Sie können ein benötigtes Element anfordern, sei es ein Gerät (z. B. ein Notebook) oder etwas nicht Greifbares (z. B. Zugriff auf einen bestimmten Server oder eine Anwendung).

Ich muss etwas tun.

Auf der Seite **Meine Aufgaben** finden Sie alle ausstehenden Genehmigungs- oder Bereitstellungsaufgaben im Identity Manager-System.

Was habe ich?

Ihre aktuellen Berechtigungen finden Sie auf der Seite **Meine Berechtigungen**, die eine Liste der Rollen und Ressourcen anzeigt, auf die Sie Zugriff haben.

Wie habe ich das bekommen?

Auf der Seite **Anforderungsverlauf** sind alle bisherigen Anforderungen sowie der Status aller ausstehenden Anforderungen aufgeführt.

Wenn Sie über eine Administratorrolle für die Identitätsanwendungen verfügen, passen Sie im Dashboard die Seite **Anwendungen** für alle Benutzer an. Konfigurieren Sie die Seite, um die Elemente und Links anzuzeigen, die Ihre Benutzer sehen müssen. Sie sind nach den Kategorien strukturiert, die für Ihr Unternehmen sinnvoll sind. Die folgenden Elementtypen stehen zur Verfügung:

- Identity Manager-Funktionen wie Erstellen von Gruppen oder Ausführen von Berichten
- Berechtigungen, die die meisten Benutzer anfordern müssen
- Links zu häufig besuchten Websites oder webbasierten Anwendungen
- REST-Endpunkte
- Badges, wie die Anzahl der Elemente eines bestimmten Typs, auf die Benutzer zugreifen

Die Benutzer können wahlweise auf einem Computer oder einem Tablet über einen unterstützten Webbrowser auf das Dashboard zugreifen. Weitere Informationen finden Sie in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen).

II Planen der Installation von Identity Manager

In diesem Abschnitt finden Sie nützliche Informationen zur Planung der Identity Manager-Umgebung. Die Voraussetzungen und Systemanforderungen für die Computer, auf denen die einzelnen Identity Manager-Komponenten installiert werden sollen, finden Sie in den jeweiligen Abschnitten zur Installation dieser Komponenten.

Zum Installieren und Ausführen von Identity Manager benötigen Sie keinen Aktivierungscode. Wenn Sie keinen Aktivierungscode angeben, ist Identity Manager nach Ablauf von 90 Tagen ab der Installation jedoch nicht mehr nutzbar. Sie können Identity Manager jederzeit während oder auch nach dieser 90-Tage-Frist aktivieren.

- Kapitel 5, „Überblick über die Planung“, auf Seite 33

5 Überblick über die Planung

In diesem Abschnitt erfahren Sie, wie Sie den Installationsvorgang für Identity Manager planen. Einige Komponenten müssen in einer bestimmten Reihenfolge installiert werden, da der Installationsvorgang auf verschiedene bereits installierte Komponenten zugreift. Beispielsweise muss das Identitätsdepot vor der Installation der Identity Manager-Engine installiert und konfiguriert werden.

5.1 Checkliste für die Planung

Die nachfolgende Checkliste enthält die Hauptschritte für die Planung der Identity Manager-Installation in Ihrer Umgebung. In den Abschnitten zur Installation der Identity Manager-Komponenten finden Sie detaillierte Checklisten.

	Checkliste
❑	1. Sehen Sie sich die Informationen zur Produktarchitektur an, um die Identity Manager-Komponenten kennenzulernen. Weitere Informationen finden Sie in Teil I, „Einführung“, auf Seite 15.
❑	2. (Bedingt) Stellen Sie beim Installieren von Komponenten in einer Umgebung mit Red Hat Enterprise Linux 7.*x* sicher, dass die richtigen Bibliotheken auf dem Server vorliegen. Weitere Informationen finden Sie in Abschnitt 5.9.4, „Installieren von Identity Manager auf Servern mit RHEL 7.3 (oder höher)“, auf Seite 45.
❑	3. Stellen Sie sicher, dass eine Lizenz für die Ausführung von Identity Manager vorliegt. Weitere Informationen finden Sie in Abschnitt 5.8, „Erläuterungen zur Lizenzierung und zur Aktivierung“, auf Seite 42.
❑	4. Prüfen Sie die Standardports für die einzelnen Identity Manager-Komponenten, und passen Sie die Installationseinstellungen bei Bedarf entsprechend an. Weitere Informationen finden Sie in Abschnitt 5.2, „Erläuterungen zur Identity Manager-Kommunikation“, auf Seite 34.
❑	5. Stellen Sie fest, ob die Installationsprogramme in Ihrer bevorzugten Sprache ausgeführt werden können. Weitere Informationen finden Sie in Abschnitt 5.10, „Erläuterungen zur Sprachunterstützung“, auf Seite 48.

	Checkliste
❑	6. Stellen Sie sicher, dass die erforderlichen Dateien für die Installation von Identity Manager vorliegen. Weitere Informationen finden Sie in Abschnitt 5.11, „Herunterladen der Installationsdateien“, auf Seite 50.
❑	7. (Bedingt) Wenn Identity Manager in einem Cluster installiert werden soll, überprüfen Sie, ob Ihre Umgebung den Anforderungen entspricht. Weitere Informationen finden Sie in Abschnitt 5.9.1, „Sicherstellen der Hochverfügbarkeit von Identity Manager“, auf Seite 43.
❑	8. Überprüfen Sie, ob Sie den erforderlichen Berechtigungsnachweis zum Installieren der Identity Manager-Komponenten auf dem Server sowie zum Erstellen der Konten während der Installation besitzen.
❑	9. Stellen Sie sicher, dass die Computer, auf denen die Identity Manager-Komponenten installiert werden sollen, den angegebenen Anforderungen entsprechen. Weitere Informationen finden Sie unter den Systemanforderungen zu den einzelnen Komponenten. ◆ Abschnitt 8.3.4, „Systemanforderungen für Identity Manager-Engine, Remote Loader und iManager“, auf Seite 65 ◆ Abschnitt 8.5.3, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 83 ◆ Abschnitt 8.6.4, „Systemanforderungen für die Identitätsberichterstellung“, auf Seite 88 ◆ Abschnitt 12.3, „Systemanforderungen für Designer“, auf Seite 184 ◆ Abschnitt 14.3, „Systemanforderungen für Analyzer“, auf Seite 190 **HINWEIS:** NetIQ empfiehlt, die Konten zu notieren, die Sie während des Installationsvorgangs erstellen.
❑	10. Aktivieren Sie die Identity Manager-Komponenten. Weitere Informationen finden Sie unter Abschnitt 24, „Aktivieren von Identity Manager“, auf Seite 245.

5.2 Erläuterungen zur Identity Manager-Kommunikation

NetIQ empfiehlt, die in der nachfolgenden Tabelle aufgeführten Standardports zu öffnen, damit die ordnungsgemäße Kommunikation zwischen den Identity Manager-Komponenten gewährleistet ist.

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

Port-Nummer	Komponente auf dem Computer	Verwendung durch den Port
389	Identitätsdepot	Für die LDAP-Kommunikation in Klartext mit Identity Manager-Komponenten
465	Identitätsberichterstellung	Für die Kommunikation mit dem SMTP-Mailserver
524	Identitätsdepot	Für die Kommunikation mit dem NetWare-Kernprotokoll (NCP)
636	Identitätsdepot	Für die LDAP-TLS/SSL-Kommunikation mit Identity Manager-Komponenten
5432	Identitätsanwendungen	Für die Kommunikation mit der Datenbank der Identitätsanwendungen

Port-Nummer	Komponente auf dem Computer	Verwendung durch den Port
7707	Identitätsberichterstellung	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	Identitätsanwendungen	Wird von Tomcat für den Empfang von Befehlen zum Herunterfahren verwendet
8009	Identitätsanwendungen	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	Identitätsanwendungen iManager	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.
8180	Identitätsanwendungen	Wird vom Tomcat-Anwendungsserver, auf dem die Identitätsanwendungen ausgeführt werden, für die HTTP-Kommunikation verwendet
8443	Identitätsanwendungen iManager	Wird von Tomcat für die HTTPS-Kommunikation (SSL-Kommunikation) oder zum Umleiten von Anforderungen für die SSL-Kommunikation verwendet
8543	Identitätsanwendungen	Wird von Tomcat zum Umleiten von Anforderungen verwendet, für die der SSL-Transport erforderlich ist, wenn Sie das TLS/SSL-Protokoll nicht nutzen
9009	iManager	Wird vom Tomcat für MOD_JK verwendet
15432	Identitätsberichterstellung	Wird für die PostgreSQL-Datenbank verwendet
45654	Benutzeranwendung	Wird vom Server, auf dem die Datenbank für die Identitätsanwendungen installiert ist, zum Empfang der Kommunikation verwendet, wenn Tomcat mit einer Clustergruppe ausgeführt wird

5.3 Erläuterungen zu den Installationsdateien

Die folgenden Dateien stehen für die Version zur Verfügung:

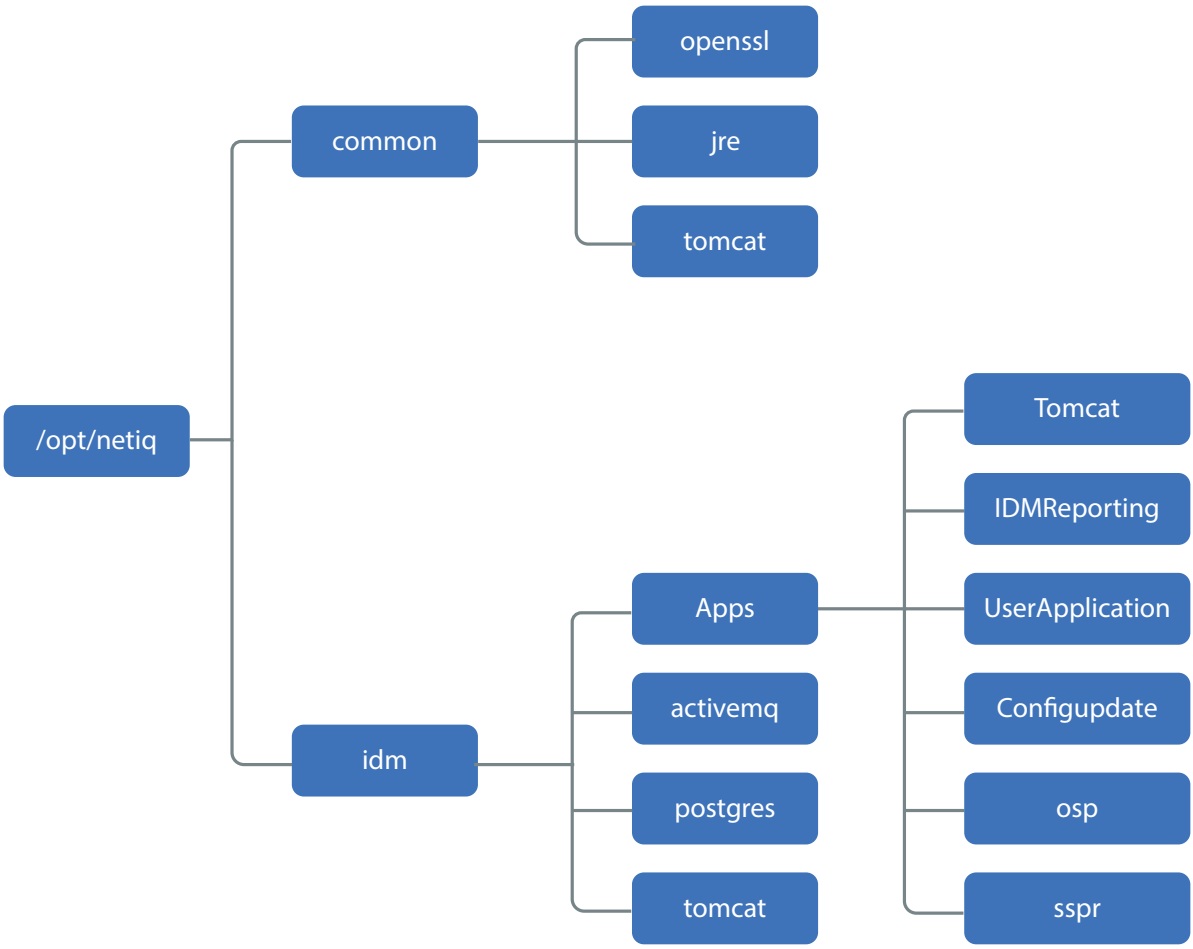
Dateiname	Beschreibung
`Identity_Manager_4.7_Linux.iso`	Enthält die folgenden Identity Manager-Komponenten: ◆ Identity Manager-Engine ◆ Remote Loader-Service ◆ Fan-out-Agent ◆ Designer ◆ iManager-Webverwaltung ◆ Identitätsberichterstellung ◆ Identitätsanwendungen ◆ Analyzer
`SentinelLogManagementForIGA8.1.1.0.tar.gz`	Enthält Sentinel Log Management für IGA.
`Identity_Manager_4.7_Linux_Designer.tar.gz`	Enthält Designer für Identity Manager.
`Identity_Manager_4.7_Linux_Analyzer.tar.gz`	Enthält Analyzer für Identity Manager.

HINWEIS: Die Datei `Identity_Manager_4.7_Linux.iso` enthält außerdem die unterstützende Software und die erforderlichen Komponenten für die Ausführung von Identity Manager, z. B. Oracle JRE, PostgreSQL, ActiveMQ und Apache Tomcat.

5.4 Verzeichnisstruktur

Beim Installationsvorgang wird die folgende Verzeichnisstruktur angelegt:

- Das Verzeichnis `/opt/netiq` ist der Ausgangspunkt der Verzeichnisstruktur. Alle anderen Dateien und Verzeichnisse befinden sich in diesem Verzeichnis.
- Das Verzeichnis `common` enthält unterstützende Software. Diese Software wird gemeinsam von allen Komponenten genutzt.
- Das Verzeichnis `idm` enthält komponentenspezifische Unterverzeichnisse mit Binärdateien für die Installation und Konfiguration der Komponenten.



5.5 Standardmäßige Speicherorte für die Installation

Beim Installationsvorgang werden die Komponenten in den nachfolgenden vordefinierten Speicherorten abgelegt.

Identity Manager-Komponente	Standardmäßiger Installationspfad
Identity Manager-Engine	`/opt/novell/eDirectory/lib/dirxml`
Remote Loader	`/opt/novell/dirxml/bin/x86_64`
Fan-out-Agent	`/opt/novell/dirxml/fanoutagent`
Designer	`/root/designer`
iManager	`/var/opt/novell/iManager`
Benutzeranwendung	`/opt/netiq/idm/apps/UserApplication`
Identitätsanwendungen	`/opt/netiq/idm/apps`
Konfigurationsaktualisierungsprogramm	`/opt/netiq/idm/apps/configupdate`
Identitätsberichterstellung	`/opt/netiq/idm/apps/IDMReporting`
SLM für IGA	`/opt/novell/sentinel`

Identity Manager-Komponente	Standardmäßiger Installationspfad
Analyzer	`/root/analyzer`

Unterstützende Komponenten	Standardmäßiger Installationspfad
Oracle JRE	`/opt/netiq/common/jre`
Apache Tomcat	`/opt/netiq/idm/tomcat`
PostgreSQL	`/opt/netiq/idm/postgres`
Apache ActiveMQ	`/opt/netiq/idm/activemq`

Die Installationsprotokolldateien werden im Verzeichnis `/var/opt/netiq/idm/log` erzeugt.

5.6 Installierte Komponentenversionen

Diese Version umfasst Komponenten und unterstützende Software mit den folgenden Versionen:

Identity Manager-Komponente	Version
Identitätsdepot	`9.1` **HINWEIS:** Wenn Sie auf Identity Manager 4.7 aufrüsten, muss das Identitätsdepot auf Version 9.1 aufgerüstet werden.
Identity Manager-Engine, Remote Loader, Fan-out-Agent	`4.7`
Designer	`4.7`
iManager	`3.1`
One SSO-Anbieter	`6.2.1`
Self-Service Password Reset	`4.2.0.4`
Identitätsanwendungen	`4.7`
Identitätsberichterstellung	`6.0`
SLM für IGA	`8.1.1.0`

Unterstützende Komponenten	Version
Oracle Java Development Kit (JRE)	`1.8.0_162`
Apache Tomcat	`8.5.27`
PostgreSQL	`9.6.6`
Apache ActiveMQ	`5.15.2`

5.7 Empfehlungen für Installationsszenarien und Servereinrichtung

Bei einer Standalone-Installation installieren Sie die Komponenten in einer bestimmten Reihenfolge auf bestimmten Servern. Die Installationsprogramme bestimmter Komponenten benötigen Informationen zu bereits installierten Komponenten.

Anhand der Informationen in diesem Abschnitt ermitteln Sie die richtige Installationsreihenfolge und die richtigen Servertypen für verschiedene Revisions- und Berichterstellungsszenarien.

- Abschnitt 5.7.1, „Senden von Ereignissen an einen Revisionsdienst ohne Berichterstellung in Identity Manager“, auf Seite 39
- Abschnitt 5.7.2, „Senden von Ereignissen an Identity Manager und Generieren von Berichten“, auf Seite 39
- Abschnitt 5.7.3, „Senden von Ereignissen an einen externen Dienst, bevor Ereignisse im Push-Verfahren an Identity Manager übermittelt werden“, auf Seite 40
- Abschnitt 5.7.4, „Empfohlene Servereinrichtung“, auf Seite 40
- Abschnitt 5.7.5, „Auswählen einer Betriebssystemplattform für Identity Manager“, auf Seite 41

5.7.1 Senden von Ereignissen an einen Revisionsdienst ohne Berichterstellung in Identity Manager

In diesem Szenario planen Sie die Revision der in Identity Manager auftretenden Ereignisse mit Sentinel. Das Generieren von Berichten in Identity Manager ist nicht geplant. Installieren Sie die Komponenten in der nachstehenden Reihenfolge:

1. Sentinel Log Management für IGA
2. Identity Manager-Engine, Treiber und iManager-Plugins
3. (Optional) iManager
4. Designer
5. SSPR
6. Identitätsanwendungen
7. (Optional) Analyzer

5.7.2 Senden von Ereignissen an Identity Manager und Generieren von Berichten

In diesem Szenario planen Sie die Revision in Identity Manager mit Sentinel Log Management für IGA (in Identity Manager enthalten). Unter Umständen sollen auch Berichte für diese Ereignisse generiert werden. Installieren Sie die Komponenten in der nachstehenden Reihenfolge:

1. Sentinel Log Management für IGA
2. Identity Manager-Engine, Treiber und iManager-Plugins
3. (Optional) iManager
4. Designer
5. SSPR
6. Identitätsanwendungen

7. Identitätsberichterstellung
8. (Optional) Analyzer

5.7.3 Senden von Ereignissen an einen externen Dienst, bevor Ereignisse im Push-Verfahren an Identity Manager übermittelt werden

In diesem Szenario planen Sie die Revision von Identity Manager mit einem Dienst wie Sentinel. Installieren Sie die Komponenten in der nachstehenden Reihenfolge:

1. Externer Revisionsdienst, z. B. Sentinel
2. Identity Manager-Engine, Treiber und iManager-Plugins
3. (Optional) iManager
4. Designer
5. SSPR
6. Identitätsanwendungen
7. Identitätsberichterstellung
8. (Optional) Analyzer

5.7.4 Empfohlene Servereinrichtung

Planen Sie die Installation anhand der folgenden Überlegungen:

Komponententreue

Komponente	Unabhängige Installation	Anmerkungen
Identity Manager-Engine	Ja	
Identitätsanwendungen	Ja	Eigener OSP erforderlich. Die Identitätsanwendungen und der OSP müssen auf demselben Computer installiert werden.
Identitätsberichterstellung	Ja	Eigener OSP möglich. Das Installationsprogramm unterstützt einen lokal oder entfernt installierten OSP zur Installation oder Aufrüstung von Identity Reporting.
OSP	Nein	Das Installationsprogramm unterstützt keinen entfernt installierten OSP-Server für die Identitätsanwendungen. Sie müssen den OSP und die Identitätsanwendungen auf demselben Computer installieren.
SSPR	Ja	Das Installationsprogramm unterstützt die eigenständige Installation und Aufrüstung von SSPR.
Datenbank der Identitätsanwendungen	Ja	
Berichterstellungsdatenbank	Ja	
Sentinel Log Management für IGA	Ja	

In einer typischen Produktionsumgebung wird Identity Manager beispielsweise auf mindestens sieben Servern und auf Client-Arbeitsstationen installiert. Beispiel:

Einzurichtende(r) Computer	Einzurichtende Komponente(n)
Komplett (nur für Demo-/POC-Einrichtung)	Installieren und konfigurieren Sie alle Komponenten (Identity Manager-Engine, Identitätsanwendungen, Identity Reporting, OSP, SSPR, Datenbank der Identitätsanwendungen und Berichterstellungsdatenbank) auf einem einzigen Computer und Sentinel Log Management für IGA auf einem separaten Computer.
Verteilte Einrichtung	
Server 1	◆ Identitätsdepot ◆ Identity Manager-Engine
Server 2	Identitätsanwendungen und OSP (Clustern möglich)
Server 3	Identity Reporting (OSP)
Server 4	SSPR
Server 5 und 6	Identity Manager-Datenbanken für: ◆ Identitätsanwendungen ◆ Identitätsberichterstellung
Server 7	Sentinel Log Management für IGA

5.7.5 Auswählen einer Betriebssystemplattform für Identity Manager

Die Identity Manager-Komponenten können auf verschiedenen Betriebssystemplattformen installiert werden. Anhand der nachfolgenden Tabelle ermitteln Sie die geeigneten Server für Ihre Identitätsmanagement-Lösung.

Plattform	Komponente
openSUSE	Analyzer Designer
Red Hat Linux Server (RHEL)	Identitätsanwendungen Identity Manager-Engine Identitätsberichterstellung iManager Remote Loader Sentinel Log Management für IGA
SUSE Linux Enterprise Desktop (SLED)	Designer

Plattform	Komponente
SUSE Linux Enterprise Server (SLES)	Analyzer
	Designer
	Identitätsanwendungen
	Identity Manager-Engine
	Identitätsberichterstellung
	iManager
	Remote Loader
	Sentinel Log Management für IGA

Weitere Informationen zu den Systemanforderungen und Voraussetzungen finden Sie in den folgenden Abschnitten:

- „Planen der Installation von Designer“, auf Seite 183
- „Planen der Installation der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting“, auf Seite 61

5.8 Erläuterungen zur Lizenzierung und zur Aktivierung

Identity Manager setzt sich aus einem breiten Spektrum von Funktionen zusammen. Damit unterschiedliche Kundenanforderungen erfüllt werden können, ist Identity Manager sowohl in einer Advanced Edition als auch in einer Standard Edition mit jeweils entsprechender Funktionalität verfügbar. Die Advanced Edition von Identity Manager enthält alle Funktionen. Die Standard Edition enthält nur einen Teil der Funktionen, die in der Advanced Edition verfügbar sind. Eine Gegenüberstellung der Funktionen der Advanced und der Standard Edition finden Sie im Versionenvergleich zu Identity Manager. NetIQ bietet verschiedene Lizenzierungsmodelle für die Editions.

NetIQ vereint die Advanced und die Standard Edition in einer einzigen ISO-Datei, über die sich neue Funktionen, Patches und Dokumentationen einfacher bereitstellen lassen. Der Support ist einfacher und Kunden haben die Möglichkeit, genau die Lösungsmerkmale auszuwählen, die am besten zu ihren Anforderungen passen.

Sie können eine Testversion von Identity Manager installieren und 90 Tage lang kostenlos nutzen. Die Komponenten von Identity Manager müssen jedoch innerhalb von 90 Tagen nach der Installation aktiviert werden, anderenfalls wird ihre Funktion eingestellt. Sie können jederzeit während oder auch nach dieser 90-Tage-Frist eine Produktlizenz erwerben und Identity Manager aktivieren. Weitere Informationen, Abschnitt 24, „Aktivieren von Identity Manager“, auf Seite 245.

Abhängig von der erworbenen Edition stellt Ihnen NetIQ die entsprechenden Lizenzschlüssel zur Aktivierung der richtigen Funktionen in Identity Manager zur Verfügung. Sie können über die NetIQ Identity Manager-Bestell-Website eine Identity Manager-Produktlizenz erwerben. Wenn Sie eine Produktlizenz erworben haben, wird Ihnen von NetIQ die Kunden-ID zugesendet. Die Email enthält außerdem die URL der NetIQ-Website, auf der Sie eine Produktaktivierungsberechtigung erhalten. Wenn Sie Ihre Kunden-ID nicht erhalten haben oder nicht mehr wissen, wenden Sie sich an Ihren zuständigen Vertriebsmitarbeiter.

5.9 Vorbereitung der Installation

In diesem Abschnitt finden Sie die allgemeinen Voraussetzungen für die Computer, auf denen die Identity Manager-Komponenten gehostet werden sollen. Für ein uneingeschränktes Identitätsmanagement in Ihrer Umgebung sollten Sie generell alle Komponenten installieren. Die Installation aller Komponenten (z. B. Analyzer oder iManager) ist jedoch nicht zwingend erforderlich.

Die Identity Manager-Implementierung richtet sich nach den Anforderungen Ihrer Umgebung. Ziehen Sie daher vor der Fertigstellung der Identity Manager-Architektur für Ihre Umgebung die NetIQ Consulting Services oder einen NetIQ Identity Manager-Partner zurate.

Die Hardwarevoraussetzungen sowie die unterstützten Betriebssysteme und Browser sind auf der Website mit technischen Daten zu NetIQ Identity Manager aufgeführt.

5.9.1 Sicherstellen der Hochverfügbarkeit von Identity Manager

Durch die Hochverfügbarkeit lassen sich wichtige Netzwerkressourcen wie Daten, Anwendungen und Dienste effizient verwalten. NetIQ unterstützt durch Clustering oder Hypervisor-Clustering wie VMWare Vmotion die Hochverfügbarkeit Ihrer Identity Manager-Lösung. Bei der Planung einer Hochverfügbarkeitsumgebung gelten die folgenden Überlegungen:

- Die folgenden Komponenten stehen zur Installation in einer Hochverfügbarkeitsumgebung zur Verfügung:
  - Identity Manager-Engine
  - Remote Loader
  - Identitätsanwendungen mit Ausnahme der Identitätsberichterstellung
- Wenn Sie das Identitätsdepot (eDirectory) in einer Clusterumgebung ausführen, wird auch die Identity Manager-Engine geclustert.

Weitere Informationen zum...	Erklärt in...
Festlegen der Serverkonfiguration für Identity Manager-Komponenten	Abschnitt 5.7.4, „Empfohlene Servereinrichtung“, auf Seite 40
Ausführen des Identitätsdepots in einem Cluster	Abschnitt 8.3.3, „Voraussetzungen für die Installation des Identitätsdepots in einer Cluster-Umgebung“, auf Seite 65 Bereitstellen von eDirectory in Hochverfügbarkeits-Clustern im NetIQ eDirectory-Installationshandbuch.

Weitere Informationen zum...	Erklärt in...
Ausführen der Identitätsanwendungen in einem Cluster	„Konfigurieren von OSP und SSPR für Clustering“, auf Seite 165 „Voraussetzungen für die Installation der Identitätsanwendungen in einer Cluster-Umgebung“, auf Seite 81 „Aktivieren des Berechtigungsindex für das Clustering“, auf Seite 77 „Vorbereiten eines Clusters für die Identitätsanwendungen“, auf Seite 82 „Konfigurieren des Benutzeranwendungstreibers für das Clustering“, auf Seite 143 Abschnitt 22.3, „Aktualisieren der SSPR-Links im Dashboard für eine dezentrale Umgebung oder eine Cluster-Umgebung“, auf Seite 239

5.9.2 Mindestspeicheranforderungen auf Linux-Servern

Die Identity Manager-Komponenten haben Mindestspeicheranforderungen

In Tabelle 5-1 auf Seite 44 sehen Sie, wie viel sicherer Speicherplatz mindestens für die verschiedenen Komponenten erforderlich ist:

Tabelle 5-1 *Mindestanforderung für sicheren Speicherplatz*

Pfad	Komponente	Mindestens erforderlicher sicherer Speicherplatz
/opt	IDM	3 GB
/var	IDM	5 GB für DIB von 100.000 Objekten
/etc	IDM	5 MB
/opt	iManager	700 MB
/var	iManager	3 GB
/etc	iManager	10 MB
/opt	Server für Identitätsanwendungen	5 GB
/var	Server für Identitätsanwendungen	100 MB

Bei der Installation muss der Ordner `/temp` als „exec“ eingehängt sein, 5 GB freien Speicherplatz enthalten und Schreibberechtigungen besitzen.

5.9.3 Installieren von Identity Manager auf Servern mit SLES 12 SP2 (oder höher)

- Zur geführten Installation der Identity Manager-Komponenten mit den einzelnen Komponenten-Installationsprogrammen oder dem integrierten Installationsprogramm müssen bereits bestimmte Pakete auf dem Server mit SLES 12 SP2 (oder höher) installiert sein.
  - `libXtst6-32bit-1.2.1-4.4.1.x86_64`
  - `libXrender1-32bit`
  - `libXi6-32bit`
- (Bedingt) Wenn Sie die Identity Manager-Komponenten in einer Umgebung mit SLES 12 SP3 installieren, muss `glibc-32bit-*x86_64.rpm` installiert sein. (`*` bezeichnet die aktuelle Version der RPM.)

HINWEIS: NetIQ empfiehlt, die abhängigen Pakete vom Betriebssystem-Abonnementdienst zu beziehen, damit Sie weiterhin Unterstützung von Ihrem Betriebssystemanbieter erhalten. Falls Sie keinen Abonnementdienst besitzen, finden Sie die aktuellen Pakete im Internet, beispielsweise unter http://rpmfind.net/linux.

5.9.4 Installieren von Identity Manager auf Servern mit RHEL 7.3 (oder höher)

Soll Identity Manager auf einem Server mit dem Betriebssystem Red Hat Enterprise Linux 7.3 (oder höher) installiert werden, muss der Server bestimmte Voraussetzungen erfüllen.

- „Voraussetzungen“, auf Seite 45
- „Überprüfen der Voraussetzungen“, auf Seite 46
- „Prüfen der abhängigen Bibliotheken für den Server“, auf Seite 46
- „Erstellen eines Repository für die Installationsmedien“, auf Seite 46

Voraussetzungen

NetIQ empfiehlt die Prüfung der folgenden Voraussetzungen:

- Wenn Sie über einen Loopback-Adressen-Alias für den Hostnamen des Systems im Eintrag `/etc/hosts` verfügen, muss dieser in den Hostnamen oder die IP-Adresse geändert werden. Wenn Ihr Eintrag in der Datei `/etc/hosts` also dem unten angegebenen ähnelt, muss er in den korrekten Eintrag (siehe das unten angegebene zweite Beispiel) geändert werden.

  Bei dem folgenden Beispiel treten Probleme auf, wenn ein Dienstprogramm versucht, die Auflösung für den ndsd-Server durchzuführen:

  ```
  <loopback IP address> test-system localhost.localdomain localhost
  ```

  Nachfolgend finden Sie ein Beispiel für einen korrekten Eintrag in der Datei `/etc/hosts`:

  ```
  <loopback IP address> localhost.localdomain localhost
  <loopback IP address> test-system
  ```

Wenn ein Tool oder Dienstprogramm eines Drittanbieters die Auflösung über localhost durchführt, muss dies so geändert werden, dass die Auflösung über einen Hostnamen oder eine IP-Adresse und nicht über die localhost-Adresse erfolgt.

- Installieren Sie die entsprechenden Bibliotheken auf dem Server. Weitere Informationen finden Sie in „Prüfen der abhängigen Bibliotheken für den Server“, auf Seite 46.

Überprüfen der Voraussetzungen

Sie können für die einzelnen Manager-Komponenten einen Bericht über die nicht erfüllten Voraussetzungen generieren. Führen Sie das Skript `./II-rhel-Prerequisite.sh` aus, das sich im Verzeichnis `<Extraktionsspeicherort des Identity Manager-Builds>\install\utilities` des Installations-Kits befindet.

Prüfen der abhängigen Bibliotheken für den Server

Auf einer 64-Bit-Plattform sind die erforderlichen Bibliotheken für RHEL abhängig vom gewählten Installationsverfahren. Installieren Sie die abhängigen Bibliotheken oder RPMs in der angegebenen Reihenfolge.

HINWEIS: Geben Sie zum Hinzufügen einer`ksh`-Datei den folgenden Befehl ein:

```
yum -y install ksh
```

- `glibc-*.i686.rpm`
- `libstdc++-*.i686.rpm`
- `libgcc-*.i686.rpm`
- `compat-libstdc++-33-*.x86_64.rpm`
- `compat-libstdc++-33-*.i686.rpm`
- `libXtst-*.i686.rpm`
- `libXrender-*.i686.rpm`

Erstellen eines Repository für die Installationsmedien

Wenn der RHEL 7.x-Server ein Repository für die Installationsmedien benötigt, ist es möglich, dieses Repository manuell zu erstellen.

HINWEIS

- Auf dem RHEL-Server müssen außerdem die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in „Prüfen der abhängigen Bibliotheken für den Server“, auf Seite 46.
- Vor der Installation von Identity Manager muss auf jeden Fall die `unzip`-RPM installiert sein. Das gilt für alle Linux-Plattformen.

So richten Sie ein Repository für die Installation ein:

1. Erstellen Sie einen Einhängepunkt auf Ihrem lokalen Server.

   Beispiel: `/mnt/rhel (mkdir –p /mnt/rhel)`

2. Wenn Sie ein Installationsmedium verwenden, lässt sich der folgende Befehl einhängen:

```
# mount -o loop /dev/sr0 /mnt/rhel
```

ODER

Hängen Sie die RHEL 7-Installations-ISO mit dem folgenden Befehl in einem Verzeichnis wie `/mnt/rhel`, ein:

```
# mount -o loop RHEL7.x.iso /mnt/rhel
```

Laden Sie die ISO-Datei für RHEL 7.4 herunter und hängen Sie sie ein.

Beispiel: `mount -o loop <path_to_downloaded rhel*.iso> /mnt/rhel`

3 Kopieren Sie die Datei `media.repo` vom Root des eingehängten Verzeichnisses zu `/etc/yum.repos.d/` und legen Sie die erforderlichen Berechtigungen fest.

Beispiel:

```
# cp /mnt/rhel/media.repo /etc/yum.repos.d/rhel7dvd.repo
# chmod 644 /etc/yum.repos.d/rhel7dvd.repo
```

4 Bearbeiten Sie die neue Repo-Datei, indem Sie die Einstellung `gpgcheck=0` zu `1` ändern und Folgendes hinzufügen:

```
enabled=1
baseurl=file:///mnt/rhel/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

Die neue Repo-Datei würde schließlich wie folgt aussehen (obwohl die Media-ID abhängig von der RHEL-Version anders wäre):

```
[InstallMedia]
name=DVD for Red Hat Enterprise Linux 7.1 Server
mediaid=1359576196.686790
metadata_expire=-1
gpgcheck=1
cost=500
enabled=1
baseurl=file:///mnt/rhel
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

5 Zum Installieren der 32-Bit-Pakete ändern Sie in der Datei `/etc/yum.conf` den Eintrag „exactarch=1“ zu „exactarch=0“.

6 Erstellen Sie zur Installation der erforderlichen Pakete für Identity Manager auf RHEL 7.x eine install.sh-Datei und fügen Sie der Datei die folgenden Inhalte hinzu:

```
#!/bin/bash
yum clean all
yum repolist
yum makecache

PKGS="ksh gettext.x86_64 libXrender.i686 libXau.i686 libxcb.i686 libX11.i686
libXext.i686 libXi.i686 libXtst.i686 glibc.x86_64 libstdc++.i686
libstdc++.x86_64 libgcc.x86_64"

for PKG in $PKGS;
do
yum -y install "$PKG"
done
```

HINWEIS: Da das Installationsmedium `compat-libstdc++-33-*.i686.rpm` und compat-libstdc++-33-*.x86_64.rpm nicht enthält, muss es vom Red Hat-Portal heruntergeladen werden.

Beispiel: Führen Sie zur Installation von `compat-libstdc++-33-*.x86_64.rpm` den folgenden Befehl aus:

```
yum -y install compat-libstdc++-33-*.x86_64.rpm
```

7 Führen Sie die je nach RHEL-Version in Schritt 8 oder Schritt 7 erstellte install.sh-Datei aus.

8 Führen Sie das in Abschnitt 6.3.2 angegebene Skript aus, um zu prüfen, ob die Voraussetzungen erfüllt sind.

9 Installieren Sie Identity Manager 4.7.

5.10 Erläuterungen zur Sprachunterstützung

NetIQ übersetzt (lokalisiert) die Benutzeroberfläche für Identity Manager und die zugehörigen Installationsprogramme nach Möglichkeit gemäß der Sprache des Betriebssystems auf den lokalen Computern. Leider können nicht alle Sprachen unterstützt werden. Während der Installation ermitteln einige Installationsprogramme anhand der Ländereinstellung des Computers die Sprache für den Installationsvorgang.

Soll das Installationsprogramm in einer bestimmten Sprache ausgeführt werden, legen Sie die Variable LANG im Profil oder über die Befehlszeile fest.

5.10.1 Übersetzte Komponenten und Installationsprogramme

In der nachfolgenden Tabelle sind die verfügbaren Übersetzungen für die einzelnen Installationen der Komponenten aufgeführt. Komponenten, die nicht in der Tabelle genannt sind, stehen nur auf Englisch bereit. Wenn die Komponente nicht in die Sprache des Betriebssystems übersetzt wurde, wird das Programm standardmäßig in englischer Sprache ausgeführt. Auch die Endbenutzer-Lizenzvereinbarung (EULA) steht ggf. nicht in allen unterstützten Sprachen zur Verfügung.

Länder-einstellung	Designer	Identity Manager-Engine	iManager	iManager-Plugins	Identitäts-anwendungen
Chinesisch-vereinfacht	Ja	Ja	Ja	Ja	Ja
Chinesisch-traditionell	Ja	Ja	Ja	Ja	Ja
Dänisch	–	–	–	–	Ja
Niederländisch	Ja	–	–	–	Ja
Englisch	Ja	Ja	Ja	Ja	Ja
Französisch	Ja	Ja	Ja	Ja	Ja
Deutsch	Ja	Ja	Ja	Ja	Ja
Italienisch	Ja	–	Ja	–	Ja
Japanisch	Ja	Ja	Ja	Ja	Ja

Länder-einstellung	Designer	Identity Manager-Engine	iManager	iManager-Plugins	Identitäts-anwendungen
Portugiesisch (Brasilien	Ja	–	Ja	–	Ja
Russisch	–	–	Ja	–	Ja
Spanisch	Ja	–	Ja	–	Ja
Schwedisch	–	–	–	–	Ja

Identitätsanwendungen umfassen das Dashboard, die Verwaltung der Identitätsanwendungen, das Identity Reporting, die Identitätsgenehmigungen und die Benutzeranwendung.

5.10.2 Besondere Überlegungen zur Sprachunterstützung

Wenn Sie die Verwendung einer übersetzten Version von Identity Manager erwägen, empfiehlt NetIQ, die nachfolgenden Überlegungen zu lesen.

- Im Allgemeinen gilt: Wenn eine Identity Manager-Komponente die Sprache des Betriebssystems nicht unterstützt, wird die Benutzeroberfläche dieser Komponente standardmäßig auf Englisch dargestellt. Die Identity Manager-Treiber sind beispielsweise in denselben Sprachen wie die Identity Manager-Engine verfügbar. Wenn Identity Manager die Treibersprache nicht unterstützt, wird die Treiberkonfiguration standardmäßig in englischer Sprache angeboten.
- Die nachfolgenden iManager-Plugins sind in den Sprachen Spanisch, Russisch, Italienisch und Portugiesisch erhältlich, außerdem in den Sprachen, die in der vorstehenden Tabelle angegeben sind.
- Beim Installieren von Designer müssen Sie die gettext-Dienstprogramme installieren. Die GNU-gettext-Dienstprogramme bieten einen Rahmen für internationalisierte und mehrsprachige Meldungen.
- Wenn Sie das Installationsprogramm für eine Identity Manager-Komponente starten, gilt Folgendes:
  - Wenn das Betriebssystem in einer Sprache ausgeführt wird, die das Installationsprogramm unterstützt, wird diese Sprache im Programm standardmäßig ausgewählt. Sie können jedoch eine andere Sprache für den Installationsvorgang festlegen.
  - Wenn das Installationsprogramm die Sprache des Betriebssystems nicht unterstützt, wird das Programm standardmäßig in englischer Sprache ausgeführt.
  - Wenn im Betriebssystem eine Sprache mit lateinischen Buchstaben verwendet wird, können Sie im Installationsprogramm eine beliebige Sprache mit lateinischen Buchstaben auswählen.
  - Wenn im Betriebssystem eine unterstützte asiatische Sprache oder Russisch verwendet wird, können Sie im Installationsprogramm lediglich dieselbe Sprache wie das Betriebssystem oder aber Englisch auswählen.

5.11 Herunterladen der Installationsdateien

Zum Installieren der Identity Manager-Komponenten laden Sie die folgenden Installationsdateien von der NetIQ Downloads-Website herunter:

- **Identity Manager-Engine, Identitätsanwendungen und Identity Reporting:**

  `Identity_Manager_4.7_Linux.iso`
- **Sentinel Log Management für Identity Governance and Administration:**

  `SentinelLogManagementForIGA8.1.1.0.tar.gz`
- **Designer:** `Identity_Manager_4.7_Linux_Designer.tar.gz`
- **Analyzer:** `Identity_Manager_4.7_Linux_Analyzer.tar.gz`

So laden Sie die Installationsdateien herunter:

1. Gehen Sie zur NetIQ Downloads-Website.
2. Klicken Sie neben der herunterzuladenden Datei auf die Schaltfläche **Herunterladen**.
3. Befolgen Sie die Bildschirmanweisungen, um die Datei in einen Ordner auf Ihrem Computer herunterzuladen.

III Installieren von Sentinel for Log Management für Identity Governance and Administration

In diesem Abschnitt werden Sie durch die Installation von SLM für IGA geführt, dem Standard-Revisionsdienst für Identity Manager.

Das Installationsprogramm für SLM für IGA führt die folgenden Funktionen aus:

- Installieren (und optional Konfigurieren) des Dienstes
- Erstellen des Benutzerkontos, mit dem Verwaltungsaufgaben für den Dienst ausgeführt werden können (**admin**)
- Erstellen des Datenbankadministratorkontos, über das der Dienst mit der Datenbank interagiert (**dbauser**)

6 Planen der Installation von SLM für IGA

In diesem Abschnitt finden Sie Anweisungen zum Vorbereiten der Installation von SLM für IGA, dem Standard-Revisionsdienst für Identity Manager.

6.1 Checkliste für die Installation von SLM für IGA

NetIQ empfiehlt, die Schritte in der folgenden Checkliste auszuführen:

	Checkliste
❑	1. Überprüfen Sie die Systemvoraussetzungen vor der Installation. Weitere Informationen finden Sie in Abschnitt 6.2, „Systemvoraussetzungen“, auf Seite 53.
❑	2. (Bedingt) Stellen Sie bei Computern mit RHEL 7.4-Betriebssystem sicher, dass die erforderlichen Bibliotheken installiert sind.
❑	3. Entscheiden Sie, ob eine standardmäßige oder eine typische Installation von SLM für IGA durchgeführt werden soll. Weitere Informationen finden Sie unter Abschnitt 7, „Installieren von SLM für IGA“, auf Seite 55.

6.2 Systemvoraussetzungen

In diesem Abschnitt finden Sie die Mindestanforderungen für die Server, auf denen die Installation erfolgen soll. Weitere Informationen finden Sie auf der Website für technische Informationen zu NetIQ Sentinel.

Überprüfen Sie außerdem die Voraussetzungen und Überlegungen zur Installation, insbesondere im Zusammenhang mit dem Betriebssystem.

Kategorie	Anforderung
Prozessor	4 bis 8 CPU-Kerne
Festplattenspeicher	200 GB
Arbeitsspeicher	24 GB
Betriebssystem (zertifiziert)	Eines der folgenden 64-Bit-Betriebssysteme (ggf. höhere Version): ◆ SLES 12 SP2 ◆ RHEL 7.3 **HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird.

Kategorie	Anforderung
Betriebssysteme (unterstützt)	Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme **HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert.

7 Installieren von SLM für IGA

Sie können Sentinel Log Management für Identity Governance and Administration (IGA) mit der Standardinstallation oder der angepassten Installation installieren.

7.1 Standardinstallation

1. Laden Sie die Datei `SentinelLogManagementForIGA8.1.1.0.tar.gz` von der NetIQ Downloads-Website herunter.
2. Navigieren Sie zu dem Verzeichnis, in dem die Datei extrahiert werden soll.
3. Extrahieren Sie die Datei mit dem folgenden Befehl:

   ```
   tar -zxvf SentinelLogManagementForIGA8.1.1.0.tar.gz
   ```
4. Navigieren Sie zum Verzeichnis `SentinelLogManagementforIGA`.
5. Installieren Sie SLM für IGA mit dem folgenden Befehl:

   ```
   ./install.sh
   ```
6. Geben Sie die Sprache an, die für die Installation verwendet werden soll. Drücken Sie dann die `Eingabetaste`.
7. Akzeptieren Sie die Lizenzvereinbarung mit `j`.

   Das Laden der Installationspakete kann einige Sekunden in Anspruch nehmen.
8. Soll die Standardinstallation vorgenommen werden, geben Sie `1` an.

   Der Installationsvorgang wird mit dem standardmäßigen Evaluierungslizenzschlüssel, der im Installationsprogramm enthalten ist, fortgesetzt. Sie können die Evaluierungslizenz zu jedem beliebigen Zeitpunkt während des Testzeitraums oder danach durch einen gekauften Lizenzschlüssel ersetzen.
9. Geben Sie das Passwort für den Administratorbenutzer `admin` an.
10. Bestätigen Sie das Passwort.

    Die Benutzer `admin`, `dbauser` und `appuser` verwenden dieses Passwort.

Die Installation wird beendet und der Server wird gestartet. Nach der Installation nimmt das Starten der Services möglicherweise einige Minuten in Anspruch, da das System eine einmalige Initialisierung ausführt. Warten Sie, bis die Installation abgeschlossen ist, bevor Sie sich am Sentinel-Server anmelden.

Geben Sie in einem Webbrowser folgende URL ein, um auf die Hauptoberfläche von SLM für IGA zuzugreifen:

`https://<IP_Address/DNS_SLM for IGA_server>:8443/SLM for IGA/views/main.html`

<IP_Address/DNS_SLM for IGA_server> bezeichnet hierbei die IP-Adresse bzw. den DNS-Namen des SLM für IGA-Server und *8443* den Standardport für den SLM für IGA-Server.

7.2 Angepasste Installation

1. Laden Sie die Datei `SentinelLogManagementForIGA8.1.1.0.tar.gz` von der NetIQ Downloads-Website herunter.
2. Navigieren Sie zu dem Verzeichnis, in dem die Datei extrahiert werden soll.
3. Extrahieren Sie die Datei mit dem folgenden Befehl:

   ```
   tar -zxvf SentinelLogManagementForIGA8.1.1.0.tar.gz
   ```
4. Navigieren Sie zum Verzeichnis `SentinelLogManagementforIGA`.
5. Führen Sie den folgenden Befehl aus:

   ```
   ./install.sh
   ```
6. Geben Sie `j` ein, um die Lizenzvereinbarung zu akzeptieren und mit der Installation fortzufahren.

   Das Laden der Installationspakete kann einige Sekunden in Anspruch nehmen.
7. Soll eine angepasste Konfiguration von SLM für IGA vorgenommen werden, geben Sie `2` an.
8. Geben Sie `1` ein, um den standardmäßigen Evaluierungslizenzschlüssel zu verwenden.

   Alternativ:

   Geben Sie `2` ein, um einen erworbenen Lizenzschlüssel für SLM für IGA einzugeben.
9. Geben Sie das Passwort für den Administratorbenutzer `admin` ein und bestätigen Sie das Passwort.
10. Geben Sie das Passwort für den Datenbankbenutzer `dbauser` ein und bestätigen Sie das Passwort.

    Das `dbauser`-Konto wird von SLM für IGA zur Interaktion mit der Datenbank verwendet. Das hier eingegebene Passwort kann zum Ausführen von Datenbankwartungsaufgaben verwendet werden, unter anderem zum Zurücksetzen des Administratorpasswords, falls dieses vergessen wird bzw. nicht mehr auffindbar ist.
11. Geben Sie das Passwort für den Anwendungsbenutzer `appuser` ein und bestätigen Sie das Passwort.
12. Geben Sie die erforderliche Nummer ein, um die Portzuweisungen zu ändern.

    Beispielsweise hat der Standardport für den Webserver die Nummer 8443. Soll die Portnummer für den Webserver bearbeitet werden, geben Sie `4` an. Geben Sie den neuen Portwert für den Webserver ein, beispielsweise „8643“.
13. Geben Sie nach dem Ändern der Ports 8 ein, um den Änderungsvorgang abzuschließen.
14. Geben Sie `1` ein, um Benutzer nur über die interne Datenbank zu authentifizieren.

    Alternativ:

    Wenn in der Domäne ein LDAP-Verzeichnis konfiguriert ist, geben Sie `2` ein, um Benutzer über das LDAP-Verzeichnis zu authentifizieren.

    Der Standardwert ist `1`.
15. Geben Sie `n` ein, wenn Sie aufgefordert werden, den FIPS 140-2-Modus zu aktivieren.
16. Geben Sie `n` ein, wenn Sie aufgefordert werden, den skalierbaren Speicher zu aktivieren.

Die Installation wird beendet und der Server wird gestartet. Nach der Installation nimmt das Starten der Services möglicherweise einige Minuten in Anspruch, da das System eine einmalige Initialisierung ausführt. Warten Sie, bis die Installation abgeschlossen ist, bevor Sie sich am Sentinel-Server anmelden.

Geben Sie in einem Webbrowser folgende URL ein, um auf die Hauptoberfläche von SLM für IGA zuzugreifen:

`https://<IP_Address/DNS_SLM for IGA_server>:<port>/SLM for IGA/views/main.html`

<IP_Address/DNS_SLM for IGA_server> bezeichnet hierbei die IP-Adresse bzw. den DNS-Namen des SLM für IGA-Server und *<port>* den Standardport für den SLM für IGA-Server.

IV Installieren und Konfigurieren der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting

In diesem Abschnitt finden Sie die Schritte für die Installation der Identity Manager-Engine, der Identitätsanwendungen und der Identity Reporting-Komponenten. Legen Sie vor dem Beginn der Installation fest, wie Identity Manager implementiert werden soll. Sie können die Identity Manager-Komponenten wahlweise auf einem einzelnen Server oder auch auf separaten Servern installieren. Weitere Informationen finden Sie unter Abschnitt 5.7.4, „Empfohlene Servereinrichtung“, auf Seite 40.

Die Komponenten können im interaktiven oder im unbeaufsichtigten Modus installiert und konfiguriert werden. Das Installationsprogramm umfasst separate Phasen für die Installation und die Konfiguration der Komponenten. Weitere Informationen finden Sie in Abschnitt 8.2, „Erläuterungen zum Installationsprogramm“, auf Seite 62. Die Installations- und Konfigurationsskripten (`install.sh` und `configure.sh`) befinden sich im Stammverzeichnis der `.iso`-Image-Datei mit dem Identity Manager-Installationspaket. Standardmäßig installiert das Installationsprogramm die Komponenten an den Standardspeicherorten. Weitere Informationen finden Sie unter Abschnitt 5.5, „Standardmäßige Speicherorte für die Installation“, auf Seite 37.

HINWEIS: Führen Sie `install.sh` in dem Speicherort aus, in dem Sie die `.iso`-Datei eingehängt haben. Wenn Sie `install.sh` von einem benutzerdefinierten Speicherort aus ausführen, treten Fehler auf.

NetIQ empfiehlt, die Voraussetzungen und Systemanforderungen zu lesen, bevor Sie die Installation starten. Weitere Informationen finden Sie unter Kapitel 8, „Planen der Installation der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting“, auf Seite 61.

8 Planen der Installation der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting

In diesem Abschnitt finden Sie die Voraussetzungen, die Überlegungen und die Systemeinrichtung für die Installation der Identity Manager-Engine, der Identitätsanwendungen und der Identity Reporting-Komponenten. Informieren Sie sich zunächst anhand der Checkliste über den Installationsvorgang.

8.1 Checkliste für die Installation der Identity Manager-Komponenten

NetIQ empfiehlt, vor Beginn des Installationsvorgangs die nachfolgenden Schritte auszuführen.

	Checkliste
❑	1. Informieren Sie sich über die Interaktion zwischen den Identity Manager-Komponenten. Weitere Informationen finden Sie in Teil I, „Einführung“, auf Seite 15.
❑	2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.7, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 39.
❑	3. Lesen Sie die Überlegungen zur Installation der Identity Manager-Engine, und prüfen Sie, ob die Computer den Voraussetzungen entsprechen. Weitere Informationen finden Sie in Abschnitt 8.3, „Planen der Installation der Identity Manager-Engine“, auf Seite 64.
❑	4. Prüfen Sie die Hardware- und Software-Voraussetzungen der Computer, auf denen die Identity Manager-Engine gehostet werden soll. Weitere Informationen finden Sie in „Systemanforderungen für Identity Manager-Engine, Remote Loader und iManager“, auf Seite 65.
❑	5. Informieren Sie sich, welche Treiber nach der Installation der Identity Manager-Engine automatisch aktiviert werden. Weitere Informationen finden Sie in Abschnitt 8.3.2, „Überlegungen für die Installation von Treibern zusammen mit der Identity Manager-Engine“, auf Seite 64.
❑	6. (Bedingt) Stellen Sie bei Computern mit RHEL 7.3 (oder höher) sicher, dass die erforderlichen Bibliotheken installiert sind.

	Checkliste
❑	7. Anweisungen zum Installieren der Identity Manager-Engine finden Sie in den folgenden Abschnitten: ◆ Abschnitt 9.1.1, „Durchführen einer interaktiven Installation“, auf Seite 91 ◆ Abschnitt 9.1.2, „Ausführen einer unbeaufsichtigten Installation der Identity Manager-Engine“, auf Seite 92
❑	8. (Bedingt) Soll der Remote Loader installiert werden, beachten Sie die Anweisungen in Abschnitt 8.4, „Planen der Installation des Remote Loaders“, auf Seite 68.
❑	9. (Bedingt) Wenn Sie eine Nicht-Root-Installation durchführen, aktualisieren Sie den Treibersatz, um Grafiken in Email-Benachrichtigungen zu unterstützen. Weitere Informationen finden Sie in Abschnitt 11.1.2, „Unterstützung für Grafiken in Email-Benachrichtigungen“, auf Seite 109.
❑	10. Starten Sie die Treiberinstanz im Remote Loader. Weitere Informationen finden Sie in Kapitel 11.3, „Konfigurieren des Remote Loader und der Treiber“, auf Seite 118.

8.2 Erläuterungen zum Installationsprogramm

Das Identity Manager-Installationsprogramm installiert und konfiguriert die Identity Manager-Komponenten in separaten Phasen. Die tatsächlich installierten Komponenten sind von der Identity Manager-Edition abhängig, die bei der Installation ausgewählt wurde (Advanced oder Standard Edition). Wenn Sie beispielsweise Identity Manager Advanced Edition ausgewählt haben, werden die folgenden Optionen angezeigt:

- Identity Manager-Engine
- Identity Manager Remote Loader-Dienst
- Identity Manager-Fan-out-Agent
- iManager-Webverwaltung
- Identitätsberichterstellung
- Identitätsanwendungen

Sie können die Identity Manager-Komponenten direkt nach der Installation konfigurieren oder auch zu einem späteren Zeitpunkt. Identity Manager bietet zwei Konfigurationsoptionen (typisch und 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 können Sie den Großteil der Einstellungen konfigurieren.

Weitere Informationen zur komponentenweisen Konfiguration finden Sie unter Abschnitt 10.1, „Erläuterungen zu den Konfigurationsparametern“, auf Seite 101.

In den folgenden Abschnitten werden die Komponenten erläutert, die mit den verschiedenen Installationsoptionen im Installationsprogramm installiert werden können:

8.2.1 Identity Manager-Engine

Installiert das Identitätsdepot, die Identity Manager-Engine und die Identity Manager-Treiber.

8.2.2 Identity Manager Remote Loader-Server

Installiert den Remote Loader-Dienst und die Treiberinstanzen im Remote Loader. Mit dem Remote Loader können Sie Identity Manager-Treiber auf verbundenen Systemen ausführen, auf denen das Identitätsdepot und die Identity Manager-Engine nicht gehostet werden.

8.2.3 Identity Manager-Fan-out-Agent

Installiert den Fan-out-Agenten für den JDBC-Fan-out-Treiber. Der JDBC-Fan-out-Treiber erstellt mit dem Fan-out-Agenten mehrere JDBC-Fan-out-Treiberinstanzen. Der Fan-out-Agent lädt die JDBC-Treiberinstanzen basierend auf der Konfiguration der Verbindungsobjekte im Fan-out-Treiber. Weitere Informationen finden Sie im NetIQ Identity Manager-Treiber für JDBC-Fan-out – Implementierungshandbuch.

8.2.4 iManager-Webverwaltung

Installiert die iManager-Webverwaltungskonsole und die iManager-Plugins.

8.2.5 Identitätsanwendungen

Mit dieser Installationsoption werden verschiedene Komponenten installiert, die das zugrunde liegende Rahmenwerk für die Identitätsanwendungen bilden.

- Identity Manager-Dashboard
- Identity Manager-Administrationskonsole
- Benutzeranwendung
- Benutzeranwendungstreiber (UAD)
- Rollen- und Ressourcenservice-Treiber (RRSD)

Das Installationsprogramm installiert intern einen Authentifizierungsdienst, der den Single-Sign-On-Zugriff auf die Identitätsanwendungen und Identity Reporting unterstützt. Das Installationsprogramm installiert außerdem einen Passwortverwaltungsdienst, mit dem Sie Identity Manager so konfigurieren, dass die Benutzer ihre Passwörter zurücksetzen können.

Der Installationsvorgang stellt den Benutzeranwendungstreiber sowie den Rollen- und den Ressourcenservice-Treiber bereit.

8.2.6 Identitätsberichterstellung

Mit dieser Installationsoption werden verschiedene Komponenten installiert, die das zugrunde liegende Rahmenwerk für Identity Reporting bilden.

- Identitätsberichterstellung
- Treiber „Verwaltetes System – Gateway“ (MSGW-Treiber)
- Datenerfassungsdiensttreiber (DCS)

Identity Reporting kommuniziert zu Revisionszwecken mit SLM für IGA. Zum Protokollieren der Ereignisse benötigt die Identitätsberichterstellung die SIEM-Datenbank, die zusammen mit SLM für IGA installiert wird.

Der Installationsvorgang stellt die MSGW- und DCS-Treiber bereit.

8.3 Planen der Installation der Identity Manager-Engine

In diesem Abschnitt wird die Installation der Identity Manager-Engine und der Treiber beschrieben.

- Abschnitt 8.3.1, „Überlegungen für die Installation der Identity Manager-Engine“, auf Seite 64
- Abschnitt 8.3.2, „Überlegungen für die Installation von Treibern zusammen mit der Identity Manager-Engine“, auf Seite 64
- Abschnitt 8.3.3, „Voraussetzungen für die Installation des Identitätsdepots in einer Cluster-Umgebung“, auf Seite 65
- Abschnitt 8.3.4, „Systemanforderungen für Identity Manager-Engine, Remote Loader und iManager“, auf Seite 65

8.3.1 Überlegungen für die Installation der Identity Manager-Engine

Lesen Sie vor dem Installieren der Identity Manager-Engine die folgenden Überlegungen:

- Je nach Version des Identitätsdepots installiert das Installationsprogramm die 64-Bit-Version des Identity Manager.
- (Bedingt) Soll der Remote Loader auf demselben Computer installiert werden wie die Identity Manager-Engine, benötigen Sie ein Betriebssystem, das beide Komponenten unterstützt. Weitere Informationen zu den Systemanforderungen für den Remote Loader finden Sie in Abschnitt 8.4.5, „Voraussetzungen und Überlegungen für die Installation des Remote Loader“, auf Seite 71.
- (Bedingt) Wenn Sie die Identity Manager-Engine als Nicht-`Root`-Benutzer installieren, werden der NetIQ Sentinel-Plattformagent, der Linux-Kontentreiber und der Remote Loader während des Installationsprogramms nicht installiert. Sie müssen diese Komponenten separat installieren.

HINWEIS: Installieren Sie den neuesten Patch für den Novell Audit-Plattformagenten, um die Revision mit einer Nicht-Root-Installation der Engine zu unterstützen. Wenden Sie sich an das Team für technischen Support, um weitere Informationen zu erhalten.

8.3.2 Überlegungen für die Installation von Treibern zusammen mit der Identity Manager-Engine

Die Leistung des Servers, auf dem Sie die Identity Manager-Engine installieren, ist von mehreren Faktoren abhängig, unter anderem von der Anzahl der Treiber, die auf diesem Server ausgeführt werden. Beim Planen des Installationsorts für die Treiber empfiehlt NetIQ Folgendes:

- Die Anzahl der Treiber, die auf dem Server ausgeführt werden, ist im Allgemeinen abhängig von der Belastung des Servers durch diese Treiber. Einige Treiber verarbeiten zahlreiche Objekte, andere dagegen nicht.
- Wenn Millionen von Objekten mit jedem Treiber synchronisiert werden sollen, beschränken Sie die Anzahl der Treiber auf dem Server. Stellen Sie in diesem Fall beispielsweise maximal 10 Treiber bereit.

- Wenn pro Treiber maximal 100 Objekte synchronisiert werden sollen, können Sie ggf. mehr als 10 Treiber auf dem Server ausführen.
- Mit den Werkzeugen für die Überwachung des Treiberzustands erstellen Sie einen Grundwert zur Serverleistung, der bei der Ermittlung der optimalen Anzahl an Treibern hilfreich ist. Weitere Informationen zu den Werkzeugen für die Überwachung des Treiberzustands finden Sie unter „Überwachen des Treiberzustands“ im NetIQ Identity Manager-Treiber-Administrationshandbuch.

Weitere Informationen zum Aktivieren der Identity Manager-Treiber nach der Installation finden Sie in Kapitel 24, „Aktivieren von Identity Manager“, auf Seite 245.

8.3.3 Voraussetzungen für die Installation des Identitätsdepots in einer Cluster-Umgebung

NetIQ empfiehlt, vor der Installation des Identitätsdepots in einer Cluster-Umgebung die folgenden Überlegungen zu lesen:

- 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.
  - NetIQ empfiehlt, alle weiteren eDirectory-Konfigurationsdaten und Protokolldaten im gemeinsam genutzten Speicher abzulegen.
- Sie müssen eine virtuelle IP-Adresse besitzen.
- (Bedingt) Wenn Sie eDirectory als Rahmenstruktur für das Identitätsdepot verwenden, unterstützt das Dienstprogramm `nds-cluster-config` lediglich die Root-eDirectory-Instanz. eDirectory bietet keine Unterstützung für die Konfiguration von mehreren Instanzen und die Nicht-Root-Installation von 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 im *NetIQ eDirectory-Installationshandbuch*.

8.3.4 Systemanforderungen für Identity Manager-Engine, Remote Loader und iManager

Die folgende Tabelle zeigt die komponentenweisen Mindestsystemanforderungen für die Installation:

HINWEIS: Das BTRFS-Dateisystem wird nicht für das Identitätsdepot unterstützt.

Kategorie	Identitätsdepot	Identity Manager-Engine	Remote Loader (64 Bit)	iManager
Prozessor	1 GHz	1 GHz	1 GHz	1 GHz
Festplattenspeicher	◆ 300 MB für das Identitätsdepot ◆ 150 MB zusätzlicher Festplattenspeicher pro 50.000 Benutzer	◆ 1 GB ◆ 150 MB zusätzlicher Festplattenspeicher pro 50.000 Benutzer		200 MB
Arbeitsspeicher	2 GB	◆ 2 GB für die Identity Manager-Engine ◆ 2 GB für Identity Manager-Treiber	512 MB	512 MB
Betriebssystem (zertifiziert) **HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird. NetIQ empfiehlt, vor der Installation von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden.	Eines der folgenden 64-Bit-Betriebssysteme: ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3	Eines der folgenden 64-Bit-Betriebssysteme: ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3	Eines der folgenden 64-Bit-Betriebssysteme: ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3	Eines der folgenden 64-Bit-Betriebssysteme: ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3
Betriebssystem (unterstützt) **HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert.	Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme	Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme	Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme	Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme

Kategorie	Identitätsdepot	Identity Manager-Engine	Remote Loader (64 Bit)	iManager
Virtualisierungssystem NetIQ unterstützt Identity Manager auf Enterprise-Virtualisierungssystemen, die die Betriebssysteme, unter denen die NetIQ-Produkte ausgeführt werden können, offiziell unterstützen. Sofern die Anbieter der Virtualisierungssysteme diese Betriebssysteme offiziell unterstützen, unterstützt NetIQ den gesamten Identity Manager-Stack auf diesen Systemen.	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 und höher ◆ Windows Server 2012 R2 -Virtualisierung mit Hyper-V (unterstützt)	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 und höher ◆ Windows Server 2012 R 2-Virtualisierung mit Hyper-V (unterstützt)	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 und höher ◆ Windows Server 2012 R 2-Virtualisierung mit Hyper-V (unterstützt)	
Software	eDirectory 9.1	Identity Manager Engine 4.7	Remote Loader 4.7	iManager 3.1
Java (Java-Laufzeitumgebung (JRE) von Oracle)	JRE 1.8.0_162	JRE 1.8.0_162	JRE 1.8.0_162	JRE 1.8.0_162
Webbrowser				Einer der folgenden Browser (ggf. höhere Version): ◆ Google Chrome 61 ◆ Mozilla Firefox 51
Anwendungsserver				Apache Tomcat 8.5.27 im Bundle mit iManager
Standardports				8080, 8443 und 9009

8.4 Planen der Installation des Remote Loaders

In diesem Abschnitt finden Sie Informationen, die Ihnen bei der Vorbereitung auf die Installation des Remote Loaders und des Java Remote Loaders helfen.

8.4.1 Checkliste für die Installation des Remote Loaders

NetIQ empfiehlt, die Schritte in der folgenden Checkliste auszuführen:

	Checkliste
❑	1. Informieren Sie sich über die Interaktion zwischen den Identity Manager-Komponenten. Weitere Informationen finden Sie in Abschnitt 3.3.3, „Remote Loader“, auf Seite 23.
❑	2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.7, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 39.
❑	3. Stellen Sie sicher, dass die Identity Manager-Engine installiert ist.
❑	4. Lesen Sie die Überlegungen zur Installation des Remote Loader, und prüfen Sie, ob die Computer den Voraussetzungen entsprechen. Weitere Informationen finden Sie in Abschnitt 8.4.5, „Voraussetzungen und Überlegungen für die Installation des Remote Loader“, auf Seite 71.
❑	5. Prüfen Sie die Hardware- und Software-Voraussetzungen der Computer, auf denen der Remote Loader gehostet werden soll. Weitere Informationen finden Sie in Abschnitt 8.3.4, „Systemanforderungen für Identity Manager-Engine, Remote Loader und iManager“, auf Seite 65.
❑	6. (Bedingt) Stellen Sie bei Computern mit RHEL 7.3-Betriebssystem (oder höher) sicher, dass die erforderlichen Bibliotheken installiert sind. Weitere Informationen finden Sie in Abschnitt 5.9.4, „Installieren von Identity Manager auf Servern mit RHEL 7.3 (oder höher)“, auf Seite 45.
❑	7. (Bedingt) Soll der Remote Loader auf einem Server installiert werden, auf dem die Identity Manager-Engine nicht gehostet wird, muss es möglich sein, eine sichere Verbindung zur Engine herzustellen. Weitere Informationen finden Sie in Abschnitt 11.3.1, „Herstellen einer sicheren Verbindung zur Identity Manager-Engine“, auf Seite 119.
❑	8. Entscheiden Sie, ob die 32-Bit- oder die 64-Bit-Version des Remote Loader installiert werden soll. Weitere Informationen finden Sie in Abschnitt 8.4.4, „Verwenden des 32-Bit- und des 64-Bit-Remote Loader auf demselben Computer“, auf Seite 71.
❑	9. Entscheiden Sie, ob der Remote Loader oder der Java Remote Loader verwendet werden soll. Weitere Informationen finden Sie in „Erläuterungen zum Java Remote Loader“, auf Seite 71.

	Checkliste
❑	10. Installieren Sie den Remote Loader. Weitere Informationen finden Sie in Kapitel 9, „Installieren der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting“, auf Seite 91.
❑	11. (Bedingt) Soll der Java Remote Loader installiert werden, beachten Sie die Anweisungen in Abschnitt 9.2, „Installieren des Java Remote Loader“, auf Seite 96.
❑	12. Prüfen Sie die Parameter zum Konfigurieren einer Treiberinstanz. Weitere Informationen finden Sie in Abschnitt 11.3.2, „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 122.
❑	13. Befolgen Sie die Anweisungen zum Konfigurieren einer Treiberinstanz im Remote Loader in einem der folgenden Abschnitte: ◆ Abschnitt 11.3.3, „Konfigurieren des Remote Loader für Treiberinstanzen“, auf Seite 131 ◆ Abschnitt 11.3.4, „Konfigurieren des Java Remote Loader für Treiberinstanzen“, auf Seite 132
❑	14. Bereiten Sie die Treiber für den Remote Loader vor. Weitere Informationen finden Sie in Abschnitt 11.3.5, „Konfigurieren von Identity Manager-Treibern für die Verwendung mit dem Remote Loader“, auf Seite 133.
❑	15. Starten Sie die Treiberinstanz im Remote Loader. Weitere Informationen finden Sie in Abschnitt 11.3.8, „Starten einer Treiberinstanz im Remote Loader“, auf Seite 141.
❑	16. (Bedingt) Weitere Informationen zum Konfigurieren der beiderseitigen Authentifizierung zwischen dem Remote Loader und der Identity Manager-Engine finden Sie in Abschnitt 11.3.6, „Konfigurieren der beiderseitigen Authentifizierung mit der Identity Manager-Engine“, auf Seite 134.
❑	17. Stellen Sie sicher, dass der Remote Loader und der Treiber mit der Identity Manager-Engine und dem verbundenen System kommunizieren. Weitere Informationen finden Sie in Abschnitt 11.3.7, „Überprüfen der Konfiguration“, auf Seite 140.
❑	18. Installieren Sie die restlichen Identity Manager-Komponenten, z. B. Designer und Analyzer.

8.4.2 Erläuterungen zum Remote Loader

Mit dem Remote Loader können Sie Identity Manager-Treiber auf verbundenen Systemen ausführen, auf denen das Identitätsdepot und die Identity Manager-Engine nicht gehostet werden.

Der Remote Loader kann die in den plattformspezifischen Dateien enthaltenen Identity Manager-Anwendungsschnittstellenmodule über JNI sowie die häufiger verwendeten Identity Manager-Anwendungsschnittstellenmodule in plattformunabhängigen JAR-Dateien hosten. Der Remote Loader kann auf jeder Plattform ausgeführt werden. Plattformspezifische Schnittstellenmodule müssen jedoch auf der jeweils nativen Plattform ausgeführt werden (beispielsweise `.iso`-Dateien unter Linux).

Erläuterungen zu Schnittstellenmodulen

Der Remote Loader kommuniziert über Schnittstellenmodule mit der Anwendung auf einem verwalteten System. Ein *Schnittstellenmodul* besteht aus einer oder mehreren Dateien, in denen sich der Code zum Verarbeiten der Ereignisse befindet, die zwischen dem Identitätsdepot und der Anwendung synchronisiert werden. Vor Verwendung des Remote Loader müssen Sie das Anwendungsschnittstellenmodul so konfigurieren, dass eine sichere Verbindung zur Identity

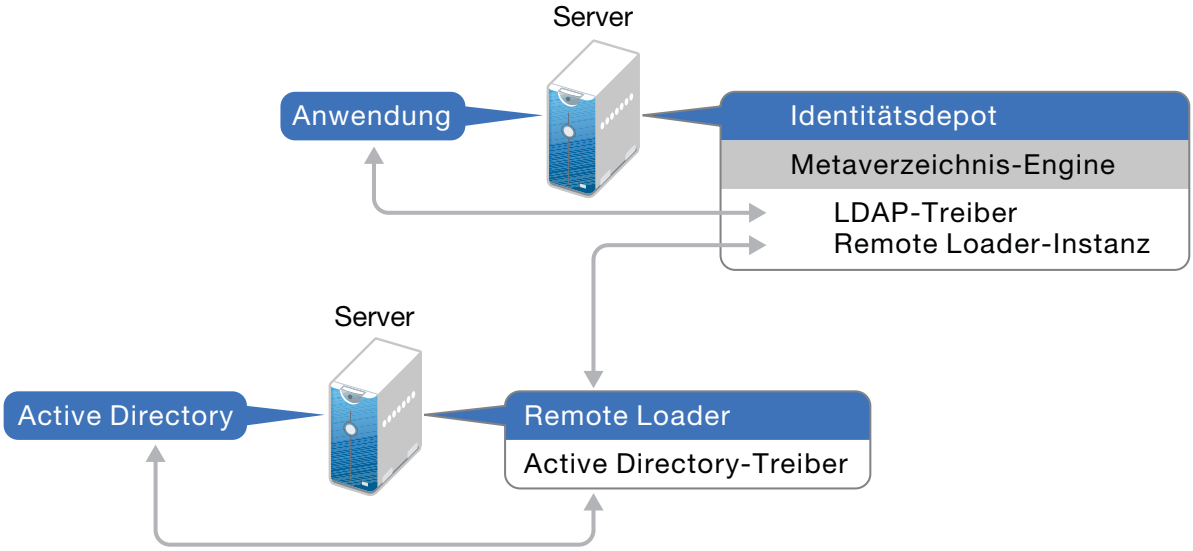
Manager-Engine hergestellt wird. Außerdem müssen sowohl der Remote Loader als auch die Identity Manager-Treiber konfiguriert werden. Weitere Informationen finden Sie in Kapitel 11.3, „Konfigurieren des Remote Loader und der Treiber“, auf Seite 118.

Ermitteln des richtigen Zeitpunkts zum Verwenden des Remote Loader

Sie können die Identity Manager-Engine, das Identitätsdepot und das Treiberschnittstellenmodul auf demselben Server installieren. Die Identity Manager-Engine wird als Teil eines eDirectory-Prozesses ausgeführt. Die Identity Manager-Treiber können auf dem Server ausgeführt werden, auf dem sich Identity Manager befindet. Sie können zudem Teil desselben Prozesses sein, in dem die Identity Manager-Engine ausgeführt wird. In den folgenden Szenarien sollten die Identity Manager-Treiber jedoch aus strategischen Gründen als separater Prozess auf dem Server ausgeführt werden, auf dem die Identity Manager-Engine gehostet wird:

- Schutz der Identitätsdepots vor Ausnahmefehlern, die durch das Treiberschnittstellenmodul ausgelöst werden.
- Erhöhen der Leistung des Servers, auf dem die Identity Manager-Engine ausgeführt wird, durch das Auslagern von Treiberbefehlen an die Remote-Anwendung oder Datenbank.
- Ausführen von weiteren Treibern auf Servern, auf dem die Identity Manager-Engine nicht gehostet wird.

In diesen Szenarien stellt der Remote Loader einen Kommunikationskanal zwischen der Identity Manager-Engine und dem Treiber bereit. Sie installieren beispielsweise einen LDAP-Treiber auf demselben Server wie die Identity Manager-Engine und das Identitätsdepot. Dann installieren Sie den AD-Treiber (Active Directory) mit dem Remote Loader auf einem anderen Server. Damit die Treiber auf die Anwendung zugreifen und mit dem Identitätsdepot kommunizieren können, installieren Sie den Remote Loader auf beiden Servern (siehe Abbildung):



NetIQ empfiehlt, nach Möglichkeit die Remote Loader-Konfiguration für die Treiber zu verwenden. Nutzen Sie den Remote Loader selbst dann, wenn sich die Anwendung auf demselben Server wie die Identity Manager-Engine befindet.

Erläuterungen zum Java Remote Loader

Der Java Remote Loader bietet die Flexibilität zum Laden eines Treiberschnittstellenmoduls auf Computern mit Linux-Servern, die der native Remote Loader nicht unterstützt. Der Java Remote Loader ist eine Java-Anwendung. Java Remote Loader funktioniert mit jeder öffentlich unterstützten Version von Java.

Öffnen Sie die Anwendung mit dem Skript `dirxml_jremote`. Weitere Informationen finden Sie in Abschnitt 11.3.4, „Konfigurieren des Java Remote Loader für Treiberinstanzen“, auf Seite 132.

8.4.3 Erläuterungen zum Installationsprogramm

Das Installationsprogramm der Identity Manager-Engine installiert eine 32-Bit- und/oder eine 64-Bit-Version eines Remote Loader. Neben dem Remote Loader können Sie im Installationsprogramm die Treiber auswählen, die auf dem verbundenen System installiert werden sollen.

8.4.4 Verwenden des 32-Bit- und des 64-Bit-Remote Loader auf demselben Computer

Standardmäßig erkennt das Installationsprogramm die Betriebssystemversion und installiert anschließend die entsprechende Version des Remote Loader. Sie können sowohl den 32-Bit- als auch den 64-Bit-Remote Loader auf einem 64-Bit-Betriebssystem installieren:

- Wenn Sie eine 32-Bit-Version von Remote Loader aufrüsten, die auf einem 64-Bit-Betriebssystem installiert ist, rüstet der Prozess den 32-Bit-Remote Loader auf die aktuelle Version auf und installiert darüber hinaus den 64-Bit-Remote Loader.
- Wenn Sie sowohl einen 32-Bit- als auch einen 64-Bit-Remote Loader auf demselben Computer installieren, werden die Audit-Ereignisse nur mit dem 64-Bit-Remote Loader generiert. Wenn zuerst ein 64-Bit-Remote Loader und dann ein 32-Bit-Remote Loader installiert wird, werden die Ereignisse im 32-Bit-Cache protokolliert.

8.4.5 Voraussetzungen und Überlegungen für die Installation des Remote Loader

NetIQ empfiehlt, vor dem Installieren des Remote Loader die folgenden Überlegungen zu lesen:

- Vor der Installation des Remote Loader muss die Identity Manager-Engine installiert werden.

  Wenn Sie den Remote Loader installiert haben, ohne zuvor die Identity Manager-Engine installiert zu haben, müssen Sie die Datei `novell-openssl-9.1.0-0.x86_64.rpm` installieren, bevor Sie die Identity Manager-Engine konfigurieren können.

  1. Navigieren Sie zum folgenden Verzeichnis:

     ```
     <Speicherort, in dem die Datei „Identity_Manager_4.7_Linux.iso" eingehängt ist>/IDM/packages/OpenSSL/x86_64/
     ```

  2. Installieren Sie die Datei `novell-openssl-9.1.0-0.x86_64.rpm` mit dem folgenden Befehl:

     ```
     rpm -ivh novell-openssl-9.1.0-0.x86_64.rpm
     ```

- Installieren Sie den Remote Loader auf einem Server, der mit den verbundenen Systemen kommunizieren kann. Der Treiber für die einzelnen verwalteten Systeme muss mit den relevanten APIs zur Verfügung stehen.

- Sie können den Remote Loader auf demselben Computer installieren wie die Identity Manager-Engine.
- Sie können sowohl den 32-Bit- als auch den 64-Bit-Remote Loader auf demselben Computer installieren.
- Sie können den Java Remote Loader auf Plattformen installieren, die den nativen Remote Loader nicht unterstützen. Weitere Informationen zu den unterstützten Plattformen finden Sie unter Abschnitt 8.3.4, „Systemanforderungen für Identity Manager-Engine, Remote Loader und iManager“, auf Seite 65.
- NetIQ empfiehlt, nach Möglichkeit die Remote Loader-Konfiguration für die Treiber zu verwenden. Nutzen Sie den Remote Loader selbst dann, wenn sich das verbundene System auf demselben Server wie die Identity Manager-Server-Engine befindet.

  Wenn Sie das Treiberschnittstellenmodul in der Remote Loader-Konfiguration ausführen, erzielen Sie die folgenden Vorteile:

  - Die Trennung des Arbeitsspeichers und der Verarbeitung zwischen den Treiberschnittstellenmodulen steigert die Leistung der Identity Manager-Lösung und erleichtert ihre Überwachung.
  - Das Installieren von Patches und das Aufrüsten des Treiberschnittstellenmoduls wirken sich nicht auf das Identitätsdepot oder andere Treiber aus.
  - Das Identitätsdepot wird vor schwerwiegenden Fehlern geschützt, die eventuell im Treiberschnittstellenmodul auftreten.
  - Die Last wird von den Treiberschnittstellenmodulen auf andere Server verteilt.
- Die folgenden Treiber unterstützen die Funktionen des Remote Loader:
  - Access Review
  - ACF2
  - Azure Active Directory
  - Banner
  - Schwarzes Brett
  - Datenerfassungsdienst
  - Text mit Begrenzungszeichen
  - GoogleApps
  - REST
  - GroupWise 2014 (für den 32-Bit-Remote Loader)
  - JDBC
  - JMS
  - LDAP
  - Linux-Einstellungen
  - Lotus Notes
  - Verwaltetes System – Gateway
  - „Manuelle Aufgabe“-Services
  - Null- und Loopback
  - Office 365
  - Oracle EBS HRMS
  - Oracle EBS TCA

    - Oracle EBS User Management
    - PeopleSoft 5.2
    - Privileged User Management
    - Remedy
    - SalesForce.com
    - SAP Business Logic
    - SAP Portal
    - SAP HR (wird für Java Remote Loader nicht unterstützt)
    - SAP User Management (wird für Java Remote Loader nicht unterstützt)
    - ServiceNow
    - Integrationsmodul V2.0 für Sentinel
    - SharePoint
    - SOAP
    - Streng geheim
    - Auftrag
  - Die folgenden Treiber bieten keine Unterstützung für den Remote Loader:
    - eDirectory bidirektional
    - eDirectory
    - Berechtigungsservices
    - Rollenservice
    - Benutzeranwendung

8.5 Planen der Installation der Identitätsanwendungen

Die Installation der Identitätsanwendungen enthält die folgenden Komponenten:

- Identity Manager-Dashboard
- Identity Manager-Verwaltungsoberfläche
- Benutzeranwendung
- Rollen- und Ressourcenservice-Treiber
- Benutzeranwendungstreiber

Der Abschnitt enthält folgende Informationen:

8.5.1 Checkliste für die Installation der Identitätsanwendungen

NetIQ empfiehlt, vor Beginn des Installationsvorgangs die nachfolgenden Schritte auszuführen:

	Checkliste
❑	1. Informieren Sie sich über die Interaktion zwischen den Identity Manager-Komponenten. Weitere Informationen finden Sie in Abschnitt 4.3.1, „Benutzeranwendung und rollenbasiertes Bereitstellungsmodul“, auf Seite 28.
❑	2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.7.4, „Empfohlene Servereinrichtung“, auf Seite 40.
❑	3. Legen Sie fest, ob ein Sentinel vor der Installation der Identitätsanwendungen installiert werden soll. Weitere Informationen finden Sie in Abschnitt 5.7, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 39.
❑	4. Stellen Sie sicher, dass die Identity Manager-Engine installiert ist. Weitere Informationen zum Installieren der Engine finden Sie in Abschnitt 8.3.4, „Systemanforderungen für Identity Manager-Engine, Remote Loader und iManager“, auf Seite 65.
❑	5. Lesen Sie die Überlegungen zur Installation der Identitätsanwendungen und des unterstützenden Rahmenwerks, und prüfen Sie, ob die Server den Voraussetzungen entsprechen. Weitere Informationen finden Sie in Abschnitt 8.5.2, „Voraussetzungen und Überlegungen für die Installation der Identitätsanwendungen“, auf Seite 75.
❑	6. (Bedingt) Zur geführten Installation auf Computern mit dem Betriebssystem SLES 12 SP2 (oder höher) müssen die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in Abschnitt 5.9.3, „Installieren von Identity Manager auf Servern mit SLES 12 SP2 (oder höher)“, auf Seite 45.
❑	7. (Bedingt) Stellen Sie bei Computern mit RHEL 7.3-Betriebssystem (oder höher) sicher, dass die erforderlichen Bibliotheken installiert sind. Weitere Informationen finden Sie in Abschnitt 5.9.4, „Installieren von Identity Manager auf Servern mit RHEL 7.3 (oder höher)“, auf Seite 45.
❑	8. Prüfen Sie die Hardware- und Software-Voraussetzungen der Computer, auf denen die Identitätsanwendungen und ihr Rahmenwerk gehostet werden soll. Weitere Informationen finden Sie in Abschnitt 8.5.3, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 83.
❑	9. Installieren und konfigurieren Sie eine Datenbank für die Identitätsanwendungen auf dem lokalen Computer oder auf einem verbundenen Server. ◆ Weitere Informationen zur Datenbank finden Sie in „Voraussetzungen für die Installation der Datenbank für die Identitätsanwendungen“, auf Seite 78. ◆ Anweisungen zum Installieren der Datenbank finden Sie in Kapitel , „Konfigurieren der Datenbank für die Identitätsanwendungen“, auf Seite 79.
❑	10. Installieren Sie die Identitätsanwendungen. Beachten Sie einen der folgenden Abschnitte: ◆ Abschnitt 9.1.1, „Durchführen einer interaktiven Installation“, auf Seite 91 ◆ Abschnitt 9.1.2, „Ausführen einer unbeaufsichtigten Installation der Identity Manager-Engine“, auf Seite 92
❑	11. Führen Sie die abschließenden Aufgaben im Installationsvorgang gemäß den Anweisungen in Kapitel 11, „Abschließende Konfigurationsschritte“, auf Seite 109 aus.

	Checkliste
❑	12. Stellen Sie sicher, dass die Identitätsanwendungen und die Single-Sign-On-Einstellungen fehlerfrei konfiguriert sind. Weitere Informationen finden Sie in Kapitel 19, „Überprüfen des Single-Sign-On-Zugriffs auf die Identitätsanwendungen“, auf Seite 213.
❑	13. (Optional) Weitere Informationen zum Aufnehmen der Arbeit mit den Identitätsanwendungen finden Sie im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

8.5.2 Voraussetzungen und Überlegungen für die Installation der Identitätsanwendungen

NetIQ empfiehlt, die Voraussetzungen und die Computeranforderungen für die Identitätsanwendungen zu lesen, bevor Sie den Installationsvorgang beginnen. Weitere Informationen zum Konfigurieren der Benutzeranwendungsumgebung finden Sie im NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen.

Überlegungen zur Installation der Identitätsanwendungen

Für die Installation der Identitätsanwendungen gelten die nachfolgenden Überlegungen.

- Es ist eine unterstützte Version der folgenden Identity Manager-Komponenten erforderlich:
  - Identity Manager-Engine
  - Remote Loader
- (Optional) NetIQ empfiehlt, das SSL-Protokoll (Secure Sockets Layer) für die Kommunikation zwischen den Identity Manager-Komponenten zu aktivieren. Zur Verwendung des SSL-Protokolls müssen Sie SSL in Ihrer Umgebung aktivieren und **https** während der Installation angeben. Weitere Informationen zum Aktivieren von SSL finden Sie unter Konfigurieren der Sicherheit in den Identitätsanwendungen im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.
- Der Rollen- und Ressourcenservice-Treiber kann nicht zusammen mit dem Remote Loader genutzt werden, da der Treiber jClient verwendet.

- Der Installationsvorgang legt die Programmdateien standardmäßig im Verzeichnis `/opt/netiq/idm` ab. Wenn die Benutzeranwendung in einem nicht standardmäßigen Speicherort installiert werden soll, muss das neue Verzeichnis den folgenden Voraussetzungen entsprechen, bevor Sie den Installationsvorgang beginnen können:
  - Das Verzeichnis ist vorhanden, und es kann in das Verzeichnis geschrieben werden.
  - Nicht-`Root`-Benutzer können in das Verzeichnis schreiben.
- Jede Benutzeranwendungsinstanz kann nur jeweils einen einzigen Benutzer-Container verarbeiten. Sie können beispielsweise Benutzer nur zu dem Container hinzufügen, der mit der Instanz verknüpft ist, die Benutzer nur in diesem Container suchen und eine Abfrage nur für diesen Container durchführen. Außerdem sollte die Verknüpfung eines Benutzeranwendungscontainers mit einer Anwendung dauerhaft sein.
- (Optional) Sollen Autorisierungen von verwalteten Systemen abgerufen werden, installieren Sie mindestens einen Identity Manager-Treiber.
  - Sie müssen Treiber verwenden, die von Identity Manager 4.6 oder höher unterstützt werden. Weitere Informationen zum Installieren dieser Treiber finden Sie in den einzelnen Treiberhandbüchern auf der Website zur NetIQ Identity Manager-Treiberdokumentation.
  - Damit die Treiber verwaltet werden können, müssen Designer oder die entsprechenden Plugins für iManager bereits installiert sein. Die iManager-Plugins befinden sich im Installationspaket für die Identity Manager-Engine.

Überlegungen zur Konfiguration und Nutzung der Identitätsanwendungen

Für die Konfiguration und die erste Verwendung der Identitätsanwendungen gelten die nachfolgenden Überlegungen.

- Bevor die Benutzer auf die Identitätsanwendungen zugreifen können, müssen Sie die folgenden Schritte ausführen:
  - Stellen Sie sicher, dass alle erforderlichen Identity Manager-Treiber installiert sind.
  - Stellen Sie sicher, dass sich die Indizes für das Identitätsdepot im Online-Modus befinden. Weitere Informationen zum Konfigurieren eines Index während der Installation finden Sie in „Sonstige“, auf Seite 153.
  - Aktivieren Sie Cookies in allen Browsern. Die Anwendungen sind nicht funktionsfähig, wenn Cookies deaktiviert sind.
- Während des Installationsvorgangs legt das Installationsprogramm Protokolldateien im Installationsverzeichnis ab. Diese Dateien enthalten Informationen über Ihre Konfiguration. Nach erfolgter Konfiguration der Identitätsanwendungen 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 Identitätsanwendungen erfolgen, müssen die Identitätsberichterstellung und ein Revisionsdienst in der Umgebung installiert und für die Erfassung von Ereignissen konfiguriert sein. Sie müssen außerdem die Identitätsanwendungen für die Revision konfigurieren.

Festlegen eines Speicherorts für den Berechtigungsindex

Beim Installieren der Identitätsanwendungen wird ein Berechtigungsindex für Tomcat angelegt. Wenn Sie keinen Speicherort für diesen Index angeben, erstellt das Installationsprogramm einen Ordner in einem temporären Verzeichnis. Beispiel: `/opt/netiq/idm/apps/tomcat/temp/permindex` auf Tomcat.

In einer Testumgebung ist der Speicherort im Normalfall unerheblich. In einer Produktions- oder Staging-Umgebung sollte der Berechtigungsindex jedoch nicht in einem temporären Verzeichnis abgelegt werden.

So legen Sie einen Speicherort für den Berechtigungsindex fest:

1. Halten Sie Tomcat an.
2. Öffnen Sie die Konfigurationsdatei `ism-configuration.properties` in einem Texteditor.
3. Fügen Sie am Ende der Datei den folgenden Text an:

   `com.netiq.idm.cis.indexdir = path/permindex`

   Beispiel:

   `com.netiq.idm.cis.indexdir = /opt/netiq/idm/apps/tomcat/temp/permindex`
4. Speichern und schließen Sie die Datei.
5. Löschen Sie den vorhandenen Ordner `permindex` im temporären Verzeichnis.
6. Starten Sie Tomcat.

Aktivieren des Berechtigungsindex für das Clustering

In diesem Abschnitt finden Sie Anweisungen zur Aktivierung des Berechtigungsindex für das Clustering.

1. Melden Sie sich bei iManager im ersten Knoten des Clusters an und navigieren Sie zu **Objekte anzeigen**.
2. Navigieren Sie unter **System** zum Treibersatz mit dem **Benutzeranwendungstreiber**.
3. Wählen Sie **AppConfig** > **AppDefs** > **Konfiguration** aus.
4. Wählen Sie das XMLData-Attribut aus, 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>
   ```
5. Klicken Sie auf **OK**.

Voraussetzungen für die Installation der Datenbank für die Identitätsanwendungen

In der Datenbank werden die Identitätsanwendungsdaten und die Konfigurationsinformationen gespeichert.

Beachten Sie vor dem Installieren der Datenbankinstanz die folgenden Voraussetzungen:

- Zum Konfigurieren einer Datenbank für die Verwendung mit Tomcat müssen Sie einen JDBC-Treiber erstellen. Die Identitätsanwendungen greifen über Standard-JDBC-Aufrufe auf die Datenbank zu und nehmen auch die Aktualisierung der Datenbank über diese Aufrufe vor. Die Identitätsanwendungen stellen über eine JDBC-Datenquelle, die an den JNDI-Baum gebunden ist, eine Verbindung mit der Datenbank her.
- Es muss eine Datenquellendatei vorhanden sein, die auf die Datenbank verweist. Das Installationsprogramm für die Benutzeranwendung erstellt einen Datenquelleneintrag für Tomcat in `server.xml` und `context.xml`, der auf die Datenbank verweist.
- Vergewissern Sie sich, dass Ihnen die folgenden Informationen vorliegen:
  - Host und Port des Datenbankservers.
  - Name der zu erstellenden Datenbank. Die Standard-Datenbank für die Identitätsanwendungen ist `idmuserappdb`.
  - Benutzername und Passwort für die Datenbank. Der Datenbankbenutzername muss zu einem Administratorkonto gehören oder über ausreichende Rechte zum Erstellen von Tabellen auf dem Datenbankserver verfügen. Der standardmäßige Administrator für die Benutzeranwendung ist `idmadmin`.
  - Die Treiber-`.jar`-Datei für die zu verwendende Datenbank (beim Hersteller der Datenbank erhältlich). NetIQ unterstützt keine Treiber-JAR-Dateien von Drittanbietern.
- Die Datenbankinstanz kann sich auf dem lokalen Computer oder auf einem verbundenen Server befinden.
- Der Datenbank-Zeichensatz muss die Unicode-Kodierung nutzen. So ist beispielsweise UTF-8 ein Zeichensatz, der die Unicode-Kodierung verwendet, Latin-1 hingegen verwendet keine Unicode-Kodierung. Weitere Informationen zum Festlegen des Zeichensatzes finden Sie in „Konfigurieren des Zeichensatzes“, auf Seite 81 oder „Konfigurieren einer Oracle-Datenbank“, auf Seite 79.
- Bei der Sortierung muss zwischen Groß- und Kleinschreibung unterschieden werden, damit keine Fehler durch doppelte Schlüssel entstehen. Wenn ein Fehler durch doppelte Schlüssel auftritt, müssen Sie die Sortierung überprüfen und korrigieren. Installieren Sie anschließend die Identitätsanwendungen erneut.
- (Bedingt) Soll eine Datenbankinstanz sowohl für die Revision als auch für die Identitätsanwendungen herangezogen werden, empfiehlt NetIQ, die Datenbank auf einem separaten dedizierten Server zu installieren, also nicht auf dem Server, auf dem Tomcat gehostet wird, auf dem wiederum die Identitätsanwendungen ausgeführt werden.
- (Bedingt) Wenn Sie auf eine neue Version der Identitätsanwendungen migrieren, müssen Sie dieselbe Datenbank verwenden wie in der bisherigen Installation.
- Die Datenbankserver ermöglichen jeweils das Datenbank-Clustering. NetIQ führt 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. NetIQ bietet die nötigen Fachkenntnisse für die Analyse, Planung und Fehlersuche der NetIQ-Produkte. Der Kunde muss Fachkenntnisse für die Analyse, Planung und Fehlersuche von Drittanbieterprodukten erbringen. NetIQ bittet 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 NetIQ-Produkten getrennt werden können.

Konfigurieren der Datenbank für die Identitätsanwendungen

Die Datenbank für die Identitätsanwendungen 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 den unterstützten Datenbanken finden Sie in „Systemanforderungen für die Identitätsanforderungen“, auf Seite 83. Weitere Informationen zu den Überlegungen für die Benutzeranwendungsdatenbank finden Sie in „Voraussetzungen für die Installation der Datenbank für die Identitätsanwendungen“, auf Seite 78.

- „Konfigurieren einer Oracle-Datenbank“, auf Seite 79
- „Konfigurieren einer SQL Server-Datenbank“, auf Seite 80

Konfigurieren einer Oracle-Datenbank

In diesem Abschnitt finden Sie die Konfigurationsoptionen zur Verwendung einer Oracle-Datenbank für die Benutzeranwendung. Weitere Informationen zu den unterstützten Oracle-Versionen finden Sie in „Systemanforderungen für die Identitätsanforderungen“, auf Seite 83.

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 die Identitätsanwendungen 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: 12.1.0.2

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
```

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. Weitere Informationen zu den unterstützten SQL Server-Versionen finden Sie in „Systemanforderungen für die Identitätsanforderungen“, auf Seite 83.

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.

Konfigurieren des Admin-Benutzerkontos

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

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

HINWEIS: Die JDBC-JAR-Version `sqljdbc42.jar` wird empfohlen.

Voraussetzungen für die Installation der Identitätsanwendungen in einer Cluster-Umgebung

Wenn die Datenbank für die Identitätsanwendungen 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 Identitätsanwendungen angeben.
  - Für jedes Mitglied des Clusters müssen Sie denselben Hostnamen oder dieselbe IP-Adresse für den Server angeben, auf dem die Datenbank der Identitätsanwendungen 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.
- NetIQ rät 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.

Vorbereiten eines Clusters für die Identitätsanwendungen

Die Identitätsanwendungen 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 die Identitätsanwendung in einem Cluster installieren, bereiten Sie die Umgebung vor.

- „Erläuterungen zu Clustergruppen in Tomcat-Umgebungen“, auf Seite 82
- „Festlegen der Systemeigenschaften für Workflow-Engine-IDs“, auf Seite 82
- „Verwenden eines einzigen Master-Schlüssels für alle Benutzeranwendungen im Cluster“, auf Seite 83

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.

Weitere Informationen zu den Voraussetzungen für die Installation in einer Cluster-Umgebung finden Sie in Abschnitt 8.5.2, „Voraussetzungen und Überlegungen für die Installation der Identitätsanwendungen“, auf Seite 75.

Festlegen der Systemeigenschaften für Workflow-Engine-IDs

Auf jedem Server im Cluster, auf dem die Identitätsanwendungen 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 Identitätsanwendungen erfolgt.

Legen Sie die Systemeigenschaften für Tomcat fest, damit die Workflow-Engines ordnungsgemäß ausgeführt werden.

1. Erstellen Sie für jeden Identitätsanwendungsserver 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

Die Identitätsanwendungen verschlüsseln vertrauliche Daten mit einem Master-Schlüssel. Alle Identitätsanwendungen in einem Cluster müssen denselben Master-Schlüssel verwenden. In diesem Abschnitt wird beschrieben, wie Sie sicherstellen, dass alle Identitätsanwendungen in einem Cluster denselben Master-Schlüssel verwenden.

Weitere Informationen zum Verschlüsseln vertraulicher Daten in den Identitätsanwendungen finden Sie unter Verschlüsseln vertraulicher Identitätsanwendungsdaten im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

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 die Identitätsanwendungen enthält. Standardmäßig befindet sich diese Datei im Installationsverzeichnis.
3. Installieren Sie die Identitätsanwendungen 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.

8.5.3 Systemanforderungen für die Identitätsanforderungen

In diesem Abschnitt finden Sie die Mindestanforderungen für die Server, auf denen die Identitätsanwendungen und das unterstützende Rahmenwerk (z. B. PostgreSQL, Tomcat, OSP und SSPR) installiert werden sollen.

Kategorie	Anforderung
Prozessor	1 GHz
Festplattenspeicher	1 GB **HINWEIS:** Ausreichend Speicherplatz für den Inhalt unterstützender Anwendungen, z. B. Datenbank und Anwendungsserverprotokolle.
Arbeitsspeicher	Mindestens 512 MB (empfohlen 4 GB)
Betriebssystem (zertifiziert)	Eines der folgenden 64-Bit-Betriebssysteme: ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3 NetIQ empfiehlt, vor der Installation von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden. **HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird.

Kategorie	Anforderung
Betriebssysteme (unterstützt)	Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme **HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert..
Virtualisierungssystem	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.5 und höher NetIQ unterstützt Identity Manager auf Enterprise-Virtualisierungssystemen, die die Betriebssysteme, unter denen die NetIQ-Produkte ausgeführt werden können, offiziell unterstützen. Sofern die Anbieter der Virtualisierungssysteme diese Betriebssysteme offiziell unterstützen, unterstützt NetIQ den gesamten Identity Manager-Stack auf diesen Systemen.
Datenbank	◆ PostgreSQL 9.6.6 ◆ Oracle 12c ◆ MsSQL 2016 **HINWEIS:** Tragen Sie keine PostgreSQL-Versionen (z. B. 9.6.6) in den Tomcat-Klassenpfad ein. Wenn diese Versionen angegeben sind, werden die Bilder auf der Startseite unter Umständen nicht geladen.
Anwendungsserver	Apache Tomcat 8.5.27
Java	Java Development Kit (JDK) Alternativ: Java-Laufzeitumgebung (JRE) Version 1.8.0_162 (oder höher) von Sun (Oracle)
Anschluss	8180
Webbrowser	Einer der folgenden Browser (ggf. höhere Version): ◆ Apple Safari 9 ◆ Google Chrome 61 (oder höher) ◆ Microsoft Edge 20.10240.17146.0 ◆ Microsoft Internet Explorer 11.0.10240.17443 **HINWEIS:** Die Option „Kompatibilitätsansicht“ wird in Internet Explorer nicht unterstützt. ◆ Mozilla Firefox 51 oder höher **HINWEIS:** Es müssen Cookies im Browser aktiviert sein. Wenn Cookies deaktiviert sind, ist das Produkt nicht funktionsfähig.
Revision	Plattformagent 2011.1r6 (oder höher)
Verzeichnisservices	NetIQ eDirectory 9.1

8.6 Planen der Installation der Identitätsberichterstellung

In diesem Abschnitt finden Sie Anweisungen zum Vorbereiten der Installation der Komponenten für die Identitätsberichterstellung. Sentinel wird zum Prüfen von Ereignissen verwendet.

8.6.1 Checkliste für die Installation der Identitätsberichterstellung

NetIQ empfiehlt, die Schritte in der folgenden Checkliste auszuführen:

	Checkliste
❑	1. Informieren Sie sich über die Interaktion zwischen den Identity Manager-Komponenten. Weitere Informationen finden Sie in Abschnitt 3.3.4, „Identitätsberichterstellung“, auf Seite 23.
❑	2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.7, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 39.
❑	3. Lesen Sie die Überlegungen zur Installation der Identitätsberichterstellung. Weitere Informationen finden Sie in Abschnitt 8.6.2, „Voraussetzungen für die Installation der Komponenten für die Identitätsberichterstellung“, auf Seite 86.
❑	4. Prüfen Sie die Hardware- und Software-Voraussetzungen der Computer, auf denen die Identitätsberichterstellung gehostet werden soll. Weitere Informationen finden Sie in Abschnitt 8.6.4, „Systemanforderungen für die Identitätsberichterstellung“, auf Seite 88.
❑	5. (Bedingt) Stellen Sie bei Computern mit RHEL 7.3-Betriebssystem (oder höher) sicher, dass die erforderlichen Bibliotheken installiert sind.
❑	6. (Bedingt) Stellen Sie sicher, dass die Identitätsanwendungen installiert sind. Dieser Schritt ist erforderlich, wenn Sie die Advanced Edition installiert haben. Weitere Informationen finden Sie in Kapitel 8, „Planen der Installation der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting“, auf Seite 61.
❑	7. Installieren Sie Sentinel. Weitere Informationen finden Sie in Abschnitt 7, „Installieren von SLM für IGA“, auf Seite 55
❑	8. Installieren Sie die Identitätsberichterstellung. Beachten Sie einen der folgenden Abschnitte: ◆ Abschnitt 9.1.1, „Durchführen einer interaktiven Installation“, auf Seite 91 ◆ Abschnitt 9.1.2, „Ausführen einer unbeaufsichtigten Installation der Identity Manager-Engine“, auf Seite 92
❑	9. Richten Sie die Identitätsberichterstellung vollständig ein. Weitere Informationen finden Sie in Kapitel 11.10, „Konfigurieren der Identitätsberichterstellung“, auf Seite 176.
❑	10. Konfigurieren Sie die Umgebung für die Treiber. Weitere Informationen finden Sie in Abschnitt 11.9, „Konfigurieren der Laufzeitumgebung“, auf Seite 167.

8.6.2 Voraussetzungen für die Installation der Komponenten für die Identitätsberichterstellung

NetIQ empfiehlt, die nachfolgenden Informationen zu lesen, bevor Sie mit dem Installationsvorgang beginnen.

- „Voraussetzungen für die Identitätsberichterstellung“, auf Seite 86
- „Ermitteln von Revisionsereignissen für die Identitätsberichterstellung“, auf Seite 86

Voraussetzungen für die Identitätsberichterstellung

Beachten Sie beim Installieren der Identitätsberichterstellung die folgenden Voraussetzungen und Überlegungen:

- Es ist eine unterstützte und konfigurierte Version der folgenden Identity Manager-Komponenten erforderlich:
  - Identitätsanwendungen (auch Benutzeranwendungstreiber) (nur für Advanced Edition)
  - Sentinel ist auf einem separaten Linux-Computer installiert.
- Installieren Sie die Identitätsberichterstellung nicht auf einem Server in einer Cluster-Umgebung.
- Sollen Berichte über eine Oracle-Datenbank ausgeführt werden, muss die Datei `ojdbc8.jar` kopiert werden. Weitere Informationen finden Sie unter Abschnitt 11.10.2, „Ausführen von Berichten über eine Oracle-Datenbank“, auf Seite 176.
- Weisen Sie den Benutzern, die auf die Berichterstellungsfunktionen zugreifen sollen, die Berichtsadministratorrolle zu.
- Prüfen Sie, ob alle Server in der Identity Manager-Umgebung auf dieselbe Uhrzeit eingestellt sind. Wenn Sie die Uhrzeit auf den Servern nicht synchronisieren, sind einige Berichte unter Umständen nach dem Ausführen leer. Dieses Problem kann sich beispielsweise auf Daten zu neuen Benutzern auswirken, wenn die Server, auf denen die Identity Manager-Engine und das Warehouse gehostet werden, unterschiedliche Zeitstempel aufweisen. Wenn Sie einen Benutzer erstellen und dann bearbeiten, werden Daten in die Berichte eingetragen.
- Der Installationsvorgang bearbeitet den Eintrag `JAVA_OPTs` oder `CATALINA_OPTS` für die JRE-Zuordnung in der Datei `setenv.sh` für Tomcat.

Ermitteln von Revisionsereignissen für die Identitätsberichterstellung

In diesem Abschnitt erfahren Sie, wie Sie Revisionsereignisse ermitteln, die für Identity Manager-Berichte und für benutzerdefinierte Berichte erforderlich sind. Sie können alle Berichtquellen dekomprimieren und mit dem folgenden Skript die Revisionsereignisse ermitteln:

```
find . -name *.jrxml -print0 |xargs -0 grep -H "'000[B3]" | perl -ne '($file) = /
^\.\/(.*?)\//;@a = /000[3B]..../g; foreach $a (@a) { print "$file;$a\n"}' |sort -u
```

Im nachfolgenden Abschnitt erfahren Sie, wie Sie verschiedene Revisionsereignisse für Identity Manager-Berichte und für benutzerdefinierte Berichte ermitteln und auswählen:

Ereignisname	Revisions-Flag
Authentifizierung und Passwortänderung	**Auswahl des Revisions-Flags über SSPR:** Starten Sie den **SSPR-Konfigurations-Editor**, wählen Sie **Revisionskonfiguration** und wählen Sie unter den folgenden Revisions-Flags: ◆ Authenticate ◆ Passwort ändern ◆ Passwort entsperren ◆ Passwort wiederherstellen ◆ Unbefugter Zugriffsversuch ◆ Sperre gegen unbefugten Zugriff ◆ Benutzer mit Sperre gegen unbefugten Zugriff **Auswahl des Revisions-Flags über iManager:** Wählen Sie in iManager die Option **Rollen und Aufgaben** > **eDirectory-Revision** > **Revisionskonfiguration** > **Novell Auditing** und wählen Sie unter den folgenden Revisions-Flags: ◆ Passwort ändern ◆ Passwort bestätigen ◆ Anmelden ◆ Abmelden
Alle anderen Berichterstellungsereignisse	Wählen Sie in der **NetIQ Identity Manager-Benutzeranwendung** die Option **Administration** > **Protokollierung** > **Auditdienst aktivieren**

8.6.3 Erläuterungen zum Installationsvorgang für die Komponenten der Identitätsberichterstellung

NetIQ empfiehlt, Sentinel und die Berichterstellung auf separaten Servern zu installieren.

Bei einer Neuinstallation erstellt das Installationsprogramm verschiedene Tabellen in der Datenbank und die Verbindungen werden geprüft. Außerdem wird eine JAR-Datei für den PostgreSQL-JDBC-Treiber installiert, die dann automatisch für die Verbindungen zur Datenbank herangezogen wird.

Wenn Sie Ihre Daten (z. B. SIEM) von EAS zur PostgreSQL-Datenbank migriert haben, stellt das Installationsprogramm eine Verbindung zur bestehenden Datenbank her.

Der Installationsvorgang für die Identitätsberichterstellung führt folgende Funktionen aus:

- Konfigurieren der Authentifizierungsdienste für die Identitätsberichterstellung
- Konfigurieren des Email-Zustellungssystems für die Identitätsberichterstellung
- Konfigurieren der Kernberichterstellungsdienste für die Identitätsberichterstellung
- Bereitstellen der erforderlichen Treiber (Managed System Gateway und Data Collection Services) für die Ausführung von Identity Reporting.
- Konfigurieren der PostgreSQL-Datenbank für Identity Reporting.

8.6.4 Systemanforderungen für die Identitätsberichterstellung

In diesem Abschnitt finden Sie die Mindestanforderungen für die Server, auf denen die Identitätsberichterstellung installiert werden soll.

Überprüfen Sie außerdem die Voraussetzungen und Überlegungen zur Installation, insbesondere im Zusammenhang mit dem Betriebssystem.

Kategorie	Anforderung
Prozessor	1 GHz
Festplattenspeicher	1 GB **HINWEIS:** Ausreichend Speicherplatz für den Inhalt unterstützender Anwendungen, z. B. Datenbank und Anwendungsserverprotokolle.
Arbeitsspeicher	Mindestens 512 MB (empfohlen 4 GB)
Betriebssystem (zertifiziert)	Eines der folgenden 64-Bit-Betriebssysteme: ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3 NetIQ empfiehlt, vor der Installation von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden. **HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird.
Betriebssysteme (unterstützt)	Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme **HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert..
Virtualisierungssystem	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.5 und höher NetIQ unterstützt Identity Manager auf Enterprise-Virtualisierungssystemen, die die Betriebssysteme, unter denen die NetIQ-Produkte ausgeführt werden können, offiziell unterstützen. Sofern die Anbieter der Virtualisierungssysteme diese Betriebssysteme offiziell unterstützen, unterstützt NetIQ den gesamten Identity Manager-Stack auf diesen Systemen.
Datenbank	◆ PostgreSQL 9.6.6 ◆ Oracle 12.2.01
Anwendungsserver	Apache Tomcat 8.5.27
Java	Java Development Kit (JDK) Alternativ: Java-Laufzeitumgebung (JRE) Version 1.8.0_162 (oder höher) von Sun (Oracle)

Kategorie	Anforderung
Webbrowser	Einer der folgenden Browser (ggf. höhere Version): **Desktop** ◆ Apple Safari 9 ◆ Google Chrome 61 (oder höher) ◆ Microsoft Internet Explorer 11 ◆ Mozilla Firefox 51 oder höher **iPad** ◆ Apple Safari 9 ◆ Google Chrome 61 (oder höher) **HINWEIS:** Es müssen Cookies im Browser aktiviert sein. Wenn Cookies deaktiviert sind, ist das Produkt nicht funktionsfähig.
Revision	Sentinel Log Management für IGA

9 Installieren der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting

In diesem Abschnitt finden Sie die Schritte für die Installation der erforderlichen Komponenten für die Identity Manager-Engine, der Identitätsanwendungen und der Identity Reporting-Komponenten.

Sie können die Installation im interaktiven oder im unbeaufsichtigten Modus ausführen. Das Installationsprogramm bietet eine Option zum Erstellen einer Eigenschaftsdatei für die unbeaufsichtigte Installation. Sie können die Installationsoptionen für mehrere Komponenten in der Eigenschaftsdatei festhalten und dann die unbeaufsichtigte Installation mithilfe dieser Datei auf verschiedenen Servern in Ihrer Umgebung ausführen. Das Programm für die unbeaufsichtigte Installation übernimmt die Werte aus der Datei für die Installation.

Sie können die Identity Manager-Komponenten direkt nach der Installation konfigurieren oder auch zu einem späteren Zeitpunkt.

Das Installationsprogramm installiert die Komponente in vordefinierte Speicherorte (siehe Abschnitt 5.5, „Standardmäßige Speicherorte für die Installation“, auf Seite 37).

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie in Kapitel 8, „Planen der Installation der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting“, auf Seite 61.

9.1 Installieren der Identity Manager-Engine

Die Identity Manager-Engine kann wie folgt installiert werden:

9.1.1 Durchführen einer interaktiven Installation

1. Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` von der NetIQ Downloads-Website herunter.
2. Hängen Sie die heruntergeladene `.iso`-Datei ein.
3. Führen Sie im Stammverzeichnis der `.iso`-Datei den folgenden Befehl aus:

   ```
   ./install.sh
   ```
4. Lesen Sie die Lizenzvereinbarung.
5. Akzeptieren Sie die Lizenzvereinbarung mit `j`.
6. Entscheiden Sie, welche Edition des Identity Manager-Servers installiert werden soll. Geben Sie `j` für die Advanced Edition bzw. `n` für die Standard Edition ein.

7 Wählen Sie die Identity Manager-Engine aus und setzen Sie die Installation fort.

8 Konfigurieren Sie die installierten Komponenten. Weitere Informationen finden Sie unter Kapitel 10, „Konfigurieren der installierten Komponenten“, auf Seite 101.

9.1.2 Ausführen einer unbeaufsichtigten Installation der Identity Manager-Engine

1 Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` von der NetIQ Downloads-Website herunter.

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

3 Führen Sie im Stammverzeichnis der `.iso`-Datei den folgenden Befehl aus:

```
./create_silent_props.sh
```

4 Bestätigen Sie die Dateierstellung mit `j`.

5 Zum Installieren der JRE geben Sie `j` ein.

6 Zum Aufrüsten der vorhandenen Identity Manager-Komponenten geben Sie `j` ein.

7 Entscheiden Sie, welche Edition des Identity Manager-Servers installiert werden soll. Geben Sie `j` für die Advanced Edition bzw. `n` für die Standard Edition ein.

8 Wählen Sie einen Konfigurationsmodus für die Komponenten aus. Weitere Informationen finden Sie unter Kapitel 10, „Konfigurieren der installierten Komponenten“, auf Seite 101.

9 Geben Sie die zu installierenden Komponenten an.

10 Führen Sie eine unbeaufsichtigte Installation mit dem folgenden Befehl aus:

```
./install.sh -s -f <Speicherort der Eigenschaftsdatei für die unbeaufsichtigte Installation>
```

Beispiel:

`./install.sh -s -f /mnt/silent.properties`, wobei `/mnt/silent.properties` den Speicherort bezeichnet, an dem Sie die Eigenschaftsdatei für die unbeaufsichtigte Installation abgelegt haben.

9.1.3 Installieren der Identity Manager-Engine als Nicht-Root-Benutzer

Die Installation der Identity Manager-Engine als Nicht-`Root`-Benutzer erhöht die Sicherheit des Linux-Servers. Die Identity Manager-Engine kann nicht als Nicht-`Root`-Benutzer installiert werden, falls Sie das Identitätsdepot als `Root`-Benutzer installiert haben. Soll die Engine als Nicht-Root-Benutzer installiert werden, führen Sie die folgenden Schritte aus:

1. Prüfen Sie, ob NICI installiert ist. Weitere Informationen finden Sie unter „NICI installieren“, auf Seite 93.
2. Führen Sie eine Nicht-Root-Installation des Identitätsdepots aus. Weitere Informationen finden Sie unter „Ausführen einer Nicht-Root-Installation des Identitätsdepots“, auf Seite 93.
3. Führen Sie eine Nicht-Root-Installation der Identity Manager-Engine aus. Weitere Informationen finden Sie unter „Ausführen einer Nicht-Root-Installation der Engine“, auf Seite 95.

NICI installieren

Sie müssen NICI installieren, bevor Sie die Installation des Identitätsdepots fortsetzen können. Die erforderlichen NICI-Pakete werden systemweit genutzt. Es wird daher empfohlen, die nötigen Pakete als Root-Benutzer zu installieren. Bei Bedarf können Sie jedoch den Zugriff mit `sudo` an ein anderes Konto delegieren und die NICI-Pakete über dieses Konto installieren.

1. Navigieren Sie in der eingehängten `iso`-Datei zum Verzeichnis `/IDVault/setup/`.
2. Führen Sie den folgenden Befehl aus:

   ```
   rpm -ivh nici64-3.1.0-0.00.x86_64.rpm
   ```

3. Vergewissern Sie sich, dass NICI auf den Servermodus festgelegt ist. Geben Sie den folgenden Befehl ein:

   ```
   /var/opt/novell/nici/set_server_mode
   ```

   Dieser Schritt ist obligatorisch, um sicherzustellen, dass die Konfiguration des Identitätsdepots nicht fehlschlägt.

Ausführen einer Nicht-Root-Installation des Identitätsdepots

In diesem Abschnitt wird beschrieben, wie Sie das Identitätsdepot mit Tarball installieren. Beim Extrahieren der Datei erstellt das System die Verzeichnisse `etc`, `opt` und `var`.

1. Melden Sie sich als `sudo`-Benutzer mit den entsprechenden Rechten an dem Computer an, auf dem das Identitätsdepot installiert werden soll.

   HINWEIS: Wenn Sie einen benutzerdefinierten Installationspfad angeben möchten, können Sie sich auch als `Root`-Benutzer anmelden.

2. Navigieren Sie in der eingehängten `iso`-Datei zum Verzeichnis `/IDVault/`.
3. Erstellen Sie ein neues Verzeichnis und kopieren Sie die Datei `eDir_NonRoot.tar.gz` in dieses Verzeichnis. Beispiel: /home/user/install/eDirectory.
4. Extrahieren Sie die Datei mithilfe des folgenden Befehls:

   ```
   tar -zxvf eDir_NonRoot.tar.gz
   ```

5. (Bedingt) Sollen die Pfade für die Umgebungsvariablen manuell exportiert werden, geben Sie den folgenden Befehl ein:

   ```
   export LD_LIBRARY_PATH=custom_location/eDirectory/opt/novell/eDirectory/
   lib64:custom_location/eDirectory/opt/novell/eDirectory/lib64/ndsmodules:
   custom_location/eDirectory/opt/novell/lib64:$LD_LIBRARY_PATH

   export PATH=custom_location/eDirectory/opt/novell/eDirectory/
   bin:custom_location/eDirectory/opt/novell/eDirectory/sbin:/opt/novell/
   eDirectory/bin:$PATH

   export MANPATH=custom_location/eDirectory/opt/novell/man:custom_location/
   eDirectory/opt/novell/eDirectory/man:$MANPATH

   export TEXTDOMAINDIR=custom_location/eDirectory/opt/novell/eDirectory/
   share/locale:$TEXTDOMAINDIR
   ```

6 (Bedingt) Wenn die Pfade der Umgebungsvariablen mit dem ndspath-Skript exportiert werden sollen, müssen Sie dem Dienstprogramm das ndspath-Skript voranstellen. Führen Sie die folgenden Schritte durch:

6a Führen Sie das Dienstprogramm im Verzeichnis `Benutzerdefinierter_Speicherort/eDirectory/opt` mit dem folgenden Befehl aus:

```
custom_location/eDirectory/opt/novell/eDirectory/bin/ndspath
utility_name_with_parameters
```

6b Exportieren Sie die Pfade in der aktuellen Shell mit dem folgenden Befehl:

```
. custom_location/eDirectory/opt/novell/eDirectory/bin/ndspath
```

6c Führen Sie die Dienstprogramme wie gewohnt aus.

6d Hängen Sie die Anweisungen zum Exportieren des Pfads an das Ende des Skripts `/etc/profile`, `~/bashrc` oder eines ähnlichen Skripts an.

Mit diesem Schritt können Sie die Dienstprogramme direkt starten, sobald Sie sich anmelden oder eine neue Shell öffnen.

7 Konfigurieren Sie das Identitätsdepot mit einem der folgenden Schritte:

7a Geben Sie zum Starten des ndsconfig-Dienstprogramms den folgenden Text in die Befehlszeile ein:

```
ndsconfig new [-t treename] [-n server_context] [-a admin_FDN] [-w
admin password] [-i] [-S server_name] [-d path_for_dib] [-m module] [e] [-L
ldap_port] [-l SSL_port] [-o http_port] -O https_port] [-p IP
address:[port]] [-c] [-b port_to_bind] [-B interface1@port1,
interface2@port2,..] [-D custom_location] [--config-file
configuration_file]
```

Beispiel:

```
ndsconfig new -t mary-tree -n novell -a admin.novell -S linux1 -d /home/
mary/inst1/data -b 1025 -L 1026 -l 1027 -o 1028 -O 1029 -D /home/mary/
inst1/var --config-file /home/mary/inst1/nds.conf
```

HINWEIS

- Sie müssen eine Portnummer zwischen 1024 und 65535 angeben. Der Standardport 524 darf nicht für eDirectory-Anwendungen verwendet werden.

  Diese Einschränkung der Portnummer kann sich negativ auf die folgenden Anwendungstypen auswirken:

  - Anwendungen, die keine Option zum Festlegen des Zielserverports bieten.
  - Ältere Anwendungen, die NCP nutzen und als Root für 524 ausgeführt werden.
- Mit den Optionen `-B` und `-P` können Sie IPv6-Adressen angeben. Die IPv6-Adressen müssen dabei in eckigen Klammern `[ ]` gesetzt werden. Beispiel: `-B [2015::4]@636`.

7b Mit dem ndsmanage-Dienstprogramm konfigurieren Sie eine neue Instanz. Weitere Informationen finden Sie in „Erstellen einer neuen Instanz im Identitätsdepot“, auf Seite 117.

Ausführen einer Nicht-Root-Installation der Engine

Mit dieser Methode können Sie die folgenden Komponenten nicht installieren:

- **Remote Loader:** Soll der Remote Loader von einem Nicht-Root-Benutzer installiert werden, verwenden Sie den Java Remote Loader. Weitere Informationen finden Sie unter „Installieren des Java Remote Loader“, auf Seite 96.
- **Linux-Kontentreiber:** Erfordert `Root`-Berechtigungen.

HINWEIS: Wenn Sie die Identity Manager-Engine als Nicht-Root-Benutzer installieren, befinden sich die Installationsdateien im Verzeichnis des Nicht-Root-Benutzers. Beispiel: `/home/user`, wobei „user“ ein Nicht-Root-Benutzer ist. Die Installationsdateien sind nicht zur Ausführung von Identity Manager erforderlich. Es ist möglich, die Dateien nach der Installation zu löschen.

So installieren Sie die Identity Manager-Engine als Nicht-Root-Benutzer:

1. Melden Sie sich als der Nicht-Root-Benutzer an, mit dem Sie das Identitätsdepot installiert haben.

   Das Benutzerkonto muss über Schreibzugriff für die Verzeichnisse und Dateien der Nicht-Root-Installation des Identitätsdepots verfügen.
2. Navigieren Sie zu dem Speicherort, an dem Sie die Datei `Identity_Manager_4.7_Linux.iso` eingehängt haben.
3. Navigieren Sie im Einhänge-Speicherort zum Verzeichnis `/IDM`.
4. Führen Sie den folgenden Befehl aus:

   ```
   ./idm-nonroot-install.sh
   ```
5. Mithilfe der folgenden Informationen wird die Installation ausgeführt:

   Basisverzeichnis für die Nicht-Root-Installation von eDirectory

   Geben Sie das Verzeichnis an, in dem die Nicht-`Root`-Version von eDirectory installiert ist. Beispiel: `/home/user/install/eDirectory`.

   NDS-Schema erweitern

   Wenn dies der erste Identity Manager-Server ist, der in dieser eDirectory-Instanz installiert wird, geben Sie zum Erweitern des Schemas `Y` ein. Wenn das Schema nicht erweitert ist, funktioniert Identity Manager nicht.

   Sie werden aufgefordert, das Schema für jede eDirectory-Instanz zu erweitern, die dem Nicht-`Root`-Benutzer gehören, der von der Nicht-`Root`-Installation von eDirectory gehostet wird.

   Wenn Sie die Schemaerweiterung auswählen, geben Sie den vollständigen eindeutigen Namen (Distinguished Name, DN) des eDirectory-Benutzers an, der über Berechtigungen zum Erweitern des Schemas verfügt. Der Benutzer kann das Schema nur erweitern, wenn er über Supervisor-Berechtigungen für die gesamte Baumstruktur verfügt. Weitere Informationen zur Erweiterung des Schemas als Nicht-`Root`-Benutzer finden Sie in der Datei `schema.log`, die im `data`-Verzeichnis jeder eDirectory-Instanz gespeichert ist.

   Führen Sie das Programm `/opt/novell/eDirectory/bin/idm-install-schema` aus, um das Schema nach abgeschlossener Installation auf weiteren eDirectory-Instanzen zu installieren.
6. Fahren Sie zum Abschließen des Installationsvorgangs mit Abschnitt 11.1, „Durchführen einer Nicht-Root-Installation“, auf Seite 109 fort.

7 Aktivieren Sie Identity Manager. Weitere Informationen finden Sie in Kapitel 24, „Aktivieren von Identity Manager“, auf Seite 245.

8 Anweisungen zum Erstellen und Konfigurieren der Treiberobjekte finden Sie im jeweiligen Handbuch für die einzelnen Treiber. Weitere Informationen finden Sie auf der Website der Identity Manager-Treiberdokumentation.

9.2 Installieren des Java Remote Loader

Im Allgemeinen installieren Sie den Java Remote Loader (`dirxml_jremote`) auf Rechnern, deren Betriebssystem mit dem nativen Remote Loader nicht kompatibel ist. Der Java Remote Loader wird jedoch auch auf denselben Servern ausgeführt, auf denen Sie auch den nativen Remote Loader installieren. 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 `dirxml_jremote` auf einem beliebigen unterstützten Linux-Rechner mit einer öffentlich unterstützten Version von Java.

1 Kopieren Sie die `ISO`- oder `JAR`-Dateien für das Anwendungsschnittstellenmodul (standardmäßig im Verzeichnis `/opt/novell/eDirectory/lib/dirxml/classes`) auf den Server, auf dem die Identity Manager-Engine gehostet wird.

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 Greifen Sie mit einem der folgenden Schritte auf das Installationsprogramm zu:

   4a (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die Installationsdateien für den Java Remote Loader befinden (standardmäßig unter `products/IDM/java_remoteloader`).

   4b (Bedingt) Wenn Sie die Installationsdateien für den Java Remote Loader von der NetIQ Downloads-Website heruntergeladen haben, führen Sie die folgenden Schritte aus:

      4b1 Navigieren Sie zur `.tgz`-Datei für das heruntergeladene Image.

      4b2 Extrahieren Sie den Inhalt der Datei in einen Ordner auf dem lokalen Computer.

5 Kopieren Sie die Datei `dirxml_jremote_dev.tar.gz` an den gewünschten Speicherort auf dem Zielcomputer. Kopieren Sie die Datei beispielsweise in das Verzeichnis `/usr/idm`.

6 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`.

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

   Geben Sie beispielsweise `gunzip dirxml_jremote.tar.gz` oder `tar -xvf dirxml_jremote_dev.tar` ein.

8 Legen Sie die `.iso`- oder `.jar`-Dateien für das Anwendungsschnittstellenmodul, die Sie in Schritt 1 kopiert haben, im Verzeichnis `dirxml/classes` unter dem Verzeichnis `lib` ab.

9 Soll das Skript `dirxml_jremote` so angepasst werden, dass der Zugriff auf die ausführbare Java-Datei über die Umgebungsvariable `RDXML_PATH` möglich ist, führen Sie einen der folgenden Schritte aus:

   9a Legen Sie die Umgebungsvariable `RDXML_PATH` mit einem der folgenden Befehle fest:

      - `set RDXML_PATH=path`
      - `export RDXML_PATH`

   9b Bearbeiten Sie das `dirxml_jremote`-Skript und fügen Sie den Pfad der Java-Programmdatei am Anfang der Skriptzeile ein, die Java ausführt.

10 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`.

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

   Die Beispieldatei befindet sich standardmäßig im Verzeichnis `/opt/novell/dirxml/doc/`. Weitere Informationen finden Sie in Kapitel 11.3, „Konfigurieren des Remote Loader und der Treiber“, auf Seite 118.

9.3 Installieren von Identitätsanwendungen

Die Identitätsanwendungen können wie folgt installiert werden:

9.3.1 Durchführen einer interaktiven Installation

1 Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` von der NetIQ Downloads-Website herunter.

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

3 Führen Sie im Stammverzeichnis der `.iso`-Datei den folgenden Befehl aus:

```
./install.sh
```

4 Lesen Sie die Lizenzvereinbarung.

5 Akzeptieren Sie die Lizenzvereinbarung mit `j`.

6 Entscheiden Sie, welche Edition des Identity Manager-Servers installiert werden soll. Geben Sie `j` für die Advanced Edition bzw. `n` für die Standard Edition ein.

7 Wählen Sie die Identitätsanwendungen aus und setzen Sie die Installation fort.

8 Konfigurieren Sie die installierten Komponenten. Weitere Informationen finden Sie unter Kapitel 10, „Konfigurieren der installierten Komponenten“, auf Seite 101.

9.3.2 Ausführen einer automatischen Installation

1. Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` von der NetIQ Downloads-Website herunter.
2. Hängen Sie die heruntergeladene `.iso`-Datei ein.
3. Führen Sie im Stammverzeichnis der `.iso`-Datei den folgenden Befehl aus:

   ```
   ./create_silent_props.sh
   ```

4. Bestätigen Sie die Dateierstellung mit `j`.
5. Zum Installieren der JRE geben Sie `j` ein.
6. Entscheiden Sie, welche Edition des Identity Manager-Servers installiert werden soll. Geben Sie `j` für die Advanced Edition bzw. `n` für die Standard Edition ein.
7. Wählen Sie einen Konfigurationsmodus für die Komponenten aus. Weitere Informationen finden Sie unter Kapitel 10, „Konfigurieren der installierten Komponenten“, auf Seite 101.
8. Wählen Sie die Identitätsanwendungen aus und setzen Sie die Installation fort.
9. Führen Sie eine unbeaufsichtigte Installation mit dem folgenden Befehl aus:

   ```
   ./install.sh -s -f <Speicherort der Eigenschaftsdatei für die unbeaufsichtigte Installation>
   ```

   Beispiel:

   `./install.sh -s -f /mnt/silent.properties`, wobei `/mnt/silent.properties` den Speicherort bezeichnet, an dem Sie die Eigenschaftsdatei für die unbeaufsichtigte Installation abgelegt haben.

9.3.3 Durchführen einer interaktiven Installation von SSPR

Sollen die Identitätsanwendungen und SSPR in einer verteilten Umgebung installiert werden, bietet das Installationsprogramm eine Option, mit der Sie SSPR separat installieren.

1. Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` von der NetIQ Downloads-Website herunter.
2. Hängen Sie die heruntergeladene `.iso`-Datei ein.
3. Navigieren Sie im Stammverzeichnis der `.iso`-Datei zum Verzeichnis `SSPR`.
4. Führen Sie den folgenden Befehl aus:

   ```
   ./install.sh
   ```

5. Lesen Sie die Lizenzvereinbarung.
6. Akzeptieren Sie die Lizenzvereinbarung mit `j`.
7. Konfigurieren Sie die installierten Komponenten. Weitere Informationen finden Sie unter Kapitel 10, „Konfigurieren der installierten Komponenten“, auf Seite 101.

9.3.4 Durchführen einer unbeaufsichtigten Installation von SSPR

1. Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` von der NetIQ Downloads-Website herunter.
2. Hängen Sie die heruntergeladene `.iso`-Datei ein.
3. Navigieren Sie im Stammverzeichnis der `.iso`-Datei zum Verzeichnis `SSPR`.

4 Führen Sie den folgenden Befehl aus:

```
./install.sh -s sspr_silentinstall.properties
```

9.4 Installieren der Identitätsberichterstellung

Identity Reporting kann wie folgt installiert werden:

- Abschnitt 9.4.1, „Durchführen einer interaktiven Installation“, auf Seite 99
- Abschnitt 9.4.2, „Ausführen einer automatischen Installation“, auf Seite 99

9.4.1 Durchführen einer interaktiven Installation

1 Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` von der NetIQ Downloads-Website herunter.

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

3 Führen Sie im Stammverzeichnis der `.iso`-Datei den folgenden Befehl aus:

```
./install.sh
```

4 Lesen Sie die Lizenzvereinbarung.

5 Akzeptieren Sie die Lizenzvereinbarung mit `j`.

6 Entscheiden Sie, welche Edition des Identity Manager-Servers installiert werden soll. Geben Sie `j` für die Advanced Edition bzw. `n` für die Standard Edition ein.

7 Wählen Sie Identity Reporting aus und setzen Sie die Installation fort.

8 Konfigurieren Sie die installierten Komponenten. Weitere Informationen finden Sie unter Kapitel 10, „Konfigurieren der installierten Komponenten“, auf Seite 101.

9.4.2 Ausführen einer automatischen Installation

1 Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` von der NetIQ Downloads-Website herunter.

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

3 Führen Sie im Stammverzeichnis der `.iso`-Datei den folgenden Befehl aus:

```
./create_silent_props.sh
```

4 Bestätigen Sie die Dateierstellung mit `j`.

5 Zum Installieren der JRE geben Sie `j` ein.

6 Entscheiden Sie, welche Edition des Identity Manager-Servers installiert werden soll. Geben Sie `j` für die Advanced Edition bzw. `n` für die Standard Edition ein.

7 Wählen Sie einen Konfigurationsmodus für die Komponenten aus. Weitere Informationen finden Sie unter Kapitel 10, „Konfigurieren der installierten Komponenten“, auf Seite 101.

8 Wählen Sie Identity Reporting aus und setzen Sie die Installation fort.

9 Führen Sie eine unbeaufsichtigte Installation mit dem folgenden Befehl aus:

```
./install.sh -s -f <Speicherort der Eigenschaftsdatei für die unbeaufsichtigte Installation>
```

Beispiel:

`./install.sh -s -f /mnt/silent.properties`, wobei `/mnt/silent.properties` den Speicherort bezeichnet, an dem Sie die Eigenschaftsdatei für die unbeaufsichtigte Installation abgelegt haben.

10 Konfigurieren der installierten Komponenten

In diesem Abschnitt finden Sie die Schritte zum Konfigurieren der Identity Manager-Komponenten, die Sie in Kapitel 9, „Installieren der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting“, auf Seite 91 installiert haben. Sie können die Konfiguration im interaktiven Modus (Konsolenmodus) oder im unbeaufsichtigten Modus ausführen.

Informieren Sie sich vor Beginn des Konfigurationsvorgangs über die Konfigurationsoptionen der einzelnen Komponenten. Weitere Informationen finden Sie unter Abschnitt 10.1, „Erläuterungen zu den Konfigurationsparametern“, auf Seite 101.

10.1 Erläuterungen zu den Konfigurationsparametern

In diesem Abschnitt werden die Parameter definiert, die zur Konfiguration der Identity Manager-Installation erforderlich sind. Sie können im Installationsprogramm angeben, dass die Komponenten direkt nach ihrer Installation oder auch erst zu einem späteren Zeitpunkt konfiguriert werden.

HINWEIS

- Wenn Sie die Identitätsanwendungen und Identity Reporting im typischen Konfigurationsmodus konfigurieren, können Sie keine Verbindung zu einer Datenbank herstellen, die auf einem anderen Computer installiert ist.
- Der Installationsvorgang bietet Ihnen nicht die Möglichkeit, die Revision zu aktivieren. Sie müssen sie separat für die Identity Manager-Komponenten aktivieren. Weitere Informationen finden Sie unter NetIQ Identity Manager – Configuring Auditing in Identity Manager (NetIQ Identity Manager – Konfigurieren der Revision in Identity Manager).

Parameter für typische Konfiguration	
Identity Manager-Engine	
Allgemeines Passwort	Gibt an, ob ein allgemeines Passwort festgelegt werden soll.
Name des Identitätsdepot-Administrators	Gibt den relativen eindeutigen Namen (RDN) des Administratorobjekts im Baum an, das über vollständige Rechte verfügt (zumindest für den Kontext, dem dieser Server hinzugefügt werden soll).
Identitätsanwendungen	
Allgemeines Passwort	Gibt an, ob ein allgemeines Passwort festgelegt werden soll.
Name des Identitätsdepot-Administrators	Gibt den relativen eindeutigen Namen (RDN) des Administratorobjekts im Baum an, das über vollständige Rechte verfügt (zumindest für den Kontext, dem dieser Server hinzugefügt werden soll).
Hostname (FQDN in Kleinbuchstaben)	Gibt den vollständig qualifizierten eindeutigen Namen oder die standardmäßige IP-Adresse des Servers an.

Parameter für typische Konfiguration	
DNS/IP-Adresse des Anwendungsservers	Gibt die IP-Adresse des Tomcat-Servers an.
Name des Identitätsanwendungs-Administrators	Gibt den Namen des Administratorkontos für die Identitätsanwendungen an.
Identitätsberichterstellung	
Allgemeines Passwort	Gibt an, ob ein allgemeines Passwort festgelegt werden soll.
Name des Identitätsdepot-Administrators	Gibt den relativen eindeutigen Namen (RDN) des Administratorobjekts im Baum an, das über vollständige Rechte verfügt (zumindest für den Kontext, dem dieser Server hinzugefügt werden soll).
Hostname (FQDN in Kleinbuchstaben)	Gibt den vollständig qualifizierten eindeutigen Namen oder die standardmäßige IP-Adresse des Servers an.
Mit externem One SSO-Server verbinden	Gibt an, ob eine Verbindung zu einem anderen One SSO-Server hergestellt werden soll.
DNS/IP-Adresse des Anwendungsservers	Gibt die IP-Adresse des Tomcat-Servers an.
DNS/IP-Adresse des One SSO-Servers	Gibt die IP-Adresse des Servers an, auf dem der Single-Sign-On-Dienst installiert ist.
Name des Identity Reporting-Administrators	Gibt den Namen des Administrators für Identity Reporting an. Der Standardwert lautet `cn=uaadmin,ou=sa,o=data`.

Parameter für benutzerdefinierte Konfiguration	
Identity Manager-Engine	
Name des Identitätsdepotbaums	Gibt einen neuen Baum für das Identitätsdepot an. Der Baumname muss den folgenden Anforderungen entsprechen: ◆ Der Baumname muss im Netzwerk eindeutig sein. ◆ Der Baumname muss 2 bis 32 Zeichen lang sein. ◆ Der Baumname darf nur Buchstaben (A–Z), Ziffern (0–9), Bindestriche (-) und Unterstriche (_) enthalten.
Name des Identitätsdepot-Administrators	Gibt den relativen eindeutigen Namen (RDN) des Administratorobjekts im Baum an, das über vollständige Rechte verfügt (zumindest für den Kontext, dem dieser Server hinzugefügt werden soll).
Identitätsdepot-Administratorpasswort	Gibt das Passwort für das Administratorobjekt an. Beispiel: *Passwort*.
Speicherort des NDS-var-Ordners	Gibt den Pfad dieser Identitätsdepot-Instanz auf diesem Server an. Der Standardpfad ist `/var/opt/novell/eDirectory`.
NDS-Datenspeicherort	Gibt den Pfad im lokalen System an, in dem die DIB-Dateien (Directory Information Base) installiert werden sollen. Die DIB-Dateien sind die Identitätsdepot-Datenbankdateien. Der standardmäßige Speicherort lautet `/var/opt/novell/eDirectory/data/dib`.

Parameter für benutzerdefinierte Konfiguration	
NCP-Port	Gibt den NCP-Port (NetWare Core Protocol) an, über den das Identitätsdepot mit den Identity Manager-Komponenten kommuniziert. Der Standardwert ist `524`.
LDAP-Nicht-SSL-Port	Gibt den Port an, den das Identitätsdepot auf LDAP-Anforderungen im Klartext überwachen soll. Der Standardwert ist `389`.
LDAP-SSL-Port	Gibt den Port an, den das Identitätsdepot mit dem SSL-Protokoll (Secure Sockets Layer) auf LDAP-Anforderungen überwachen soll. Der Standardwert ist `636`.
Identitätsdepot-HTTP-Port	Gibt den Port an, an dem der HTTP-Stack im Klartext arbeitet. Der Standardwert ist `8028`.
Identitätsdepot-HTTPS-Port	Gibt den Port an, an dem der HTTP-Stack mit dem TLS/SSL-Protokoll arbeitet. Der Standardwert ist `8030`.
NDS-Konfigurationsdatei mit Pfad	Gibt den Speicherort der Konfigurationsdatei für das Identitätsdepot an. Der Standardwert lautet `/etc/opt/novell/eDirectory/conf/nds.conf`.
Name des Identitätsdepot-Treibersatzes	Gibt den Namen für ein neues Identity Manager-Treibersatzobjekt an.
Bereitstellungskontext für Identitätsdepot-Treibersatz	Gibt den LDAP-DN für den Container an, in dem das Treibersatzobjekt erstellt werden soll.
Identitätsanwendungen	
Hostname (FQDN in Kleinbuchstaben)	Gibt den vollständig qualifizierten eindeutigen Namen oder die standardmäßige IP-Adresse des Servers an. **HINWEIS:** Der FQDN muss in Kleinbuchstaben angegeben werden. Der Server, auf dem die Komponente gehostet wird, muss zudem für die Verwendung des FQDN in Kleinbuchstaben konfiguriert werden.
Hostname/IP-Adresse des Identitätsdepots	Gibt die IP-Adresse des Servers an, auf dem das Identitätsdepot installiert ist.
Name des Identitätsdepot-Administrators	Gibt den relativen eindeutigen Namen (RDN) des Administratorobjekts im Baum an, das über vollständige Rechte verfügt (zumindest für den Kontext, dem dieser Server hinzugefügt werden soll).
Identitätsdepot-Administratorpasswort	Gibt das Passwort für das Administratorobjekt an. Beispiel: *Passwort*.
DNS/IP-Adresse des Anwendungsservers	Gibt die IP-Adresse des Tomcat-Servers an.
Benutzerdefinierter Name für OSP-Anmeldebildschirm	Gibt den Namen an, der auf dem OSP-Anmeldebildschirm angezeigt werden soll.
SSPR-Konfigurationspasswort	*Gilt nur, wenn Sie für das gemeinsame Passwort die Option* **Nein** festgelegt haben. Gibt das Passwort für die Passwortverwaltung in den Identitätsanwendungen an.

Parameter für benutzerdefinierte Konfiguration	
Passwort für OAuth-Keystore	*Gilt nur, wenn Sie für das gemeinsame Passwort die Option* **Nein** festgelegt haben. Gibt das Passwort an, das zum Laden des neuen Keystores auf dem OAuth-Server erstellt werden soll.
Benutzersuchcontainer-DN	Gibt den Standardcontainer für alle Benutzerobjekte im Identitätsdepot an.
Adminsuchcontainer-DN	Gibt alle Datenobjekte für Identity Manager-Speicherorte in der Datenorganisation an. Die Administratoren sollen allen Benutzern den Zugriff auf diesen Container und alle Untercontainer ermöglichen.
Anwendungsserver-HTTPS-Port	Gibt den HTTPS-Port an, über den der Tomcat-Server mit den Client-Computern kommunizieren soll. Der Standardwert ist `8543`.
One–SSO-Server-SSL-Port	Gibt den Port an, auf dem der Single-Sign-On-Dienst zugreifen soll. Der Standardwert ist `8543`.
One–SSO-Dienstpasswort für Identitätsanwendungen	*Gilt nur, wenn Sie für das gemeinsame Passwort die Option* **Nein** festgelegt haben. Gibt das Passwort für den Single-Sign-On-Client in den Identitätsanwendungen an.
Name des Identitätsanwendungs-Administrators	Gibt den Namen des Administratorkontos für die Identitätsanwendungen an.
LDAP-Nicht-SSL-Port	Gibt den Port an, den das Identitätsdepot auf LDAP-Anforderungen im Klartext überwachen soll. Der Standardwert ist `389`.
Name des Identitätsdepot-Treibersatzes	Gibt den Namen des Treibersatzes für das Identitätsdepot an.
Bereitstellungskontext für Identitätsdepot-Treibersatz	Gibt den LDAP-DN für den Container an, in dem das Treibersatzobjekt erstellt werden soll.
Datenbankplattform	Gibt die erforderlichen Datenbanken für die Identitätsanwendungen an.
PostgreSQL auf aktuellem Server konfigurieren	Gib an, ob die PostgreSQL-Datenbank auf demselben Server konfiguriert werden soll.
Port der Identitätsanwendungs-Datenbank	Gibt den Datenbankport für die Identitätsanwendungen an.
Name der Identitätsanwendungs-Datenbank	Gibt den Namen der Datenbank an. Der Standardwert lautet `idmuserappdb`.
Benutzername für Identitätsanwendungs-Datenbank	Gibt den Benutzernamen des Administrators für die Datenbank der Identitätsanwendungen an.
JDBC-jar-Datei für Identitätsanwendungs-Datenbank	Gibt die JAR-Datei für die Datenbankplattform an.
Schema erstellen	Gibt an, ob das Datenbankschema im Rahmen des Installationsvorgangs erstellt werden soll. Verfügbare Optionen: **Jetzt**, **Start** und **Datei**.

Parameter für benutzerdefinierte Konfiguration	
Neue Datenbank erstellen oder vorhandene Datenbank aufrüsten/ migrieren	Gibt an, ob eine neue Datenbank erstellt oder eine vorhandene Datenbank aufgerüstet werden soll.
Benutzerdefinierten Container als Root-Container verwenden	Gibt an, ob ein benutzerdefinierter Container als Root-Container verwendet werden soll. Standardmäßig wird `o=data` durch das Installationsprogramm erstellt und als Benutzercontainer festgelegt, wobei diesem Computer die Passwortrichtlinien und die erforderlichen Trustee-Rechte zugewiesen werden. Soll ein benutzerdefinierter Container erstellt werden, wählen Sie **Ja**.
LDIF-Dateipfad für benutzerdefinierten Container	*Gilt nur, wenn Sie für den benutzerdefinierten Container die Option* **Ja** festgelegt haben. Gibt den Pfad der LDIF-Datei für den benutzerdefinierten Container an.
Root-Container	Gibt den Root-Container an. Der Standardwert lautet `o=data`.
Gruppensuch-Root-Container-DN	Gibt den DN des Gruppensuch-Root-Containers an.
Identitätsberichterstellung	
Hostname (FQDN in Kleinbuchstaben)	Gibt den vollständig qualifizierten eindeutigen Namen oder die standardmäßige IP-Adresse des Servers an. **HINWEIS:** Der FQDN muss in Kleinbuchstaben angegeben werden. Der Server, auf dem die Komponente gehostet wird, muss zudem für die Verwendung des FQDN in Kleinbuchstaben konfiguriert werden.
Hostname/IP-Adresse des Identitätsdepots	Gibt die IP-Adresse des Servers an, auf dem das Identitätsdepot installiert ist.
LDAP-SSL-Port	Gibt den Port an, den das Identitätsdepot mit dem SSL-Protokoll (Secure Sockets Layer) auf LDAP-Anforderungen überwachen soll. Der Standardwert ist 636.
Name des Identitätsdepot-Administrators	Gibt den relativen eindeutigen Namen (RDN) des Administratorobjekts im Baum an, das über vollständige Rechte verfügt (zumindest für den Kontext, dem dieser Server hinzugefügt werden soll).
Identitätsdepot-Administratorpasswort	Gibt das Passwort für das Administratorobjekt an. Beispiel: *Passwort*.
DNS/IP-Adresse des Anwendungsservers	Gibt die IP-Adresse des Tomcat-Servers an.
Benutzerdefinierter Name für OSP-Anmeldebildschirm	Gibt den Namen an, der auf dem OSP-Anmeldebildschirm angezeigt werden soll.
Benutzersuchcontainer-DN	Gibt den Standardcontainer für alle Benutzerobjekte im Identitätsdepot an.
Adminsuchcontainer-DN	Gibt alle Datenobjekte für Identity Manager-Speicherorte in der Datenorganisation an. Die Administratoren sollen allen Benutzern den Zugriff auf diesen Container und alle Untercontainer ermöglichen.

Parameter für benutzerdefinierte Konfiguration	
Anwendungsserver-HTTPS-Port	Gibt den HTTPS-Port an, über den der Tomcat-Server mit den Client-Computern kommunizieren soll. Der Standardwert ist `8543`.
DNS/IP-Adresse des One SSO-Servers	Gibt die IP-Adresse des Servers an, auf dem der Single-Sign-On-Dienst installiert ist.
One–SSO-Server-SSL-Port	Gibt den Port an, auf dem der Single-Sign-On-Dienst zugreifen soll. Der Standardwert ist 8543.
Identity Reporting-Datenbankname	Gibt den Namen der Datenbank für Identity Reporting an. Der Standardwert lautet `idmrptdb`.
Identity Reporting-Datenbankbenutzer	Gibt das Administratorkonto an, mit dem Identity Reporting auf die Daten in den Datenbanken zugreifen und diese Daten bearbeiten kann. Der Standardwert lautet `rptadmin`.
Identity Reporting-Datenbankhost	Gibt den DNS-Namen oder die IP-Adresse des Servers an, auf dem die Datenbank erstellt werden soll.
Identity Reporting-Datenbankport	Gibt den Port für die Verbindung mit der Datenbank an. Der Standardport hat die Nummer 5432.
JDBC-jar-Datei für Identitätsanwendungs-Datenbank	Gibt die JAR-Datei für die Datenbankplattform an.
Passwort für Identity Reporting-Datenbankkonto	Gibt das Passwort für das Datenbankkonto für Identity Reporting an.
Schema erstellen	Gibt an, ob das Datenbankschema im Rahmen des Installationsvorgangs erstellt werden soll. Verfügbare Optionen: **Jetzt**, **Start** und **Datei**. Wenn Sie für die Erstellung der Datenbank die Option **Start** oder **Datei** wählen, müssen Sie die Datenquelle manuell in die Seite der Identity-Datenerfassungsdienste aufnehmen. Weitere Informationen finden Sie unter Abschnitt 11.10.1, „Manuelles Hinzufügen der Datenquelle auf der Seite der Identity-Datenerfassungsdienste“, auf Seite 176. Wenn die Datenbank auf einem separaten Server ausgeführt wird, müssen Sie eine Verbindung zu dieser Datenbank herstellen. Bei einer entfernt installierten PostgreSQL-Datenbank prüfen Sie, ob die Datenbank ausgeführt wird. Anweisungen zum Verbinden mit einer entfernten PostgreSQL-Datenbank finden Sie unter Abschnitt 11.10.6, „Verbinden mit einer entfernten PostgreSQL-Datenbank“, auf Seite 178. Soll eine Verbindung zu einer Oracle-Datenbank hergestellt werden, müssen Sie zuvor eine Oracle-Datenbankinstanz anlegen. Weitere Informationen finden Sie in der Dokumentation zu Oracle. Wenn Sie für die Erstellung der Datenbank die Option **Start** oder **Datei** wählen, müssen Sie nach der Konfiguration manuell die Tabellen erstellen und die Verbindung zur Datenbank herstellen. Weitere Informationen finden Sie unter Abschnitt 11.10.3, „Manuelles Erstellen des Datenbankschemas“, auf Seite 176.
Standardmäßige Email-Adresse	Gibt die Email-Adresse an, die die Identitätsberichterstellung als Absender für Email-Benachrichtigungen verwenden soll.

Parameter für benutzerdefinierte Konfiguration	
SMTP-Server	Gibt die IP-Adresse oder den DNS-Namen des SMTP-Email-Hosts an, den die Identitätsberichterstellung für Bereitstellungs-Emails verwendet.
Port des SMTP-Servers	Gibt die Port-Nummer für den SMTP-Server an. Der Standardport ist 465.
MSGW- und DCS-Treiber für Identity Reporting erstellen	Gibt an, ob die MSGW- und DCS-Treiber erstellt werden sollen.

10.2 Durchführen der Konfiguration

In den nachfolgenden Abschnitten finden Sie Informationen zum Konfigurieren der Identity Manager-Komponenten.

10.2.1 Durchführen einer interaktiven Konfiguration

1. Navigieren Sie zu dem Speicherort, an dem Sie die Datei „Identity_Manager_4.7_Linux.iso“ eingehängt haben.
2. Führen Sie den folgenden Befehl aus:

   ```
   ./configure.sh
   ```

3. Entscheiden Sie, ob eine typische oder eine benutzerdefinierte Konfiguration durchgeführt werden soll. Die Konfigurationsoptionen sind abhängig von den Komponenten, die Sie zur Konfiguration auswählen.
4. Weitere Informationen zum Konfigurieren der Komponenten finden Sie unter Abschnitt 10.1, „Erläuterungen zu den Konfigurationsparametern“, auf Seite 101.

10.2.2 Ausführen einer automatischen Konfiguration

1. Navigieren Sie zu dem Speicherort, an dem Sie die Datei `Identity_Manager_4.7_Linux.iso` eingehängt haben.
2. Führen Sie den folgenden Befehl aus:

   ```
   ./configure.sh -s -f <Speicherort der Eigenschaftsdatei für die
   unbeaufsichtigte Installation>
   ```

   Beispiel:

   `./configure.sh -s -f /mnt/silent.properties`, wobei `/mnt/silent.properties` den Speicherort bezeichnet, an dem Sie die Eigenschaftsdatei für die unbeaufsichtigte Installation abgelegt haben.
3. Weitere Informationen zum Konfigurieren der Komponenten finden Sie unter Abschnitt 10.1, „Erläuterungen zu den Konfigurationsparametern“, auf Seite 101.

11 Abschließende Konfigurationsschritte

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:

11.1 Durchführen einer Nicht-Root-Installation

Wenn Sie die Identity Manager-Engine und -Plugins als Nicht-`Root`-Benutzer installieren, werden alle beabsichtigten Installationsaktivitäten ausgeführt. In diesem Abschnitt werden Sie durch den manuellen Vorgang geführt, der zur Durchführung der Installation erforderlich ist.

11.1.1 Erstellen eines Containers für Passwortrichtlinien

Identity Manager benötigt Passwortrichtlinienobjekte im Identitätsdepot. Der Nicht-`Root`-Installationsvorgang erstellt keinen Container für Passwortrichtlinien.

1. Melden Sie sich im Identity Manager-Baum in iManager an.
2. Navigieren Sie zum Sicherheitscontainer in eDirectory.

11.1.2 Unterstützung für Grafiken in Email-Benachrichtigungen

Wenn Sie das Identitätsdepot und die Identity Manager-Engine als Nicht-`Root`-Benutzer installieren, sind in den Email-Benachrichtigungen möglicherweise die in der Email-Schablone enthaltenen Grafiken und Bilder nicht vorhanden. Wenn Sie beispielsweise `do-send-email-from-template` ausführen, wird die Email zwar von Identity Manager gesendet, doch die Bilder fehlen. Sie müssen den Treibersatz aktualisieren, um die Unterstützung von Grafiken sicherzustellen.

1. Melden Sie sich bei Ihrem Projekt in Designer an.
2. Erweitern Sie **Identitätsdepot** im Bereich „Gliederung“.

3 Klicken Sie mit der rechten Maustaste auf **Treibersatz**.

4 Wählen Sie **Eigenschaften > Java** aus.

5 Geben Sie für JVM-Optionen den folgenden Inhalt ein:

```
-Dcom.novell.nds.dirxml.util.mail.templatepath=path_to_graphics_files
```

Beispiel:

```
-Dcom.novell.nds.dirxml.util.mail.templatepath=/prod/eDirectory/opt/novell/
eDirectory/lib/dirxml/rules/manualtask/mt_files
```

6 Klicken Sie auf **OK**.

7 Stellen Sie dem Treibersatz die Änderungen bereit:

7a Klicken Sie mit der rechten Maustaste auf **Treibersatz**.

7b Wählen Sie **Live > Bereitstellen**.

7c Wählen Sie **Bereitstellen**.

8 Starten Sie das Identitätsdepot neu.

11.2 Konfigurieren des Identitätsdepots nach der Installation

Nach dem Installieren des Identitätsdepots können Sie das Verzeichnis mit dem ndsconfig-Dienstprogramm konfigurieren und Serverinstanzen mit dem ndsmanage-Dienstprogramm erstellen, starten und anhalten. Außerdem können Sie das Identitätsdepot für die Verwendung von IPv6-Adressen konfigurieren, wenn der Server bereits die IPv6-Adressierung unterstützt.

11.2.1 Ändern des eDirectory-Baums und des Reproduktionsservers mit dem ndsconfig-Dienstprogramm

Nach der Installation wird das Identitätsdepot mit dem ndsconfig-Dienstprogramm konfiguriert. Zum Verwenden des ndsconfig-Dienstprogramms müssen Sie über Administratorrechte verfügen. Wenn Sie dieses Dienstprogramm mit Argumenten verwenden, überprüft es alle Argumente und fordert zur Eingabe des Passworts des Benutzers mit Administratorrechten auf. Wird das Dienstprogramm ohne Argumente aufgerufen, zeigt ndsconfig eine Beschreibung des Dienstprogramms und der verfügbaren Optionen.

Mit diesem Dienstprogramm können Sie außerdem den eDirectory-Reproduktionsserver entfernen und die aktuelle Konfiguration des eDirectory-Servers ändern. Weitere Informationen finden Sie in Kapitel 11.2, „Konfigurieren des Identitätsdepots nach der Installation“, auf Seite 110.

Für die Verwendung des ndsconfig-Dienstprogramms gelten die folgenden Bedingungen:

- Die Variablen *treename*, *admin_FDN* und *server_FDN* dürfen maximal die folgende Anzahl von Zeichen enthalten:
  - *treename:* 32 Zeichen
  - *admin_FDN:* 255 Zeichen
  - *server_FDN:* 255 Zeichen
- Wenn Sie einen Server zu einem vorhandenen Baum hinzufügen und dabei einen Kontext angeben, der nicht im Serverobjekt vorhanden ist, erstellt das ndsconfig-Dienstprogramm diesen Kontext beim Hinzufügen des Servers.

- Nach der Installation des Identitätsdepots können Sie LDAP- und Sicherheitsdienste zum vorhandenen Baum hinzufügen.
- Soll die verschlüsselte Reproduktion auf dem Server aktiviert werden, geben Sie bei den Befehlen zum Hinzufügen eines Servers zu einem vorhandenen Baum die Option `-E` an. Weitere Informationen zur verschlüsselten Reproduktion finden Sie unter Encrypted Replication (Verschlüsselte Reproduktion) im NetIQ eDirectory-Administrationshandbuch.

Weitere Informationen zum Bearbeiten von eDirectory mit dem ndsconfig-Dienstprogramm finden Sie im *NetIQ eDirectory -Administrationshandbuch*.

Erläuterungen zu den Parametern des ndsconfig-Dienstprogramms

Das ndsconfig-Dienstprogramm unterstützt die folgenden Parameter:

new

Erstellt einen neuen Baum. Wenn Sie die Parameter nicht in der Befehlszeile angeben, fordert das Dienstprogramm Sie jeweils zur Eingabe der Werte für die fehlenden Parameter auf.

def

Erstellt einen neuen Baum. Wenn Sie die Parameter nicht in der Befehlszeile angeben, verwendet das Dienstprogramm jeweils den Standardwert für die fehlenden Parameter.

add

Fügt einen Server zu einem vorhandenen Baum hinzu. Fügt außerdem LDAP- und SAS-Services hinzu, nachdem Sie das Identitätsdepot im vorhandenen Baum konfiguriert haben.

rm

Entfernt das Serverobjekt und die Directory Services aus einem Baum.

HINWEIS: Die Schlüsselmaterialobjekte werden mit dieser Option nicht entfernt. Diese Objekte müssen manuell entfernt werden.

---

upgrade

Aktualisiert eDirectory auf eine spätere Version.

-i

Weist das Dienstprogramm beim Konfigurieren eines neuen Baums an, nicht zu prüfen, ob ein Baum mit demselben Namen bereits vorhanden ist. Es können mehrere Bäume mit demselben Namen vorhanden sein.

-t *Baumname*

Gibt den Name des Baums an, zu dem der Server hinzugefügt werden soll. Es sind maximal 32 Zeichen zulässig. Ist die Option nicht angegeben, entnimmt ndsconfig den Baumnamen aus dem Parameter `n4u.nds.tree-name` in der Datei `/etc/opt/novell/eDirectory/conf/nds.conf`. Der standardmäßige Baumname ist `$LOGNAME-$HOSTNAME-NDStree`.

-n *Serverkontext*

Gibt den Kontext des Servers an, zu dem das Serverobjekt hinzugefügt werden soll. Es sind maximal 64 Zeichen zulässig. Ist die Option nicht angegeben, entnimmt NDSCONFIG den Kontext aus dem Parameter `n4u.nds.server-context` in der Datei `/etc/opt/novell/eDirectory/conf/nds.conf`. Der Serverkontext sollte mit Typenangabe angegeben werden. Der Standardkontext ist `org`.

-d ***Pfad_für_DIB***

Gibt den Verzeichnis-Pfad an, wo die Datenbank-Dateien gespeichert werden sollen.

-r

Erzwingt das Hinzufügen der Reproduktion des Servers unabhängig von der Anzahl der Server, die dem Server bereits hinzugefügt wurden.

-L ***LDAP_Port***

Legt die TCP-Portnummer auf dem LDAP-Server fest. Wenn der Standardport 389 bereits verwendet wird, werden Sie aufgefordert, einen neuen Port einzugeben.

-l ***SSL_Port***

Legt die SSL-Portnummer auf dem LDAP-Server fest. Wenn der Standardport 636 bereits verwendet wird, werden Sie aufgefordert, einen neuen Port einzugeben.

-a ***Admin_FDN***

Legt den vollständig eindeutigen Namen des Benutzerobjekts mit Supervisor-Rechten für den Kontext fest, in dem das Serverobjekt und die Directory Services erstellt werden sollen. Der Admin-Name sollte mit Typenangabe angegeben werden. Es sind maximal 64 Zeichen zulässig. Der Standardwert ist admin.org.

-e

Aktiviert unverschlüsselte Passwörter für LDAP-Objekte.

-m ***Modulname***

Gibt den Namen des Moduls an, das installiert oder konfiguriert werden soll. Wenn Sie einen neuen Baum konfigurieren, können Sie nur das Modul DS angeben. Nach der Konfiguration des Moduls DS können Sie NMAS-, LDAP-, SAS-, SNMP- und HTTP-Dienste sowie NetIQ SecretStore (ss) mit dem Befehl „add“ hinzufügen. Wenn der Modulname nicht angegeben wird, werden alle Module installiert.

HINWEIS: Soll der SecretStore beim Aufrüsten von eDirectory mit dem Befehl `nds-install` nicht konfiguriert werden, geben Sie den Wert `no_ss` für diese Option an. Beispiel: `ndsinstall '-m no_ss'`.

-o

Legt die unverschlüsselte HTTP-Portnummer fest.

-O

Legt die sichere HTTP-Portnummer fest.

-p ***IP_Adresse:[Port]***

Gibt die IP-Adresse des Remote-Hosts an, auf dem sich eine Reproduktion der Partition befindet, der dieser Server hinzugefügt werden soll. Verwenden Sie diese Option, wenn Sie einen Sekundärserver einem Baum hinzufügen (mit dem Befehl „add“). Die Standardportnummer lautet 524. Hiermit wird die SLP-Suche umgangen, sodass die Suche im Baum beschleunigt wird.

-R

Reproduziert die Partition, zu der der Server hinzugefügt werden soll, auf dem lokalen Server. Diese Option verhindert das Hinzufügen von Reproduktionen zum lokalen Server.

-c

Verhindert die Anzeige von Eingabeaufforderungen bei der Verwendung von ndsconfig, z. B. Ja/Nein zum Fortsetzen des Vorgangs oder Aufforderungen zum erneuten Eingeben der Portnummern bei Konflikten. Das Dienstprogramm fordert Sie weiterhin auf, die erforderlichen Parameter einzugeben, wenn Sie diese nicht in der Befehlszeile angegeben haben.

-w *Admin_Passwort*

Mit dieser Option wird das Admin-Benutzerpasswort im Klartext weitergegeben.

HINWEIS: NetIQ empfiehlt, diese Option nicht in einer Umgebung zu verwenden, in der die Passwortsicherheit nicht gewährleistet ist.

-E

Aktiviert die verschlüsselte Reproduktion für den hinzuzufügenden Server.

-j

Weist das Dienstprogramm an, die Option für die Zustandsprüfung zu überspringen (außer Kraft zu setzen), bevor das Identitätsdepot installiert wird.

-b *Port_für_Bindung*

Gibt die Nummer des Standardports an, den eine bestimmte Instanz überwachen soll. Hiermit legen Sie die Standardportnummer für `n4u.server.tcp-port` und `n4u.server.udp-port` fest. Wenn Sie einen NCP-Port mit der Option -b angeben, setzt das Dienstprogramm voraus, dass dieser Port als Standardport fungiert, und die TCP- und UDP-Parameter werden entsprechend aktualisiert.

HINWEIS: Die Parameter `-b` und `-B` schließen sich gegenseitig aus.

-B *Schnittstelle1@Port1,Schnittstelle2@Port2,...*

Gibt die Portnummer zusammen mit der IP-Adresse oder der Schnittstelle an. Beispiel: `-B eth0@524`, `-B 100.1.1.2@524`, `-B[2015::3]@524`.

HINWEIS

- Die Parameter `-b` und `-B` schließen sich gegenseitig aus.
- IPv6-Adressen müssen in eckigen Klammern (`[ ]`) gesetzt werden.

--config-file *Konfigurationsdatei*

Gibt den absoluten Pfad und den Dateinamen zum Speichern der Konfigurationsdatei `nds.conf` an. Soll die Konfigurationsdatei beispielsweise im Verzeichnis `/etc/opt/novell/eDirectory/gespeichert werden, geben Sie den folgenden Befehl ein:`

```
--config-file /etc/opt/novell/eDirectory/nds.conf
```

-P LDAP_URL(s)

Ermöglicht die Konfiguration der LDAP-Schnittstelle im LDAP-Serverobjekt über die LDAP-URLs. Trennen Sie mehrere URLs jeweils mit Kommas voneinander ab. Beispiel:

```
-P ldap://1.2.3.4:389,ldaps://1.2.3.4:636,ldap://[2015::3]:389
```

HINWEIS

- IPv6-Adressen müssen in eckigen Klammern (`[ ]`) gesetzt werden. Beispiel: ldap://[2015::3]:389.
- Falls Sie die LDAP-URLs nicht bei der ersten Konfiguration angegeben haben, können Sie sie nachträglich über das Attribut `ldapInterfaces` im Befehl `ldapconfig` bzw. in iManager hinzufügen.

-D Pfad_für_Daten

Erstellt die Verzeichnisse `data`, `dib` und `log` im angegebenen Pfad.

set Werteliste

Legt den Wert für die konfigurierbaren Parameter fest, die Sie für das Identitätsdepot angegeben haben. Mit dieser Option legen Sie die Boot-Strapping-Parameter fest, bevor Sie einen Baum konfigurieren.

Wenn Sie die Konfigurationsparameter ändern, müssen Sie ndsd neu starten, damit der neue Wert in Kraft tritt. Bei den folgenden Konfigurationsparametern ist ein Neustart von ndsd nicht erforderlich:

- `n4u.nds.inactivity-synchronization-interval`
- `n4u.nds.synchronization-restrictions`
- `n4u.nds.janitor-interval`
- `n4u.nds.backlink-interval`
- `n4u.nds.drl-interval`
- `n4u.nds.flatcleaning-interval`
- `n4u.nds.server-state-up-threshold`
- `n4u.nds.heartbeat-schema`
- `n4u.nds.heartbeat-data`

get help Parameterliste

Zeigt die Hilfetexte für die konfigurierbaren Parameter an, die Sie für das Identitätsdepot angegeben haben. Wenn Sie keine Parameterliste angeben, zeigt das Dienstprogramm die Hilfetexte für alle konfigurierbaren Parameter an.

Konfigurieren des Identitätsdepots mit einem bestimmten Gebietsschema

Soll das Identitätsdepot mit einem bestimmten Gebietsschema konfiguriert werden, müssen Sie LC_ALL und LANG in dieses Gebietsschema exportieren, bevor Sie die Konfiguration vornehmen. Geben Sie beispielsweise die folgenden Befehle im ndsconfig-Dienstprogramm ein:

```
export LC_ALL=ja
```

```
export LANG=ja
```

Hinzufügen eines neuen Baums zum Identitätsdepot

Wenn Sie einen neuen Baum im Identitätsdepot erstellen, können Sie sich wahlweise vom ndsconfig-Dienstprogramm durch die Konfiguration führen lassen oder auch alle Parameterwerte mit einem einzigen Befehl festlegen. Falls der Identitätsdepot-Server bereits IPv6-Adressen unterstützt, können Sie eine IPv6-Adresse für den neuen Baum angeben.

1. (Bedingt) Wenn das ndsconfig-Dienstprogramm eine Aufforderung zur Eingabe der Parameter für einen neuen Baum im Identitätsdepot anzeigen soll, geben Sie den folgenden Befehl ein:

   ```
   ndsconfig new [-t tree_name] [-n server_context] [-a admin_FDN]
   ```

   Beispiel:

   ```
   ndsconfig new -t corp-tree -n o=company -a cn=admin.o=company
   ```

2. (Bedingt) Wenn Sie zum Erstellen des neuen Baums im Identitätsdepot alle Parameter in der Befehlszeile angeben möchten, geben Sie den folgenden Text ein:

   ```
   ndsconfig new [-t Baumname] [-n Serverkontext] [-a Admin_FDN] [-i] [-S
   Servername] [-d Pfad_für_DIB] [-m Modul] [e] [-L LDAP_Port] [-l SSL_Port] [-o
   HTTP_Port] [-O HTTPS_Port] [-p IP_Adresse:[Port]] [-R] [-c] [-w Admin_Passwort]
   [-b Port_für_Bindung] [-B Schnittstelle1@Port1,Schnittstelle2@Port2,...] [-D
   Benutzerdefinierter_Speicherort] [--config-file Konfigurationsdatei]
   ```

   Alternativ:

   ```
   ndsconfig def [-t Baumname] [-n Serverkontext] [-a Admin_FDN] [-w
   Admin_Passwort] [-c] [-i] [-S Servername] [-d Pfad_für_DIB] [-m Modul] [-e] [-
   L LDAP_Port] [-l SSL_Port] [-o HTTP_Port] [-O HTTPS_Port] [-D
   Benutzerdefinierter_Speicherort] [--config-file Konfigurationsdatei]
   ```

Hinzufügen eines Servers zu einem vorhandenen Baum

Zum Hinzufügen eines Servers zu einem vorhandenen Baum geben Sie den folgenden Befehl ein:

```
ndsconfig add [-t treename] [-n server context] [-a admin_FDN] [-i] [-S
server_name] [-d path_for_dib] [-m module] [e] [-L ldap_port] [-l SSL_port] [-o
http_port] [-O https_port] [-p IP_address:[port]] [-R] [-c] [-w admin_password] [-
b port_to_bind] [-B interface1@port1,interface2@port2,..] [-D custom_location] [--
config-file configuration_file]
```

Beispiel:

```
ndsconfig add -t corp-tree -n o=company -a cn=admin.o=company -S srv1
```

Entfernen des Identitätsdepots und der zugehörigen Datenbank vom Server

1. Navigieren Sie zum Verzeichnis `dsreports` (standardmäßig unter `/var/opt/novell/eDirectory/data/`).
2. Löschen Sie die HTML-Dateien, die Sie mit iMonitor erstellt hatten.
3. Geben Sie im ndsconfig-Dienstprogramm den folgenden Befehl ein:

   ```
   ndsconfig rm [-a admin_FDN] [-w admin_password] [-p IP_address:[port]] [-c]
   ```

Entfernen eines eDirectory-Serverobjekts und der Verzeichnisdienste aus einem Baum

Zum Entfernen des Serverobjekts und der Verzeichnisdienste aus einem Baum geben Sie den folgenden Befehl ein:

```
ndsconfig rm -a Admin_FDN
```

Konfigurieren von mehreren Instanzen des Identitätsdepots

Sie können mehrere Instanzen des Identitätsdepots auf einem einzelnen Host konfigurieren. Die Konfiguration mehrerer Instanzen mit dem ndsconfig-Dienstprogramm ist ähnlich aufgebaut wie die mehrfache Konfiguration einer einzigen Instanz. Jede Instanz muss durch eindeutige Angaben gekennzeichnet sein, beispielsweise:

- Unterschiedliche Speicherorte für Daten und Protokolldatei. Verwenden Sie die Optionen `--config-file`, `-d` und `-D`.
- Eindeutige Portnummer, die durch jede Instanz überwacht werden soll. Verwenden Sie die Optionen `-b` und `-B`.
- Eindeutiger Servername für die Instanz. Verwenden Sie die Option `-S Servername`.

Weitere Informationen finden Sie unter „Using ndsconfig to Configure Multiple Instances of eDirectory“ (Konfigurieren mehrerer eDirectory-Instanzen mit ndsconfig) im *NetIQ eDirectory-Installationshandbuch*.

HINWEIS:

- Bei der Konfiguration des Identitätsdepots wird der Name des standardmäßigen NCP-Servers als Name des Hostservers übernommen. Wenn Sie mehrere Instanzen konfigurieren, müssen Sie den NCP-Servernamen ändern. Geben Sie mit der ndsconfig-Befehlszeilenoption `-S Servername` einen anderen Servernamen an. Beim Konfigurieren mehrerer Instanzen (auf demselben Baum oder auf verschiedenen Bäumen) muss der NCP-Servername jeweils eindeutig sein.
- Alle Instanzen verwenden denselben Serverschlüssel (NICI).

11.2.2 Verwalten von Instanzen mit dem ndsmanage-Dienstprogramm

Mit dem ndsmanage-Dienstprogramm können Sie Serverinstanzen im Identitätsdepot erstellen, starten und anhalten. Außerdem können Sie eine Liste der konfigurierten Instanzen abrufen.

Auflisten der Identitätsdepot-Instanzen

Mit dem ndsmanage-Dienstprogramm können Sie den Pfad der Konfigurationsdatei, den vollständigen eindeutigen Namen und den Port der Serverinstanz sowie den Status der Instanz (aktiv oder inaktiv) für die angegebenen Benutzer abrufen. Das Dienstprogramm unterstützt die folgenden Parameter:

ndsmanage

Zeigt eine Liste aller konfigurierten Instanzen.

ndsmanage -a|--all

Zeigt eine Liste aller Instanzen der Benutzer, die eine bestimmte Installation des Identitätsdepots verwenden.

ndsmanage *Benutzername*

Zeigt eine Liste der von einem bestimmten Benutzer konfigurierten Instanzen.

Erstellen einer neuen Instanz im Identitätsdepot

1. Geben Sie in der Befehlszeile den Befehl `ndsmanage` ein.
2. Geben Sie `c` ein.
3. Befolgen Sie die Anweisungen in der Befehlszeile zum Erstellen der neuen Instanz.

Konfigurieren und Dekonfigurieren einer Instanz im Identitätsdepot

Zum Konfigurieren einer Instanz geben Sie den folgenden Befehl ein:

```
ndsconfig new -t treename -n server_context -a admin_FDN -b port_to_bind -D
path_for_data
```

Beispiel:

```
ndsconfig new -t mytree -n o=netiq -a cn=admin.o=company -b 1524 -D
/home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

HINWEIS: Beim Linux-Betriebssystem können Sockets ausschließlich im gemounteten Dateisystem erstellt werden. Für eDirectory empfiehlt NetIQ, das Verzeichnis `var` im lokalen Dateisystem (Option `-D` in `ndsconfig`) zu verwenden; das DIB-Verzeichnis kann aus einem beliebigen Dateisystem stammen (Option `-d` in `ndsconfig`).

So dekonfigurieren Sie eine Instanz:

1. Geben Sie in der Befehlszeile den Befehl `ndsmanage` ein.
2. Wählen Sie die Instanz aus, die dekonfiguriert werden soll.
3. Geben Sie `d` ein.

Aufrufen eines Dienstprogramms für eine Instanz im Identitätsdepot

Sie können verschiedene Dienstprogramme, beispielsweise DSTrace, für eine Instanz ausführen. Beispiel: Sie möchten das DSTrace-Dienstprogramm für Instanz 1 ausführen, die den Port 1524 überwacht. Die Konfigurationsdatei dieser Instanz befindet sich im Verzeichnis `/home/mary/inst1/nds.conf` und die zugehörige `DIB`-Datei im Verzeichnis `/home/mary/inst1/var`. Hier können Sie einen der folgenden Befehle eingeben:

```
ndstrace --config-file /home/mary/inst1/nds.conf
```

Alternativ:

```
ndstrace -h 192.168.0.1:1524
```

Wenn Sie keine Angaben zu den Instanzen nennen, zeigt das Dienstprogramm alle Instanzen an. Anschließend können Sie eine Instanz auswählen.

Starten und Anhalten von Instanzen im Identitätsdepot

Bei Bedarf können Sie eine oder mehrere konfigurierte Instanzen starten oder anhalten.

1 (Bedingt) Soll eine einzelne Instanz mit einem geführten Verfahren gestartet oder angehalten werden, führen Sie die folgenden Schritte aus:

   1a Geben Sie in der Befehlszeile den Befehl `ndsmanage` ein.

   1b Wählen Sie die Instanz aus, die gestartet oder angehalten werden soll.

   1c Geben Sie `s`zum Starten der Instanz bzw. `k` zum Anhalten ein.

2 (Bedingt) Zum Starten oder Anhalten einer einzelnen Instanz geben Sie Folgendes ein:

```
ndsmanage start --config-file configuration_file_of_the_instance
```

   Alternativ:

```
ndsmanage stop --config-file configuration_file_of_the_instance
```

3 (Bedingt) Zum Starten oder Anhalten aller Instanzen geben Sie Folgendes ein:

```
ndsmanage startall
```

   Alternativ:

```
ndsmanage stopall
```

11.3 Konfigurieren des Remote Loader und der Treiber

Der Remote Loader kann die in den `.iso`- oder `.jar`-Dateien enthaltenen Identity Manager-Anwendungsschnittstellenmodule hosten. Der Java Remote Loader hostet nur Java-Treiberschnittstellenmodule. Das Laden oder Hosten nativer (C++-)Treiberschnittstellenmodule ist nicht möglich.

Vor Verwendung des Remote Loader müssen Sie das Anwendungsschnittstellenmodul so konfigurieren, dass eine sichere Verbindung zur Identity Manager-Engine hergestellt wird. Außerdem müssen sowohl der Remote Loader als auch die Identity Manager-Treiber konfiguriert werden. Weitere Informationen zu Schnittstellenmodulen finden Sie in „Erläuterungen zu Schnittstellenmodulen“, auf Seite 69.

11.3.1 Herstellen einer sicheren Verbindung zur Identity Manager-Engine

Die Datenübertragung zwischen dem Remote Loader und der Identity Manager-Engine muss in jedem Fall geschützt sein. NetIQ empfiehlt die Kommunikation über die TLS/SSL-Protokolle (Transport Layer Security/Secure Socket Layer). Damit TLS/SSL-Verbindungen unterstützt werden, muss ein geeignetes eigensigniertes Zertifikat in einer Keystore-Datei oder KMO vorliegen. In diesem Abschnitt wird beschrieben, wie Sie dieses Zertifikat erstellen, exportieren und speichern.

HINWEIS: Verwenden Sie dieselbe SSL-Version auf den Servern, auf denen die Identity Manager-Engine gehostet werden, und für den Remote Loader. Wenn die SSL-Version auf dem Server nicht mit der SSL-Version des Remote Loader übereinstimmt, gibt der Server die Fehlermeldung `SSL3_GET_RECORD:Falsche Versionsnummer` zurück. Diese Meldung ist lediglich ein Warnhinweis; die Kommunikation zwischen dem Server und dem Remote Loader wird nicht unterbrochen. Der Fehler kann jedoch zu Verwirrungen führen.

Erläuterungen zum Kommunikationsvorgang

Der Remote Loader öffnet ein Client-Socket und überwacht die vom Remote-Schnittstellenmodul kommenden Verbindungen. Zum Einrichten eines sicheren Kanals führen das Remote-Schnittstellenmodul und der Remote Loader einen SSL-Handshake aus. Anschließend authentifiziert sich das Remote-Schnittstellenmodul beim Remote Loader. Wenn die Authentifizierung des Remote-Schnittstellenmoduls erfolgreich ausgeführt wurde, authentifiziert sich der Remote Loader beim Remote-Schnittstellenmodul. Nur wenn beide Seiten übereinkommen, dass sie mit einer autorisierten Entität kommunizieren, findet der Synchronisierungsverkehr statt.

Die Abläufe beim Einrichten einer SSL-Verbindung zwischen einem Treiber und der Identity Manager-Engine sind abhängig vom Treibertyp:

- **Bei einem nativen Treiber**, beispielsweise dem Active Directory-Treiber, verweisen Sie auf ein base64-verschlüsseltes Zertifikat. Weitere Informationen finden Sie in „Verwalten von eigensignierten Serverzertifikaten“, auf Seite 119.
- **Bei einem Java-Treiber** müssen Sie einen Keystore erstellen. Weitere Informationen finden Sie in „Erstellen einer Keystore-Datei für SSL-Verbindungen“, auf Seite 121.

HINWEIS: Der Remote Loader ermöglicht benutzerdefinierte Verbindungsmethoden zwischen dem Remote Loader und dem Remote-Schnittstellenmodul, das auf dem Identity Manager-Server gehostet wird. Weitere Informationen zu den Elementen, die beim Konfigurieren eines benutzerdefinierten Verbindungsmoduls in der Verbindungszeichenkette erwartet werden und zulässig sind, finden Sie in der Dokumentation des Moduls.

Verwalten von eigensignierten Serverzertifikaten

Um die sichere Kommunikation zwischen dem Remote Loader und der Identity Manager-Engine zu gewährleisten, können Sie ein eigensigniertes Serverzertifikat erstellen und exportieren. Für zusätzliche Sicherheit wird für die SSL-Kommunikation eine stärkere Verschlüsselung konfiguriert wie durch Suite B angegeben. Für diese Kommunikation müssen ECDSA (Elliptic Curve Digital

Signature Algorithm)-Zertifikate zur Verschlüsselung der Daten verwendet werden. Wenn Suite B aktiviert ist, verwendet der Remote Loader TLS 1.2 als Kommunikationsprotokoll. Weitere Informationen zu Suite B finden Sie unter Suite B-Verschlüsselungsverfahren.

Sie haben die Möglichkeit, ein neu erstelltes Zertifikat zu exportieren oder ein bestehendes Zertifikat zu verwenden.

HINWEIS: Wenn ein Server mit einer Baumstruktur verknüpft wird, erstellt eDirectory die folgenden Standardzertifikate:

- SSL CertificateIP
- SSL CertificateDNS
- Mit Suite B kompatible Zertifikate

---

1. Melden Sie sich bei NetIQ iManager an.
2. Erstellen Sie ein neues Zertifikat mit den folgenden Schritten:
   - **2a** Klicken Sie auf **NetIQ Certificate Server > Create Server Certificate** (Serverzertifikat erstellen).
   - **2b** Wählen Sie den Server aus, der als Eigentümer des Zertifikats fungieren soll.
   - **2c** Geben Sie einen Kurznamen für das Zertifikat ein. Beispiel: `remotecert`.

     HINWEIS: NetIQ empfiehlt, auf Leerzeichen in den Kurznamen der Zertifikate zu verzichten. Verwenden Sie beispielsweise `remotecert` statt `remote cert`.

     Notieren Sie sich außerdem den Kurznamen des Zertifikats. Der Kurzname wird als KMO-Name in den Remote-Verbindungsparametern des Treibers herangezogen.

   - **2d** Wählen Sie die Zertifikatserstellungsmethode aus, und klicken Sie anschließend auf **Weiter**.

     Die folgenden Optionen stehen Ihnen zur Verfügung:

     - **Standard:** Mit dieser Option wird ein Serverzertifikatsobjekt mit der größtmöglichen Schlüsselgröße erstellt und das öffentliche Schlüsselzertifikat mit der Zertifizierungsstelle Ihrer Organisation wird signiert.
     - **Benutzerdefiniert:** Bei dieser Option wird ein Serverzertifikatsobjekt mit den von Ihnen angegebenen Einstellungen erstellt. Legen Sie damit eine Reihe von benutzerdefinierten Einstellungen für das Serverzertifikatsobjekt fest. Wählen Sie diese Option zur Erstellung von ECDSA-Zertifikaten für die Suite B-Kommunikation aus.
     - **Importieren:** Diese Option erstellt ein Serverzertifikatsobjekt mithilfe der Schlüssel und Zertifikate aus einer PKCS12(PFX)-Datei. Sie können diese Option zusammen mit der Exportfunktion zur Sicherung und Wiederherstellung eines Serverzertifikats oder zum Verschieben eines Serverzertifikatsobjekts von einem Server auf einen anderen verwenden.
   - **2e** Geben Sie die Zertifikatsparameter an.
   - **2f** Übernehmen Sie die restlichen Standardeinstellungen für das Zertifikat.
   - **2g** Überprüfen Sie die Zusammenfassung, klicken Sie auf **Fertig stellen** und anschließend auf **Schließen**.

3 Exportieren Sie das Zertifikat mit den folgenden Schritten:

3a Navigieren Sie in iManager zu **Rollen und Aufgaben** > **Zugriff auf NetIQ-Zertifikate > Serverzertifikate**.

3b Suchen und wählen Sie das erstellte Zertifikat oder das vom Server erstellte Zertifikat (z. B. SSL CertificateDNS).

3c Klicken Sie auf **Exportieren**.

3d Wählen Sie im Dropdown-Menü **Zertifikat der Zertifizierungsstelle** als **OU=Unternehmen CA.O=TREEANAME** aus.

3e Wählen Sie im Dropdown-Menü das **Exportformat** als **BASE64** aus.

3f Klicken Sie auf **Weiter**.

3g Klicken Sie auf **Speichern** und anschließend auf **Schließen**.

Erstellen einer Keystore-Datei für SSL-Verbindungen

Zum Herstellen von SSL-Verbindungen zwischen einem Java-Treiber und der Identity Manager-Engine muss ein Keystore erstellt werden. Ein Keystore ist eine Java-Datei, die Verschlüsselungsschlüssel und Zertifikate (optional) enthält. Wenn Sie SSL für die Kommunikation des Remote Loader mit der Identity Manager-Engine verwenden möchten und mit einem Java-Schnittstellenmodul arbeiten, müssen Sie eine Keystore-Datei erstellen. In den folgenden Abschnitten wird erläutert, wie Sie eine Keystore-Datei erstellen:

- „Erstellen eines Keystore auf einer beliebigen Plattform“, auf Seite 121
- „Erstellen eines Keystore unter Linux“, auf Seite 121

Erstellen eines Keystore auf einer beliebigen Plattform

Wenn Sie einen Keystore auf einer belieben Plattform erstellen möchten, geben Sie in der Befehlszeile Folgendes ein:

```
keytool -import -alias trustedroot -file Name_des_eigensignierten_Zertifikats -
keystore Dateiname -storepass keystorepass
```

Sie können einen beliebigen Dateinamen angeben. Beispiel: `rdev_keystore`.

Erstellen eines Keystore unter Linux

In Linux-Umgebungen verwenden Sie die Datei `create_keystore`. Dieses Shell-Skript ruft das Keytool-Dienstprogramm auf. Die Datei wird zusammen mit rdxml installiert und befindet sich standardmäßig im Verzeichnis *`Installationsverzeichnis`*`/dirxml/bin/`. Die Datei „create_keystore“ ist auch in der Datei `dirxml_jremote.tar.gz` enthalten, die sich im Verzeichnis `\dirxml\java\remoteloader` befindet.

Geben Sie in der Befehlszeile Folgendes ein:

```
create_keystore Name_des_selbstsignierten_Zertifikats Name_des_Keystore
```

Geben Sie beispielsweise Folgendes ein:

```
create_keystore tree-root.b64 mystore
create_keystore tree-root.der mystore
```

Das `create_keystore`-Skript legt „dirxml“ als hartcodiertes Keystore-Passwort fest. Dies ist kein Sicherheitsrisiko, da im Keystore nur ein öffentliches Zertifikat und ein öffentlicher Schlüssel gespeichert werden.

11.3.2 Erläuterungen zu den Kommunikationsparametern für den Remote Loader

Damit der Remote Loader eine Treiberinstanz nutzen kann, in der ein Identity Manager-Anwendungsschnittstellenmodul gehostet wird, müssen Sie die Treiberinstanz konfigurieren. Beispielsweise müssen Sie die Verbindungs- und die Porteinstellungen für die Instanz angeben. Sie können die Einstellungen über die Befehlszeile in einer Konfigurationsdatei festlegen. Sobald die Instanz läuft, können Sie über die Befehlszeile die Konfigurationsparameter ändern oder den Remote Loader anweisen, eine Funktion auszuführen. So können Sie beispielsweise das Trace-Fenster öffnen oder den Remote Loader entladen.

In diesem Abschnitt finden Sie Informationen zu den Konfigurationsparametern. Hierbei ist ersichtlich, ob ein Parameter über die Befehlszeile gesendet werden kann, während der Remote Loader ausgeführt wird.

Weitere Informationen zum Konfigurieren einer neuen Treiberinstanz finden Sie in Abschnitt 11.3.3, „Konfigurieren des Remote Loader für Treiberinstanzen“, auf Seite 131.

Konfigurationsparameter für die Treiberinstanzen im Remote Loader

Die Treiberinstanzen können über die Befehlszeile oder mithilfe einer Konfigurationsdatei konfiguriert werden. Die Beispieldatei `config8000.txt` von NetIQ hilft Ihnen dabei, den Remote Loader und die Treiber für das Anwendungsschnittstellenmodul zu konfigurieren. Die Beispieldatei befindet sich standardmäßig im Verzeichnis `/opt/novell/dirxml/doc/`. Die Konfigurationsdatei kann beispielsweise die folgenden Zeilen enthalten:

```
-commandport 8000
-connection "port=8090 rootfile=/dirxmlremote/root.pem"
-module $DXML_HOME/dirxmlremote/libcskeldrv.so.0.0.0
-trace 3
```

Die folgenden Parameter stehen zur Verfügung:

-description *Wert* (-desc *Wert*)

(Optional) Gibt eine kurze Beschreibung in Form einer Zeichenkette (z. B. SAP) an, die die Anwendung als Titel für das Trace-Fenster und für die Protokollierung heranzieht. Beispiel:

```
-description SAP
```

```
-desc SAP
```

-class *Name* (-cl *Name*)

(Bedingt) Bei Verwendung eines Java-Treibers geben Sie den Java-Klassennamen für das zu hostende Identity Manager-Anwendungsschnittstellenmodul an. Diese Option weist die Anwendung an, die Zertifikate aus einem Java-Keystore auszulesen. Beispiel:

```
-class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim
```

HINWEIS

- Diese Option ist nicht zulässig, wenn Sie die Option `-module` angeben.
- Wenn Sie das `Tab`-Zeichen als Begrenzungszeichen in der Option `-class` verwenden, wird der Remote Loader nicht automatisch gestartet. Stattdessen muss er manuell gestartet werden. Damit der Remote Loader ordnungsgemäß gestartet wird, ersetzen Sie das `Tab`-Zeichen durch ein Leerzeichen.
- Weitere Informationen zu den zulässigen Namen bei dieser Option finden Sie unter „Erläuterungen zu den Namen für den Java-Parameter -class“, auf Seite 129.

-commandport *Port-Nummer* (-cp *Port-Nummer*)

Gibt den TCP/IP-Port an, der von der Treiberinstanz zu Steuerungszwecken verwendet wird. Beispiel: `-commandport 8001` oder `-cp 8001`. Der Standardwert ist 8000.

Sollen mehrere Treiberinstanzen mit dem Remote Loader auf einem einzigen Server verwendet werden, geben Sie für jede Instanz jeweils unterschiedliche Verbindungs- und Befehlsports an.

Wenn die Treiberinstanz ein Anwendungsschnittstellenmodul hostet, ist der Befehlsport der Port, über den eine andere Remote Loader-Instanz mit der Instanz kommuniziert, die das Schnittstellenmodul hostet. Wenn die Treiberinstanz einen Befehl an eine Instanz sendet, die ein Anwendungsschnittstellenmodul hostet, ist der Befehlsport der Port, der von der Host-Instanz überwacht wird.

Wenn Sie diesen Parameter über die Befehlszeile an eine Instanz senden, die ein Anwendungsschnittstellenmodul hostet, ist der Befehlsport der Port, der von der Host-Instanz überwacht wird. Sie können diesen Befehl senden, während der Remote Loader läuft.

-config *Dateiname*

Gibt eine Konfigurationsdatei für die Treiberinstanz an. Beispiel:

```
-config config.txt
```

Die Konfigurationsdatei kann bis auf `-config` beliebige Befehlszeilenoptionen enthalten. Die an der Befehlszeile angegebenen Optionen haben Vorrang vor den in der Konfigurationsdatei angegebenen Optionen.

Sie können diesen Befehl senden, während der Remote Loader läuft.

-connection *„Parameter“* (-conn *„Parameter“*)

Gibt die Einstellungen zum Herstellen einer Verbindung zum Server an, auf dem die Identity Manager-Engine gehostet wird, die wiederum das Identity Manager-Remote-Schnittstellenmodul ausführt. Die Standardverbindungsmethode ist TCP/IP mit SSL.

Sollen mehrere Treiberinstanzen mit dem Remote Loader auf einem einzigen Server verwendet werden, geben Sie für jede Instanz jeweils unterschiedliche Verbindungs- und Befehlsports an.

Geben Sie die Verbindungseinstellungen mit der folgenden Syntax ein:

```
-connection "parameter parameter parameter"
```

Beispiel:

```
-connection "port=8091 fromaddress=198.51.100.0 rootfile=server1.pem
keystore=ca.pem localaddress=198.51.100.0 hostname=198.51.100.0 kmo=remote
driver cert"
```

Legen Sie die Einstellungen für eine TCP/IP-Verbindung mit den folgenden Parametern fest:

address=*IP_Adresse*

(Optional) Gibt an, ob der Remote Loader eine bestimmte lokale IP-Adresse überwacht. Dies ist hilfreich, wenn der Server, der den Remote Loader hostet, mehrere IP-Adressen hat und der Remote Loader nur eine dieser Adressen überwachen soll. Die folgenden Werte sind zulässig:

- `address=Adressnummer`
- `address='localhost'`

Beispiel:

```
address=198.51.100.0
```

Wenn Sie keinen Wert angeben, überwacht der Remote Loader alle lokalen IP-Adressen.

fromaddress=*IP_Adresse*

Gibt den Server an, von dem der Remote Loader Verbindungen akzeptiert. Verbindungen von anderen Adressen werden durch die Anwendung ignoriert. Geben Sie eine IP-Adresse oder den DNS-Namen des Servers an. Beispiel:

```
fromaddress=198.51.100.0
```

```
fromaddress=testserver1.company.com
```

handshaketimeout=*Millisekunden*

(Bedingt) Gilt, wenn eine Zeitüberschreitung beim Handshake im Zusammenhang mit anderweitig gültigen Verbindungen von der Identity Manager-Engine eintritt. Bestimmt den Zeitraum für die Zeitüberschreitung (in Millisekunden) beim Handshake zwischen dem Remote Loader und der Identity Manager-Engine. Beispiel:

```
handshaketimeout=1000
```

Sie können eine Ganzzahl größer oder gleich null angeben. Der Wert null bedeutet, dass niemals eine Zeitüberschreitung für die Verbindung eintritt. Der Standardwert ist 1.000 Millisekunden.

hostname=*Server*

Gibt die IP-Adresse oder den Namen des Servers an, auf dem der Remote Loader ausgeführt wird. Beispiel:

```
hostname=198.51.100.0
```

secureprotocol=*TLS-Version*

Gibt die Version des TLS-Protokolls an, das der Remote Loader verwendet, um eine Verbindung zur Identity Manager-Engine herzustellen. Beispiel:

```
secureprotocol=TLSv1_2
```

Identity Manager unterstützt TLSv1 und TLSv1_2. Der Remote Loader verwendet standardmäßig TLSv1_2. Geben Sie zur Verwendung von TLSv1 diese Version im Parameter an.

enforceSuiteB=*true/false*

(Bedingt) Trifft nur zu, wenn der Remote Loader mithilfe des Suite B-Verschlüsselungsalgorithmus mit der Identity Manager-Engine kommunizieren soll.

Geben Sie zur Verwendung von Suite B für die Kommunikation `true` an. Diese Kommunikation wird nur unter dem TLS 1.2-Protokoll unterstützt.

Wenn Sie versuchen, eine Suite B-aktivierte Engine mit einem Remote Loader zu verbinden, der TLSv1.2 nicht unterstützt, wird der Handshake nicht ausgeführt und die Kommunikation wird nicht aufgebaut. Beispiel: Remote Loader 4.5.3, der TLS v1.2 nicht unterstützt.

useMutualAuth=*true/false*

(Bedingt) Trifft nur zu, wenn sich der Remote Loader und die Identity Manager-Engine gegenseitig authentifizieren sollen, indem sie das Zertifikat mit öffentlichem Schlüssel oder das digitale Zertifikat von der verbürgten Zertifizierungsstelle oder die eigensignierten Zertifikate überprüfen. Beispiel:

```
useMutualAuth=true
```

keystore=*Dateiname*

Gibt den Dateinamen des Java-Keystores an, der das Herkunftsverbürgungszertifikat des Herausgebers des Zertifikats enthält, das vom Remote-Schnittstellenmodul verwendet wird. Beispiel:

```
keystore=keystore filename
```

In der Regel geben Sie die Zertifizierungsstelle des Baums an, der das Remote-Schnittstellenmodul hostet.

kmo=*Name*

Gibt den Schlüsselnamen des Schlüsselmaterialobjekts (KMO) ein, das die für SSL-Verbindungen verwendeten Schlüssel und Zertifikate enthält. Beispiel:

```
kmo=remote driver cert
```

localaddress=*IP_Adresse*

Gibt die IP-Adresse an, an die der Socket für die Clientverbindung gebunden werden soll. Beispiel:

```
localaddress=198.51.100.0
```

port=*Port-Nummer*

Gibt den TCP/IP-Port an, den der Remote Loader auf Verbindungen vom Remote-Schnittstellenmodul überwacht. Mit `port=8090` legen Sie den Standardport fest.

rootfile=*Dateiname_Herkunftsverbürgungszertifikat*

Gibt den Namen der Datei an, die das Herkunftsverbürgungszertifikat des Herausgebers des Zertifikats für das Remote-Schnittstellenmodul enthält. Die Zertifikatsdatei muss im Base-64-Format (PEM) vorliegen. Beispiel:

```
rootfile=trustedcert
```

In der Regel ist die Datei die Zertifizierungsstelle des Baums, der das Remote-Schnittstellenmodul hostet.

storepass=*Passwort*

Gibt das Passwort für den Java-Keystore an, den Sie im Parameter `keystore` festgelegt haben. Beispiel:

```
storepass=mypassword
```

Geben Sie für die Kommunikation zwischen dem Remote Loader und dem Java-Treiber ein Schlüsselwertpaar mit der folgenden Syntax an:

```
keystore=keystorename storepass=password
```

-datadir *Verzeichnis* (-dd *Verzeichnis*)

Gibt das Verzeichnis für die Datendateien an, die von Remote Loader verwendet werden. Beispiel:

```
-datadir /var/opt/novell/dirxml/rdxml/data
```

Mit diesem Befehl übernimmt der `rdxml`-Prozess das angegebene Verzeichnis als aktuelles Verzeichnis. In diesem Datenverzeichnis werden Trace-Dateien und andere Dateien, für die kein expliziter Pfad angegeben ist, erstellt.

-help (-h)

Weist die Anwendung an, die Hilfe anzuzeigen.

-java (-j)

(Bedingt) Gibt an, dass Sie Passwörter für ein Java-Treiberschnittstellenmodul festlegen möchten.

HINWEIS: Verwenden Sie diese Option zusammen mit der Option `-setpasswords`, wenn Sie nicht auch einen Wert für `-class` angeben.

-javadebugport *Port-Nummer* (-jdp *Port-Nummer*)

Weist die Instanz an, das Java-Debugging auf dem angegebenen Port zu aktivieren. Beispiel:

```
-javadebugport 8080
```

Nutzen Sie diesen Befehl beim Entwickeln von Identity Manager-Anwendungsschnittstellenmodulen. Sie können diesen Befehl senden, während der Remote Loader läuft.

-javaparam *Parameter* (-jp *Parameter*)

Gibt die Parameter für die Java-Umgebung an. Geben Sie die Java-Umgebungsparameter mit der folgenden Syntax ein:

```
-javaparam parameter
-jp parameter
-jp parameter
```

HINWEIS: Verwenden Sie diesen Parameter nicht mit dem Java Remote Loader.

Sollen mehrere Werte für einen einzelnen Parameter angegeben werden, schließen Sie die Parameter in Anführungszeichen ein. Beispiel:

```
-javaparam DHOST_JVM_MAX_HEAP=512M
-jp DHOST_JVM_MAX_HEAP=512M
-jp "DHOST_JVM_OPTIONS=-Dfile.encoding=utf-8 -Duser.language=en"
```

Mit den folgenden Parametern richten Sie die Java-Umgebung ein:

DHOST_JVM_ADD_CLASSPATH

Gibt weitere Pfade an, in denen die JVM nach Paket- (`.jar`) und Klassendateien (`.class`) suchen soll. Sollen mehrere Klassenpfade für eine Linux-JVM angegeben werden, trennen Sie die einzelnen Pfade jeweils mit Kommas voneinander ab.

DHOST_JVM_INITIAL_HEAP

Gibt die anfängliche (minimale) JVM-Heap-Größe in Dezimalschreibweise in Byte an. Geben Sie einen numerischen Wert gefolgt von „G“, „M“ oder „K“ für den Byte-Typ ein. Beispiel:

```
100M
```

Wenn Sie keinen Byte-Typ angeben, wird die Größe standardmäßig in Byte dargestellt. Dieser Parameter entspricht dem Java-Befehl `-Xms`.

Dieser Parameter hat Vorrang vor der Option zum Festlegen der Attribute im Treiber. Durch das Erhöhen der Ausgangs-Heap-Größe können die Startzeit und die Durchsatzleistung verbessert werden.

DHOST_JVM_MAX_HEAP

Gibt die maximale JVM-Heap-Größe in Dezimalschreibweise in Byte an. Geben Sie einen numerischen Wert gefolgt von „G“, „M“ oder „K“ für den Byte-Typ ein. Beispiel:

```
100M
```

Wenn Sie keinen Byte-Typ angeben, wird die Größe standardmäßig in Byte dargestellt.

Dieser Parameter hat Vorrang vor der Option zum Festlegen der Attribute im Treiber.

DHOST_JVM_OPTIONS

Gibt die Argumente an, die beim Starten der JVM-Instanz des Treibers verwendet werden sollen. Trennen Sie die Optionszeichenfolgen jeweils mit Leerzeichen voneinander ab. Beispiel:

```
-Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000
```

Die Option zum Festlegen der Attribute im Treiber hat Vorrang vor diesem Parameter. Diese Umgebungsvariable wird an das Ende der Option zum Festlegen der Attribute im Treiber angehängt. Weitere Informationen zu gültigen Optionen finden Sie in der JVM-Dokumentation.

-password *Wert* (-p *Wert*)

Gibt das Passwort für die Treiberinstanz an, wenn Sie Befehle eingeben, die die Einstellungen ändern oder sich auf die Funktionsweise der Instanz auswirken. Sie müssen dasselbe Passwort als erstes Passwort mit „setpasswords“ für die Instanz festlegen, für das die Befehle eingegeben werden sollen. Beispiel:

```
-password netiq4
```

Wenn Sie das Passwort beim Eingeben der Befehle nicht mitsenden, werden Sie durch die Instanz dazu aufgefordert, das Passwort einzugeben.

Sie können diesen Befehl senden, während der Remote Loader läuft.

-piddir *Verzeichnis* (-pd *Verzeichnis*)

Gibt den Pfad zum Verzeichnis für die Prozess-ID-Datei (PID-Datei) an, die im Remote Loader-Prozess verwendet wird. Beispiel:

```
-piddir /var/opt/novell/dirxml/rdxml/data
```

Die PID-Datei ist vorrangig für init-Skripte im SysV-Stil vorgesehen. Der Standardwert lautet `/var/run`. Alternativ entspricht der Standardwert dem aktuellen Verzeichnis, wenn der Remote Loader von einem Benutzer ausgeführt wird, der nicht über ausreichende Rechte zum Öffnen der PID-Datei zum Lesen und Schreiben in `/var/run` verfügt.

Dieser Parameter ist mit dem Parameter `-datadir` vergleichbar.

-setpasswords *Remote_Loader_Passwort Optionales_Passwort* (-sp *Remote_Loader_Passwort Optionales_Passwort*)

Gibt das Passwort für die Treiberinstanz und das Passwort für das Identity Manager-Treiberobjekt des Remote-Schnittstellenmoduls an, mit dem der Remote Loader kommuniziert.

Sie müssen kein Passwort angeben. In diesem Fall werden Sie vom Remote Loader aufgefordert, die Passwörter einzugeben. Wenn Sie jedoch das Passwort für den Remote Loader angeben, müssen Sie auch das Passwort für das Identity Manager-Treiberobjekt nennen, das mit dem Remote-Schnittstellenmodul auf dem Server der Identity Manager-Engine verbunden ist. Geben Sie die Passwörter mit der folgenden Syntax an:

```
-setpasswords Remote_Loader_password driver_object_password
```

Beispiel:

```
-setpasswords netiq4 idmobject6
```

HINWEIS: Mithilfe dieser Option wird die Treiberinstanz mit den angegebenen Passwörtern konfiguriert. Es wird jedoch weder ein Identity Manager-Anwendungsschnittstellenmodul geladen noch mit anderen Instanzen kommuniziert.

Einstellungen für die Trace-Datei

(Bedingt) Gibt beim Hosten eines Identity Manager-Anwendungsschnittstellenmoduls die Einstellungen für eine Trace-Datei an, in der sich Informationsmeldungen vom Remote Loader und vom Treiber für diese Instanz befinden.

Fügen Sie der Konfigurationsdatei die folgenden Parameter hinzu:

-trace *Ganzzahl* (-t *Ganzzahl*)

Gibt die Stufen der Meldungen an, die in einem Trace-Fenster angezeigt werden sollen. Beispiel:

```
-trace 3
```

Die Trace-Stufen für den Remote Loader sind mit den Stufen identisch, die auf dem Server verwendet werden, auf dem die Identity Manager-Engine gehostet wird.

-tracefile *Dateipfad* (-tf *Dateipfad*)

Gibt den Pfad zu einer Datei an, in der die Trace-Meldungen protokolliert werden sollen. Für jede Treiberinstanz auf einem Computer müssen Sie eine eindeutige Trace-Datei festlegen. Beispiel:

```
-tracefile /home/trace.txt
```

Die Anwendung schreibt Meldungen in die Datei, wenn der Parameter `-trace`größer als null ist. Die Meldungen werden auch dann in die Datei geschrieben, wenn das Trace-Fenster nicht geöffnet ist.

-tracefilemax *Größe* (-tf *Größe*)

Gibt die maximale Größe der Trace-Datei für diese Instanz an. Legen Sie den Wert in Kilobyte, Megabyte oder Gigabyte fest, und nennen Sie auch die Abkürzung für den Byte-Typ. Beispiel:

- `-tracefilemax 1000K`
- `-tf 100M`
- `-tf 10G`

HINWEIS

- Wenn die Trace-Datei beim Starten des Remote Loader größer als das angegebene Maximum ist, dann behält die Trace-Datei diese Größe bei, bis das Rollover über alle 10 Dateien ausgeführt wurde.
- Wenn Sie diese Option in die Konfigurationsdatei aufnehmen, nutzt die Anwendung den angegebenen Namen für die Trace-Datei, und es werden bis zu 9 „Rollover"-Dateien eingeschlossen. Der Name der Rollover-Dateien wird aus dem Namen der Haupt-Trace-Datei und dem Suffix _n zusammengesetzt, wobei 1 bis 9 gültige Werte für n sind.

-tracechange *Ganzzahl* (-tc *Ganzzahl*)

(Bedingt) Wenn bereits eine Treiberinstanz vorhanden ist, die ein Anwendungsschnittstellenmodul hostet: Gibt eine neue Stufe für Informationsmeldungen an. Die Trace-Stufen entsprechen den auf dem Identity Manager-Server verwendeten Trace-Stufen. Beispiel:

```
-trace 3
```

Sie können diesen Befehl senden, während der Remote Loader läuft.

-tracefilechange *Dateipfad* (-tfc *Dateipfad*)

(Bedingt) Wenn bereits eine Treiberinstanz vorhanden ist, die ein Anwendungsschnittstellenmodul hostet: Weist diese Instanz an, eine Trace-Datei zu verwenden bzw. die bisher genutzte Datei zu schließen und zu dieser neuen Datei zu wechseln. Beispiel:

```
-tracefilechange \temp\newtrace.txt
```

Sie können diesen Befehl senden, während der Remote Loader läuft.

Zertifikatpasswort-Einstellungen

(Bedingt) Nur wenn `useMutualAuth` in der Konfigurationsdatei als wahr festgelegt wurde.

-keystorepassword (-ksp)

Hiermit wird das Keystore-Passwort festgelegt, mit dem ausschließlich die gegenseitige Authentifizierung für Java Remote Loader-Treiber aktiviert wird.

-keypassword (-kp)

Hiermit wird das Schlüsselpasswort festgelegt, mit dem ausschließlich die gegenseitige Authentifizierung für Java und native Remote Loader-Treiber aktiviert wird.

-unload (-u)

Weist die Treiberinstanz an, sich zu entladen. Wenn der Remote Loader als Win32-Dienst ausgeführt wird, wird der Dienst durch diese Option gestoppt.

Sie können diesen Befehl senden, während der Remote Loader läuft.

Erläuterungen zu den Namen für den Java-Parameter -class

Wenn Sie mit dem Parameter eine Treiberinstanz `-class` für den Remote Loader und den Java Remote Loader konfigurieren, müssen Sie den Java-Klassennamen für das zu hostende Identity Manager-Anwendungsschnittstellenmodul angeben.

Java-Klassenname	Treiber
com.novell.nds.dirxml.driver.dcsshim.DCSShim	Treiber für den Datenerfassungsdienst

Java-Klassenname	Treiber
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	Treiber für Text mit Begrenzungszeichen
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	Treiber für Remedy ARS
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	Berechtigungs-Service-Treiber
com.novell.gw.dirxml.driver.rest.shim.GWdriverShim	GroupWise 2014-Treiber
com.novell.idm.drivers.idprovider.IDProviderShim	ID-Provider-Treiber
com.novell.nds.dirxml.driver.jdbc.JDBCDriverShim	JDBC-Treiber
com.novell.nds.dirxml.driver.jms.JMSDriverShim	JMS-Treiber
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	LDAP-Treiber
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	Loopback-Treiber
com.novell.nds.dirxml.driver.ebs.user.EBSUserDriver	Treiber für die Oracle-Benutzerverwaltung
com.novell.nds.dirxml.driver.ebs.hr.EBSHRDriver	Oracle HR-Treiber
com.novell.nds.dirxml.driver.ebs.tca.EBSTCADriver	Oracle TCA-Treiber
com.novell.nds.dirxml.driver.msgateway.MSGatewayDriverShim	Treiber „Verwaltetes System – Gateway“
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	Treiber für manuelle Aufgaben
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	NIS-Treiber
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes-Treiber
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft-Treiber
com.netiq.nds.dirxml.driver.pum.PUMDriverShim	Treiber für Privileged User Management
com.novell.nds.dirxml.driver.salesforce.SFDriverShim	SalesForce-Treiber
com.novell.nds.dirxml.driver.SAPHRShim.SAPDriverShim	SAP HR-Treiber
com.novell.nds.dirxml.driver.sap.portal.SAPPortalShim	SAP Portal-Treiber
com.novell.nds.dirxml.driver.sapumshim.SAPDriverShim	Treiber für die SAP-Benutzerverwaltung
com.novell.nds.dirxml.driver.soap.SOAPDriver	SOAP-Treiber
com.novell.idm.driver.ComposerDriverShim	Benutzeranwendung
com.novell.nds.dirxml.driver.workorder.WorkOrderDriverShim	WorkOrder-Treiber

11.3.3 Konfigurieren des Remote Loader für Treiberinstanzen

Der Remote Loader kann die in den `.dll-`, `.so-` oder `.jar`-Dateien enthaltenen Identity Manager-Anwendungsschnittstellenmodule hosten. Damit der Remote Loader auf einem Linux-Computer ausgeführt werden kann, benötigt die Anwendung je eine Konfigurationsdatei (z.–B. `LDAPShim.txt`) für die einzelnen Treiberinstanzen. Konfigurationsdateien können auch mithilfe von Befehlszeilenoptionen erstellt und bearbeitet werden.

Standardmäßig stellt der Remote Loader über TCP/IP mit den TLS/SSL-Protokollen eine Verbindung zur Identity Manager-Engine her. Der standardmäßige TCP/IP-Port für diese Verbindung ist 8090. Mit dem Remote Loader können Sie mehrere Instanzen auf einem einzigen Server ausführen. Jede Instanz hostet eine separate Anwendungsschnittstellenmodulinstanz des Identity Manager. Sollen mehrere Remote Loader-Instanzen auf einem einzigen Server verwendet werden, geben Sie für jede Instanz jeweils unterschiedliche Verbindungs- und Befehlsports an.

HINWEIS

- Die Konfigurationsdatei kann bis auf `-config` beliebige Befehlszeilenoptionen enthalten.
- Die Parameter können wahlweise in der Langform oder in der Kurzform in die Konfigurationsdatei eingetragen werden. Beispiel: `-description` oder `-desc`.
- Im nachfolgenden Verfahren wird zunächst die Langform angegeben und dann die Kurzform in Klammern. Beispiel: `-description` *`Wert`* `(-desc` *`Wert`*`)`.
- Weitere Informationen zu den Parametern in diesem Abschnitt finden Sie unter „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 122.

So erstellen Sie eine Konfigurationsdatei:

1. Erstellen Sie in einem Texteditor eine neue Datei.

   Die Beispieldatei `config8000.txt` von NetIQ hilft Ihnen dabei, den Remote Loader und die Treiber für das Anwendungsschnittstellenmodul zu konfigurieren. Die Beispieldatei befindet sich standardmäßig im Verzeichnis `/opt/novell/dirxml/doc/`.

2. Fügen Sie der Datei die folgenden Konfigurationsparameter hinzu:
   - -description (optional)
   - -commandport
   - Verbindungsparameter:
     - port (obligatorisch)
     - Adresse
     - fromaddress
     - handshaketimeout
     - Rootfile
     - Keystore
     - localaddress
     - Hostname
     - kmo
     - secureprotocol
     - enforceSuiteB
     - useMutualAuth

- Trace-Dateiparameter (optional):
  - -trace
  - -tracefile
  - -tracefilemax
- -javaparam
- -class oder -module

Weitere Informationen zum Festlegen von Werten für diese Parameter finden Sie in Abschnitt 11.3.2, „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 122.

3 Speichern Sie die Datei.

Damit der Remote Loader beim Hochfahren des Computers automatisch gestartet wird, speichern Sie die Datei im Verzeichnis `/etc/opt/novell/dirxml/rdxml`.

11.3.4 Konfigurieren des Java Remote Loader für Treiberinstanzen

Der Java Remote Loader hostet nur Java-Treiberschnittstellenmodule. Das Laden oder Hosten nativer (C++-)Treiberschnittstellenmodule ist nicht möglich.

Konfigurieren Sie mit den nachfolgenden Schritten eine neue Instanz für den Java Remote Loader auf Linux-Plattformen. Weitere Informationen zu den Parametern in diesem Abschnitt finden Sie unter „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 122.

1 Erstellen Sie in einem Texteditor eine neue Datei.

Die Beispieldatei `config8000.txt` von NetIQ hilft Ihnen dabei, den Remote Loader und die Treiber für das Anwendungsschnittstellenmodul zu konfigurieren. Die Beispieldatei befindet sich standardmäßig im Verzeichnis `/opt/novell/dirxml/doc/`.

2 Fügen Sie der neuen Konfigurationsdatei die folgenden Parameter hinzu:
  - -description (optional)
  - -class oder -module

    Beispiel: `-class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim`
  - -commandport
  - Verbindungsparameter:
    - port (obligatorisch)
    - Adresse
    - fromaddress
    - handshaketimeout
    - Rootfile
    - Keystore
    - localaddress
    - Hostname
    - kmo
    - secureprotocol
    - enforceSuiteB
    - useMutualAuth
  - -java (bedingt)

- -javadebugport
- -password
- -service
- -keypassword
- -keystorepassword (nur für Java-Treiber)
- Trace-Dateiparameter (optional):
  - -trace
  - -tracefile
  - -tracefilemax

3 Speichern Sie die neue Konfigurationsdatei.

Damit der Remote Loader beim Hochfahren des Computers automatisch gestartet wird, speichern Sie die Datei im Verzeichnis `/etc/opt/novell/dirxml/jremote`.

4 Öffnen Sie eine Befehlszeilen-Eingabeaufforderung.

5 Geben Sie an der Eingabeaufforderung Folgendes ein: `-config` *`Dateiname`*. Hierbei gilt: *Dateiname* bezeichnet den Namen der neuen Konfigurationsdatei. Beispiel:

```
dirxml_jremote -config filename
```

11.3.5 Konfigurieren von Identity Manager-Treibern für die Verwendung mit dem Remote Loader

Sie können einen neuen Treiber konfigurieren oder einen vorhandenen Treiber für die Kommunikation mit dem Remote Loader aktivieren. Sie müssen ein Identity Manager-Anwendungsschnittstellenmodul für die Verwendung mit dem Remote Loader konfigurieren.

HINWEIS: In diesem Abschnitt erhalten Sie allgemeine Informationen darüber, wie Sie Treiber für die Kommunikation mit dem Remote Loader konfigurieren. Treiberspezifische Informationen finden Sie im relevanten Treiberimplementierungshandbuch auf der Website der Identity Manager-Treiberdokumentation.

Zum Hinzufügen eines neuen Treiberobjekts bzw. zum Bearbeiten eines vorhandenen Treiberobjekts in Designer oder iManager müssen Sie Einstellungen konfigurieren, mit denen die Treiberinstanz für den Remote Loader aktiviert wird. Weitere Informationen zu den Parametern in diesem Abschnitt finden Sie unter „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 122.

1 Wählen Sie unter **Überblick** das gewünschte Identity Manager-Treiberobjekt aus.

2 Führen Sie in den Eigenschaften des Treiberobjekts die folgenden Schritte aus:

2a Aktivieren Sie unter **Treibermodul** die Option **Verbindung zu Remote Loader aufbauen**.

2b Geben Sie unter **Treiberobjektpasswort** das Passwort ein, mit dem sich der Remote Loader beim Server der Identity Manager-Engine authentifiziert.

Dieses Passwort muss mit dem Passwort übereinstimmen, das im Remote Loader für das Treiberobjekt definiert ist.

2c Geben Sie unter **Verbindungsparameter für Remote Loader** die erforderlichen Informationen zum Herstellen der Verbindung zum Remote Loader an. Verwenden Sie die folgende Syntax:

```
hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename
localaddress=xxx.xxx.xxx.xxx
```

Hierbei gilt:

Hostname

Gibt die IP-Adresse des Servers an, auf dem der Remote Loader gehostet wird. Beispiel: `hostname=192.168.0.1`.

port

Gibt den Port an, den der Remote Loader überwacht. Der Standardwert ist 8090.

kmo

Gibt den Schlüsselnamen des Schlüsselmaterialobjekts (KMO) ein, das die für SSL-Verbindungen verwendeten Schlüssel und Zertifikate enthält. Beispiel: `kmo=remotecert`.

localaddress

Gibt die Quell-IP-Adresse an, falls mehrere IP-Adressen auf dem Server konfiguriert sind, auf dem die Identity Manager-Engine gehostet wird.

2d Geben Sie unter **Remote Loader-Passwort** das Passwort an, mit dem sich die Identity Manager-Engine (oder das Remote Loader-Schnittstellenmodul) beim Remote Loader authentifiziert.

3 Definieren Sie einen sicherheitsäquivalenten Benutzer.

4 Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

11.3.6 Konfigurieren der beiderseitigen Authentifizierung mit der Identity Manager-Engine

Sie können die beiderseitige Authentifizierung konfigurieren, um die sichere Kommunikation zwischen dem Remote Loader und der Identity Manager-Engine sicherzustellen. Die beiderseitige Authentifizierung verwendet für den Handshake Zertifikate anstatt von Passwörtern. Der Remote Loader und die Identity Manager-Engine authentifizieren sich gegenseitig, indem sie das Zertifikat mit öffentlichem Schlüssel oder das digitale Zertifikat von der verbürgten Zertifizierungsstelle oder die eigensignierten Zertifikate austauschen und überprüfen. Wenn die beiderseitige Authentifizierung erfolgreich ist, authentifiziert sich der Remote Loader bei der Engine. Synchronisierungsdatenverkehr findet statt, nachdem sowohl der Remote Loader als auch die Identity Manager-Engine sicher sind, dass sie mit einer autorisierten Entität kommunizieren.

Führen Sie zum Konfigurieren der beiderseitigen Authentifizierung die folgenden Aufgaben aus:

- „Exportieren der Zertifikate für die Identity Manager Engine und den Remote Loader“, auf Seite 135
- „Aktivieren eines Treibers für die beiderseitige Authentifizierung“, auf Seite 137

Exportieren der Zertifikate für die Identity Manager Engine und den Remote Loader

Damit die beiderseitige Authentifizierung ordnungsgemäß funktioniert, brauchen Sie ein Serverzertifikat für die Engine und ein Client-Zertifikat für den Remote Loader. Sie können die Zertifikate von eDirectory exportieren oder sie von einem Drittanbieter importieren. In den meisten Fällen exportieren Sie ein Serverzertifikat von eDirectory ohne zusätzliche Kosten. In einigen Fällen möchten Sie möglicherweise ein Drittanbieter-Client-Zertifikat für den Remote Loader exportieren.

- „Exportieren eines Zertifikats von eDirectory“, auf Seite 135
- „Exportieren eines Drittanbieter-Zertifikats für Remote Loader“, auf Seite 137

Exportieren eines Zertifikats von eDirectory

Ein Zertifikatsobjekt im Identitätsdepot wird KMO (Key Material Object) genannt. Dieses Objekt enthält sowohl die Zertifikatsdaten einschließlich des öffentlichen Schlüssels und den privaten Schlüssel, der mit dem für SSL-Verbindungen verwendeten Zertifikat verknüpft ist. Für die beiderseitige Authentifizierung benötigen Sie zwei KMOs , jeweils eines für die Engine und eines für den Remote Loader.

Sie können ein vorhandenes KMO exportieren oder ein neues KMO erstellen und es dann exportieren. Die Abläufe beim Erstellen eines Client-KMO und eines Server-KMO sind nicht identisch.

Erstellen von KMOs

So erstellen Sie ein Server-KMO:

1. Melden Sie sich bei NetIQ iManager an.
2. Klicken Sie im linken Bereich auf **NetIQ-Zertifikatserver** und wählen Sie das Serverzertifikat aus.
3. Wählen Sie den Server aus, der als Eigentümer für das erstellte Zertifikat fungieren soll.
4. Geben Sie einen Kurznamen für das Zertifikat ein. Beispiel: `serverkmo`.
5. Wählen Sie für die Zertifikaterstellungsmethode die Option **Standard** und klicken Sie auf **Weiter**.
6. Überprüfen Sie die Zusammenfassung, klicken Sie auf **Fertig stellen** und anschließend auf **Schließen**.

So erstellen Sie ein Client-KMO:

1. Melden Sie sich bei NetIQ iManager an.
2. Klicken Sie im linken Bereich auf **NetIQ-Zertifikatserver** und wählen Sie das Serverzertifikat aus.
3. Wählen Sie den Server aus, der als Eigentümer für das erstellte Zertifikat fungieren soll.
4. Geben Sie einen Kurznamen für das Zertifikat ein. Beispiel: `clientkmo`
5. Wählen Sie für die Zertifikaterstellungsmethode die Option **Benutzerdefiniert** und klicken Sie auf **Weiter**.
6. Behalten Sie die standardmäßige **Organisations-Zertifizierungsstelle** unverändert bei und klicken Sie auf **Weiter**.
7. Deaktivieren Sie die Option **Erweiterte Schlüsselnutzung aktivieren** und klicken Sie auf **Weiter**.
8. Übernehmen Sie die restlichen Standardeinstellungen für das Zertifikat.
9. Überprüfen Sie die Zusammenfassung, klicken Sie auf **Fertig stellen** und anschließend auf **Schließen**.

Exportieren von KMOs

Exportieren Sie die KMOs aus eDirectory, die die Engine und der Remote Loader zur gegenseitigen Authentifizierung verwenden.

Führen Sie zum Exportieren des KMO für die Identity Manager-Engine das DirXML-Befehlszeilen-Dienstprogramm (dxcmd) aus:

```
dxcmd -user <admin DN> -password <password of admin> -exportcerts <kmoname>
<server|client> <java|native|dotnet> <output dir>
```

Hierbei gilt:

- `user` gibt den Namen eines Benutzers mit Verwaltungsrechten für den Treiber an.
- `password` gibt das Passwort des Benutzers mit Verwaltungsrechten für den Treiber an.
- `exportcerts` exportiert die Zertifikate und privaten/öffentlichen Schlüssel von eDirectory. Sie müssen angeben, ob Sie ein Server- oder Client-Zertifikat exportieren, welcher Treibertyp das Zertifikat verwendet und in welchem Zielordner der Befehl diese Informationen speichert.

Beispiel: `dxcmd -user admin.sa.system -password novell -exportcerts serverkmo server java '/home/certs'`

Dieser Befehl generiert die Datei `serverkmo_server.ks` im Verzeichnis `/home/certs/`. Das Standardpasswort für den Keystore lautet `dirxml`.

Bei der Ausführung des dxcmd-Befehls zum Exportieren des KMO für den Remote Loader gelten die folgenden Überlegungen:

- Das dxcmd-Dienstprogramm wird im LDAP-Modus ausgeführt. Wenn Sie es zum ersten Mal verwenden, werden Sie aufgefordert, anzugeben, in welcher Weise Sie dem Zertifikat von eDirectory vertrauen möchten. Abhängig von Ihrer Umgebung wählen Sie, dass Sie dem Zertifikat nur für die aktuelle Sitzung oder für die aktuelle und zukünftige Sitzung vertrauen oder dass Sie allen Zertifikaten vertrauen. Sie können auch auswählen, dass dem Zertifikat nicht vertraut werden soll.
- Führen Sie den Befehl entweder im LDAP-Format oder im DOT-Format aus, wenn der Remote Loader auf dem Identity Manager-Server ausgeführt wird. Führen Sie den Befehl nur im LDAP-Format aus, wenn der Remote Loader auf einem separaten Server installiert ist.
- Geben Sie den `-host`-Parameter im Befehl an, um die Server-IP-Adresse oder den Hostnamen aufzulösen und sich beim Identity Manager-Server zu authentifizieren.

Führen Sie den Befehl mit der folgenden Syntax aus:

```
dxcmd -dnform ldap -host <IP-Adresse des Hosts> -user <Administrator-DN> -password
<Passwort des Administrators> -exportcerts <KMO-Name> <Client>
<java|native|dotnet> <Ausgabeverzeichnis>
```

Tabelle 11-1 Beispiele für verschiedene Treibertypen

Treibertyp	Befehl	Ausgabe
Java-Treiber	`dxcmd -dnform ldap -host 192.168.0.1 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client java '/home/certs'`	Datei `clientkmo_client.ks` im Verzeichnis `/home/certs/` Das Standardpasswort für den Keystore lautet `dirxml`.

Exportieren eines Drittanbieter-Zertifikats für Remote Loader

Zur Verwendung von Drittanbieter-Zertifikaten mit dem Remote Loader müssen Sie ein Zertifikat in die `PFX`-Datei exportieren sowie eine Herkunftsverbürgungsdatei im Base 64-Format und anschließend das `PFX`-Zertifikat in das Format konvertieren, das der Treiber verwendet. Beispiel: Ein nativer Treiber benötigt den privaten Schlüssel und den Zertifikatsschlüssel im `PEM`-Format, während ein Java-Treiber den Keystore im `JKS`-Format benötigt.

Java-Treiber

Erstellen Sie einen Java-Keystore aus der `PFX`-Datei. Geben Sie einen Befehl ein, beispielsweise `keytool -importkeystore -srckeystore servercert.pfx -srcstoretype pkcs12 -destkeystore servercert.jks -deststoretype JKS`.

Geben Sie im letzten Schritt abhängig vom Treibertyp die Informationen in der Konfigurationsdatei für den Remote Loader an. Weitere Informationen finden Sie unter Aktivieren eines Treibers für die beiderseitige Authentifizierung.

Aktivieren eines Treibers für die beiderseitige Authentifizierung

Sie aktivieren eine Treiberkommunikation für die beiderseitige Authentifizierung, indem Sie die folgenden Aufgaben ausführen:

- „Konfigurieren eines Treibers mit KMO oder Keystore“, auf Seite 137
- „Konfigurieren des Remote Loader für Treiberinstanzen“, auf Seite 139

Konfigurieren eines Treibers mit KMO oder Keystore

Sie haben die Möglichkeit, den Treiber mit KMO oder Keystore in Designer oder iManager zu konfigurieren.

In Designer wird der Treiber im ersten Treibererstellungsvorgang oder nach Erstellung des Treibers konfiguriert.

So konfigurieren Sie einen Treiber in Designer:

1. Öffnen Sie Ihr Projekt in Designer.
2. Wählen Sie in der Palette der Ansicht "Modellierer" den zu erstellenden Treiber aus.
3. Ziehen Sie das Symbol für den Treiber auf die Ansicht "Modellierer".
4. Befolgen Sie die Anweisungen im Installationsassistenten.

5 Wählen Sie im Remote Loader-Fenster die Option **Ja**.

5a **Hostname:** Geben Sie den Hostnamen oder die IP-Adresse des Servers an, auf dem der Remote Loader-Service ausgeführt wird. Beispiel: Geben Sie hostname=192.168.0.1 ein. Wenn Sie für diesen Parameter keinen Wert angeben, wird standardmäßig der Wert "localhost" verwendet.

5b **Port:** Geben Sie die Nummer des Ports an, an dem der Remote Loader installiert ist und für diesen Treiber ausgeführt wird. Die Standard-Port-Nummer lautet 8090.

5c **KMO:** Geben Sie den Schlüsselnamen des KMO an, das die Schlüssel und das Zertifikat enthält, die der Remote Loader für eine SSL-Verbindung verwendet. Beispiel: Geben Sie kmo=`serverkmo` ein. Wenn Sie die beiderseitige Authentifizierung mit KMO konfigurieren, müssen Sie einen Wert für diesen Parameter angeben. Außerdem müssen Sie einen Wert für den Parameter **Stammdatei** unter „Andere Parameter“ angeben.

5d **Andere Parameter:** Legen Sie die Einstellungen für den zu verwendenden Remote Loader fest. In diesem Parameter fügen Sie Informationen zur Kommunikation bei der beiderseitigen Authentifizierung hinzu. Die festgelegten Parameter müssen das folgende Schlüsselwertformat aufweisen: `paraName1=paraValue1 paraName2=paraValue2`

Verwenden Sie beispielsweise das folgende Format für Keystore:

```
UseMutualAuth=true keystore='/home/certs/serverkmo_server.ks'
storepass='dirxml' keypass='dirxml' key='serverkmo'
```

Verwenden Sie beispielsweise die folgende Syntax für KMO:

```
useMutualAuth=true rootFile='/home/cacert.b64'
```

5e **Remote-Passwort:** Legen Sie das Remote Loader-Passwort fest.

5f **Treiberpasswort:** Geben Sie das Treiberpasswort an.

6 Klicken Sie auf **Weiter**.

7 Befolgen Sie die restlichen Anweisungen im Assistenten, bis die Installation des Treibers abgeschlossen ist.

8 Sehen Sie sich die Zusammenfassung der Aufgaben an, die zur Erstellung des Treibers ausgeführt werden. Klicken Sie anschließend auf **Fertig stellen**.

Alternativ wird der Treiber nach seiner Erstellung konfiguriert. Führen Sie dazu die folgenden Schritte durch:

1 Klicken Sie in der Ansicht "Gliederung" in Designer mit der rechten Maustaste auf den Treiber.

2 Wählen Sie **Eigenschaften** aus.

3 Wählen Sie im Navigationsbereich die Option **Treiberkonfiguration** aus.

4 Wählen Sie **Authentifizierung** aus.

5 Geben Sie im Abschnitt **Remote Loader-Authentifizierung** die Informationen an, die zur Konfiguration der beiderseitigen Authentifizierung zwischen dem Remote Loader und der Identity Manager-Engine erforderlich sind.

Verwenden Sie die folgende Syntax für KMO:

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true kmo=certificatename
rootFile=<absolute path to the file>
```

Beispiel:

```
hostname=192.168.0.1 port=8090 useMutualAuth=true kmo=serverkmo rootFile='/
home/cacert.b64'
```

Verwenden Sie die folgende Syntax für Keystore:

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true keystore=<absolute path
to the keystore file> storepass=<keystore password> key=<alias name> keypass=
<password for the key>
```

Beispiel:

```
hostname=192.168.0.1 port=8097 useMutualAuth=true keystore='/home/certs/
serverkmo_server.ks' storepass='dirxml' key='serverkmo' keypass='dirxml'
```

So bearbeiten Sie die Konfiguration in iManager:

1. Starten Sie iManager.
2. Wählen Sie unter Überblick das gewünschte Identity Manager-Treiberobjekt aus.
3. Führen Sie in den Eigenschaften des Treiberobjekts die folgenden Schritte aus:
   - **3a** Aktivieren Sie unter **Treibermodul** die Option **Verbindung zu Remote Loader aufbauen**.
   - **3b** Geben Sie unter **Treiberobjektpasswort** das Passwort ein, mit dem sich der Remote Loader bei der Engine authentifiziert.

     Dieses Passwort muss mit dem Passwort übereinstimmen, das im Remote Loader für das Treiberobjekt definiert ist.
   - **3c** Geben Sie unter **Verbindungsparameter für Remote Loader** die erforderlichen Informationen zum Herstellen der Verbindung zum Remote Loader an.

     Verwenden Sie die folgende Syntax für KMO:

     ```
     hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true kmo=certificatename
     rootFile=<absolute path to the file>
     ```

     Beispiel:

     ```
     hostname=192.168.0.1 port=8090 useMutualAuth=true kmo=serverkmo rootFile='/
     home/cacert.b64'
     ```

     Verwenden Sie die folgende Syntax für Keystore:

     ```
     hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true keystore=<absolute
     path to the keystore file> storepass=<keystore password> key=<alias name>
     keypass= <password for the key>
     ```

     Beispiel:

     ```
     hostname=192.168.0.1 port=8097 useMutualAuth=true keystore='/home/certs/
     serverkmo_server.ks' storepass='dirxml' key='serverkmo' keypass='dirxml'
     ```
   - **3d** (Optional) Geben Sie unter **Remote Loader-Passwort** das Passwort an, mit dem sich die Identity Manager-Engine (oder das Remote Loader-Schnittstellenmodul) beim Remote Loader authentifiziert.
   - **3e** Klicken Sie auf **Anwenden** und dann auf **OK**.

Konfigurieren des Remote Loader für Treiberinstanzen

Sie müssen die Treiberinstanz in der Remote Loader-Konfigurationsdatei konfigurieren. Geben Sie unbedingt den absoluten Pfad zu dem Verzeichnis, in dem die Schlüsseldatei, die Zertifikatsdatei und die Stammdatei gespeichert sind, in der Remote Loader-Konfigurationsdatei für einen Treiber an.

Ergänzen Sie die Remote Loader-Konfigurationsdatei für einen Treiber mit dem Inhalt, der zur Aktivierung der beiderseitigen Authentifizierung erforderlich ist. Die Datei befindet sich im Verzeichnis `/opt/novell/dirxml/doc`.

So bearbeiten Sie die Konfiguration:

1. Melden Sie sich bei dem Server an, auf dem Sie den Treiber und Remote Loader installiert haben.
2. Stoppen Sie den Remote Loader.

   Geben Sie beispielsweise den folgenden Befehl ein:

   ```
   rdxml -config /home/drivershim.conf -u
   ```

3. Geben Sie das Keystore- oder Schlüsselpasswort an (je nach Remote Loader-Typ):

   Java Remote Loader:

   Geben Sie die Kombination aus Keystore-Passwort und Schlüsselpasswort mit der folgenden Syntax an:

   ```
   dirxml_jremote -config /home/drivershim.conf -ksp <keystorepassword> -kp
   <keypassword>
   ```

   Beispiel:

   ```
   dirxml_jremote -config /home/drivershim.conf -ksp dirxml -kp dirxml
   ```

   Nativer Remote Loader:

   Geben Sie das Schlüsselpasswort mit der folgenden Syntax an:

   ```
   dirxml_jremote -config /home/drivershim.conf -kp <keypassword>
   ```

   Beispiel:

   ```
   dirxml_jremote -config /home/drivershim.conf -kp dirxml
   ```

4. Öffnen Sie in einem Texteditor die Remote Loader-Konfigurationsdatei für den Treiber.
5. Fügen Sie der Datei den Inhalt hinzu, der zur Aktivierung der beiderseitigen Authentifizierung erforderlich ist.
   - Beispieleintrag für einen Java-Treiber:

     ```
     -connection "port=8090 useMutualAuth=true keystore='/home/certs/
     clientkmo_client.ks' key='clientkmo'
     ```

   - Beispieleintrag für einen nativen Treiber:

     ```
     -connection "useMutualAuth=true port=8090 rootfile='/home/certs/
     trustedcert.b64' certfile='/home/certs/clientkmo_clientcert.pem'
     keyfile='/home/certs/clientkmo_clientkey.pem' certform=PEM keyform=PEM"
     ```

6. Speichern und schließen Sie die Datei.
7. Starten Sie den Treiber neu.

11.3.7 Überprüfen der Konfiguration

1. Starten Sie den Remote Loader. Beispiel:

   ```
   dirxml_remote -config config.txt
   ```

2. Starten Sie das Remote-Schnittstellenmodul mit iManager.
3. Stellen Sie sicher, dass der Remote Loader ordnungsgemäß funktioniert.

4. Stoppen Sie den Remote Loader. Beispiel:

   ```
   dirxml_remote -config config.txt -u
   ```

11.3.8 Starten einer Treiberinstanz im Remote Loader

Sie können jede Plattform so konfigurieren, dass beim Hochfahren des Hostcomputers automatisch eine Treiberinstanz gestartet wird. Außerdem können Sie eine Instanz manuell starten.

NetIQ bietet zwei Möglichkeiten zum Starten einer Treiberinstanz für den Remote Loader:

- „Automatisches Starten von Treiberinstanzen“, auf Seite 141
- „Starten von Treiberinstanzen über die Befehlszeile“, auf Seite 141

Automatisches Starten von Treiberinstanzen

Sie können eine Treiberinstanz für den Remote Loader so konfigurieren, dass sie beim Hochfahren des Computers automatisch gestartet wird. Speichern Sie die Konfigurationsdatei im Verzeichnis `/etc/opt/novell/dirxml/rdxml`.

Starten von Treiberinstanzen über die Befehlszeile

Die Binärkomponente `rdxml` unterstützt die Befehlszeilenfunktionen für den Remote Loader. Diese Komponente befindet sich standardmäßig im Verzeichnis `/usr/bin/`.

1. Öffnen Sie eine Befehlszeilen-Eingabeaufforderung.
2. (Bedingt) Geben Sie die Passwörter zum Authentifizieren der Treiberinstanz bei der Identity Manager-Engine mit einem der folgenden Befehle ein:
   - **Remote Loader:** `rdxml -config filename –keystorepassword <Keystore-Passwort> -keypassword <Schlüsselpasswort>`
   - **Java Remote Loader:** `dirxml_jremote -config filename -keystorepassword <Keystore-Passwort> -keypassword <Schlüsselpasswort>`
3. (Bedingt) Wenn die beiderseitige Authentifizierung zwischen der Treiberinstanz für den Remote Loader und der Identity Manager-Engine aktiviert ist, geben Sie die Zertifikatspasswörter mit einem der folgenden Befehle an:
   - **Remote Loader:** `rdxml -config filename -keystorepassword <Keystore-Passwort> -keypassword <Schlüsselpasswort>`
   - **Java Remote Loader:** `dirxml_jremote -config filename -keypassword <Schlüsselpasswort>`
4. Starten Sie die Treiberinstanz mit dem folgenden Befehl:

   `rdxml -config` *`Dateiname`*
5. Melden Sie sich bei iManager an, und starten Sie den Treiber.
6. Stellen Sie sicher, dass der Remote Loader ordnungsgemäß funktioniert.

   Prüfen Sie mit dem Befehl `ps` oder mit einer Trace-Datei, ob die Befehls- und Verbindungsports überwacht werden.

   Der Remote Loader lädt das Identity Manager-Anwendungsschnittstellenmodul nur dann, wenn der Remote Loader mit dem Remote-Schnittstellenmodul auf dem Server der Identity Manager-Engine kommuniziert. Dies bedeutet beispielsweise, dass das Anwendungsschnittstellenmodul heruntergefahren wird, wenn der Remote Loader die Kommunikation mit dem Server der Identity Manager-Engine verliert.

11.3.9 Anhalten einer Treiberinstanz im Remote Loader

Für jede Plattform gilt eine andere Methode, mit der Sie eine Treiberinstanz im Remote Loader anhalten.

HINWEIS

- Wenn mehrere Remote Loader-Instanzen auf einem LINUX-Computer ausgeführt werden, geben Sie auch die Option `-cp` *Befehlsport* an, damit der Remote Loader die entsprechende Instanz anhalten kann.
- Zum Anhalten einer Treiberinstanz müssen Sie entweder über ausreichende Rechte verfügen oder das Remote Loader-Passwort angeben. Sie besitzen genügend Rechte, den Dienst zu stoppen. Sie geben ein ungültiges Passwort ein. Der Remote Loader wird dennoch angehalten, weil der Remote Loader das Passwort nicht im eigentlichen Sinne „akzeptiert“. Da das Passwort jedoch in diesem Fall nicht erforderlich ist, wird es ignoriert. Wenn Sie den Remote Loader als Anwendung und nicht als Dienst ausführen, wird das Passwort verwendet.

So halten Sie eine Treiberinstanz an:

Remote Loader

Geben Sie den Befehl `rdxml -config` *`Dateiname`* `-u` ein. Beispiel:

```
rdxml -config config.txt -u
```

Java Remote Loader

Geben Sie den Befehl `dirxml_jremote -config` *`Dateiname`* `-u` ein. Beispiel:

```
dirxml_jremote -config config.txt -u
```

11.4 Konfigurieren des Identitätsdepots für die Identitätsanwendungen

Die Identitätsanwendungen müssen mit den Objekten im Identitätsdepot interagieren können.

Um die Leistung der Identitätsanwendungen zu erhöhen, sollte der eDirectory-Administrator jeweils einen Wertindex für die Attribute manager, ismanager und srvprvUUID erstellen. Sind für diese Attribute keine Wertindizes vorhanden, kann dies insbesondere in einer Cluster-Umgebung eine eingeschränkte Leistung zur Folge haben.

Mit der Option "Erweitert" > "eDirectory-Indizes erstellen" im RBPM-Konfigurationsprogramm werden diese Wertindizes automatisch im Rahmen der Installation erstellt. Weitere Informationen zum Erstellen von Wertindizes mit dem Indexmanager finden Sie im *NetIQ eDirectory-Administrationshandbuch*.

11.5 Konfigurieren des Benutzeranwendungstreibers 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.

1. Melden Sie sich bei der Instanz von iManager an, die Ihr Identitätsdepot verwaltet.
2. Wählen Sie im Navigationsrahmen die Option **Identity Manager** aus.
3. Wählen Sie **Identity Manager-Überblick**.
4. Verwenden Sie die Suche-Seite, um den Identity Manager-Überblick für den Treibersatz anzuzeigen, der Ihren Benutzeranwendungstreiber enthält.
5. Klicken Sie auf den runden Statusindikator in der rechten oberen Ecke des Treibersymbols.
6. Wählen Sie **Eigenschaften bearbeiten** aus.
7. Geben Sie unter **Treiberparameter**für **Host** den Hostnamen oder die IP-Adresse des Dispatchers ein.
8. Klicken Sie auf **OK**.

11.6 Konfigurieren der Einstellungen für die Identitätsanwendungen

Mit dem Konfigurationsprogramm der Identitätsanwendungen verwalten Sie die Einstellungen für die Benutzeranwendungstreiber und die Identitätsanwendungen. Das Installationsprogramm für die Identitätsanwendungen 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 zum Ausführen des Konfigurationsprogramms (`configupdate.sh`) befindet sich standardmäßig im Verzeichnis `/opt/netiq/idm/apps/configupdate`:

HINWEIS

- Führen Sie die Datei `configupdate.sh` ausschließlich aus dem Verzeichnis `configupdate` heraus aus. Wenn Sie `configupdate.sh` von einem benutzerdefinierten Speicherort aus ausführen, treten Fehler auf.
- In einem Cluster müssen die Konfigurationseinstellungen für alle Clustermitglieder identisch sein.

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

- Abschnitt 11.6.1, „Ausführen des Konfigurationsprogramms der Identitätsanwendungen“, auf Seite 144
- Abschnitt 11.6.2, „Parameter für Benutzeranwendung“, auf Seite 144
- Abschnitt 11.6.3, „Parameter für die Berichterstellung“, auf Seite 155
- Abschnitt 11.6.4, „Parameter für Authentifizierung“, auf Seite 156

- Abschnitt 11.6.5, „Parameter für SSO-Clients“, auf Seite 160
- Abschnitt 11.6.6, „CEF-Revisionsparameter“, auf Seite 164

11.6.1 Ausführen des Konfigurationsprogramms der Identitätsanwendungen

1 Überprüfen Sie, ob die folgenden Optionen in Datei `configupdate.sh.properties` ordnungsgemäß konfiguriert sind:

```
edit_admin="true"

use_console="false"
```

HINWEIS: Stellen Sie den Wert für `-use_console` nur dann auf `true` ein, wenn das Dienstprogramm im Konsolenmodus ausgeführt werden soll.

2 Speichern und schließen Sie die Datei `configupdate.sh`.

3 Starten Sie das Konfigurationsprogramm mit dem folgenden Befehl an der Befehlszeile:

```
./configupdate.sh
```

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

11.6.2 Parameter für Benutzeranwendung

Beim Konfigurieren der Identitätsanwendungen 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 145
- „Identitätsdepot-DNs“, auf Seite 146
- „Identitätsdepot-Benutzeridentität“, auf Seite 148
- „Identitätsdepot-Benutzergruppen“, auf Seite 149
- „Identitätsdepot-Zertifikate“, auf Seite 150
- „Email-Serverkonfiguration“, auf Seite 150
- „Speicher für Herkunftsverbürgungsschlüssel“, auf Seite 152
- „Zertifikat und Schlüssel für NetIQ Sentinel-Digitalsignatur“, auf Seite 153
- „Sonstige“, auf Seite 153
- „Containerobjekt“, auf Seite 154

Identitätsdepoteinstellungen

In diesem Abschnitt werden die Einstellungen für den Zugriff der Identitätsanwendungen 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 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 die Identitätsanwendungen 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 Identitätsanwendungen und anderen 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 Identitätsanwendungen anmelden.
- Wenn Sie Tomcat, auf dem die Identitätsanwendungen gehostet werden, bereits gestartet haben, können Sie diese Einstellung nicht mithilfe der Datei `configupdate.sh` 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 die Identitätsanwendungen gehostet werden, bereits gestartet haben, können Sie diese Einstellung nicht mithilfe der Datei `configupdate.sh` 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.sh` 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 iManager, 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 Identitätsanwendungen 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 Identitätsanwendungen 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 Identitätsanwendungen 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 Identitätsanwendungen 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 Identitätsanwendungen 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 Identitätsanwendungen 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 Identitätsanwendungen anmelden.

- Wenn Sie Tomcat, auf dem die Identitätsanwendungen gehostet werden, bereits gestartet haben, können Sie diese Einstellung nicht mithilfe der Datei `configupdate.sh` 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 Identitätsanwendungen 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 die Identitätsanwendungen gehostet werden, bereits gestartet haben, können Sie diese Einstellung nicht mithilfe der Datei `configupdate.sh` 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 die Identitätsanwendungen bearbeitet. Unter Linux benötigt der Benutzer eine entsprechende Berechtigung zum Schreiben in diese Datei.

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 unter „Aktivieren der Unterstützung für digitale Signaturen“ im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen* und unter „Verwalten von Genehmigungen per Email“ in der *Hilfe zu den Identitätsanwendungen*.

Benachrichtigungsschablonen-Host

Gibt den Namen oder die IP-Adresse von Tomcat an, auf dem die Identitätsanwendungen 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 die Identitätsanwendungen 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 die Identitätsanwendungen 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 die Identitätsanwendungen die Email-Benachrichtigungen senden.

SMTP-Servername

Gibt die IP-Adresse oder den DNS-Namen des SMTP-Email-Hosts an, den die Identitätsanwendungen 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. Beispiel: `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 **Email signieren** *aktivieren.*

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

Beispiel: `/opt/netiq/idm/apps/jre/lib/security/cacerts`.

Keystore-Passwort

Gilt nur, wenn Sie die Option **Email signieren** *aktivieren.*

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

Alias des Signaturschlüssels

Gilt nur, wenn Sie die Option **Email signieren** *aktivieren.*

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

Signaturschlüsselpasswort

Gilt nur, wenn Sie die Option **Email 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 die Identitätsanwendungen 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 die Identitätsanwendungen 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 die Identitätsanwendungen 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 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 während der Installation an, ob das Installationsprogramm Indizes für die Attribute „manager“, „ismanager“ 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 Identitätsanwendungen zur Folge haben.
- Nach der Installation der Identitätsanwendungen können Sie diese Indizes manuell mit iManager erstellen.
- Zur Erzielung einer optimalen Leistung sollten Sie den Index während der Installation erstellen.
- Die Indizes müssen sich im Online-Modus befinden, bevor Sie die Identitätsanwendungen 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 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 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 die Identitätsanwendungen erneut bereitstellen.

IDMReport-URL

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

Kontextname für benutzerdefinierte Themen

Gibt den Namen des benutzerdefinierten Themas an, mit dem die Identitätsanwendungen 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 iManager auch eigene Container erstellen und mithilfe der Option **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.

11.6.3 Parameter für die Berichterstellung

Beim Konfigurieren der Identitätsanwendungen definieren Sie auf dieser Registerkarte die Werte für die Verwaltung der Identitätsberichterstellung. Diese Registerkarte wird zum Dienstprogramm hinzugefügt, sobald Sie die Identitätsberichterstellung 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 155
- „Berichtbeibehaltungswerte“, auf Seite 156
- „Gebietsschema bearbeiten“, auf Seite 156
- „Rollenkonfiguration“, auf Seite 156

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 die Identitätsberichterstellung 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 die Identitätsberichterstellung 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 der Identitätsberichterstellung 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: `/opt/netiq/IdentityReporting`.

Gebietsschema bearbeiten

In diesem Abschnitt werden die Werte für die Sprache der Identitätsberichterstellung definiert. Die Identitätsberichterstellung nutzt die angegebenen Gebietsschemas in den Suchvorgängen. Weitere Informationen finden Sie im Verwaltungshandbuch für die NetIQ-Identitätsberichterstellung.

Rollenkonfiguration

In diesem Abschnitt werden die Werte für die Authentifizierungsquellen der Identitätsberichterstellung definiert.

Authentifizierungsquelle hinzufügen

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

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

11.6.4 Parameter für Authentifizierung

Beim Konfigurieren der Identitätsanwendungen werden auf dieser Registerkarte die Parameter definiert, mit denen Tomcat die Benutzer zu den Seiten der Identitätsanwendungen 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 157
- „Authentifizierungskonfiguration“, auf Seite 157
- „Authentifizierungsmethode“, auf Seite 158
- „Passwortverwaltung“, auf Seite 158
- „Zertifikat und Schlüssel für Sentinel-Digitalsignatur“, auf Seite 159

Beglaubigungsserver

In diesem Abschnitt werden die Einstellungen zum Herstellen einer Verbindung der Identitätsanwendungen 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.

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 die Identitätsanwendungen 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 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 Identity Manager anmelden, in OSP definiert.

Methode

Gibt den Typ der Authentifizierung an, die in 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 Identity Manager. Mit dieser Option können Sie außerdem ein externes Passwortverwaltungsprogramm angeben.

Vergessenes Passwort

Dieser Kontrollkästchen-Parameter gilt nur dann, wenn Sie SSPR verwenden möchten.

Gibt an, ob die Benutzer ein vergessenes Passwort wiederherstellen können, ohne sich an einen Helpdesk zu wenden.

Sie müssen außerdem die Challenge-Response-Richtlinien für die „Passwort vergessen“-Funktion konfigurieren. Weitere Informationen finden Sie im *NetIQ Self Service Password Reset Administration Guide* (NetIQ-Administrationshandbuch für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung).

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
```

Zertifikat und Schlüssel für Sentinel-Digitalsignatur

In diesem Abschnitt werden die Werte für die Kommunikation von 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.

11.6.5 Parameter für SSO-Clients

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

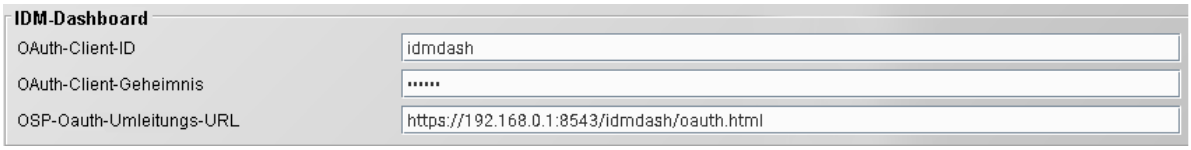
Standardmäßig werden auf dieser Registerkarte nur die grundlegenden Optionen angezeigt. Mit **Erweiterte Optionen anzeigen** lassen Sie alle Einstellungen einblenden. Diese Registerkarte umfasst die folgenden Gruppen von Einstellungen:

- „IDM-Dashboard“, auf Seite 160
- „IDM-Administrator“, auf Seite 161
- „RBPM“, auf Seite 161
- „Berichte“, auf Seite 162
- „IDM-Datenerfassungsdienst“, auf Seite 163
- „DCS-Treiber“, auf Seite 163
- „Zurücksetzen von Passwörtern per Selbstbedienung“, auf Seite 164

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 die Identitätsanwendungen.

Abbildung 11-1 *IDM-Dashboard*



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 Identity Manager-Administrators zugreifen.

OAuth-Client-ID

Erforderlich

Gibt den Namen an, mit dem sich der Single-Sign-On-Client für den 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 Identity Manager-Administrator an.

OSP-OAuth-Umleitungs-URL

Erforderlich

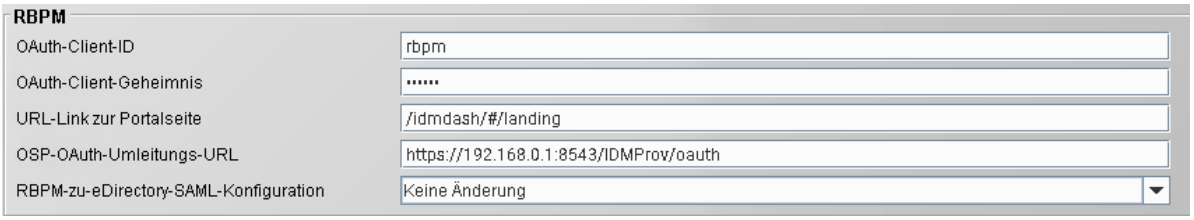
Gibt die absolute URL an, zur der der Authentifizierungsserver einen Browser-Client nach erfolgter Authentifizierung weiterleiten soll.

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.

Abbildung 11-2 *RBPM*



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-eDirectory-SAML-Konfiguration

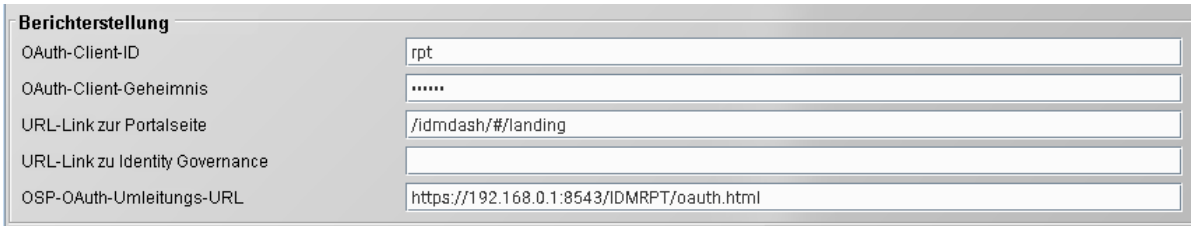
Erforderlich

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

Berichte

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

Abbildung 11-3 *Berichte*



OAuth-Client-ID

Erforderlich

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

OAuth-Client-Geheimnis

Erforderlich

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

URL-Link zur Portalseite

Erforderlich

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

Wenn Sie die Identitätsberichterstellung und die Identitätsanwendungen 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 Identity Manager-Datenerfassungsdiensts zugreifen.

OAuth-Client-ID

Erforderlich

Gibt den Namen an, mit dem sich der Single-Sign-On-Client für den 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 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 11-4

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.

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/sspr/public/oauth.html`.

11.6.6 CEF-Revisionsparameter

In diesem Abschnitt werden die Werte zur Verwaltung der CEF-Revisionsparameter für den Single-Sign-On-Client definiert.

Auditereignisse senden

Gibt an, ob Auditereignisse 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: Für das Cache-Verzeichnis müssen die `novlua`-Berechtigungen festgelegt werden. Ansonsten können Sie nicht auf die IDMDash- und IDMProv-Anwendungen zugreifen. Außerdem werden keine OSP-Ereignisse im Cache-Verzeichnis gespeichert. Ändern Sie die Berechtigungen und das Eigentum für das Verzeichnis beispielsweise mit dem Befehl `chown novlua:novlua /<Verzeichnispfad>`, wobei `<Verzeichnispfad>` den Pfad zum Cache-Dateiverzeichnis bezeichnet.

11.7 Starten der Identitätsanwendungen

Nach dem Konfigurieren der Identitätsanwendungen müssen der Tomcat- und der ActiveMQ-Dienst in jedem Fall neu gestartet werden.

```
systemctl restart netiq-tomcat
```

```
systemctl restart netiq-activemq
```

11.8 Konfigurieren von OSP und SSPR für Clustering

Identity Manager unterstützt die SSPR-Konfiguration in einer Tomcat-Clusterumgebung.

11.8.1 Konfigurieren von SSPR zur Unterstützung von Clustering

Starten Sie zur Aktualisierung der SSPR-Informationen im ersten Knoten des Clusters das Konfigurationsprogramm unter `opt/netiq/idm/apps/configupdate/configupdate.sh`.

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.

11.8.2 Konfigurieren der Aufgaben in Clusterknoten

Führen Sie die folgenden Konfigurationsaufgaben in den Clusterknoten durch:

1. Melden Sie sich zur Aktualisierung des Links "Passwort vergessen" mit der SSPR-IP-Adresse bei der Benutzeranwendung im ersten Knoten an und klicken Sie auf **Verwaltung** > **Passwort vergessen**.

   Weitere Informationen zur SSPR-Konfiguration finden Sie unter Abschnitt 22, „Konfigurieren der "Passwort vergessen"-Verwaltung“, auf Seite 235.

2. Weitere Informationen zum Link "Passwort ändern" finden Sie in Abschnitt 22.3, „Aktualisieren der SSPR-Links im Dashboard für eine dezentrale Umgebung oder eine Cluster-Umgebung“, auf Seite 239.

3. Überprüfen Sie, ob die Links "Passwort vergessen" und "Passwort ändern" mit der SSPR-IP-Adresse in den anderen Knoten im Cluster aktualisiert sind.

   HINWEIS: Wenn die Links "Passwort vergessen" und "Passwort ändern" bereits mit der SSPR-IP-Adresse aktualisiert sind, brauchen Sie keine Änderungen vorzunehmen.

4. Stoppen Sie Tomcat im ersten Knoten und generieren Sie eine neue `osp.jks`-Datei. Geben Sie dazu den DNS-Namen des Lastausgleichservers an und führen Sie den folgenden Befehl aus:

   ```
   /opt/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: `/opt/netiq/common/jre/bin/keytool -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.

5 (Bedingt) Führen Sie folgenden Befehl aus, um zu überprüfen, ob die `osp.jks`-Datei mit den Änderungen aktualisiert wurde:

```
/opt/netiq/common/jre/bin/keytool -list -v -keystore osp.jks -storepass
changeit
```

6 Sichern Sie die ursprüngliche `osp.jks`-Datei, die sich unter `/opt/netiq/idm/apps/osp` befindet, und kopieren Sie die neue `osp.jks`-Datei an diesen Speicherort. Die neue `osp.jks`-Datei wurde in Schritt 3 erstellt.

7 Kopieren Sie die neue `osp.jks`-Datei, die sich unter `/opt/netiq/idm/apps/osp/` befindet, vom ersten Knoten zu allen anderen Benutzeranwendungsknoten im Cluster.

8 Starten Sie das Konfigurationsprogramm im ersten Knoten 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".

8a Speichern Sie die Änderungen im Konfigurationsprogramm.

8b Kopieren Sie Datei `ism-configuration properties`, die sich unter `/TOMCAT_INSTALLED_HOME/conf` befindet, vom ersten Knoten zu allen anderen Benutzeranwendungsknoten, um die Änderungen auf alle anderen Knoten im Cluster zu übertragen.

HINWEIS: Sie haben die Datei `ism.properties` vom ersten Knoten 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 die Benutzeranwendung auf verschiedenen Servern installiert sind, müssen Sie die OSP-URLs in einen 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.

9 Führen Sie die folgenden Schritte in der Datei `setenv.sh` im Verzeichnis `/TOMCAT_INSTALLED_HOME/bin/` durch:

9a 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.

9b Fügen Sie "-Dcom.novell.afw.wf.Engine-id=Engine” in Datei `setenv.sh` im ersten Knoten hinzu.

Der Engine-Name sollte eindeutig sein. Geben Sie den Namen an, der bei der Installation des ersten Knotens vergeben wurde. Der Standardname lautet "Engine”, falls kein anderer Name angegeben wurde.

Fügen Sie entsprechend einen eindeutigen Engine-Namen für die anderen Knoten im Cluster hinzu. Beispielsweise kann der Engine-Name für den zweiten Knoten "Engine2" lauten.

10 Aktivieren Sie das Clustering in der Benutzeranwendung.

11 Aktivieren Sie den Berechtigungsindex für das Clustering. Weitere Informationen hierzu finden Sie unter, „Aktivieren des Berechtigungsindex für das Clustering“, auf Seite 77.

12 Starten Sie Tomcat in allen Knoten neu.

13 Konfigurieren Sie den Benutzeranwendungstreiber für das Clustering. Weitere Informationen hierzu finden Sie unter, Abschnitt 11.5, „Konfigurieren des Benutzeranwendungstreibers für das Clustering“, auf Seite 143.

11.9 Konfigurieren der Laufzeitumgebung

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:

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 *NetIQ Identity Reporting Module Guide* (Handbuch zum Berichterstellungsmodul in NetIQ Identity Manager).

11.9.1 Konfigurieren des DCS-Treibers für das Erfassen von Daten aus den Identitätsanwendungen

Damit die Identitätsanwendungen ordnungsgemäß mit der Identitätsberichterstellung 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 die Identitätsberichterstellung 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. Weitere Informationen zu den Software-Anforderungen finden Sie in Abschnitt 8.6.2, „Voraussetzungen für die Installation der Komponenten für die Identitätsberichterstellung“, auf Seite 86.

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 des Berichterstellungsmoduls 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**.

11.9.2 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 iManager an.

2 Wählen Sie in der Kontrollleiste **Überblick** für den DCS-Treiber Kontrollleiste die Option Datenerfassungsdiensttreiber, auswählen **Von Identitätsdepot migrieren**.

3 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.

---

4 Warten Sie ab, bis der Migrationsvorgang abgeschlossen ist.

5 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:

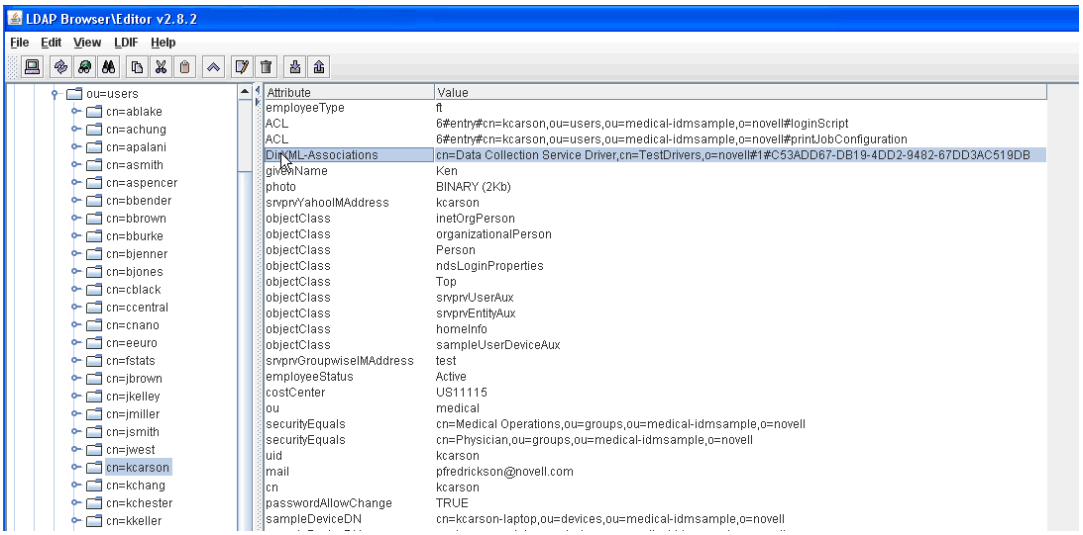
File Edit View Tools Help

No limit

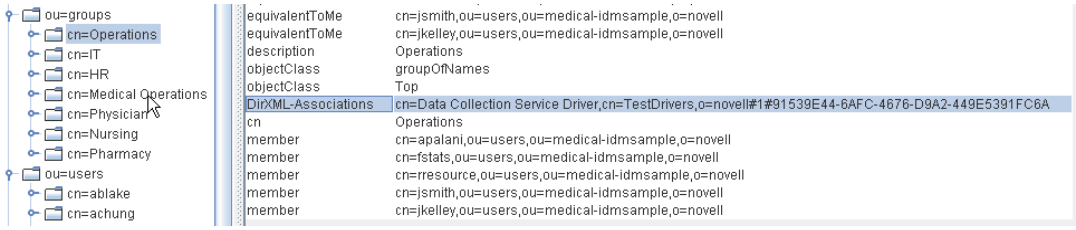
	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4	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	

6 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:



7 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_grou 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 Operati	Medical Operati	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.

8 (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

9 (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.

11.9.3 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 170
- „Angeben eines Namens und einer Beschreibung in der Datenbank“, auf Seite 171
- „Hinzufügen von erweiterten Attributen zu bekannten Objekttypen“, auf Seite 172

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.

11.9.4 Zusätzliche Unterstützung für mehrere Treibersätze

Das neue DCS-Scoping-Paket (NOVLDCSSCPNG) bietet statische und dynamische Scoping-Funktionen 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.

  Wenn Sie mit der integrierten Installation einen zweiten Server zum Baum hinzugefügt haben, erhält dieser Server lediglich eine Kopie des Stammverzeichnisses sowie eine eigene Treibersatzpartition. Wird der DCS-Treiber auch auf diesem Sekundärserver als primärer Treiber eingesetzt, so kann der Treiber die zu meldenden Objektänderungen nicht erkennen.
- **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 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* 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 Identity Manager-Server. (Einige Partitionen gehören zu mehreren 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.

11.9.5 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 ein Serverzertifikat in iManager.
   - **1a** Klicken Sie in der Ansicht **Rollen und Aufgaben** auf **NetIQ Certificate Server > Serverzertifikat erstellen**.
   - **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 iManager.
   - **2a** Klicken Sie in der Ansicht **Rollen und Aufgaben** auf **NetIQ Certificate Server > Serverzertifikate**.
   - **2b** Wählen Sie das Zertifikat aus, das Sie in Schritt 1 auf Seite 174 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 174 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 Bearbeiten Sie die MSGW-Konfiguration so mit iManager, dass der Keystore verwendet werden.

4a Klicken Sie unter **Identity Manager-Überblick** auf den Treibersatz, in dem sich der MSGW-Treiber befindet.

4b Klicken Sie auf das Symbol für den Treiberstatus, und wählen Sie **Eigenschaften bearbeiten > Treiberkonfiguration**.

4c Stellen Sie **Verbindungsparameter anzeigen** auf „Wahr“ ein, und wählen Sie unter **Treiberkonfigurationsmodus** die Option „Remote“.

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

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

5 Bearbeiten Sie die DCS-Konfiguration so mit iManager, dass der Keystore verwendet werden.

5a Klicken Sie unter **Identity Manager-Überblick** auf den Treibersatz, in dem sich der MSGW-Treiber befindet.

5b Klicken Sie auf das Symbol für den Treiberstatus, und wählen Sie **Eigenschaften bearbeiten > Treiberkonfiguration**.

5c Wählen Sie unter **'Verwaltetes System – Gateway' – Registrierung** für **Konfigurationsmodus des Treibers 'Verwaltetes System – Gateway'** die Option „Remote“.

5d Geben Sie den vollständigen Pfad zur Keystore-Datei, das Passwort und das Alias aus Schritt 1c auf Seite 174 ein.

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

11.10 Konfigurieren der Identitätsberichterstellung

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

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

11.10.1 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**.

11.10.2 Ausführen von Berichten über eine Oracle-Datenbank

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

Weitere Informationen zu den unterstützten Oracle-Datenbanken finden Sie in Abschnitt 8.6.4, „Systemanforderungen für die Identitätsberichterstellung“, auf Seite 88.

11.10.3 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

1 Nehmen Sie die erforderlichen Rollen mit den SQLs „create_dcs_roles_and_schemas.sql“ und `create_rpt_roles_and_schemas.sql` (unter `/mnt/reporting/sql`) in die Datenbank auf.

   1. Melden Sie sich als Postgres-Benutzer bei PGAdmin an.
   2. Führen Sie das Abfragewerkzeug aus.
   3. 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.
   4. Zum Erstellen der Rollen IDM_RPT_DATA, IDM_RPT_CFG und IDMRPTUSER führen Sie die folgenden Befehle in der angegebenen Reihenfolge aus:

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

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

   5. Zum Erstellen des Schemas IDM_RPT_DATA kopieren Sie den Inhalt von `get_formatted_user_dn.sql` aus `/mnt/reporting/sql` in das Abfragewerkzeug und starten Sie dann die Ausführung gegen die verbundene Datenbank.

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

1 Nehmen Sie die erforderlichen Rollen mit „create_dcs_roles_and_schemas-orcale.sql“ und `create_rpt_roles_and_schemas-orcale.sql` (unter `/mnt/reporting/sql`) in die Datenbank auf.

   1. Melden Sie sich als Datenbank-Administratorbenutzer bei SQL Developer an.
   2. Zum Erstellen der Verfahren `Create_rpt_roles_and_schemas` und `Create_dcs_roles_and_schemas` kopieren Sie den Inhalt dieser SQLs in SQL Developer und starten Sie dann die Ausführung gegen die verbundene Datenbank.
   3. Zum Erstellen der Rollen IDM_RPT_DATA, IDM_RPT_CFG und IDMRPTUSER führen Sie die folgenden Befehle in der angegebenen Reihenfolge aus:

      ```
      begin
      CREATE_DCS_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>');
      end;

      begin
      CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>', '<Set pwd for
      IDMRPTUSER>');
      end;
      ```

   4. Zum Erstellen des Schemas IDM_RPT_DATA kopieren Sie den Inhalt von `get_formatted_user_dn-oracle.sql` aus `/mnt/reporting/sql in SQL Developer und starten Sie dann die Ausführung gegen die verbundene Datenbank`.

11.10.4 Löschen der Datenbank-Prüfsummen

1 Navigieren Sie zu den folgenden `.sql`-Dateien in `/opt/netiq/idm/apps/IDMReporting/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.

11.10.5 Bereitstellen von REST-APIs für die Identitätsberichterstellung

Die Identitätsberichterstellung 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.

11.10.6 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 `/opt/netiq/idm/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 `/opt/netiq/idm/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.

V Installation von Designer

In diesem Abschnitt finden Sie die Schritte für die Installation von Designer für Identity Manager.

12 Planen der Installation von Designer

In diesem Abschnitt finden Sie die Voraussetzungen, die Überlegungen und die notwendige Systemeinrichtung für die Installation von Designer.

12.1 Checkliste für die Installation von Designer

NetIQ empfiehlt, vor Beginn der Installation die nachfolgenden Schritte auszuführen.

	Checkliste
❑	1. Lesen Sie die Überlegungen zur Installation von Designer, und prüfen Sie, ob der Computer den Voraussetzungen entspricht. Weitere Informationen finden Sie in Abschnitt 12.2, „Voraussetzungen für die Installation von Designer“, auf Seite 183.
❑	2. Stellen Sie sicher, dass der Computer, auf dem Sie Designer installieren, den angegebenen Software- und Hardware-Voraussetzungen entspricht. Weitere Informationen finden Sie in Abschnitt 12.3, „Systemanforderungen für Designer“, auf Seite 184.
❑	3. Installieren Sie Designer. Weitere Informationen finden Sie in Abschnitt 13, „Installation von Designer“, auf Seite 185.
❑	4. (Optional) Starten Sie ein Projekt für die Identity Manager-Lösung gemäß den Anweisungen unter Understanding Designer for Identity Manager (Erläuterungen zu Designer für Identity Manager).

12.2 Voraussetzungen für die Installation von Designer

In diesem Abschnitt finden Sie die Voraussetzungen und die Überlegungen für die Installation von Designer.

- Vor dem Installieren von Designer auf einem Computer mit Linux-Betriebssystem müssen Sie auch die GNU-gettext-Dienstprogramme installieren. Diese Dienstprogramme bieten einen Rahmen für internationalisierte und mehrsprachige Meldungen. Weitere Informationen zur Sprachunterstützung finden Sie in Abschnitt 5.10, „Erläuterungen zur Sprachunterstützung“, auf Seite 48.
- Bevor Sie Designer auf einem Computer mit dem Betriebssystem RHEL 7.4 installieren, müssen Sie `gtk2-2.24.31-1.el7.x86_64.rpm` installieren. Laden Sie das Paket beispielsweise von der Website des Betriebssystemanbieters herunter.

12.3 Systemanforderungen für Designer

In diesem Abschnitt finden Sie die Mindestanforderungen für die Server, auf denen Designer installiert werden soll. Überprüfen Sie die Voraussetzungen und Überlegungen zur Installation, insbesondere im Zusammenhang mit dem Betriebssystem.

Kategorie	Anforderung
Prozessor	1 GHz
Festplattenspeicher	1 GB
Arbeitsspeicher	1 GB
Betriebssysteme (zertifiziert)	Eines der folgenden 64-Bit-Betriebssysteme: **Server** ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3 ◆ openSUSE Leap 42.1 **müssen zuerst entfernt werden** ◆ SLED 12 SP3 ◆ SLED 12 SP2 **HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird.
Betriebssysteme (unterstützt)	Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme **HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert.
Virtualisierungssystem	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.5 (oder höher) NetIQ unterstützt Identity Manager auf Enterprise-Virtualisierungssystemen, die die Betriebssysteme, unter denen die NetIQ-Produkte ausgeführt werden können, offiziell unterstützen. Sofern die Anbieter der Virtualisierungssysteme diese Betriebssysteme offiziell unterstützen, unterstützt NetIQ den gesamten Identity Manager-Stack auf diesen Systemen.

13 Installation von Designer

In diesem Abschnitt wird der Installationsvorgang für Designer beschrieben. Sie können die Installation wahlweise über die Benutzeroberfläche oder im Konsolenmodus ausführen.

So installieren Sie Designer:

1. Laden Sie die Datei `Identity_Manager_Linux_LDAP_Designer.tar.gz` von der NetIQ Downloads-Website herunter.
2. Navigieren Sie zu dem Verzeichnis, in dem die Datei extrahiert werden soll.
3. Führen Sie den folgenden Befehl aus:

   ```
   tar -zxvf Identity_Manager_Linux_LDAP_Designer.tar.gz
   ```

4. Installieren Sie Designer mit einem der nachfolgenden Befehle.

   Konsole: `./install`

   GUI: `./install -i console`

5. Setzen Sie die Installation anhand der Eingabeaufforderungen fort.

VI Installation von Analyzer

In diesem Abschnitt finden Sie die Schritte für die Installation von Analyzer für 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 Identity Manager-Lösung eingebunden werden sollen. Wenn Sie Analyzer in der Planungsphase einsetzen, wird ersichtlich, welche Änderungen auf welche Weise vorgenommen werden müssen.

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie in Abschnitt 14.1, „Checkliste für die Installation von Analyzer“, auf Seite 189.

14 Planen der Installation von Analyzer

In diesem Abschnitt finden Sie Anweisungen zum Vorbereiten der Installation von Analyzer für Identity Manager. NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren.

14.1 Checkliste für die Installation von Analyzer

NetIQ empfiehlt, vor Beginn des Installationsvorgangs die nachfolgenden Schritte auszuführen.

	Checkliste
❑	1. Informieren Sie sich über die Interaktion zwischen den Identity Manager-Komponenten. Weitere Informationen finden Sie in Kapitel 1, „Übersicht der Komponenten von Identity Manager“, auf Seite 17.
❑	2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.7, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 39.
❑	3. Stellen Sie sicher, dass Ihre Umgebung den Überlegungen und Voraussetzungen für das Hosten von Analyzer entspricht. Weitere Informationen finden Sie in den folgenden Abschnitten: ◆ Abschnitt 14.2, „Voraussetzungen für die Installation von Analyzer“, auf Seite 190 ◆ Abschnitt 14.3, „Systemanforderungen für Analyzer“, auf Seite 190
❑	4. Befolgen Sie die Anweisungen zum Installieren von Analyzer in einem der folgenden Abschnitte: ◆ Anweisungen zur Verwendung des Installationsassistenten finden Sie in Abschnitt 15.1, „Installieren von Analyzer mit dem Assistenten“, auf Seite 193 ◆ Anweisungen zur automatischen Installation finden Sie in Abschnitt 15.2, „Automatische Installation von Analyzer“, auf Seite 194.
❑	5. (Optional) Sollen Audit-Ereignisse automatisch von Analyzer empfangen und angezeigt werden, installieren Sie den XDAS-Client. Weitere Informationen finden Sie in Abschnitt 15.4, „Installieren eines Audit-Clients für Analyzer“, auf Seite 195.
❑	6. Aktivieren Sie Analyzer gemäß den Anweisungen in Abschnitt 24.4.2, „Aktivieren von Analyzer“, auf Seite 247.
❑	7. (Optional) Rüsten Sie Analyzer gemäß den Anweisungen in Abschnitt 26.7, „Aufrüsten von Analyzer“, auf Seite 282 auf.

14.2 Voraussetzungen für die Installation von Analyzer

In diesem Abschnitt finden Sie die Voraussetzungen und die Überlegungen für die Installation von Analyzer.

- Bevor Sie Analyzer auf einem Computer mit dem Betriebssystem SLES 12 SP3 installieren, müssen die folgenden Bibliotheken installiert werden:
  - `libswt3-gtk2-3.3.0-0.20.8.9mdv2008.0.i586.rpm`
  - `libxcomposite1-0.4.1-1mdv2010.1.i586.rpm`
  - `libgdk_pixbuf2.0_0-2.20.1-1mdv2010.1.i586.rpm`
  - `libgtk+-x11-2.0_0-2.12.1-2.1mdv2008.0.i586.rpm`
- Bevor Sie Analyzer auf einem Computer mit RHEL 7.3 (oder höher) installieren, müssen Sie `gtk2.i686.rpm` installieren. Laden Sie das Paket beispielsweise von der Website des Betriebssystemanbieters herunter.

14.3 Systemanforderungen für Analyzer

In diesem Abschnitt finden Sie die Mindestanforderungen für die Server, auf denen Analyzer installiert werden soll. Überprüfen Sie die Voraussetzungen und Überlegungen zur Installation, insbesondere im Zusammenhang mit dem Betriebssystem.

Kategorie	Anforderung
Prozessor	1 GHz
Arbeitsspeicher	2 GB
Bildauflösung	1024 × 768 (empfohlen 1280 × 1025)
Betriebssystem (zertifiziert)	Eines der folgenden Betriebssysteme: ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3 ◆ openSUSE Leap 42.1 **HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird.
Betriebssysteme (unterstützt)	Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme **HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert.
Virtualisierungssystem	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 und höher NetIQ unterstützt Identity Manager auf Enterprise-Virtualisierungssystemen, die die Betriebssysteme, unter denen die NetIQ-Produkte ausgeführt werden können, offiziell unterstützen. Sofern die Anbieter der Virtualisierungssysteme diese Betriebssysteme offiziell unterstützen, unterstützt NetIQ den gesamten Identity Manager-Stack auf diesen Systemen.

Kategorie	Anforderung
Zusätzliche Software	◆ gettext-Dienstprogramm

15 Installation von Analyzer

In diesem Abschnitt finden Sie die Schritte für die Installation von Analyzer und die Konfiguration Ihrer Umgebung für Analyzer.

15.1 Installieren von Analyzer mit dem Assistenten

Im Folgenden wird beschrieben, wie Sie Analyzer auf einer Linux- oder Windows-Plattform mithilfe eines Installationsassistenten installieren (wahlweise über die Benutzeroberfläche oder an der Konsole). Anweisungen für die automatische, unbeaufsichtigte Installation finden Sie in Abschnitt 15.2, „Automatische Installation von Analyzer“, auf Seite 194.

Überprüfen Sie in Vorbereitung auf die Installation die Voraussetzungen und Systemanforderungen in Abschnitt 14.1, „Checkliste für die Installation von Analyzer“, auf Seite 189.

1. Melden Sie sich als `Root` oder Administrator an dem Computer an, auf dem Analyzer installiert werden soll.
2. (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zu dem Verzeichnis, in dem sich die Analyzer-Installationsdateien befinden (standardmäßig unter `/Analyzer/packages`).
3. (Bedingt) Wenn Sie die Analyzer-Installationsdateien heruntergeladen haben, führen Sie die folgenden Schritte aus:
   - **3a** Navigieren Sie zur `.tgz`- oder `win.zip`-Datei für das heruntergeladene Image.
   - **3b** Extrahieren Sie den Inhalt der Datei in einen Ordner auf dem lokalen Computer.
4. Führen Sie das Installationsprogramm aus:

   ```
   ./install
   ```
5. Befolgen Sie die Anweisungen im Installationsassistenten, bis die Installation von Analyzer abgeschlossen ist.
6. Überprüfen Sie in der Zusammenfassung nach der Installation den Installationsstatus und den Speicherort der Protokolldatei für Analyzer.
7. Klicken Sie auf **Fertig**.
8. (Bedingt) Führen Sie die Schritte in Abschnitt 15.3, „Hinzufügen von XULrunner zu Analyzer.ini“, auf Seite 194 aus.
9. (Optional) Sollen rollenbasierte Dienste für Analyzer auf einem Windows-Computer konfiguriert werden, öffnen Sie den Link zur Website `gettingstarted.html` (standardmäßig im Verzeichnis `C:\Programme (x86)\NetIQ\Tomcat\webapp\nps\help\en\install`).

   Die rollenbasierten Dienste werden mit iManager konfiguriert.
10. Aktivieren Sie Analyzer gemäß den Anweisungen in „Aktivieren von Analyzer“, auf Seite 247.

15.2 Automatische Installation von Analyzer

Bei der automatischen (nicht interaktiven) Installation wird keine Benutzeroberfläche angezeigt, und der Benutzer muss keinerlei Fragen beantworten. Stattdessen ruft InstallAnywhere die Daten aus einer standardmäßigen Datei `analyzerInstaller.properties` ab. Sie können die automatische Installation wahlweise mit der Standarddatei ausführen oder die Datei bearbeiten und so den Installationsvorgang anpassen.

Standardmäßig wird Analyzer in das Verzeichnis `Programme (x86)\NetIQ\Analyzer` installiert.

1. Melden Sie sich als `Root` oder Administrator an dem Computer an, auf dem Analyzer installiert werden soll.
2. (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die Analyzer-Installationsdateien befinden (standardmäßig unter `products/Analyzer/`).
3. (Bedingt) Wenn Sie die Installationsdateien für Analyzer von der NetIQ Downloads-Website heruntergeladen haben, führen Sie die folgenden Schritte aus:
   - **3a** Navigieren Sie zur `.tgz`- oder `win.zip`-Datei für das heruntergeladene Image.
   - **3b** Extrahieren Sie den Inhalt der Datei in einen Ordner auf dem lokalen Computer.
4. (Optional) Soll ein nicht standardmäßiger Installationspfad festgelegt werden, führen Sie die folgenden Schritten aus:
   - **4a** Öffnen Sie die Datei `analyzerInstaller.properties` (standardmäßig im Verzeichnis `/products/Analyzer/`).
   - **4b** Fügen Sie der Eigenschaftsdatei den folgenden Text hinzu:

     `USER_INSTALL_DIR=`*`installation_path`*
5. Starten Sie die automatische Installation mit einem der folgenden Befehle:
   - **Linux:** `install -i silent -f analyzerInstaller.properties`
   - **Windows:** `install.exe -i silent -f analyzerInstaller.properties`
6. (Bedingt) Führen Sie auf einem Linux-Computer die in Abschnitt 15.3, „Hinzufügen von XULrunner zu Analyzer.ini“, auf Seite 194 aufgeführten Schritte aus.
7. Aktivieren Sie Analyzer gemäß den Anweisungen in „Aktivieren von Analyzer“, auf Seite 247.

15.3 Hinzufügen von XULrunner zu Analyzer.ini

Bevor Sie Analyzer auf einer Linux-Plattform ausführen können, müssen Sie die XULRunner-Zuordnung ändern.

HINWEIS: Wir empfehlen XULrunner Version 1.9.0.19 unter SLED 11 bzw. Version 1.9.0.2. unter openSUSE 11.4. Diese Versionen sind im Lieferumfang des Betriebssystems enthalten.

---

1. Navigieren Sie zum Installationsverzeichnis von `Analyzer`, das sich standardmäßig in den folgenden Verzeichnissen befindet:

   `home/admin/analyzer`
2. Öffnen Sie die Datei `Analyzer.ini` im gedit-Editor.
3. Fügen Sie die folgende Zeile an das Ende der Parameterliste an:

   `-Dorg.eclipse.swt.browser.XULRunnerPath=/usr/lib/xulrunner-1.9/`

Die Datei `Analyzer.ini` sollte beispielsweise wie folgt aussehen:

```
-vmargs
-Xms256m
-Xmx1024m
-XX:MaxPermSize=128m
-XX:+UseParallelGC
-XX:ParallelGCThreads=20
-XX:+UseParallelOldGC
-Dorg.eclipse.swt.browser.XULRunnerPath=/usr/lib/xulrunner-1.9/
```

4 Speichern Sie die Datei `Analyzer.ini`.

5 Starten Sie Analyzer.

15.4 Installieren eines Audit-Clients für Analyzer

Analyzer umfasst eine XDAS-Bibliothek, mit der automatisch Audit-Ereignisse im Data Browser-Editor generiert werden, wenn Sie Datenaktualisierungen an die Anwendung zurücksenden. Weitere Informationen zum Aktualisieren von Daten in der Quellanwendung mit dem Data Browser-Editor finden Sie unter „Modifying Data“ (Ändern von Daten) im *NetIQ Analyzer for Identity Manager Administration Guide* (Administrationshandbuch für NetIQ Analyzer für Identity Manager).

Zum Anzeigen dieser Audit-Ereignisse installieren Sie einen XDAS-Client, der die Audit-Ereignisse von Analyzer empfangen kann. Weitere Informationen zu XDAS finden Sie im OpenXDAS-Projekt (http://openxdas.sourceforge.net).

Das herunterladbare Paket von Analyzer umfasst einen XDAS-Client. Der CDAS-Client wird jedoch nicht mit dem Installationsprogramm von Analyzer installiert.

1 Installieren Sie Analyzer.

2 Navigieren Sie zu den OpenXDAS-Installationsdateien (standardmäßig im Verzeichnis `products/Analyzer/openxdas/`*`Betriebssystem`* in der `.iso`-Image-Datei).

3 Starten Sie das Installationsprogramm für den XDAS-Client mit dem Befehl „rpm“.

4 Installieren Sie den XDAS-Client gemäß den Anweisungen auf dem Bildschirm.

5 Sobald die Installation abgeschlossen ist, starten Sie den XDAS-Client, sodass Audit-Ereignisse automatisch von Analyzer empfangen und angezeigt werden.

VII Konfiguration des Single-Sign-On-Zugriffs in Identity Manager

Standardmäßig erfolgt der Single-Sign-On-Zugriff in Identity Manager über OSP. Beim Installieren der Identitätsberichterstellung und der Identitätsanwendungen legen Sie die grundlegenden Einstellungen für die Benutzerauthentifizierung fest. Sie können den OSP-Authentifizierungsserver jedoch auch für die Authentifizierung per Kerberos-Ticketserver oder SAML-IDP konfigurieren. So können Sie beispielsweise die Authentifizierung aus NetIQ Access Manager über SAML unterstützen.

16 Vorbereiten der Konfiguration des Single-Sign-On-Zugriffs

Standardmäßig erfolgt der Single-Sign-On-Zugriff in Identity Manager über OSP. Beim Installieren der Identitätsberichterstellung und der Identitätsanwendungen legen Sie die grundlegenden Einstellungen für die Benutzerauthentifizierung fest. Sie können den OSP-Authentifizierungsserver jedoch auch für die Authentifizierung per Kerberos-Ticketserver oder SAML-IDP konfigurieren. So können Sie beispielsweise die Authentifizierung aus NetIQ Access Manager über SAML unterstützen.

NetIQ empfiehlt, die Schritte in der nachfolgenden Checkliste auszuführen.

	Checkliste
❑	1. Installieren Sie die Identitätsanwendungen. Weitere Informationen finden Sie in Kapitel 9, „Installieren der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting“, auf Seite 91.
❑	2. (Optional) Installieren Sie die Identitätsberichterstellung. Weitere Informationen finden Sie in Kapitel 9, „Installieren der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting“, auf Seite 91.
❑	3. Konfigurieren Sie die Identitätsanwendungen für den Single-Sign-On-Zugriff per OSP. Weitere Informationen finden Sie in Kapitel 17, „Single-Sign-On-Zugriff in Identity Manager mit One SSO Provider (OSP)“, auf Seite 201.
❑	4. Installieren Sie das gewünschte Authentifizierungssystem für Identity Manager. Beispiel: Access Manager oder Kerberos.
❑	5. (Bedingt) Konfigurieren Sie Access Manager und OSP. Weitere Informationen finden Sie in Kapitel 18, „Single Sign-On per SAML-Authentifizierung mit NetIQ Access Manager“, auf Seite 205.
❑	6. Überprüfen Sie die Single-Sign-On-Einstellungen. Weitere Informationen finden Sie in Kapitel 19, „Überprüfen des Single-Sign-On-Zugriffs auf die Identitätsanwendungen“, auf Seite 213.

17 Single-Sign-On-Zugriff in Identity Manager mit One SSO Provider (OSP)

Für den Single-Sign-On-Zugriff auf die Identitätsanwendungen müssen Sie die Einstellungen im RBPM-Konfigurationsprogramm konfigurieren. Aus der Installation von OSP sollten Sie bereits die erforderlichen Zertifikate und Schlüssel für das Single Sign-On besitzen.

Bei diesem Verfahren wird vorausgesetzt, dass in Ihrer Umgebung ein einziges Zertifikat für eDirectory, den SSO-Controller und den OAuth-Anbieter verwendet wird. Wenn in Ihrem Unternehmen eine zusätzliche Trennung erforderlich ist, erstellen Sie ein zusätzliches Zertifikat für den OAuth-Anbieter.

17.1 Vorbereiten von eDirectory auf den Single-Sign-On-Zugriff

Im Rahmen der eDirectory-Installation müssen Sie das Identitätsdepot so konfigurieren, dass der Single-Sign-On-Zugriff für die Identitätsanwendungen und die Identitätsberichterstellung unterstützt wird.

Führen Sie die Schritte in aus. Wenn Sie das eDirectory-Schema bereits mit dem SAML-Schema erweitert und die erforderlichen NMAS-Methoden installiert haben, müssen Sie diese Schritte nicht erneut ausführen. Fahren Sie stattdessen mit dem Unterabschnitt über das Erstellen des Herkunftsverbürgungscontainers fort.

17.2 Bearbeiten der grundlegenden Einstellungen für den Single-Sign-On-Zugriff

Beim Installieren der Identitätsanwendungen konfigurieren Sie in der Regel die grundlegenden Einstellungen für den Single-Sign-On-Zugriff. Mit den Angaben in diesem Abschnitt überprüfen Sie, ob die Einstellungen für Ihre Umgebung geeignet sind.

1. Führen Sie das RBPM-Konfigurationsprogramm aus. Weitere Informationen finden Sie in Abschnitt 11.6.1, „Ausführen des Konfigurationsprogramms der Identitätsanwendungen“, auf Seite 144.
2. Ändern Sie die Authentifizierungseinstellungen mit den folgenden Schritten:
   - **2a** Klicken Sie auf **Authentifizierung**.
   - **2b** (Bedingt) Soll der DNS-Name oder die IP-Adresse des tatsächlichen Servers angegeben werden, ändern Sie alle Instanzen von `localhost`.
     - Die angegebene Adresse muss von allen Clients aus auflösbar sein. Verwenden Sie `localhost` nur dann, wenn der gesamte Zugriff auf Identity Manager (auch über einen Browser) ausschließlich lokal erfolgen soll.

- Dieser „öffentliche“ Hostname (bzw. diese „öffentliche“ IP-Adresse) muss mit dem Wert für *`PublicServerName`* identisch sein, den Sie beim Installieren von OSP angegeben haben.
- In einer dezentralen Umgebung oder einer Cluster-Umgebung müssen alle OAuth-URLs identisch sein. Die URL sollte den Client-Zugriff über den L4-Switch oder den Lastenausgleich leiten. Außerdem müssen die Datei `osp.war` und die Konfigurationsdateien in jeder Bereitstellung in der Umgebung installiert sein.

2c Klicken Sie unter **LDAP-DN für Admin-Container** auf die Schaltfläche **>Durchsuchen**, und wählen Sie den Container mit dem Identitätsdepot aus, in dem sich der Administrator für die Identitätsanwendungen befindet.

2d Geben Sie die OAuth-Keystore-Datei an, die Sie beim Installieren von OSP erstellt haben.

Geben Sie den Pfad der Keystore-Datei, das Passwort für die Keystore-Datei, das Schlüsselalias und das Schlüsselpasswort an. Die standardmäßige Keystore-Datei ist `osp.jks`, und das standardmäßige Schlüsselalias lautet `osp`.

3 Ändern Sie die Single-Sign-On-Einstellungen mit den folgenden Schritten:

3a Klicken Sie auf **SSO-Clients**.

3b (Bedingt) Soll der DNS-Name oder die IP-Adresse des tatsächlichen Servers angegeben werden, ändern Sie alle Instanzen von `localhost`.

- Die angegebene Adresse muss von allen Clients aus auflösbar sein. Verwenden Sie `localhost` nur dann, wenn der gesamte Zugriff auf das Dashboard (auch über einen Browser) ausschließlich lokal erfolgen soll.
- Dieser „öffentliche“ Hostname (bzw. diese „öffentliche“ IP-Adresse) muss mit dem Wert für *`PublicServerName`* identisch sein, den Sie beim Installieren von OSP angegeben haben.
- In einer dezentralen Umgebung oder einer Cluster-Umgebung müssen alle OAuth-Umleitungs-URLs identisch sein. Die URL sollte den Client-Zugriff über den L4-Switch oder den Lastenausgleich leiten.

3c (Bedingt) Wenn Sie nicht standardmäßige Ports verwenden, aktualisieren Sie die Port-Nummern für die folgenden Identity Manager-Komponenten:

- Verwaltung der Identitätsanwendungen
- Identity Manager-Dashboard
- Identitätsberichterstellung
- Benutzeranwendung

4 Speichern Sie die Änderungen mit **OK**, und schließen Sie das Konfigurationsprogramm.

5 Starten Sie Tomcat.

17.3 Konfigurieren von SSPR für das Verbürgen des OSP

Damit Single Sign-On ordnungsgemäß funktioniert, müssen Sie ein Verbürgungsverhältnis zwischen dem OSP und der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung (SSPR) konfigurieren. Hierzu exportieren Sie ein Zertifikat aus der Keystore-Datei des OSP (`osp.jks`).

Importieren Sie das Zertifikat anschließend in die Keystore-Datei für SSPR.

Weitere Informationen zum Einrichten eines sicheren Kanals finden Sie unter „Setting Up a Secure Channel Between the Application Server and the LDAP Server “ (Einrichten eines sicheren Kanals zwischen dem Anwendungsserver und dem LDAP-Server) im „Self Service Password Reset Administration Guide“ (Administrationshandbuch für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung).

18 Single Sign-On per SAML-Authentifizierung mit NetIQ Access Manager

In diesem Abschnitt wird beschrieben, wie Sie NetIQ Access Manager und OSP für die Unterstützung des Single-Sign-On-Zugriffs in Identity Manager über die SAML 2.0-Authentifizierung konfigurieren. Lesen Sie zunächst die folgenden Überlegungen zu diesen Anweisungen:

- Sie haben eine neue, unterstützte Version von Access Manager installiert.
- Sie haben eine neue Version von Identity Manager installiert.
- Bei beiden Installationen wird der Hostname als DNS-Name konfiguriert.
- Bei beiden Installationen erfolgt die Kommunikation über das SSL-Protokoll.
- Sie müssen eine Cluster-Umgebung für Access Manager einrichten, in der das Identitätsdepot als LDAP-Benutzerspeicher fungiert. Weitere Informationen finden Sie im *NetIQ Access Manager Administration Guide* (Administratorhandbuch zu NetIQ Access Manager).

18.1 Erläuterungen zur Drittanbieter-Authentifizierung und zu Single Sign-On

Sie können Identity Manager für die Verwendung von NetIQ Access Manager über die SAML 2.0-Authentifizierung konfigurieren. Hierdurch können Sie sich über eine Technologie, die nicht auf Passwörtern beruht, über Access Manager bei den Identitätsanwendungen anmelden. Die Benutzer können sich beispielsweise über ein Benutzerzertifikat (Client-Zertifikat) anmelden, das sich z. B. auf einer Smartcard befindet.

Access Manager ordnet die Benutzer über OSP einem DN im Identitätsdepot zu. Wenn sich ein Benutzer über Access Manager bei den Identitätsanwendungen anmeldet, kann Access Manager eine SAML-Assertion (mit dem DN des Benutzers als Kennung) in einen HTTP-Header einfügen und die Anforderung an die Identitätsanwendungen weiterleiten. Die Identitätsanwendungen stellen über die SAML-Assertion eine LDAP-Verbindung mit dem Identitätsdepot her.

Zubehör-Portlets, bei denen die Single-Sign-On-Authentifizierung mithilfe von Passwörtern erfolgt, unterstützen das Single Sign-On nicht, wenn die Authentifizierung bei den Identitätsanwendungen per SAML-Assertion vorgenommen wird.

18.2 Erstellen und Installieren von SSL-Zertifikaten

Damit die Authentifizierung gewährleistet ist, müssen Access Manager und OSP die Herkunftsverbürgung ihrer SSL-Zertifikate freigeben. In diesem Abschnitt wird beschrieben, wie Sie ein neues Zertifikat für Access Manager erstellen und dann dafür sorgen, dass den Truststores die richtigen Zertifikate zur Verfügung stehen.

- Abschnitt 18.2.1, „Erstellen eines SSL-Zertifikats für Access Manager“, auf Seite 206
- Abschnitt 18.2.2, „Installieren des Access Manager-Zertifikats im Identity Manager-Truststore“, auf Seite 207
- Abschnitt 18.2.3, „Installieren des SSL-Serverzertifikats im Access Manager-Truststore“, auf Seite 207

18.2.1 Erstellen eines SSL-Zertifikats für Access Manager

Access Manager kann nicht über das eigene standardmäßige SSL-Zertifikat (`test-connector`) mit Identity Manager kommunizieren. Sie müssen stattdessen ein Zertifikat erstellen, bei dem der Hostname im Betreff-Feld eingetragen ist, und dieses Zertifikat dann zu Access Manager zuweisen.

Weitere Informationen finden Sie unter „Security and Certificate Management“ (Sicherheit und Zertifikatsverwaltung) im *NetIQ Access Manager Administration Console Guide* (Handbuch zur NetIQ Access Manager-Verwaltungskonsole).

1. Öffnen Sie die Verwaltungskonsole in Access Manager.
2. Klicken Sie auf **Sicherheit > Zertifikate**.
3. Klicken Sie auf **Neu**.
4. Geben Sie einen Namen für das neue Zertifikat an. Beispiel: *`hostname`*`_ssl`.
5. Klicken Sie rechts im Fenster auf die Schaltfläche „Bearbeiten“.
6. Geben Sie unter **Eigenname** den DNS-Namen des Servers an, auf dem Access Manager gehostet wird, und klicken Sie auf **OK**.
7. Geben Sie unter **Gültigkeit (Monate)** einen Wert bis 99 ein.
8. Geben Sie unter **Schlüsselgröße** den Wert `2048` ein.
9. Wählen Sie das soeben erstellte Zertifikat aus, und klicken Sie auf **Aktionen > Zertifikat zu Keystores hinzufügen**.
10. Klicken Sie rechts neben **Keystores** auf die Schaltfläche „Bearbeiten“.
11. Wählen Sie **SSL-Connector**, und klicken Sie auf **OK**.
12. Klicken Sie auf **OK**.
13. Installieren Sie das neue Zertifikat im OSP-Truststore. Weitere Informationen finden Sie in Abschnitt 18.2.2, „Installieren des Access Manager-Zertifikats im Identity Manager-Truststore“, auf Seite 207.

18.2.2 Installieren des Access Manager-Zertifikats im Identity Manager-Truststore

Der OSP-Truststore muss das Sicherheitszertifikat für Access Manager umfassen.

1 Exportieren Sie das neue SSL-Zertifikat mit den folgenden Schritten:
   - Exportieren Sie unter Sicherheit > Herkunftsverbürgungen **in der Verwaltungskonsole von Access Manager das Stammzertifikat des SSL-Zertifikats.** Geben Sie den Namen **configCA** für das Stammzertifikat ein.
   - Exportieren Sie das SSL-Serverzertifikat.

     Weitere Informationen finden Sie unter „Managing Trusted Roots and Trust Stores“ (Verwalten von Herkunftsverbürgungen und Truststores) im *NetIQ Access Manager Administration Console Guide* (Handbuch zur NetIQ Access Manager-Verwaltungskonsole).
2 Kopieren Sie das exportierte Zertifikat auf den Server, auf dem OSP ausgeführt wird.
3 Importieren Sie die Datei mit dem Java-Keytool in den cacerts-Keystore der JRE.

   Beispiel: `/opt/netiq/common/jre/bin/keytool -importcert -trustcacerts -alias <NAM-Zertifikat> -keystore /opt/netiq/common/jre/lib/security -storepass <Passwort> -file custom_location/<exportierte_Datei>`
4 Installieren Sie das OSP-Zertifikat im Access Manager-Truststore.

   Weitere Informationen finden Sie in Abschnitt 18.2.3, „Installieren des SSL-Serverzertifikats im Access Manager-Truststore“, auf Seite 207.

18.2.3 Installieren des SSL-Serverzertifikats im Access Manager-Truststore

Der Access Manager-Truststore muss das Sicherheitszertifikat für OSP umfassen. Weitere Informationen finden Sie unter „Managing Trusted Roots and Trust Stores“ (Verwalten von Herkunftsverbürgungen und Truststores) im *NetIQ Access Manager Administration Console Guide* (Handbuch zur NetIQ Access Manager-Verwaltungskonsole).

Rufen Sie das Serverzertifikat ab, das für SSL von der Tomcat-Instanz verwendet wird, auf der OSP ausgeführt wird.

1 Kopieren Sie das SSL-Serverzertifikat der Tomcat-Instanz, in der OSP gehostet wird, auf den Server, auf dem Sie Access Manager installiert haben.
2 Öffnen Sie die Verwaltungskonsole in Access Manager.
3 Klicken Sie zum Importieren des Zertifikats auf **Sicherheit > NIDP-Truststore**.
4 Klicken Sie auf **Hinzufügen**.
5 Wählen Sie "Herkunftsverbürgung" unter **Dialogfeld hinzufügen** > **Importieren** aus.
6 Wählen Sie das zu importierende Stammzertifikat aus, und klicken Sie auf **OK**.
7 Überprüfen Sie, ob OSP die Authentifizierungsverknüpfungen von SAML erkennt.

   Weitere Informationen finden Sie in Abschnitt 18.4.2, „Erstellen eines Attributsatzes für SAML“, auf Seite 209.

18.3 Konfigurieren von Identity Manager für das Verbürgen von Access Manager

Identity Manager benötigt die URL der SAML-Metadaten, damit Benutzer für Authentifizierungsanforderungen umgeleitet werden können. Standardmäßig speichert Access Manager die SAML-Metadaten unter der folgenden URL:

`https://server:port/nidp/saml2/metadata`

Server:*Port* bezeichnet hierbei den Access Manager-Identitätsserver.

1. (Optional) Sollen die SAML-Metadaten als `.xml`-Dokument angezeigt werden, öffnen Sie die URL in einem Browser.

   Wenn die URL nicht zum gewünschten Dokument führt, überprüfen Sie, ob der Link fehlerfrei ist.
2. Führen Sie auf dem OSP-Server das RBPM-Konfigurationsprogramm aus. Weitere Informationen finden Sie in Abschnitt 11.6.1, „Ausführen des Konfigurationsprogramms der Identitätsanwendungen“, auf Seite 144.
3. Wählen Sie im Dienstprogramm die Option **Authentifizierung**.
4. Wählen Sie unter **Authentifizierungsmethode** die Option **SAML 2.0**.
5. Geben Sie unter **Metadaten-URL** die URL an, mit der OSP die Authentifizierungsanforderungen an SAML-Metadaten von Access Manager weiterleitet.

   Beispiel: `https://Server:Port/nidp/saml2/metadata`
6. Geben Sie im Abschnitt **Authentifizierungsserver** unter **Hostkennung für OAuth-Server** den DNS-Namen des Servers an, auf dem OSP gehostet wird.
7. Klicken Sie zum Speichern der Änderungen auf **OK**.
8. Starten Sie die Tomcat-Instanz neu, in der OSP gehostet wird.

18.4 Konfigurieren von Access Manager für die Verwendung von Identity Manager

Damit Identity Manager in Access Manager als verbürgter Dienstanbieter erkannt wird, fügen Sie den Metadatentext für OSP zum Identitätsserver hinzu, und konfigurieren Sie einen Attributsatz. Dieser Vorgang umfasst folgende Schritte:

18.4.1 Kopieren der Metadaten für Identity Manager

Access Manager benötigt den Metadatentext für OSP. Kopieren Sie den Inhalt der Metadaten-`.xml`-Datei in ein Dokument, das Sie auf dem Access Manager-Identitätsserver öffnen können.

1. Navigieren Sie in einem Browser zur URL der OSP-Metadaten. Standardmäßig verwendet Identity Manager die folgende URL:

   `https://server:port/osp/a/idm/auth/saml2/spmetadata`

   Server:*Port* bezeichnet hierbei den Tomcat-Server, auf dem OSP gehostet wird.

2 Öffnen Sie den Seitenquelltext für die Datei `spmetadata.xml`.

3 Kopieren Sie den Inhalt der Datei in ein Dokument, auf das Sie unter „Hinzufügen von Identity Manager als verbürgter Dienstanbieter“, auf Seite 209 zugreifen können..

18.4.2 Erstellen eines Attributsatzes für SAML

Damit SAML die Verknüpfungen zwischen Access Manager und OSP austauschen kann, erstellen Sie einen Attributsatz in Access Manager. Attributsätze bieten ein gemeinsames Namensschema für den Austausch. OSP sucht nach einem Attributwert, der den Betreff der Verknüpfung kennzeichnet. Standardmäßig lautet das Attribut `mail`.

Weitere Informationen finden Sie unter „Configuring Attribute Sets“ (Konfigurieren von Attributsätzen) im *NetIQ Access Manager Identity Administration Guide* (Administratorhandbuch zu NetIQ Access Manager).

1 Öffnen Sie die Verwaltungskonsole in Access Manager.

2 Klicken Sie auf **Geräte > Identitätsserver > Gemeinsame Einstellungen > Attributsätze > Neu**.

3 Geben Sie einen Namen für den Attributsatz an. Beispiel: `IDM-SAML-Attribute`.

4 Klicken Sie auf **Weiter** und dann auf **Neu**.

5 Wählen Sie unter **Lokales Attribut** die Option **LDAP-Attribut: mail [LDAP-Attributprofil]**.

6 Wählen Sie unter **Remote-Attribut** die Option `mail`.

7 Klicken Sie auf **OK** und dann auf **Fertig stellen**.

18.4.3 Hinzufügen von Identity Manager als verbürgter Dienstanbieter

Konfigurieren Sie Access Manager so, dass Identity Manager als verbürgter Dienstanbieter erkannt wird. Weitere Informationen finden Sie unter „Creating a Trusted Service Provider for SAML 2.0“ (Erstellen eines verbürgten Dienstanbieters für SAML 2.0) im *NetIQ Access Manager Administration Guide* (Administratorhandbuch zu NetIQ Access Manager).

1 Öffnen Sie die Verwaltungskonsole in Access Manager.

2 Klicken Sie auf **Geräte > Identitätsserver > Bearbeiten > SAML 2.0**.

3 Klicken Sie auf **Neu > Dienstanbieter**

4 Wählen Sie unter **Anbietertyp** die Option **Allgemein**.

5 Wählen Sie unter **Ursprung** die Option **Metadatentext**.

6 Fügen Sie in das Feld **Text** den Inhalt der Datei `spmetadata.xml` ein, den Sie in „Kopieren der Metadaten für Identity Manager“, auf Seite 208 kopiert haben.

7 Geben Sie einen Namen für den neuen OSP-Dienstanbieter an.

8 Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

9 Wählen Sie auf der Registerkarte **SAML 2.0** den OSP-Dienstanbieter aus, den Sie in Schritt 7 erstellt haben.

10 Klicken Sie auf **Attribute**.

11 Wählen Sie den Attributsatz aus, den Sie in „Erstellen eines Attributsatzes für SAML“, auf Seite 209 erstellt haben. Beispiel: `IDM-SAML-Attribute`.

12 Verschieben Sie die verfügbaren Attribute für den OSP-Dienstanbietersatz in die Kontrollleiste **Mit Authentifizierung senden** links auf der Seite.

   Die Attribute, die Sie in die Kontrollleiste **Mit Authentifizierung senden** verschieben, sind die Attribute, die während der Authentifizierung abgerufen werden sollen.

13 Klicken Sie zwei Mal auf **OK**.

14 Aktualisieren Sie den Identitätsserver mit **Geräte > Identitätsserver > Aktualisieren > Gesamte Konfiguration aktualisieren**.

18.5 Aktualisieren der Anmeldeseiten für Access Manager

Die standardmäßigen Anmeldeseiten für Access Manager umfassen HTML-iFrame-Elemente, die sich mit den Elementen für die Identitätsanwendungen überschneiden. In diesem Abschnitt finden Sie Anweisungen, wie Sie eine neue Anmeldemethode und einen neuen Vertrag für Access Manager erstellen und so diesen Konflikt beheben. Die in diesem Abschnitt genannten `.jsp`-Dateien befinden sich standardmäßig im Verzeichnis `/opt/novell/idm/apps`.

Weitere Informationen finden Sie unter „Customizing the Identity Server Login Page“ (Anpassen der Identitätsserver-Anmeldeseite) im *NetIQ Access Manager Administration Guide* (Administratorhandbuch zu NetIQ Access Manager).

1 Bearbeiten Sie die `top.jsp`-Datei gemäß TID 7004020 und TID 7018468.

2 (Optional) Zur Sicherung kopieren Sie die Datei `login.jsp`, und benennen Sie sie um. Benennen Sie die Datei beispielsweise in `idm_login.jsp` um.

3 Öffnen Sie die Verwaltungskonsole in Access Manager.

4 Erstellen Sie eine neue Anmeldemethode mit den folgenden Schritten:

   4a Klicken Sie auf **Geräte > Identitätsserver > Bearbeiten > Lokal > Methoden**.

   4b Klicken Sie auf **Neu**, und geben Sie unter **Anzeigename** den Anzeigenamen für die neue Methode ein. Beispiel: `IDM-Name/Passwort`.

   4c Wählen Sie unter **Klasse** die Option **Name/Passwort-Form**.

   4d Wählen Sie unter **Benutzerspeicher** das Identitätsdepot als LDAP-Benutzerspeicher aus.

   4e Klicken Sie im Abschnitt **Eigenschaften** auf **Neu**, und legen Sie die folgenden Eigenschaften fest:

Name	Wert
JSP	idm_login
MainJSP	true

   4f Klicken Sie auf **OK**.

5 Erstellen Sie einen neuen Vertrag, der die neue Anmeldemethode verwendet, mit den folgenden Schritten:

   5a Klicken Sie auf **Verträge > Neu**.

   5b Geben Sie auf der Registerkarte **Konfiguration** unter **Anzeigename** den Anzeigenamen für den neuen Vertrag ein. Beispiel: `IDM-Name/Passwort`.

   5c Geben Sie unter **URI** den Text `name/password/uri/idm` an.

5d Fügen Sie unter **Methoden** die Methode hinzu, die Sie in Schritt 4 erstellt haben. Beispiel: `IDM-Name/Passwort`.

5e Geben Sie auf der Registerkarte **Authentifizierungskarten** eine **ID** für die Karte an. Beispiel: `IDM_NamePasswort`.

5f Geben Sie ein Image für die Karte an.

5g Klicken Sie auf **OK**.

6 Legen Sie mit den folgenden Schritten die Standardwerte fest, wie der neue Authentifizierungsvertrag im System verarbeitet werden soll:

6a Klicken Sie auf der Registerkarte **Lokal** auf **Standardwerte**.

6b Wählen Sie unter „Benutzerspeicher“ das Identitätsdepot als LDAP-Benutzerspeicher aus.

6c Wählen Sie unter **Authentifizierungsvertrag** den Vertrag aus, den Sie in Schritt 5 erstellt haben. Beispiel: `IDM-Name/Passwort-Form`.

6d Klicken Sie auf **OK**.

7 Aktualisieren Sie den Identitätsserver mit **Geräte > Identitätsserver > Aktualisieren > Gesamte Konfiguration aktualisieren**.

19 Überprüfen des Single-Sign-On-Zugriffs auf die Identitätsanwendungen

Sobald Sie die Identitätsanwendungen installiert und die Einstellungen für Single Sign-On konfiguriert haben, überprüfen Sie, ob Sie sich bei den einzelnen Anwendungen anmelden und dann zwischen den Anwendungen wechseln können, ohne sich jeweils abmelden zu müssen. Standardmäßig enthält der URL-Link der Anwendungen das folgende Suffix:

- Verwaltung der Identitätsanwendungen: `/idmadmin`
- Identity Manager-Dashboard: `/idmdash`
- Benutzeranwendung: `/IDMProv`
- Identitätsberichterstellung: `/IDMRPT`

Passen Sie das Suffix bei Bedarf mit dem RBPM-Konfigurationsprogramm an. Weitere Informationen finden Sie in Kapitel 11.6, „Konfigurieren der Einstellungen für die Identitätsanwendungen“, auf Seite 143.

So überprüfen Sie die Funktionsfähigkeit von Single Sign-On:

1. Öffnen Sie ein neues Browserfenster auf dem Identitätsanwendungsserver und geben Sie die URL des Dashboards ein:

   `https://server:port/idmdash`

   Melden Sie sich nicht beim Dashboard an.
2. Navigieren Sie im Browser zur Benutzeranwendung:

   `https://server:port/IDM-context`
3. Überprüfen Sie, ob die Benutzeranwendung dieselbe Anmeldeseite anzeigt wie in Schritt 1.
4. Melden Sie sich bei der Benutzeranwendung an.
5. Klicken Sie oben rechts auf das Symbol **Startseite** und überprüfen Sie, ob Sie auf das Dashboard zugreifen können, ohne sich erneut anmelden zu müssen.

20 Sichere Kommunikation mit SSL

Die Identitätsanwendungen und die Identitätsberichterstellung nehmen die Authentifizierung über HTML-Formulare vor. Beim Anmeldevorgang wird daher unter Umständen der Benutzerberechtigungsnachweis offengelegt. NetIQ empfiehlt, das SSL-Protokoll zum Schutz vertraulicher Daten zu aktivieren. Mit dem SSL-Protokoll wird gewährleistet, dass zwischen Komponenten des Identity Manager stattfindende Kommunikationen geschützt werden.

Zur Konfiguration des Tomcat-Servers für die Kommunikation über SSL sind Zertifikate erforderlich. Diese Zertifikate können Sie mit zwei Verfahren erhalten:

- Von vertrauenswürdiger externer Zertifizierungsstelle (Certificate Authority, CA) ausgestelltes Zertifikat
- Eigensigniertes Zertifikat

Das Installationsprogramm konfiguriert die Identitätsanwendungen und die Identity Reporting-Komponenten anhand des vom Identitätsdepot ausgestellten Zertifikats automatisch mit einer sicheren Verbindung (HTTPS). In·einer·Produktionsumgebung wird empfohlen, ein von einer externen Zertifizierungsstelle ausgestelltes Zertifikat zu verwenden.

20.1 Checkliste für SSL-Verbindungen

NetIQ empfiehlt, die Schritte in der folgenden Checkliste auszuführen, damit sichere Verbindungen zwischen den Identitätsanwendungen, der Identitätsberichterstellung, SSPR und OSP gewährleistet sind:

	Checkliste
❑	1. Verwenden Sie Keystore, um Authentifizierungszertifikate zu speichern. Weitere Informationen finden Sie in Abschnitt 20.2, „Erstellen eines Keystore und eines Zertifizierungsantrags“, auf Seite 216.
❑	2. (Bedingt) Sie können in Ihrer Umgebung ein von einer externen CA ausgestelltes oder ein eigensigniertes Zertifikat verwenden. Weitere Informationen finden Sie in Abschnitt 20.4, „Aktivieren von SSL mit einem eigensignierten Zertifikat“, auf Seite 219. Für Produktionsumgebungen werden von externen CA ausgestellte Zertifikate empfohlen.
❑	3. (Bedingt) In einer Produktionsumgebung importieren Sie ein signiertes Zertifikat. Weitere Informationen finden Sie in Abschnitt 20.3, „Aktivieren von SSL mit einem externen, CA-signierten Zertifikat“, auf Seite 217.
❑	4. Konfigurieren Sie Authentifizierungsserver, Identitätsanwendungen und Identitätsberichterstellung so, dass sie SSL-Kommunikation unterstützen. Weitere Informationen hierzu finden Sie in Abschnitt 20.6, „Aktualisieren der SSL-Einstellungen für den Anwendungsserver“, auf Seite 224 und Abschnitt 20.7, „Aktualisieren der SSL-Einstellungen im Konfigurationsprogramm“, auf Seite 225.

20.2 Erstellen eines Keystore und eines Zertifizierungsantrags

Ein Keystore ist eine Java-Datei, die Verschlüsselungsschlüssel und (optional) Sicherheitszertifikate enthält. Der Keystore kann mit dem Java-Dienstprogramm in der JRE erstellt werden. Sie erstellen die `.jks`-Datei und generieren ein Zertifikat in den Keystore. Jedes Zertifikat ist mit einem eindeutigen Alias verknüpft. Sie platzieren den Keystore im `conf`-Verzeichnis für Ihren Anwendungsserver, der die Identitätsanwendungen und die Identitätsberichterstellung unterstützt.

Das Installationsprogramm erstellt standardmäßig einen Keystore (`tomcat.ks`) im Verzeichnis `/opt/netiq/idm/apps/tomcat/conf` und konfiguriert die `https`-Verbindung mithilfe dieses Keystores. Wenn Sie eine Keystore-Datei mit demselben Namen erstellen, wird diese Keystore-Datei in diesem Verzeichnis ersetzt.

1. Navigieren Sie in einer Befehlszeile zum `conf`-Verzeichnis für Ihre Anwendungsserverinstallation, in der Sie die Identitätsanwendungen bereitgestellt haben. Beispiel: `/opt/netiq/idm/apps/tomcat/conf`.

   Der Pfad `tomcat/conf` ist der standardmäßige Pfad der Identitätsanwendungen in Tomcat. Der Pfad ist abhängig vom Installationsort für die Anwendung und Tomcat.

2. Legen Sie mithilfe des folgenden Befehls den Umgebungspfad für die Keystore-Erstellung fest:

   ```
   cd /opt/netiq/idm/apps/tomcat/conf
   export PATH=/opt/netiq/common/jre/bin:$PATH
   ```

3. Erstellen Sie den Keystore mit folgendem Befehl:

   ```
   keytool -genkey -alias keystore_name -keyalg RSA -keystore
   keystore_name.keystore -validity 3650 -keysize 2048
   ```

   Beispiel:

   ```
   keytool -genkey -alias IDMkey -keyalg RSA -keystore IDMkey.keystore -validity
   3650 -keysize 2048
   ```

4. Wenn Sie dazu aufgefordert werden, geben Sie die Parameterwerte gemäß den folgenden Überlegungen an:

   - Geben Sie als Vor- und Nachnamen den vollständig qualifizierten Namen des Servers an. Beispiel:

     ```
     MyTomcatServer.NetIQ.com
     ```

   - Achten Sie auf die richtige Schreibweise. Bei Schreibfehlern treten Fehler im generierten signierten Zertifikat der Signierungsstelle auf.

5. (Optional) Erstellen Sie eine einfache Textdatei, und speichern Sie darin eine Kopie der Parameterwerte.

   Auf diese Weise ist sichergestellt, dass Sie stets dieselben Daten angeben, wenn Sie einen Antrag an die Signierungsstelle richten und das Zertifikat importieren.

6. Kopieren Sie die Keystore-Datei in das Verzeichnis `tomcat/conf` für jede Anwendungsserverinstanz, in der Sie die Identity Manager-Komponenten und SSPR bereitgestellt haben.

7. Generieren Sie den CA-Zertifizierungsantrag mit den folgenden Schritten:

   7a Erstellen Sie im Verzeichnis `conf` eine einfache Textdatei mit dem Namen `Ihr_Antrag.csr`. Beispiel: `IDMZertAntrag.csr`.

   7b Führen Sie den folgenden Befehl aus:

```
keytool -certreq -v -alias keystore_name -file your_request.csr -keypass
keystore_password -keystore your.keystore -storepass your_password
```

Beispiel:

```
keytool -certreq -v -alias IDMkey.keystore -file IDMcertrequest.csr -
keypass IDMkeypass -keystore IDMkey.keystore -storepass IDMpass
```

Beim Ausführen des Befehls trägt das Keytool-Dienstprogramm die entsprechenden Daten für den Zertifizierungsantrag in die .csr-Datei ein.

8 (Bedingt) Reichen Sie für die Anforderung eines signierten Zertifikats die CRS-Datei bei einer gültigen Zertifizierungsstelle ein.

9 Kopieren Sie das Zertifikat in das Konfigurationsverzeichnis auf dem Anwendungsserver.

Beispiel: `/opt/netiq/idm/apps/tomcat/conf`.

10 Halten Sie Tomcat an.

Nach Erstellung eines Keystore und Erzeugung einer CA-Zertifizierungsanfrage. Folgen Sie den unten beschriebenen Schritten, um Zertifikate in den Keystore zu importieren:

- Angaben zu von externen CA signierten Zertifikaten finden Sie in Abschnitt 20.3, „Aktivieren von SSL mit einem externen, CA-signierten Zertifikat“, auf Seite 217.
- Angaben zu eigensignierten Zertifikaten finden Sie in Abschnitt 20.4, „Aktivieren von SSL mit einem eigensignierten Zertifikat“, auf Seite 219.

20.3 Aktivieren von SSL mit einem externen, CA-signierten Zertifikat

In einer Produktionsumgebung verwenden Sie ein signiertes Zertifikat, das von einer gültigen Zertifizierungsstelle ausgegeben wurde. In diesem Abschnitt wird beschrieben, wie Sie ein signiertes Zertifikat in den standardmäßigen Tomcat-Anwendungsserver für die Identitätsanwendungen importieren.

Bei diesem Verfahren wird vorausgesetzt, dass Ihnen ein signiertes Zertifikat einer gültigen Zertifizierungsstelle vorliegt. Weitere Informationen finden Sie in Abschnitt 20.2, „Erstellen eines Keystore und eines Zertifizierungsantrags“, auf Seite 216.

So verwenden Sie ein signiertes Zertifikat und SSL:

1 Kopieren Sie das Zertifikat in das Konfigurationsverzeichnis auf dem Anwendungsserver. Beispiel: `/opt/netiq/idm/apps/tomcat/conf`.

2 Konvertieren Sie das Stammzertifikat mit den folgenden Schritten in das DER-Format:

2a Doppelklicken Sie auf das Zertifikat im Verzeichnis `conf`.

2b Klicken Sie im Dialogfeld „Zertifikat“ auf **Zertifikatspfad**.

2c Wählen Sie das Stammzertifikat aus, das Sie von der Signierungsstelle erhalten haben.

2d Klicken Sie auf **Zertifikat anzeigen**.

2e Klicken Sie auf **Details > In Datei kopieren**.

2f Klicken Sie im Assistenten zum Exportieren von Zertifikaten auf **Weiter**.

2g Wählen Sie **DER-verschlüsselte Binärdatei für X.509 (.CER)**, und klicken Sie auf **Weiter**.

2h Erstellen Sie eine neue Datei für das soeben formatierte Zertifikat, und speichern Sie es im Verzeichnis `conf` auf dem Anwendungsserver.

Beispiel: `/opt/netiq/idm/apps/tomcat/conf`.

2i Klicken Sie auf **Fertig stellen**.

3 Importieren Sie das konvertierte Zertifikat mit den folgenden Schritten:

3a Navigieren Sie in einer Befehlszeile zum Verzeichnis `conf` auf dem Anwendungsserver.

3b Geben Sie den folgenden Befehl ein:

```
keytool -import -trustcacerts -alias root -keystore your.keystore -file
yourRootCA.der
```

Beispiel:

```
keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file
IDMTESTREE.der
```

HINWEIS: Sie müssen das Alias **Root** eingeben.

Nach dem Import des Zertifikats gibt der Server die Meldung aus, dass das **Zertifikat dem Keystore hinzugefügt wurde**.

3c Prüfen Sie mithilfe des folgenden Befehls, dass das signierte Zertifikat korrekt in das Verzeichnis `conf` importiert wurde:

```
keytool -list -v -alias root -keystore your.keystore
```

Beispiel:

```
keytool -list -v -alias root -keystore IDMkey.keystore
```

Der Server führt Ihre Zertifikate auf.

4 NetIQ empfiehlt, die signierten Zertifikate in „idm.jks“ zu importieren. In diesem zentralen Keystore werden alle Zertifikate gespeichert, die von den Identitätsanwendungen und Identity Reporting genutzt werden. Beispiel:

```
keytool -import -trustcacerts -alias root -keystore /opt/netiq/idm/apps/tomcat/
conf/idm.jks -file IDMTESTREE.der
```

5 Angaben zur Aktualisierung der SSL-Einstellungen für den Anwendungsserver finden Sie in Abschnitt 20.6, „Aktualisieren der SSL-Einstellungen für den Anwendungsserver“, auf Seite 224.

6 Aktualisieren Sie die SSL-Einstellungen im Konfigurationsprogramm. Weitere Informationen finden Sie in Abschnitt 20.7, „Aktualisieren der SSL-Einstellungen im Konfigurationsprogramm“, auf Seite 225.

7 Aktualisieren der SSL-Einstellungen für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung. Weitere Informationen finden Sie unter Abschnitt 20.8, „Aktualisieren der SSL-Einstellungen für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung“, auf Seite 227.

8 Starten Sie Tomcat neu.

20.4 Aktivieren von SSL mit einem eigensignierten Zertifikat

Sie können in Ihrer Testumgebung ein eigensigniertes Zertifikat verwenden. Dieses ist einfacher zu beschaffen ist als ein signiertes Zertifikat von einer gültigen Zertifizierungsstelle.

- Abschnitt 20.4.1, „Exportieren der Zertifizierungsstelle“, auf Seite 219
- Abschnitt 20.4.2, „Generieren eines eigensignierten Zertifikats“, auf Seite 220

20.4.1 Exportieren der Zertifizierungsstelle

Mit iManager können Sie die Zertifizierungsstelle (CA) aus Ihrem eDirectory-Server exportieren und so ein eigensigniertes Zertifikat generieren.

1. Melden Sie sich mit dem Benutzernamen und dem Passwort des eDirectory-Administrators bei iManager an.
2. Klicken Sie auf **Administration > Objekt bearbeiten**.
3. Wechseln Sie im Sicherheitscontainer zum CA-Objekt *Baumname*`CA.Security`.
   Beispiel:·`IDMTESTBAUM CA.Security`.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Zertifikate > Eigensigniertes Zertifikat**.
6. Wählen Sie das gewünschte eigensignierte Zertifikat aus.

   Beispiel: **Eigensigniertes RSA-Zertifikat**

   6a Prüfen Sie **Eigensigniertes RSA-Zertifikat**.

   6b Klicken Sie auf **Bestätigen**.
7. Klicken Sie auf **Exportieren**.
8. Deaktivieren Sie die Option **Privaten Schlüssel exportieren**.
9. Klicken Sie auf **Exportformat > DER**.
10. Klicken Sie auf **Weiter**.
11. Klicken Sie auf **Exportiertes Zertifikat speichern**.
12. Klicken Sie auf **Datei speichern**.

    iManager speichert die Datei als *Baumname* `cert.der`. Beispiel: `IDMTESTBAUM cert.der`.
13. Klicken Sie auf **Schließen**.
14. Kopieren Sie das Zertifikat in das Konfigurationsverzeichnis auf dem Anwendungsserver (`cert.der`).

    Beispiel: `/opt/netiq/idm/apps/tomcat/conf`.
15. Importieren Sie das Stammzertifikat mit den folgenden Schritten:

    15a Navigieren Sie mithilfe des folgenden Befehls zum Verzeichnis conf der Anwendungsserver-Installation:

    ```
    keytool -import -trustcacerts -alias root -keystore <keystore
    file>.keystore -file exported_certificate_filename.der
    ```

    Beispiel:

    ```
    keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file
    cert.der
    ```

HINWEIS: Sie müssen das Alias **Root** eingeben.

Nach dem Import des Zertifikats gibt der Server die Meldung aus, dass das **Zertifikat dem Keystore hinzugefügt wurde**.

15b NetIQ empfiehlt, Stammzertifikate auch in Java cacerts zu importieren.

Beispiel:

```
keytool -import -trustcacerts -alias root -keystore /opt/netiq/common/jre/
lib/security/cacerts -file cert.der
```

15c Prüfen Sie mithilfe des folgenden Befehls, dass das signierte Zertifikat korrekt in das Verzeichnis `conf` importiert wurde:

```
keytool -list -v -alias root -keystore your.keystore
```

Beispiel:

```
keytool -list -v -alias root -keystore IDMkey.keystore
```

Der Server führt die Zertifikate auf.

20.4.2 Generieren eines eigensignierten Zertifikats

Zum Erstellen eines eigensignierten Zertifikats benötigen Sie einen Keystore und eine Zertifizierungsantragsdatei. Weitere Informationen hierzu finden Sie unter, Abschnitt 20.2, „Erstellen eines Keystore und eines Zertifizierungsantrags“, auf Seite 216

1. Melden Sie sich bei iManager an.
2. Navigieren Sie zu **Certificate Server > Zertifikat ausstellen**.
3. Navigieren Sie zur `.csr`-Datei unter Abschnitt 20.2, „Erstellen eines Keystore und eines Zertifizierungsantrags“, auf Seite 216, die Sie in Schritt 7 erstellt haben.

   Beispiel: `IDMcertrequest.csr`
4. Klicken Sie zweimal auf **Weiter**.
5. Wählen Sie unter „Zertifikattyp“ die Option **Nicht angegeben**.
6. Klicken Sie zweimal auf **Weiter**.

   iManager speichert die Datei als `csr_Anforderungsname.der`. Beispiel: `IDMcertrequest.der`
7. Kopieren Sie das Zertifikat in das Konfigurationsverzeichnis auf dem Anwendungsserver (`IDMcertrequest.der`).

   Beispiel: `/opt/netiq/idm/apps/tomcat/conf`.
8. Importieren Sie das generierte eigensignierte Zertifikat mit den folgenden Schritten:

   8a Navigieren Sie mithilfe des folgenden Befehls zum Verzeichnis `conf` der Anwendungsserver-Installation:

   ```
   keytool -import -alias keystore_name -keystore <keystore_file> -file
   <signed_certificate_filename>.der
   ```

   Beispiel:

   ```
   keytool -import -alias IDMkey -keystore IDMkey.keystore -file
   IDMcertrequest.der
   ```

   HINWEIS: Sie müssen den Keystore-Namen als Alias angeben.

Nach dem Import des Zertifikats gibt der Server die Meldung aus, dass das **Zertifikat dem Keystore hinzugefügt wurde**.

8b NetIQ empfiehlt, eigensignierte Zertifikate auch in Java cacerts zu importieren.

Beispiel:

```
keytool -import -alias IDMkey -keystore
/opt/netiq/common/jre/lib/security/cacerts -file IDMcertrequest.der
```

8c Prüfen Sie mithilfe des folgenden Befehls, ob das signierte Zertifikat korrekt in das Verzeichnis `conf` importiert wurde:

```
keytool -list -v -alias keystore_name -keystore your.jks
```

Beispiel:

```
keytool -list -v -alias IDMkey -keystore IDMkey.jks
```

Der Server führt die Zertifikate auf.

9 Aktualisieren Sie die SSL-Einstellungen für den Anwendungsserver. Weitere Informationen finden Sie unter Abschnitt 20.6, „Aktualisieren der SSL-Einstellungen für den Anwendungsserver“, auf Seite 224.

10 Aktualisieren Sie die SSL-Einstellungen im Konfigurationsprogramm. Weitere Informationen finden Sie in Abschnitt 20.7, „Aktualisieren der SSL-Einstellungen im Konfigurationsprogramm“, auf Seite 225.

11 Aktualisieren der SSL-Einstellungen für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung. Weitere Informationen finden Sie unter Abschnitt 20.8, „Aktualisieren der SSL-Einstellungen für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung“, auf Seite 227.

12 Starten Sie Tomcat neu.

20.5 Aktivieren von SSL zwischen Sentinel und Identity Manager-Komponenten

Um die sichere Kommunikation zwischen Sentinel und den Identity Manager-Komponenten zu gewährleisten, können Sie ein eigensigniertes Serverzertifikat erstellen und exportieren. Verwenden Sie ein signiertes Zertifikat, das von einer gültigen Zertifizierungsstelle ausgestellt wurde.

20.5.1 Aktivieren von SSL zwischen Sentinel und Identity Manager-Engine/Remote Loader

1 Erstellen Sie mit den folgenden Schritten ein neues Zertifikat:

1a Melden Sie sich bei iManager an.

1b Klicken Sie auf **NetIQ Certificate Server** > **Create Server Certificate** (Serverzertifikat erstellen).

1c Wählen Sie den gewünschten Server aus.

1d Geben Sie einen Kurznamen für den Server ein.

1e Übernehmen Sie die restlichen Standardeinstellungen für das Zertifikat.

2 Exportieren Sie das Serverzertifikat mit den folgenden Schritten in das `.pfx`-Format:

2a Wählen Sie in iManager die Option **Verzeichnisverwaltung** > **Objekt bearbeiten**.

2b Navigieren Sie zum Schlüsselmaterialobjekt (Key Material Object, (KMO), und wählen Sie es aus.

2c Klicken Sie auf **Zertifikate** > **Exportieren**.

2d Stellt das Passwort bereit.

2e Speichern Sie das Serverzertifikat als PKCS#12-Datei. Beispiel: `certificate.pfx`.

3 Extrahieren Sie den privaten Schlüssel mit dem nachfolgenden Befehl aus dem exportierten Zertifikat in die Datei `dxipkey.pem`.

```
openssl pkcs12 -in certificate.pfx -nocerts -out dxipkey.pem –nodes
```

4 Extrahieren Sie das Zertifikat in die Datei `dxicert.pem`.

```
openssl pkcs12 -in certificate.pfx -nokeys -out dxicert.pem
```

5 Möchten Sie das CA-Zertifikat des eDirectory-Servers, das Sie unter Schritt 1 erstellt haben, im Format Base64 exportieren, gehen Sie wie folgt vor:

5a Navigieren Sie in iManager zu **Rollen und Aufgaben** > **Zugriff auf NetIQ-Zertifikate** > **Benutzerzertifikate**.

5b Wählen Sie das erstellte Zertifikat aus.

5c Klicken Sie auf **Exportieren**.

5d Wählen Sie im Dropdown-Menü unter **CA-Zertifikat** die Option **OU=organizationCA.O=TREENAME**.

5e Wählen Sie im Dropdown-Menü unter **Exportformat** die Option **BASE64**.

5f Klicken Sie auf **Weiter** und speichern Sie das Zertifikat. Beispiel: `cacert.b64`.

6 Importieren Sie das CA-Zertifikat mit dem folgenden Befehl in einen Keystore:

```
keytool -import -alias <Aliasname> -file <b64 file> -keystore <Keystore-Datei>
–noprompt
```

Beispiel:

```
keytool -import -alias trustedroot -file cacert.b64 -keystore idmKeystore.ks –
noprompt
```

7 Möchten Sie das Zertifikat in den Truststore des Audit Connector importieren, gehen Sie wie folgt vor:

7a Melden Sie sich als Administrator bei der Sentinel-Hauptoberfläche an.

7b Wechseln Sie im ESM-Hauptfenster zum Audit-Server.

7c Klicken Sie mit der rechten Maustaste auf den **Audit-Server** und klicken Sie auf **Bearbeiten**.

7d Wählen Sie auf der Registerkarte "Sicherheit" die Option **Streng**.

HINWEIS: Standardmäßig ist der **Offene** (unsichere) Modus aktiviert, damit zu Beginn eine Verbindung hergestellt werden kann. Beim Einsatz in einer Produktionsumgebung muss jedoch der Modus **Streng** eingestellt werden.

7e Klicken Sie auf **Importieren** und navigieren Sie zum in Schritt 6 erstellten Zertifikat. Beispiel: `idmkeystore.ks`.

7f Klicken Sie auf **Öffnen** und dann auf **Speichern**.

7g Starten Sie den Audit-Server neu.

8 Starten Sie die Identity Manager-Dienste neu.

20.5.2 Aktivieren von SSL zwischen Sentinel und Benutzeranwendung

1 Erstellen Sie mit den folgenden Schritten ein neues Zertifikat:

1a Melden Sie sich bei iManager an.

1b Klicken Sie auf **NetIQ-Zertifikatsserver** > **Benutzerzertifikat erstellen**.

1c Wählen Sie den Benutzer aus.

1d Geben Sie einen Kurznamen für den Benutzer ein.

1e Wählen Sie unter **Erstellungsmethode** die Option **Benutzerdefiniert**.

1f Übernehmen Sie die restlichen Standardeinstellungen für das Zertifikat.

1g Klicken Sie auf **Weiter**.

1h Wählen Sie unter **Benutzerdefinierte Erweiterungen** die Option **Neue DER-verschlüsselte Erweiterungen**.

1i Wechseln Sie zur benutzerdefinierten Erweiterung `\products\RBPM\ext.der`.

1j (Optional) Geben Sie die Email-Adresse an.

1k Prüfen Sie die Zertifikatparameter und klicken Sie auf **Fertig stellen**.

2 Exportieren Sie das Benutzerzertifikat mit den folgenden Schritten:

2a Klicken Sie auf **Zugriff auf NetIQ-Zertifikate > Benutzerzertifikate**

2b Wählen Sie das in Schritt 1 importierte Benutzerzertifikat aus.

2c Wählen Sie das gültige Benutzerzertifikat aus, und klicken Sie auf **Exportieren**.

2d Stellt das Passwort bereit.

2e Speichern Sie das Benutzerzertifikat als PKCS12-Datei. Beispiel: `certificate.pfx`.

3 Extrahieren Sie den privaten Schlüssel mit dem nachfolgenden Befehl aus dem exportierten Zertifikat in die Datei `key.pem`.

```
openssl pkcs12 -in certificate.pfx -nocerts -out key.pem –nodes
```

4 Extrahieren Sie das Zertifikat in die Datei `cert.pem`.

```
openssl pkcs12 -in certificate.pfx -nokeys -out cert.pem
```

5 Halten Sie die Benutzeranwendung an.

6 Fügen Sie den privaten Schlüssel und das Zertifikat zum configupdate-Dienstprogramm hinzu.

6a Öffnen Sie das configupdate-Dienstprogramm.

6b Klicken Sie auf **Erweiterte Optionen anzeigen**.

6c Kopieren Sie im Feld **Zertifikat für NetIQ Sentinel-Digitalsignatur** die Datei `cert.pem`.

6d Navigieren Sie im Feld **Privater Schlüssel für NetIQ Sentinel-Digitalsignatur** zum Speicherort, in den Sie den privaten Schlüssel (`key.pem`) exportiertiert haben, und importieren Sie den Schlüssel.

6e Speichern Sie die Änderungen am configupdate-Dienstprogramm.

7 Starten Sie die Benutzeranwendungen neu.

8 Möchten Sie das CA-Zertifikat des eDirectory-Servers, das Sie unter Schritt 1 erstellt haben, im Format Base64 exportieren, gehen Sie wie folgt vor:

   8a Navigieren Sie in iManager zu **Rollen und Aufgaben** > **Zugriff auf NetIQ-Zertifikate** > **Benutzerzertifikate**.

   8b Wählen Sie das erstellte Zertifikat aus.

   8c Klicken Sie auf **Exportieren** und deaktivieren Sie das Kontrollkästchen „Privaten Schlüssel exportieren“.

   8d Wählen Sie im Dropdown-Menü unter **Exportformat** die Option **BASE64**.

   8e Klicken Sie auf **Weiter** und speichern Sie das Zertifikat. Beispiel: `cacert.b64`.

9 Importieren Sie das CA-Zertifikat mit dem folgenden Befehl in einen Keystore:

```
keytool -import -alias <Aliasname> -file cacert.b64 -keystore <Keystore-Datei>
–noprompt
```

   Beispiel:

```
keytool -import -alias trustedroot -file cacert.b64 -keystore idmKeystore.ks –
noprompt
```

10 Möchten Sie das Zertifikat in den Truststore des Audit Connector importieren, gehen Sie wie folgt vor:

   10a Melden Sie sich als Administrator bei der Sentinel-Hauptoberfläche an.

   10b Wechseln Sie im ESM-Hauptfenster zum Audit-Server.

   10c Klicken Sie mit der rechten Maustaste auf den **Audit-Server** und klicken Sie auf **Bearbeiten**.

   10d Wählen Sie auf der Registerkarte **Sicherheit** die Option **Streng**.

   HINWEIS: Standardmäßig ist der **Offene** (unsichere) Modus aktiviert, damit zu Beginn eine Verbindung hergestellt werden kann. Beim Einsatz in einer Produktionsumgebung muss jedoch der Modus **Streng** eingestellt werden.

   10e Klicken Sie auf **Importieren** und navigieren Sie zum in Schritt 9 erstellten Zertifikat. Beispiel: `idmKeystore.ks`.

   10f Klicken Sie auf **Öffnen** und dann auf **Speichern**.

   10g Starten Sie den Audit-Server neu.

11 Starten Sie die Benutzeranwendungen neu.

20.6 Aktualisieren der SSL-Einstellungen für den Anwendungsserver

Das Installationsprogramm konfiguriert den Anwendungsserver, auf dem die Identitätsanwendungen und Identity Reporting gehostet werden, automatisch für die Unterstützung der SSL-Kommunikation. Der Connector wird standardmäßig in der Datei `server.xml` im Verzeichnis `/opt/netiq/idm/apps/tomcat/conf/` angelegt.

```
<Connector port="https_port" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLSv1.2" keystoreFile="path_to_keystore_file"
keystorePass="keystore_password" sslEnabledProtocols="TLSv1.2" />
```

wobei:

keystoreFile

Gibt den Pfad zur Keystore-Datei an, beispielsweise zur Datei `idmapps.keystore`. Legen Sie die Datei im Verzeichnis `/opt/netiq/idm/apps/tomcat/conf/` ab.

keystorePass

Gibt das Passwort für die Datei `tomcat.ks` an.

Prüfen Sie, ob das Keystore-Passwort und der Pfad zur Keystore-Datei fehlerfrei in der Datei `server.xml` eingetragen sind.

So bearbeiten Sie die im Rahmen der Installation festgelegten Werte:

1. Halten Sie Tomcat an, falls es aktuell ausgeführt werden sollte.
2. Navigieren Sie zum Verzeichnis `conf` für Tomcat, das sich standardmäßig unter `opt/netiq/idm/apps/tomcat/conf/` befindet.
3. Im `conf`-Verzeichnis muss sich eine Keystore-Datei befinden. Beispiel: `tomcat.ks`.

   Wenn Sie die Keystore-Datei nach diesem Vorgang erstellen, müssen Sie den Dateinamen verwenden, den Sie zuvor in diesem Vorgang angegeben haben. Weitere Informationen finden Sie unter Abschnitt 20.2, „Erstellen eines Keystore und eines Zertifizierungsantrags“, auf Seite 216.
4. Öffnen Sie in einem Texteditor die Datei `server.xml` im `conf`-Verzeichnis.
5. Konfigurieren Sie den SSL-Port für den Tomcat-Server.

   Der Anschluss-Port für SSL lautet beispielsweise `8543`.

   Aktualisieren Sie zudem das Attribut `redirectPort` auf `8543` und speichern Sie `server.xml`.

   Beispiel:

   ```
   <Connector port="8543" protocol="HTTP/1.1" maxThreads="150" SSLEnabled="true"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="/opt/netiq/idm/apps/tomcat/conf/idmapps.keystore"
   keystorePass="encrypted_password"
   ```
6. Starten Sie Tomcat.

   Beispiel: `systemctl start netiq-tomcat.service`

20.7 Aktualisieren der SSL-Einstellungen im Konfigurationsprogramm

Das Installationsprogramm konfiguriert automatisch die SSL-Einstellungen. So bearbeiten Sie die im Rahmen der Installation festgelegten Werte:

1. Halten Sie Tomcat mithilfe der Datei `services.msc` an, falls das Programm ausgeführt wird.

   Beispiel: `systemctl status netiq-tomcat.service`.
2. Navigieren Sie zum RBPM-Konfigurationsprogramm (standardmäßig im Installationsverzeichnis der Identitätsanwendungen).
3. Führen Sie mithilfe der Eingabeaufforderung das Konfigurationsdienstprogramm (`configupdate.sh`) aus:

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

4 (Bedingt) Wenn Sie SSL im configupdate-Dienstprogramm konfigurieren, navigieren Sie zur Registerkarte **Authentifizierung** und ersetzen Sie alle Bezüge, die in der Registerkarte **SSO-Clients** aufgeführt sind.

```
https://<IP address>:<SSL Port number>
```

Beispiel:

```
https://192.168.0.1:8543
```

5 Klicken Sie auf **Authentifizierung**, und bearbeiten Sie die folgenden Einstellungen:

TCP-Port für OAuth-Server

Gibt den Port für den Authentifizierungsserver an.

Beispiel: `8543`

OAuth-Server verwendet TLS/SSL

Gibt an, dass der Authentifizierungsserver das TLS/SSL-Protokoll für die Kommunikation verwenden soll.

Datei für optionalen TLS/SSL-Keystore

Gibt den Pfad und den Dateinamen der Java-JKS-Keystore-Datei an, die das Herkunftsverbürgungszertifikat für den Authentifizierungsserver enthält. Dieser Parameter kommt zum Einsatz, wenn der Authentifizierungsserver das TLS/SSL-Protokoll verwendet und das Herkunftsverbürgungszertifikat nicht im JRE-Herkunftsverbürgungsspeicher (`cacerts`) vorliegt.

Passwort für optionalen TLS/SSL-Keystore

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

OAuth-Keystore-Datei

Gibt den Pfad zur Java-JKS-Keystore-Datei an, die für die Authentifizierung herangezogen werden soll. Die Keystore-Datei muss mindestens ein Schlüsselpaar aus öffentlichem und privaten Schlüssel enthalten.

Passwort für OAuth-Keystore-Datei

Gibt das Passwort an, mit dem die OAuth-Keystore-Datei geladen wird.

Schlüsselalias für Schlüssel für OAuth

Gibt den Namen des Schlüsselpaars aus öffentlichem und privatem Schlüssel in der OSP-Keystore-Datei an, mit dem symmetrische Schlüssel generiert werden sollen.

Schlüsselpasswort für Schlüssel für OAuth

Gibt das Passwort für den privaten Schlüssel an, der vom Authentifizierungsserver verwendet wird.

6 Klicken Sie auf **SSO-Clients**.

7 Aktualisieren Sie alle URL-Einstellungen, wie **URL-Link zur Landeseite** und **OAuth-Umleitungs-URL**.

Mit diesen Einstellungen geben Sie die absolute URL an, zur der der Authentifizierungsserver einen Browser-Client nach erfolgter Authentifizierung weiterleiten soll.

Verwenden Sie das folgende Format: `https://DNS_name:sslport/path`. Beispiel: `https://nqserver.testsite:8543/landing/com.netiq.test`.

8 Speichern Sie die Änderungen im Konfigurationsprogramm.

9 Starten Sie Tomcat.

20.8 Aktualisieren der SSL-Einstellungen für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung

Zum Bearbeiten der SSL-Einstellungen für SSPR müssen Sie bei der Anwendung angemeldet sein.

1 Geben Sie in einem Browser die `https`-URL ein, die Sie im Konfigurationsprogramm für die Portalseite angegeben haben. Beispiel: `https://meinserver.host:8543/landing`.

2 Melden Sie sich mit einem Administratorberechtigungsnachweis bei den Identitätsanwendungen an.

   Die Anwendung zeigt eine Warnmeldung an, dass die Whitelist-URL für die Umleitung ändern müssen.

3 Ändern Sie die Whitelist-URL für die Umleitung gemäß den Anweisungen auf der Seite.

4 Navigieren Sie zu **Einstellungen > OAuth-SSO**.

5 Legen Sie für alle drei URLs das `https`-Protokoll und den Port fest.

6 Navigieren Sie zu **Einstellungen > Anwendung**.

7 Legen Sie für alle drei URLs das `https`-Protokoll und den Port fest.

8 Klicken Sie auf **Speichern** und dann auf **OK**.

9 Überprüfen Sie, ob alle URLs für die Identitätsanwendungen nun das `https`-Protokoll verwenden.

Tipp zur Fehlerbehebung

Nach Aktualisierung der SSL-Einstellungen für SSPR, falls Sie nicht auf die SSPR-Landingpage zugreifen können. Folgen Sie den Anweisungen unten, um benötigte URLs in der Datei `SSPRConfiguration.xml` zu aktualisieren.

1 Navigieren Sie zur Datei `SSPRConfiguration.xml`, die unter dem unten genannten Pfad zu finden ist:

   ```
   /opt/netiq/idm/apps/sspr/sspr_data
   ```

2 Aktualisieren Sie alle URLs mit entsprechenden IP-Adressen und Port-Nummern.

   ```
   https://<IP address>:<SSL Port number>
   ```

   Beispiel:

   ```
   https://192.168.0.1:8543
   ```

VIII 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:

21 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.

21.1 Erstellen und Konfigurieren eines Treibersatzes

Ein Treibersatz ist ein Container, der Identity Manager-Treiber enthält. Auf einem Server kann immer nur ein Treibersatz aktiv sein. Ein Treibersatz wird mit dem Designer-Tool erstellt.

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.

21.1.1 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 NetIQ Designer für Identity Manager*.

21.1.2 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 Abschnitt 21.1.3, „Erstellen des Passwortrichtlinienobjekts im Identitätsdepot“, auf Seite 232 und Abschnitt 21.1.4, „Erstellen einer benutzerdefinierten Passwortrichtlinie“, auf Seite 233.

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.

21.1.3 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 *NetIQ Designer für Identity Manager – Verwaltungshandbuch*. 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 Importieren Sie zum Hinzufügen des DirMXL-PasswordPolicy-Objekts im Identitätsdepot die Attribute der Datei:

Geben Sie im Verzeichnis mit dem ldapmodify-Dienstprogram das folgende Kommando ein:

```
ldapmodify -x -c -h hostname_or_IP_address -p 389 -D "cn=admin,ou=sa,o=system"
-w password -f path_to_ldif_file
```

Beispiel:

```
ldapmodify -x -ZZ -c -h server1.test.com -p 389 -D "cn=admin,ou=sa,o=system" -
w test123 -f /root/dirxmlpasswordpolicy.ldif
```

Das ldapmodify-Dienstprogramm befindet sich standardmäßig im Verzeichnis `/opt/novell/eDirectory/bin`.

21.1.4 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. NetIQ empfiehlt Ihnen, Passwortrichtlinien einer möglichst hohen Ebenen 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 Abschnitt 21.1.3, „Erstellen des Passwortrichtlinienobjekts im Identitätsdepot“, auf Seite 232.

21.1.5 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.

21.2 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.

21.3 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. 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 Identity Manager-Verknüpfungen verwalten.

NetIQ empfiehlt Ihnen, Richtlinien für Treiber entsprechend Ihrer Geschäftsanforderungen mit dem Designer zu definieren. Detaillierte Informationen zu Richtlinien finden Sie im Handbuch *NetIQ Identity Manager – Erstellen von Richtlinien mit Designer* und im *NetIQ Identity Manager Understanding Policies Guide* (Handbuch über Richtlinien in NetIQ Identity Manager). Informationen zu Dokumenttypdefinitionen (DTD), die Identity Manager verwendet, finden Sie in der Identity Manager DTD-Referenz. 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.

22 Konfigurieren der "Passwort vergessen"-Verwaltung

Die 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.

22.1 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 Identitätsanwendungen aktiviert. Ggf. haben Sie dabei nicht die URL der Portalseite für die Identitätsanwendungen 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:

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

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

1. Melden Sie sich bei dem Server an, auf dem Sie die Identitätsanwendungen installiert haben.
2. Führen Sie das RBPM-Konfigurationsprogramm aus. Weitere Informationen finden Sie in Abschnitt 11.6.1, „Ausführen des Konfigurationsprogramms der Identitätsanwendungen“, auf Seite 144.
3. Navigieren Sie im Dienstprogramm zu **Authentifizierung > Passwortverwaltung**.
4. Wählen Sie unter **Passwortverwaltungsanbieter** die Option **SSPR**.

5 Wählen Sie **Passwort vergessen**.

6 Navigieren Sie zu **SSO Clients > Zurücksetzen von Passwörtern per Selbstbedienung**.

7 Geben Sie unter **OSP-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 **OSP-Client-Geheimnis** das Passwort des Single-Sign-On-Clients für SSPR an.

9 Geben Sie unter **URL für die OSP-Umleitung** die absolute URL an, zur der der Authentifizierungsserver einen Browser-Client nach erfolgter Authentifizierung weiterleiten soll.

   Verwenden Sie das folgende Format: `protocol://server:port/path`. Beispiel: `http://10.10.10.48:8180/sspr/public/oauth`.

10 Speichern Sie die Änderungen, und schließen Sie das Dienstprogramm.

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

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

Wenn Sie SSPR mit Identity Manager installiert haben, haben Sie ein Passwort angegeben, mit dem ein Administrator die Anwendung konfigurieren kann. NetIQ empfiehlt, 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 (Konfigurieren der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung) im *NetIQ Self Service Password Reset Administration Guide* (NetIQ-Administrationshandbuch für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung).

3 Sperren Sie die SSPR-Konfigurationsdatei (`SSPRConfiguration.xml`). Weitere Informationen zum Sperren der Konfigurationsdatei finden Sie in „Sperren der SSPR-Konfiguration“, auf Seite 237.

4 (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.

5 Melden Sie sich bei SSPR ab.

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

22.1.3 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 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 (`SSPRConfiguration.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 aufgroupMembership=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.

22.2 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:

- Abschnitt 22.2.1, „Angeben einer externen WAR-Datei für die "Passwort vergessen"-Verwaltung“, auf Seite 238
- Abschnitt 22.2.2, „Testen der externen „Passwort vergessen“-Konfiguration“, auf Seite 239
- Abschnitt 22.2.3, „Konfigurieren der SSL-Kommunikation zwischen Anwendungsservern“, auf Seite 239

22.2.1 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 die Identitätsanwendungen installiert haben.
   - **1b** Führen Sie das RBPM-Konfigurationsprogramm aus. Weitere Informationen finden Sie in Abschnitt 11.6.1, „Ausführen des Konfigurationsprogramms der Identitätsanwendungen“, auf Seite 144.
   - **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“ die Identitätsanwendungen 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 Identitätsanwendungen gewährleistet ist. Weitere Informationen finden Sie in „Konfigurieren der SSL-Kommunikation zwischen Anwendungsservern“, auf Seite 239.

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

22.2.2 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**.

22.2.3 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 die Identitätsanwendungen und die externe WAR-Datei für die „Passwort vergessen“-Verwaltung bereitstellen. Weitere Informationen finden Sie in der Tomcat-Dokumentation.

22.3 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 die Identitätsanwendungen und die Identitätsberichterstellung 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 Identitätsanwendungen*.

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.

23 Verwalten von Treiberaktivitäten

Führen Sie Verwaltungs- und Konfigurationsfunktionen von Identity Manager-Treibern mit Designer oder iManager durch. Diese Funktionen werden im *NetIQ Identity Manager-Treiberverwaltungshandbuch* detailliert beschrieben.

23.1 Anhalten und Starten der Identity Manager-Treiber

Unter Umständen müssen die Identity Manager-Treiber gestartet oder angehalten werden, damit die richtigen Dateien im Rahmen einer Installation oder Aufrüstung geändert oder ersetzt werden können. In diesem Abschnitt werden die folgenden Vorgänge beschrieben:

- Abschnitt 23.1.1, „Anhalten der Treiber“, auf Seite 241
- Abschnitt 23.1.2, „Starten der Treiber“, auf Seite 242

23.1.1 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 241
- „Anhalten der Treiber mithilfe von iManager“, auf Seite 241

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 mithilfe von iManager

1. Klicken Sie in iManager auf **Identity Manager > Identity Manager-Überblick**.
2. Wählen Sie in der Baumstruktur den Speicherort aus, in dem nach Treibersatzobjekten gesucht werden soll, und klicken Sie dann auf das Suchsymbol .
3. Klicken Sie auf das Treibersatzobjekt.
4. Klicken Sie auf **Treiber > Alle Treiber anhalten**.
5. Führen Sie Schritt 2 bis Schritt 4 für alle Treibersatzobjekte aus.

6 Wählen Sie für die Treiber die manuelle Startoption aus, um zu vermeiden, dass die Treiber vor Abschluss der Aufrüstung starten:

   6a Klicken Sie in iManager auf **Identity Manager > Identity Manager-Überblick**.

   6b Wählen Sie in der Baumstruktur den Speicherort aus, in dem nach Treibersatzobjekten gesucht werden soll, und klicken Sie dann auf das Suchsymbol .

   6c Klicken Sie auf das Treibersatzobjekt.

   6d Klicken Sie in der oberen rechten Ecke des Treibersymbols auf **Eigenschaften bearbeiten**.

   6e Wählen Sie auf der Seite „Treiberkonfiguration“ unter **Startoption** die Option **Manuell** aus, und klicken Sie anschließend auf **OK**.

   6f Führen Sie Schritt 6a bis Schritt 6e für alle Treiber in Ihrer Baumstruktur aus.

23.1.2 Starten der Treiber

Nach dem Aktualisieren aller Identity Manager-Komponenten starten Sie die Treiber neu. NetIQ empfiehlt, die gestarteten Treiber nach dem Ausführen zu testen, ob noch alle Richtlinien funktionieren.

- „Starten der Treiber mithilfe von Designer“, auf Seite 242
- „Starten der Treiber mithilfe von iManager“, auf Seite 242

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 *NetIQ Identity Manager – Erstellen von Richtlinien mit Designer*.

Starten der Treiber mithilfe von iManager

1 Klicken Sie in iManager auf **Identity Manager > Identity Manager-Überblick**.

2 Wählen Sie in der Baumstruktur den Speicherort aus, in dem nach Treibersatzobjekten gesucht werden soll, und klicken Sie dann auf das Suchsymbol .

3 Klicken Sie auf das Treibersatzobjekt.

4 Wählen Sie **Treiber > Alle Treiber starten**, um alle Treiber gleichzeitig zu starten.

   oder

   Klicken Sie in der oberen rechten Ecke des Treibersymbols auf **Treiber starten**, um jeden Treiber einzeln zu starten.

5 Wenn Sie mehrere Treiber verwenden, wiederholen Sie Schritt 2 bis Schritt 4.

6 Legen Sie die Treiber-Startoptionen fest:

   6a Klicken Sie in iManager auf **Identity Manager > Identity Manager-Überblick**.

   6b Wählen Sie in der Baumstruktur den Speicherort aus, in dem nach Treibersatzobjekten gesucht werden soll, und klicken Sie dann auf das Suchsymbol ▸.

   6c Klicken Sie auf das Treibersatzobjekt.

   6d Klicken Sie in der oberen rechten Ecke des Treibersymbols auf **Eigenschaften bearbeiten**.

   6e Wählen Sie auf der Seite „Treiberkonfiguration“ unter **Startoption** die Option **Autom. starten** bzw. die gewünschte Methode für den Start des Treibers aus. Klicken Sie anschließend auf **OK**.

   6f Führen Sie Schritt 6b bis Schritt 6e für alle Treiber aus.

7 Testen Sie die Treiber, um sicherzustellen, dass die die Richtlinien wie gewünscht funktionieren.

   In iManager 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.

24 Aktivieren von Identity Manager

Einige Identity Manager-Komponenten werden automatisch aktiviert, sobald Sie sich erstmalig anmelden. Andere Komponenten müssen dagegen explizit aktiviert werden.

24.1 Installation einer Produktaktivierungsberechtigung

NetIQ empfiehlt, die Produktaktivierungsberechtigung mit iManager zu installieren.

HINWEIS: Aktivieren Sie für jeden zu aktivierenden Treiber das Integrationsmodul, in dem sich der betreffende Treiber befindet.

---

1. Nach dem Erwerb einer Lizenz erhalten Sie von NetIQ eine Email mit Ihrer Kunden-ID. Die Email enthält außerdem unter „Auftragsdetails“ einen Link zur Website, auf der Sie einen Berechtigungsnachweis erhalten. Rufen Sie die Website auf, indem Sie auf den Link klicken.
2. Klicken Sie auf den Link zum Herunterladen der Lizenz, und führen Sie einen der folgenden Schritte aus:
   - Öffnen Sie die Datei mit der Produktaktivierungsberechtigung und kopieren Sie ihren Inhalt in die Zwischenablage.
   - Speichern Sie die Datei mit der Produktaktivierungsberechtigung.
   - Wenn Sie den Inhalt kopieren, fügen Sie keine zusätzlichen Zeilen oder Leerzeichen ein. Markieren Sie den zu kopierenden Text vom ersten Gedankenstrich (-) der Berechtigung (`----BEGINN DER PRODUKTAKTIVIERUNGSBERECHTIGUNG`) bis zum letzten Gedankenstrich (-) der Berechtigung (`ENDE DER PRODUKTAKTIVIERUNGSBERECHTIGUNG-----`).
3. Melden Sie sich bei iManager an.
4. Wählen Sie **Identity Manager > Identity Manager-Überblick**.
5. Wählen Sie einen Treibersatz in der Baumstruktur aus. Klicken Sie hierzu auf das Durchsuchen-Symbol ( ).
6. Klicken Sie auf der Seite **Identity Manager-Überblick** auf den Treibersatz, der den zu aktivierenden Treiber enthält.
7. Klicken Sie auf der Seite **Treibersatz-Überblick** auf **Aktivierung** > **Installation**.
8. Wählen Sie den Treibersatz aus, in dem Sie eine Identity Manager-Komponente aktivieren möchten, und klicken Sie auf **Weiter**.
9. (Bedingt) Wenn Sie die Datei mit der Produktaktivierungsberechtigung gespeichert haben, geben Sie den Speicherort dieser Datei an.

10 (Bedingt) Wenn Sie den Inhalt der Datei mit der Produktaktivierungsberechtigung kopiert haben, fügen Sie den Inhalt in den Textbereich ein.

11 Klicken Sie auf **Weiter**.

12 Klicken Sie auf **Fertig stellen**.

24.2 Prüfen der Produktaktivierungen für Identity Manager und Identity Manager-Treiber

Für jeden Treibersatz werden die Produktaktivierungsberechtigungen angezeigt, die Sie für die Identity Manager-Engine-Server- und Identity Manager-Treiber installiert haben. Bei Bedarf können Sie eine Aktivierungsberechtigung auch wieder entfernen.

HINWEIS: Nach der Installation einer gültigen Produktaktivierungsberechtigung wird neben dem Treibernamen möglicherweise noch immer „Aktivierung erforderlich“ angezeigt. Starten Sie in diesem Fall den Treiber neu. Die Meldung wird nicht mehr angezeigt.

---

1 Melden Sie sich bei iManager an.

2 Klicken Sie auf **Identity Manager** > **Identity Manager-Überblick**.

3 Wählen Sie einen Treibersatz in der Baumstruktur aus. Klicken Sie hierzu auf das Durchsuchen-Symbol ( ) und auf das Suchsymbol ( ).

4 Klicken Sie auf der Seite **Identity Manager-Überblick** auf den Treibersatz, dessen Aktivierungsinformationen angezeigt werden sollen.

5 Klicken Sie auf der Seite **Treibersatz-Überblick** auf **Aktivierung > Informationen**.

Sie können den Text des Berechtigungsnachweises anzeigen oder bei einer Fehlermeldung einen Berechtigungsnachweis entfernen.

24.3 Aktivieren von Identity Manager-Treibern

Wenn Sie die Identity Manager-Engine aktivieren, werden auch die folgenden Treiber aktiviert:

Service-Treiber	Allgemeine Treiber
Datenerfassungsdienst	Active Directory
ID-Provider	Bidirektionaler Treiber für eDirectory
Verwaltetes System – Gateway	eDirectory
Rollen- und Ressourcenservice	GroupWise 2014
Benutzeranwendung	LDAP
	Lotus Notes

Sollen weitere Identity Manager-Treiber aktiviert werden, müssen Sie zusätzliche Identity Manager-Integrationsmodule erwerben, die jeweils einen oder mehrere Treiber enthalten. Sie erhalten für jedes erworbene Identity Manager-Integrationsmodul eine Produktaktivierungsberechtigung. Sobald Ihnen die Berechtigung vorliegt, führen Sie das Verfahren in Abschnitt 24.1, „Installation einer Produktaktivierungsberechtigung“, auf Seite 245 aus. Weitere Informationen zu den Treibern finden Sie auf der Website der Identity Manager-Treiberdokumentation.

24.4 Aktivieren bestimmter Identity Manager-Komponenten

In diesem Abschnitt wird beschrieben, wie Sie bestimmte Komponenten für Identity Manager aktivieren.

24.4.1 Aktivieren von Designer

Wenn Sie die Identity Manager-Engine oder die Identity Manager-Treiber aktivieren, werden auch Designer und der Katalogadministrator aktiviert.

24.4.2 Aktivieren von Analyzer

Wenn Sie die Analyzer-Perspektive ohne Lizenz starten, öffnet Analyzer die Aktivierungsseite, von der aus Sie die Analyzer-Lizenzen verwalten können.

HINWEIS: Wenn Sie das Aktivierungsdialogfeld schließen, bleibt Analyzer so lange gesperrt, bis Sie eine Lizenz zum Aktivieren bereitstellen. Sobald Ihnen eine Lizenz vorliegt, klicken Sie in der **Projektansicht** auf `Analyzer aktivieren`. Das Aktivierungsdialogfeld wird geöffnet.

---

1. Starten Sie Analyzer.
2. Im Fenster **Aktivierung von Analyzer** können Sie eine neue Lizenz hinzufügen oder für Lizenzen auf das Customer Center zugreifen.
3. (Bedingt) So fügen Sie eine neue Lizenz hinzu:
   - **3a** Klicken Sie auf **Neue Lizenz hinzufügen**.
   - **3b** Geben Sie im Fenster **Lizenz** den Aktivierungscode ein, den Sie aus dem NetIQ-Kundenservice-Portal heruntergeladen haben, und klicken Sie auf **OK**.
4. (Bedingt) So greifen Sie für Lizenzen auf das Customer Center zu:
   - **4a** Klicken Sie auf **Für Lizenz auf Customer Center zugreifen**.
   - **4b** Klicken Sie auf der Seite **Micro Focus Customer Center** auf **NetIQ Customer Center besuchen**.
   - **4c** Suchen Sie nach der Analyzer-Lizenz und wählen Sie sie aus.
   - **4d** Kopieren Sie den Aktivierungscode und schließen Sie das Kundenservice-Portal.
   - **4e** Geben Sie den Aktivierungscode in das Fenster **Lizenz** ein und klicken Sie auf **OK**.
5. Prüfen Sie im Fenster **Analyzer-Aktivierung** die Details der soeben installierten Lizenz.
6. Klicken Sie auf **OK**, und nehmen Sie die Arbeit mit Analyzer auf.

24.4.3 Aktivieren von Sentinel Log Management für IGA

Beim Installieren von Sentinel können Sie einen Lizenzschlüssel einfügen. In diesem Abschnitt erfahren Sie, wie Sie den Lizenzschlüssel nach Abschluss der Installation einfügen.

Wenn Sie einen Testlizenzschlüssel verwenden, der standardmäßig installiert wird, müssen Sie Sentinel aktivieren, bevor der Testschlüssel abläuft, damit Sie die Sentinel-Funktionen unterbrechungsfrei weiternutzen können. Weitere Informationen zum Erwerb der Lizenz finden Sie auf der Produkt-Website zu Identity Manager.

Sie können einen Lizenzschlüssel entweder über die Sentinel-Hauptoberfläche oder über die Befehlszeile hinzufügen.

- „Hinzufügen eines Lizenzschlüssels über die Sentinel-Hauptoberfläche“, auf Seite 248
- „Hinzufügen eines Lizenzschlüssels über die Befehlszeile“, auf Seite 248

Hinzufügen eines Lizenzschlüssels über die Sentinel-Hauptoberfläche

1. Melden Sie sich als Administrator bei der Sentinel-Hauptoberfläche an.
2. Klicken Sie auf **Info > Lizenzen**.
3. Klicken Sie im Abschnitt „Lizenzen“ auf **Lizenz hinzufügen**.
4. Geben Sie den Lizenzschlüssel im Feld **Schlüssel** an.

   Nach der Angabe der Lizenz werden folgende Informationen im Vorschau-Abschnitt angezeigt:

   - **Funktionen:** Die mit der Lizenz verfügbaren Funktionen.
   - **Hostname:** Dieses Feld dient ausschließlich NetIQ-internen Zwecken.
   - **Seriennummer:** Dieses Feld dient ausschließlich NetIQ-internen Zwecken.
   - **EPS:** Im Lizenzschlüssel enthaltene Ereignisrate. Wenn die Rate überschritten wird, generiert Sentinel Warnmeldungen, erfasst jedoch weiterhin Daten.
   - **Läuft ab:** Ablaufdatum der Lizenz. Um eine Unterbrechung der Funktionen zu vermeiden, müssen Sie vor dem Ablaufdatum einen gültigen Lizenzschlüssel eingeben.
5. Klicken Sie auf **Speichern**.

Hinzufügen eines Lizenzschlüssels über die Befehlszeile

Wenn Sie die herkömmliche Sentinel-Installation verwenden, können Sie den Lizenzschlüssel mit dem Skript `softwarekey.sh` über die Befehlszeile einfügen.

1. Melden Sie sich beim Sentinel-Server als Root an.
2. Wechseln Sie in das Verzeichnis `/opt/novell/sentinel/bin`.
3. Geben Sie folgenden Befehl ein, um zum Benutzer „novell“ zu wechseln:

   ```
   su novell
   ```
4. Geben Sie folgenden Befehl an, um das Skript `softwarekey.sh` auszuführen.

   ```
   ./softwarekey.sh
   ```
5. Geben Sie **1** ein, um den Lizenzschlüssel einzufügen.
6. Geben Sie den Lizenzschlüssel ein und drücken Sie die **Eingabetaste**.

IX Aufrüsten von Identity Manager

In diesem Abschnitt finden Sie Informationen zum Aufrüsten der Identity Manager-Komponenten.

25 Vorbereiten der Aufrüstung von Identity Manager

In diesem Abschnitt wird die Vorbereitung Ihrer Identity Manager-Lösung für die Aufrüstung auf die aktuelle Version beschrieben. Je nach Zielcomputer können Sie den Großteil der Identity Manager-Komponenten wahlweise mit einer ausführbaren Datei, mit einer Binärdatei oder im Textmodus installieren. Zum Aufrüsten müssen Sie das Installations-Kit für Identity Manager herunterladen und entpacken.

25.1 Checkliste für die Aufrüstung von Identity Manager

NetIQ empfiehlt, die Schritte in der nachfolgenden Checkliste für die Aufrüstung auszuführen.

	Checkliste
❑	1. Machen Sie sich mit dem Aufrüstungsvorgang vertraut. Weitere Informationen finden Sie in Abschnitt 25.2, „Erläuterungen zum Aufrüstungsvorgang“, auf Seite 253.
❑	2. Prüfen Sie die unterstützten Pfade für die Aufrüstung von Identity Manager auf Version 4.7. Weitere Informationen zu den unterstützten Aufrüstungspfaden finden Sie unter Abschnitt 25.3, „Unterstützte Aufrüstungspfade“, auf Seite 253.
❑	3. Stellen Sie sicher, dass das Installations-Kit für die Aufrüstung von Identity Manager vorliegt.
❑	4. Informieren Sie sich über die Interaktion zwischen den Identity Manager-Komponenten. Weitere Informationen finden Sie in Teil I, „Einführung“, auf Seite 15.
❑	5. Stellen Sie sicher, dass die Computer die Hardware- und Software-Anforderungen für eine höhere Version von Identity Manager erfüllen. Weitere Informationen finden Sie in Kapitel 5.9, „Vorbereitung der Installation“, auf Seite 43 sowie in den Versionshinweisen zur Version, auf die Sie aufrüsten möchten.
❑	6. Legen Sie eine Sicherungskopie des aktuellen Treibers, der Treiberkonfiguration und der Datenbanken an. Weitere Informationen finden Sie in Abschnitt 25.4, „Sichern der aktuellen Konfiguration“, auf Seite 258.
❑	7. Rüsten Sie Designer auf die aktuelle Version auf. Weitere Informationen finden Sie in Abschnitt 26.2, „Aufrüstung von Designer“, auf Seite 261.
❑	8. Rüsten Sie Sentinel Log Management für IGA auf die aktuelle Version auf. Weitere Informationen finden Sie in Abschnitt 26.6.3, „Aufrüsten von Sentinel Log Management für IGA“, auf Seite 279.

	Checkliste
❑	9. Rüsten Sie das Identitätsdepot (eDirectory) auf dem Server, auf dem Identity Manager ausgeführt wird, auf Version 9.1 auf. Dies ist der erste Schritt zur Aufrüstung der Identity Manager-Engine. Weitere Informationen finden Sie unter Abschnitt 26.3.1, „Aufrüsten des Identitätsdepots“, auf Seite 262. Die Aufrüstung von eDirectory hält ndsd an, wodurch wiederum alle Treiber angehalten werden. Weitere Informationen hierzu finden Sie im *NetIQ eDirectory-Installationshandbuch*.
❑	10. Halten Sie die Treiber an, die mit dem Server verknüpft sind, auf dem Sie die Identity Manager-Engine installiert haben. Weitere Informationen finden Sie in Abschnitt 23.1.1, „Anhalten der Treiber“, auf Seite 241.
❑	11. Rüsten Sie die Identity Manager-Engine auf. Weitere Informationen finden Sie in Abschnitt 26.3, „Aufrüsten der Identity Manager-Engine“, auf Seite 262. **HINWEIS:** Wenn Sie die Identity Manager-Engine auf einen neuen Server migrieren, können Sie eDirectory-Reproduktionen verwenden, die sich auf dem aktuellen Identity Manager-Server befinden. Weitere Informationen finden Sie in Abschnitt 29.4, „Migrieren der Identity Manager-Engine auf einen neuen Server“, auf Seite 297.
❑	12. (Bedingt) Wenn der Treibersatz für die Identity Manager-Engine einen Remote Loader-Treiber enthält, rüsten Sie die Remote Loader-Server für jeden Treiber auf. Weitere Informationen finden Sie in Abschnitt 26.3.3, „Aufrüstung von Remote Loader“, auf Seite 263.
❑	13. Rüsten Sie iManager auf Version 3.1 auf. Weitere Informationen finden Sie in Abschnitt 26.3.4, „Aktualisieren von iManager“, auf Seite 264.
❑	14. Aktualisieren Sie die iManager-Plugins auf dieselbe Version wie iManager. Weitere Informationen finden Sie in „Aktualisieren von iManager-Plugins nach einer Aufrüstung oder Neuinstallation“, auf Seite 266.
❑	15. (Bedingt) Wenn Sie Pakete verwenden, rüsten Sie die Pakete auf die vorhandenen Treiber auf, sodass neue Richtlinien erstellt werden. Weitere Informationen finden Sie unter Abschnitt 26.4, „Aufrüsten der Identity Manager-Treiber“, auf Seite 266. 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.
❑	16. Rüsten Sie die Identitätsanwendungen auf. Weitere Informationen finden Sie in Abschnitt 26.5, „Aufrüsten der Identitätsanwendungen“, auf Seite 268.
❑	17. Rüsten Sie die Identitätsberichterstellung auf. Weitere Informationen finden Sie in Abschnitt 26.6, „Aufrüsten der Identitätsberichterstellung“, auf Seite 278.
❑	18. Starten Sie die Treiber für die Identitätsanwendungen und die Identity Manager-Engine. Weitere Informationen finden Sie in Abschnitt 23.1.2, „Starten der Treiber“, auf Seite 242.
❑	19. (Bedingt) Wenn Sie die Identity Manager-Engine oder die Identitätsanwendungen auf einen neuen Server migriert haben, fügen Sie diesen neuen Server zum Treibersatz hinzu. Weitere Informationen finden Sie in Abschnitt 26.8, „Hinzufügen von neuen Servern zum Treibersatz“, auf Seite 282.
❑	20. (Bedingt) Wenn Sie benutzerdefinierte Richtlinien und Regeln verwenden, stellen Sie die benutzerdefinierten Einstellungen wieder her. Weitere Informationen finden Sie in Abschnitt 26.9, „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“, auf Seite 284.
❑	21. Analyzer aufrüsten. Weitere Informationen finden Sie in Abschnitt 26.7, „Aufrüsten von Analyzer“, auf Seite 282.

	Checkliste
❑	22. Aktivieren Sie die aufgerüstete Identity Manager-Lösung. Weitere Informationen finden Sie in Abschnitt 24, „Aktivieren von Identity Manager“, auf Seite 245.

25.2 Erläuterungen zum Aufrüstungsvorgang

Wenn Sie eine neuere Version einer vorhandenen Identity Manager-Installation installieren möchten, nehmen Sie in der Regel eine **Aufrüstung** vor. Falls diese neue Identity Manager-Version jedoch keinen Aufrüstungspfad für Ihre vorhandenen Daten bietet, müssen Sie eine Migration ausführen. NetIQ definiert die **Migration** als Vorgang, bei dem 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 Identity Manager können Sie in einigen einfachen Schritten von der Advanced Edition zur Standard Edition wechseln.

Wechseln von der Advanced Edition zur Standard Edition

In 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 Identity Manager einschränken möchten. Weitere Informationen finden Sie unter „Wechseln von der Advanced Edition zur Standard Edition“, auf Seite 287.

25.3 Unterstützte Aufrüstungspfade

Identity Manager 4.7 unterstützt die Aufrüstung von Version 4.6.x und 4.5.6. NetIQ empfiehlt, vor dem Starten der Aufrüstung die Informationen in den entsprechenden Versionshinweisen zu Ihrer aktuellen Version zu lesen.

25.3.1 Aufrüsten von Identity Manager 4.6.x

Die nachfolgende Tabelle zeigt die komponentenweisen Aufrüstungspfade für Identity Manager 4.6.x:

Komponente	Basisversion	Aufgerüstete Version
Identity Manager-Engine	4.6.x	1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie das Identitätsdepot auf Version 9.1 auf. 3. Rüsten Sie die Identity Manager-Engine auf Version 4.7 auf.

Komponente	Basisversion	Aufgerüstete Version
Remote Loader/Fan-out-Agent	4.6.x	Installieren Sie den Remote Loader/Fan-out-Agenten 4.7.
Designer	4.6.x	1. Installieren Sie Designer 4.7. 2. Konvertieren Sie den Arbeitsbereich von NCP in LDAP. Designer 4.7 beruht auf LDAP. Bevor Sie die Arbeit mit dieser Version aufnehmen, beachten Sie die *Versionshinweise zu NetIQ Identity Manager LDAP Designer*.
Identitätsanwendungen	4.6.x	Bevor Sie die Identitätsanwendungen aufrüsten, müssen das Identitätsdepot auf Version 9.1 und die Identity Manager-Engine auf Version 4.7 aufgerüstet werden. 1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. Eine Liste der unterstützten Datenbankversionen finden Sie unter Abschnitt 8.5.3, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 83. 3. (Bedingt) Wenn SSPR auf einem separaten Server installiert ist, rüsten Sie die Komponente auf Version 4.7 auf. 4. Aktualisieren Sie die Benutzeranwendungstreiber- sowie die Rollen- und Ressourcentreiberpakete. 5. Rüsten Sie die Identitätsanwendungen auf Version 4.7 auf. 6. Halten Sie Tomcat an.

Komponente	Basisversion	Aufgerüstete Version
Identitätsberichterstellung	4.6.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 unter Abschnitt 8.6.4, „Systemanforderungen für die Identitätsberichterstellung“, auf Seite 88. 3. Rüsten Sie SLM für IGA auf eine unterstützte Version auf. 4. Rüsten Sie das Data Collection Services-Treiberpaket und das Treiberpaket „Verwaltetes System – Gateway“ auf. 5. Rüsten Sie Identity Reporting 4.7 auf. 6. (Bedingt) Erstellen Sie eine Datensynchronisierungsrichtlinie auf der Seite des Identity Manager-Datenerfassungsdiensts.

NetIQ empfiehlt, vor dem Starten der Aufrüstung die Informationen in den Versionshinweisen zu Ihrer Version zu lesen:

- Versionshinweise zu NetIQ Identity Manager 4.6 Service Pack 2
- Versionshinweise zu NetIQ Identity Manager 4.6 Service Pack 1
- Versionshinweise zu NetIQ Identity Manager 4.6

25.3.2 Aufrüsten von Identity Manager 4.5.x

Die nachfolgende Tabelle zeigt die komponentenweisen Aufrüstungspfade für Identity Manager 4.5.x:

Komponente	Basisversion	Zwischenschritt	Aufgerüstete Version
Identity Manager-Engine	Identity Manager 4.5.x (x = 0 bis 5) mit eDirectory 8.8.8.x (x = 3 bis 9)	Wenden Sie den Patch 4.5.6 an.	1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie das Identitätsdepot auf Version 9.1 auf. 3. Rüsten Sie die Identity Manager-Engine auf Version 4.7 auf.
Remote Loader/ Fan-out-Agent	4.5.x (x = 0 bis 5)	Wenden Sie den Patch 4.5.6 an.	Installieren Sie den Remote Loader/Fan-out-Agenten 4.7.

Komponente	Basisversion	Zwischenschritt	Aufgerüstete Version
Designer	4.5.x (x = 0 bis 5)	Wenden Sie den Patch 4.5.6 an.	1. Installieren Sie Designer 4.7. 2. Konvertieren Sie den Arbeitsbereich von NCP in LDAP. Designer 4.7 beruht auf LDAP. Bevor Sie die Arbeit mit dieser Version aufnehmen, beachten Sie die *Versionshinweise zu NetIQ Identity Manager LDAP Designer*.
Identitäts-anwendungen	4.5.x (x = 0 bis 5)	◆ Wenn Sie mit JBoss oder Websphere arbeiten, migrieren Sie zum Tomcat-Anwendungs-server. ◆ Wenden Sie den Patch 4.5.6 an.	Bevor Sie die Identitätsanwendungen aufrüsten, müssen das Identitätsdepot auf Version 9.1 und die Identity Manager-Engine auf Version 4.7 aufgerüstet werden. 1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Aktualisieren Sie die Benutzeranwendungstreiber- sowie die Rollen- und Ressourcentreiberpakete. 3. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. Eine Liste der unterstützten Datenbankversionen finden Sie unter Abschnitt 8.5.3, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 83. 4. (Bedingt) Wenn SSPR auf einem separaten Server installiert ist, rüsten Sie die Komponente auf Version 4.7 auf. 5. Rüsten Sie die Identitätsanwendungen auf Version 4.7 auf. 6. Halten Sie Tomcat an.

Komponente	Basisversion	Zwischenschritt	Aufgerüstete Version
Identitätsbericht-erstellung	4.5.x (x = 0 bis 5)	◆ Wenn Sie mit JBoss oder Websphere arbeiten, migrieren Sie zum Tomcat-Anwendungs-server. ◆ Wenden Sie den Patch 4.5.6 an.	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 unter Abschnitt 8.6.4, „Systemanforderungen für die Identitätsberichterstellung“, auf Seite 88. 3. Migrieren Sie die Ereignisrevisionsdienst-Daten zu einer unterstützten Version einer PostgreSQL- oder Oracle-Datenbank. 4. Installieren Sie SLM für IGA. 5. Rüsten Sie das Data Collection Services-Treiberpaket und das Treiberpaket „Verwaltetes System – Gateway“ auf. 6. Migrieren Sie Identity Reporting zu Version 4.7. Weitere Informationen finden Sie unter Abschnitt 29.8, „Migrieren von Identity Reporting“, auf Seite 301. 7. (Bedingt) Erstellen Sie eine Datensynchronisierungsrichtlinie auf der Seite des Identity Manager-Datenerfassungsdiensts.

NetIQ empfiehlt, vor dem Starten der Aufrüstung die Informationen in den Versionshinweisen zu Ihrer Version zu lesen:

- Versionshinweise zu NetIQ Identity Manager 4.5 Service Pack 6
- Versionshinweise zu NetIQ Identity Manager 4.5 Service Pack 5
- Versionshinweise zu NetIQ Identity Manager 4.5 Service Pack 4
- Versionshinweise zu NetIQ Identity Manager 4.5 Service Pack 3
- Versionshinweise zu NetIQ Identity Manager 4.5 Service Pack 2
- Versionshinweise zu NetIQ Identity Manager 4.5 Service Pack 1
- Versionshinweise zu NetIQ Identity Manager 4.5

25.4 Sichern der aktuellen Konfiguration

NetIQ empfiehlt, vor dem Aufrüsten die aktuelle Konfiguration Ihrer 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:

- Abschnitt 25.4.1, „Exportieren des Designer-Projekts“, auf Seite 258
- Abschnitt 25.4.2, „Exportieren der Treiberkonfiguration“, auf Seite 259

25.4.1 Exportieren des Designer-Projekts

Ein Designer-Projekt enthält das Schema und alle Treiberkonfigurationsinformationen. Wenn Sie ein Projekt Ihrer 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 258
- „Erstellen eines neuen Projekts aus dem Identitätsdepot“, auf Seite 258

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 NetIQ Designer für Identity Manager* .
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 „Exporting a Project“ (Exportieren eines Projekts) im NetIQ Designer for Identity Manager Administration Guide (Administrationshandbuch zu NetIQ Designer für Identity Manager).

Erstellen eines neuen Projekts aus dem Identitätsdepot

Wenn Ihnen kein Designer-Projekt Ihrer aktuellen 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:

- **Hostnamen:** 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.

25.4.2 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. Verwenden Sie iManager, um zu überprüfen, ob Sie über einen Export der Treibers der rollenbasierten Berechtigungen verfügen.

- „Exportieren der Treiberkonfigurationen mit Designer“, auf Seite 259
- „Exportieren der Treiberdaten mithilfe von iManager“, auf Seite 260

Exportieren der Treiberkonfigurationen mit Designer

1 Stellen Sie sicher, dass Ihr Projekt in Designer über die aktuellste Treiberversion verfügt. Weitere Informationen finden Sie unter „Importing a Library, a Driver Set, or a Driver from the Identity Vault“ (Importieren einer Bibliothek, eines Treibersatzes oder eines Treibers vom Identitätsdepot) im *NetIQ Designer for Identity Manager Administration Guide* (Administrationshandbuch zu NetIQ Designer für Identity Manager).

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.

Exportieren der Treiberdaten mithilfe von iManager

1 Klicken Sie in iManager auf **Identity Manager > Identity Manager-Überblick**.

2 Wählen Sie in der Baumstruktur den Speicherort aus, in dem nach Treibersatzobjekten gesucht werden soll, und klicken Sie dann auf das Suchsymbol ▸.

3 Klicken Sie auf das Treibersatzobjekt, das den aufzurüstenden Treiber enthält.

4 Klicken Sie auf den aufzurüstenden Treiber und anschließend auf **Exportieren**.

5 Klicken Sie auf **Weiter** und dann auf **Alle enthaltenen Richtlinien exportieren, egal ob sie mit der Konfiguration verknüpft sind oder nicht**.

6 Klicken Sie auf **Weiter** und dann auf **Speichern unter**.

7 Wählen Sie **Auf Festplatte speichern** und klicken Sie dann auf **OK**.

8 Klicken Sie auf **Fertig stellen**.

9 Führen Sie Schritt 1 bis Schritt 8 für alle Treiber aus.

26 Aufrüsten der Identity Manager-Komponenten

In diesem Abschnitt finden Sie Informationen zum Aufrüsten einzelner Komponenten in Identity Manager. Dieser Abschnitt enthält außerdem einige Schritte, die unter Umständen nach einer Aufrüstung anfallen.

26.1 Reihenfolge bei der Aufrüstung

Sie müssen die Komponenten des Identity Manager in folgender Reihenfolge aufrüsten:

1. Designer
2. Sentinel Log Management für IGA
3. Identitätsdepot
4. Identity Manager-Engine
5. Remote Loader
6. Fan-out-Agent
7. iManager
8. Identitätsanwendungen (Advanced Edition)
9. Identitätsberichterstellung
10. Analyzer

HINWEIS: Sie können jeweils nur eine Komponente aufrüsten, nicht mehrere Komponenten gleichzeitig.

26.2 Aufrüstung von Designer

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 „Exporting a Project“ (Exportieren eines Projekts) im *NetIQ Designer for Identity Manager Administration Guide* (Administrationshandbuch zu NetIQ Designer für Identity Manager).

3 Starten Sie das Designer-Installationsprogramm. Weitere Informationen finden Sie unter Kapitel 13, „Installation von Designer“, auf Seite 185.

Nach dem Aufrüsten auf die aktuelle Version von Designer müssen Sie alle Designer-Projekte aus der früheren 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 im *NetIQ Designer for Identity Manager Administration Guide* (Administrationshandbuch zu Designer für Identity Manager).

26.3 Aufrüsten der Identity Manager-Engine

Vor dem Aufrüsten der Identity Manager-Engine muss das Identitätsdepot aufgerüstet werden. Im Rahmen des Aufrüstungsvorgangs für die Identity Manager-Engine werden die Dateien des Treiberschnittstellenmoduls aktualisiert, die im Dateisystem des Hostcomputers gespeichert sind.

26.3.1 Aufrüsten des Identitätsdepots

1 Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` gemäß den Anweisungen unter Abschnitt 5.11, „Herunterladen der Installationsdateien“, auf Seite 50 herunter.

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

3 Navigieren Sie im Stammverzeichnis der `.iso`-Datei zum Verzeichnis `IDVault/setup`.

4 Führen Sie den folgenden Befehl aus:

```
./nds-install
```

5 Akzeptieren Sie die Lizenzvereinbarung und setzen Sie die Installation fort.

6 Geben Sie den **adminDN** an. Beispiel: `cn=admin.ou=sa.o=system`.

7 Wenn Sie aufgefordert werden, die eDirectory-Instanzen anzuhalten und NICI aufzurüsten, geben Sie `j` an.

8 Geben Sie an, ob **Enhanced Background Authentication** konfiguriert werden soll.

HINWEIS: Führen Sie die `ndsconfig`-Aufrüstung nach `nds-install` aus, falls die Aufrüstung der DIB fehlschlägt und `nds-install` eine entsprechende Aufforderung anzeigt. Wenn die eDirectory-Dienste nach einer Aufrüstung nicht gestartet werden, führen Sie den Aufrüstungsbefehl „ndsconfig“ aus. Weitere Informationen finden Sie im NetIQ eDirectory-Installationshandbuch.

26.3.2 Aufrüsten der Identity Manager-Engine

Stellen Sie sicher, dass alle Treiber angehalten wurden. Weitere Informationen finden Sie in Abschnitt 23.1.1, „Anhalten der Treiber“, auf Seite 241.

Vor Beginn des Aufrüstungsvorgangs dürfen sich keine Ereignisse in der Cache-Datei befinden. Wenn Sie die Identity Manager-Engine auf Version 4.7 aufrüsten, bereinigt das Engine-Installationsprogramm die vorhandenen MapDB-Treiber-Arbeitsdateien (dx*) im Cache. Nach dem

Aufrüsten des Treibers müssen Sie allerdings die vorhandenen MapDB-Status-Cache-Dateien manuell entfernen. Ansonsten kann der Treiber eventuell nicht gestartet werden. Die folgenden Identity Manager-Treiber arbeiten mit MapDB 3.0.5:

- MS Azure
- JDBC
- DCS
- MSGW
- LDAP
- Salesforce
- ServiceNow

Rüsten Sie die Identity Manager-Engine wie folgt auf:

1. Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` von der NetIQ Downloads-Website herunter.
2. Hängen Sie die heruntergeladene `.iso`-Datei ein.
3. Führen Sie den folgenden Befehl aus:

   ```
   ./install.sh
   ```

4. Lesen Sie die Lizenzvereinbarung.
5. Akzeptieren Sie die Lizenzvereinbarung mit `j`.
6. Geben Sie an, ob die Identity Manager-Komponenten aufgerüstet werden sollen. Die verfügbaren Optionen lauten `j` und `n`.
7. Wählen Sie die Identity Manager-Engine aus.
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.

26.3.3 Aufrüstung von Remote Loader

Wenn Sie den Remote Loader ausführen, müssen die Remote Loader-Dateien aufgerüstet werden.

1. Erstellen Sie eine Sicherung der Remote Loader-Konfigurationsdateien.
2. Stellen Sie sicher, dass alle Treiber angehalten wurden. Eine Anleitung dazu finden Sie in Abschnitt 23.1.1, „Anhalten der Treiber“, auf Seite 241.
3. Halten Sie den Remote Loader-Service bzw. den Daemon für jeden Treiber an.
   - **Remote Loader:** `rdxml -config` *`Pfad_zur_Konfigurationsdatei`* `-u`
   - **Java Remote Loader:** `dirxml_jremote -config` *`Pfad_zur_Konfigurationsdatei`* `-u`
4. Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` von der NetIQ Downloads-Website herunter.
5. Hängen Sie die heruntergeladene `.iso`-Datei ein.
6. Führen Sie den folgenden Befehl aus:

   ```
   ./install.sh
   ```

7. Lesen Sie die Lizenzvereinbarung.
8. Akzeptieren Sie die Lizenzvereinbarung mit `j`.

9 Geben Sie an, ob die Identity Manager-Komponenten aufgerüstet werden sollen. Die verfügbaren Optionen lauten `j` und `n`.

10 Wählen Sie den Remote Loader aus.

11 Stellen Sie nach Abschluss der Installation sicher, dass Ihre Konfigurationsdateien die Informationen Ihrer Umgebung enthalten.

12 (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.

13 Starten Sie den Remote Loader-Service bzw. den Daemon für jeden Treiber.

- **Remote Loader:** `rdxml -config` *`Pfad_zur_Konfigurationsdatei`*
- **Java Remote Loader:** `dirxml_jremote -config` *`Pfad_zur_Konfigurationsdatei`*

26.3.4 Aktualisieren von iManager

Im Allgemeinen greift der Aufrüstvorgang für iManager auf die vorhandenen Konfigurationswerte in der Datei `configiman.properties` zurück, z. B. Portwerte und autorisierte Benutzer. Falls Sie Änderungen an den Konfigurationsdateien `server.xml` und `context.xml` vorgenommen haben, empfiehlt NetIQ, diese Dateien vor dem Aufrüsten zu sichern.

Bevor Sie iManager auf Version 3.1 aufrüsten, muss eDirectory auf Version 9.1 aufgerüstet werden.

Der Aufrüstvorgang umfasst die folgenden Aufgaben:

- „Aktualisieren von iManager“, auf Seite 264
- „Aktualisieren funktionsbasierter Services“, auf Seite 265
- „Neuinstallieren oder Migrieren von Plugin Studio-Plugins“, auf Seite 265
- „Aktualisieren von iManager-Plugins nach einer Aufrüstung oder Neuinstallation“, auf Seite 266

Aktualisieren von iManager

Stellen Sie vor dem Aufrüsten von iManager sicher, dass der Computer den Voraussetzungen und Systemanforderungen entspricht.

HINWEIS: Beim Aufrüsten werden die Werte für den HTTP-Port und den SSL-Port verwendet, die in der früheren iManager-Version konfiguriert waren.

---

1 Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` gemäß den Anweisungen unter Abschnitt 5.11, „Herunterladen der Installationsdateien“, auf Seite 50 herunter.

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

3 Führen Sie den folgenden Befehl aus:

```
./install.sh
```

4 Lesen Sie die Lizenzvereinbarung.

5 Akzeptieren Sie die Lizenzvereinbarung mit `j`.

6 Geben Sie an, dass iManager die Aufrüstung fortsetzen soll.

Aktualisieren funktionsbasierter Services

Wenn Sie sich erstmalig über iManager bei einem eDirectory-Baum anmelden, der bereits eine Sammlung rollenbasierter Services (RBS-Sammlung) enthält, werden die Rolleninformationen unter Umständen nicht vollständig angezeigt. Dies ist normal, da einige Plugins zunächst aktualisiert werden müssen, damit sie mit der aktuellen Version von iManager zusammenarbeiten. NetIQ empfiehlt, die RBS-Module auf die aktuelle Version zu aktualisieren, damit Sie alle in iManager verfügbaren Funktionen nutzen können. Die RBS-Konfigurationstabelle enthält die RBS-Module, die aufgerüstet werden.

Beachten Sie, dass mehrere Funktionen mit demselben Namen vorhanden sein können. Ab iManager 2.5 haben einige Plugin-Entwickler die Aufgaben-IDs oder Modulnamen geändert, die Anzeigenamen jedoch beibehalten. Hierdurch treten bestimmte Rollen scheinbar doppelt auf, obwohl tatsächlich eine Instanz aus einer älteren Version und eine andere Instanz aus einer neueren Version stammt.

HINWEIS

- Beim Aktualisieren oder Neuinstallieren von iManager aktualisiert das Installationsprogramm die vorhandenen Plugins nicht. Aktualisieren Sie die betreffenden Plugins daher manuell. Starten Sie hierzu iManager, und navigieren Sie zu **Konfigurieren** > **Plugin-Installation** > **Verfügbare Novell-Plugin-Module**.
- In unterschiedlichen iManager-Installationen sind ggf. unterschiedlich viele Plugins lokal installiert. Aus diesem Grund können Diskrepanzen im Modulbericht für eine bestimmte Sammlung auf der Seite **Rollenbasierte Services** > **RBS-Konfiguration** auftreten. Damit die Anzahl in verschiedenen iManager-Installationen übereinstimmt, muss in allen iManager-Instanzen im Baum jeweils dieselbe Teilmenge von Plugins installiert sein.

So suchen und aktualisieren Sie veraltete RBS-Objekte:

1. Melden Sie sich bei iManager an.
2. Wählen Sie zunächst die Ansicht "Konfigurieren" und dann **Rollenbasierte Services > RBS-Konfiguration**.

   Ermitteln Sie anhand der Tabelle auf der Seite „2.*x*-Sammlungen“, ob veraltete Module vorliegen.
3. (Bedingt) Soll ein Modul aktualisiert werden, führen Sie die folgenden Schritte aus:
   - **3a** Wählen Sie die Nummer der zu aktualisierenden Sammlung in der Spalte **Veraltet** aus.

     iManager zeigt die Liste der veralteten Module an.
   - **3b** Wählen Sie das zu aktualisierende Modul aus.
   - **3c** Klicken Sie oben in der Tabelle auf **Aktualisieren**.

Neuinstallieren oder Migrieren von Plugin Studio-Plugins

Sie können Plugin Studio-Plugins auf eine andere iManager-Instanz oder eine neue oder aktualisierte Version von iManager migrieren und auch in dieser Instanz oder Version reproduzieren.

1. Melden Sie sich bei iManager an.
2. Wählen Sie in der iManager-Ansicht „Konfigurieren“ die Option **Rollenbasierte Services > Plugin Studio**.

   Der Inhaltsrahmen zeigt die Liste der installierten benutzerdefinierten Plugins an, einschließlich des Speicherorts der RBS-Sammlung, zu der die Plugins gehören.

3 Wählen Sie das Plugin aus, das neu installiert oder migriert werden soll, und klicken Sie auf **Bearbeiten**.

HINWEIS: Es kann immer nur ein Plugin bearbeitet werden.

---

4 Klicken Sie auf **Installieren**.

5 Führen Sie diese Schritte für alle neu zu installierenden oder zu migrierenden Plugins aus.

Aktualisieren von iManager-Plugins nach einer Aufrüstung oder Neuinstallation

Wenn Sie iManager aufrüsten oder neu installieren, werden die vorhandenen Plugins nicht im Rahmen des Installationsvorgangs aktualisiert. Die Plugins müssen der richtigen iManager-Version entsprechen.

1 Öffnen Sie iManager.

2 Navigieren Sie zu **Konfigurieren > Plugin-Installation > Verfügbare Novell-Plugin-Module**.

3 Aktualisieren Sie die Plugins.

26.4 Aufrüsten der Identity Manager-Treiber

NetIQ stellt neue Treiberinhalte in Form von **Paketen** bereit. Die Pakete verwalten und erstellen Sie in Designer. iManager ist zwar paketfähig; Designer kann jedoch keine Änderungen an Treiberinhalten verwalten, die Sie in iManager vornehmen. Weitere Informationen zum Verwalten von Paketen finden Sie unter „Managing Packages“ (Verwalten von Paketen) im *NetIQ Designer for Identity Manager Administration Guide* (Administrationshandbuch zu NetIQ Designer für Identity Manager).

Sie können die Treiber wie folgt auf Pakete aufrüsten:

- Abschnitt 26.4.1, „Einen neuen Treiber erstellen“, auf Seite 266
- Abschnitt 26.4.2, „Vorhandene Inhalte durch Inhalte aus Paketen ersetzen“, auf Seite 267
- Abschnitt 26.4.3, „Aktuelle Inhalte beibehalten und neue Inhalte über Pakete hinzufügen“, auf Seite 267

26.4.1 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 Identity Manager-Treiberdokumentation. Der Treiber funktioniert nun wie vorher, seine Inhalte stammen aber aus Paketen und nicht aus einer Treiberkonfigurationsdatei.

26.4.2 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 Abschnitt 25.4.2, „Exportieren der Treiberkonfiguration“, auf Seite 259.

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 „Importing Packages into the Package Catalog“ (Importieren von Paketen in den Paketkatalog) im *Designer for Identity Manager Administration Guide* (Administrationshandbuch zu Designer für Identity Manager).

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 Identity Manager-Treiberdokumentation.

4. Stellen Sie alle benutzerdefinierten Richtlinien und Regeln für den Treiber wieder her. Eine Anleitung dazu finden Sie in Abschnitt 26.9, „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“, auf Seite 284.

26.4.3 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 Abschnitt 25.4.2, „Exportieren der Treiberkonfiguration“, auf Seite 259.

   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 „Importing Packages into the Package Catalog“ (Importieren von Paketen in den Paketkatalog) im *Designer for Identity Manager Administration Guide* (Administrationshandbuch zu Designer für Identity Manager).

2 Installieren Sie die Pakete im Treiber.

   Anweisungen finden Sie im jeweiligen Treiberhandbuch auf der Website zur Identity Manager-Treiberdokumentation.

3 Fügen Sie die gewünschten Pakete zum Treiber hinzu. Diese Schritte sind bei jedem Treiber unterschiedlich.

   Weitere Informationen finden Sie auf der Website der Identity Manager-Treiberdokumentation.

Der Treiber enthält nun die über die Pakete hinzugefügten neuen Funktionen.

26.5 Aufrüsten der Identitätsanwendungen

In diesem Abschnitt finden Sie Informationen zur Aufrüstung der Identitätsanwendungen und unterstützenden Software, wozu die Aktualisierung der folgenden Komponenten gehört:

- Identity Manager-Benutzeranwendung
- One SSO Provider (OSP)
- Self-Service Password Reset (SSPR)
- Tomcat, JDK und ActiveMQ
- PostgreSQL-Datenbank

Nach der Aufrüstung sind folgende Komponentenversionen installiert:

- Tomcat – `8.5.27`
- ActiveMQ – `5.15.2`
- Java – `1.8.0_162`
- One SSO-Anbieter – `6.2.1`
- Self-Service-Funktionen für die Passwortrücksetzung – `4.2.0.4`

Dieser Abschnitt enthält Informationen zu folgenden Themen:

26.5.1 Erläuterungen zum Aufrüstungsprogramm

Im Rahmen des Aufrüstungsvorgangs werden die Konfigurationswerte der vorhandenen Komponenten gelesen. Hierzu gehören die Dateien `ism-configuration.properties`, `server.xml`, `SSPRConfiguration` 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.

26.5.2 Voraussetzungen und Überlegungen für die Aufrüstung

Lesen Sie vor einer Aufrüstung die folgenden Überlegungen:

- **Identity Manager wird auf Version 4.5.6 aufgerüstet:** Es ist nicht möglich, von einer Version vor 4.5.6 auf Version 4.7 aufzurüsten. Weitere Informationen zum Aufrüsten auf Identity Manager 4.7 finden Sie unter Abschnitt 25.3, „Unterstützte Aufrüstungspfade“, auf Seite 253.
- **Systemanforderungen:** Für die Aufrüstung werden mindestens 3 GB freier Speicherplatz benötigt, um die aktuelle Konfiguration sowie temporäre Dateien zu speichern, die während der Aufrüstung erzeugt werden. Auf Ihrem Server muss ausreichend freier Speicherplatz für die Sicherung vorhanden sein sowie weiterer freier Speicherplatz für die Aufrüstung.

  Wenn Sie die Installationsanwendungen in einer separaten Partition installiert haben (also nicht in der Stammpartition), muss die Partition ausreichend Speicherplatz für die Sicherungskonfiguration aufweisen. Außerdem muss das Verzeichnis `/tmp` ausreichend Speicherplatz für die Protokolle und die temporären Dateien enthalten. Falls der Speicherplatz in diesem Verzeichnis nicht ausreicht, legen Sie in der Umgebungsvariable `IATEMPDIR` ein Verzeichnis auf einer Partition fest, in dem ausreichend Speicherplatz frei ist. Somit wird das Aufrüstungsprogramm zur Speicherung der Dateien an dieses Verzeichnis verwiesen.

  So legen Sie ein Verzeichnis in `IATEMPDIR` fest:

  1. Öffnen Sie ein Terminal und geben Sie folgenden Befehl ein:

     ```
     export IATEMPDIR=/opt/custom_tmp
     ```

     wobei `/opt/custom_tmp` der Pfad zu dem Verzeichnis ist, in dem ausreichend Speicherplatz zur Verfügung steht.

     HINWEIS: Sichern Sie die Zertifikate `(cacerts)` der Identitätsanwendungen.

  2. Starten Sie das Aufrüstungsprogramm über die Befehlszeile.
- **Tomcat als Anwendungsserver:** Diese Identity Manager-Version unterstützt lediglich Tomcat als Anwendungsserver.

  Wenn die Identitätsanwendungen auf einem anderen Anwendungsserver ausgeführt werden (also nicht auf Tomcat), migrieren Sie den Anwendungsserver zu Tomcat, bevor Sie eine Aufrüstung vornehmen. Weitere Informationen finden Sie unter Migrating from Websphere or JBoss to Tomcat (Migrieren von Websphere oder JBoss zu Tomcat).
- **Die Datenbankplattform wird aufgerüstet:** Dieses Programm rüstet nicht die Datenbankplattform für die Identitätsanwendungen auf. Rüsten Sie die aktuelle Datenbankversion manuell auf eine unterstützte Version auf. Weitere Informationen zum Aufrüsten der PostgreSQL-Datenbank finden Sie in Abschnitt 26.5.4, „Aufrüsten der PostgreSQL-Datenbank“, auf Seite 270.
- **Das Rollen- und Ressourcentreiberpaket wird aufgerüstet:** Weitere Informationen finden Sie unter Aufrüsten installierter Pakete im *Administrationshandbuch zu NetIQ Designer für Identity Manager*.

- **Zurücksetzen von Passwörtern per Selbstbedienung:** Stellen Sie beim Aufrüsten von SSPR 4.0 sicher, dass die Eigenschaften `CATALINA_OPTS` und `-Dsspr.application.Path` auf den Ordner verweisen, in dem die SSPR-Konfiguration gespeichert ist.

  Beispiel:

  ```
  export CATALINA_OPTS="-Dsspr.applicationPath=/home/sspr_data
  ```

  Sichern Sie die SSPR-LocalDB vor dem Aufrüsten. Führen Sie die folgenden Schritte zum Exportieren oder Herunterladen der LocalDB aus:

  1. Melden Sie sich beim SSPR-Portal als Administrator an.
  2. Klicken Sie oben rechts auf der Seite im Dropdown-Menü auf **Konfigurationsmanager**.
  3. Klicken Sie auf **LocalDB**.
  4. Klicken Sie auf **LocalDB herunterladen**.

26.5.3 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.

26.5.4 Aufrüsten der PostgreSQL-Datenbank

Vor dem Aufrüsten der PostgreSQL-Datenbank müssen die nachfolgenden Schritte ausgeführt werden.

1. Halten Sie den PostgreSQL-Dienst an.

   ```
   su -s /bin/sh - postgres -c "/opt/netiq/idm/apps/postgres/bin/pg_ctl stop -w -
   D /opt/netiq/idm/apps/postgres/data"
   ```

2. Deaktivieren Sie die vorhandene Unit-Datei für den PostgreSQL-Dienst.

   ```
   systemctl disable postgresql-9.6.service
   ```

3. Bereinigen Sie die vorhandene Unit-Datei für den PostgreSQL-Dienst.

   ```
   rm /usr/lib/systemd/system/postgresql-9.6.service
   systemctl daemon-reload
   systemctl reset-failed
   ```

4. Erstellen Sie ein Sicherungsverzeichnis und sichern Sie das vorhandene PostgreSQL-Verzeichnis.

   Beispiel:

   ```
   mkdir -p /home/backup
   cp -rvf /opt/netiq/idm/apps/postgres/ /home/backup/
   ```

5. Navigieren Sie zu dem Speicherort, an dem Sie die Datei `Identity_Manager_4.7_Linux.iso` eingehängt haben.
6. Navigieren Sie zum Verzeichnis `/common/packages/postgres/`.
7. Installieren Sie die neue Version von PostgreSQL.

   ```
   rpm -ivh netiq-postgresql-9.6.6-0.noarch.rpm
   ```

   HINWEIS: Der bisher installierte benutzerdefinierte Speicherort des PostgreSQL-Basisverzeichnisses wird durch `/opt/netiq/idm/postgres/` ersetzt.

8 Erstellen Sie ein `data`-Verzeichnis im PostgreSQL-Installationsverzeichnis.

`mkdir -p <POSTGRES_HOME>/data`; `<POSTGRES_HOME>` steht hier für `/opt/netiq/idm/postgres`

Beispiel:

```
mkdir -p /opt/netiq/idm/postgres/data
```

9 Ändern Sie die Berechtigungen für das soeben installierte PostgreSQL-Verzeichnis.

```
chown -R postgres:postgres <Pfad des Postgres-Verzeichnisses>
```

Beispiel:

```
chown -R postgres:postgres /opt/netiq/idm/postgres
```

10 Erstellen Sie ein `postgres`-Basisverzeichnis.

Beispiel: `mkdir -p /home/users/postgres`

11 Ändern Sie die Berechtigungen für das soeben erstellte PostgreSQL-Basisverzeichnis.

```
chown -R postgres:postgres <Pfad des Postgres-Basisverzeichnisses>
```

Beispiel:

```
chown -R postgres:postgres /home/users/postgres
```

12 Exportieren Sie das PostgreSQL-`home`-Verzeichnis.

```
export PGHOME=<Pfad des Postgres-home-Verzeichnisses>
```

Beispiel:

```
export PG_HOME=/opt/netiq/idm/postgres
```

13 Exportieren Sie das PostgreSQL-Passwort:

```
export PGPASSWORD=<Datenbankpasswort eingeben>
```

14 Initialisieren Sie die Datenbank.

```
su -s /bin/sh - postgres -c "LANG=en_US.UTF-8 <POSTGRES_HOME>/bin/initdb -D
<POSTGRES_HOME>/data"
```

Beispiel:

```
su -s /bin/sh - postgres -c "LANG=en_US.UTF-8 /opt/netiq/idm/postgres/bin/
initdb -D /opt/netiq/idm/postgres/data"
```

15 Ersetzen Sie den Pfad zum Postgres-Basisverzeichnis in der Datei`/etc/passwd` durch `/opt/netiq/idm/postgres/`.

15a Navigieren Sie zum Verzeichnis `/etc/`.

15b Bearbeiten Sie die Datei `passwd`.

```
vi /etc/passwd
```

15c Ersetzen Sie das Basisverzeichnis des Postgres-Benutzers durch `/opt/netiq/idm/postgres/`.

16 Navigieren Sie zum Verzeichnis `/opt/netiq/idm/postgres/`.

17 Melden Sie sich als `postgres`-Benutzer an.

Beispiel:

```
su postgres
```

18 Migrieren Sie die vorhandenen Daten.

Beispiel:

```
/opt/netiq/idm/postgres/bin/pg_upgrade --old-datadir /opt/netiq/idm/apps/
postgres/data/ --new-datadir /opt/netiq/idm/postgres/data/ --old-bindir /opt/
netiq/idm/apps/postgres/bin --new-bindir /opt/netiq/idm/postgres/bin/
```

19 Melden Sie sich als `postgres`-Benutzer ab.

20 Aktualisieren Sie die Datei `pg_hba.conf`, sodass das Server-Netzwerk als vertrauenswürdig betrachtet wird:

20a Navigieren Sie zum Verzeichnis `/opt/netiq/idm/postgres/data/`.

20b Bearbeiten Sie die Datei `pg_hba.conf`:

```
vi pg_hba.conf
```

20c Fügen Sie die folgende Zeile in die Datei `pg_hba.conf` ein:

```
host all all 0.0.0.0/0 trust
```

21 Aktualisieren Sie die Konfigurationsdatei, sodass die PostgreSQL-Instanz andere Netzwerkinstanzen überwacht, also nicht `localhost`:

21a Navigieren Sie zum Verzeichnis `/opt/netiq/idm/postgres/data/`.

21b Bearbeiten Sie die Datei `postgresql.conf`:

```
vi postgresql.conf
```

21c Fügen Sie die folgende Zeile in die Datei `postgresql.conf` ein:

```
listen_addresses = '*'
```

HINWEIS: Sollen nur bestimmte Netzwerkschnittstellen überwacht werden, geben Sie die IP-Adressen als durch Komma getrennte Liste an.

---

22 Erstellen Sie das Verzeichnis `pg_log` unter `<Pfad des Postgres-Basisverzeichnisses>/data`.

Beispiel:

```
mkdir -p /opt/netiq/idm/postgres/data/pg_log
```

23 Ändern Sie die Berechtigungen für das Verzeichnis `pg_log`.

```
chown -R postgres:postgres <Pfad des Postgres-Verzeichnisses>/data/pg_log
```

Beispiel:

```
chown -R postgres:postgres /opt/netiq/idm/postgres/data/pg_log
```

24 Starten Sie den PostgreSQL-Dienst.

```
systemctl start netiq-postgresql
```

Damit wird der neue PostgreSQL-Dienst gestartet.

25 (Optional) Starten Sie das neue pgAdmin über die Benutzeroberfläche:

25a Kopieren Sie das Verzeichnis `scripts` aus dem bisherigen `postgres`-Basisverzeichnis in das neue `postgres`-Basisverzeichnis.

Beispiel:

```
cp -rvf /opt/netiq/idm/apps/postgres/scripts /opt/netiq/idm/postgres
```

25b Navigieren Sie zum Verzeichnis `/opt/netiq/idm/postgres/scripts`.

25c Bearbeiten Sie `launchpgadmin.sh` und ersetzen Sie den bisherigen PostgreSQL-Pfad durch den neuen Pfad.

Ersetzen Sie `/opt/netiq/idm/apps/postgres/` durch `/opt/netiq/idm/postgres`.

25d Navigieren Sie zum Verzeichnis `/usr/share/application` und bearbeiten Sie die Anwendung `.desktop`, sodass der neue Pfad für `launchpgadmin.sh` angegeben wird.

SLES: Bearbeiten Sie die Anwendung `pg-pgadmin-9_6.desktop` und ersetzen Sie den Wert unter `EXEC` durch den neuen Pfad für `launchpgadmin.sh`.

Beispiel:

Ersetzen Sie den Wert für `"Exec=/opt/netiq/idm/apps/postgres/scripts/launchpgadmin.sh"` durch `:"Exec=/opt/netiq/idm/postgres/scripts/launchpgadmin.sh"`.

RHEL: Navigieren Sie zum Verzeichnis `/usr/share/application` und erstellen Sie die Datei `pg-pgadmin-9_6.desktop` mit den folgenden Details:

Beispiel:

```
[Desktop Entry]
Version=1.0
Encoding=UTF-8
Name=pgAdmin 4
Exec=/opt/netiq/idm/postgres/scripts/launchpgadmin.sh
Icon=pg-pgadmin-9_6.png
Terminal=false
Type=Application
```

25e Entfernen Sie das bisherige Postgres-Basisverzeichnis aus dem System.

```
rm -rf /opt/netiq/idm/apps/postgres/
```

25f Starten Sie das System neu, damit die Änderungen wirksam werden.

26.5.5 Aufrüsten der Treiberpakete für die Identitätsanwendungen

In diesem Abschnitt erfahren Sie, wie Sie die Pakete für den Benutzeranwendungstreiber und den Rollen- und Ressourcenservice-Treiber auf die aktuelle Version aktualisieren. Sie müssen diese Aufgabe vor der Aufrüstung der Identitätsanwendungen ausführen.

1. Öffnen Sie Ihr aktuelles Projekt in Designer.
2. Klicken Sie mit der rechten Maustaste auf **Paketkatalog**, und wählen Sie „Paket importieren“.
3. Wählen Sie das gewünschte Paket aus. Beispiel: **Benutzeranwendungstreiber-Basispaket**.
4. Klicken Sie auf **OK**.
5. Klicken Sie in der Entwickler-Ansicht mit der rechten Maustaste auf den Treiber, und klicken Sie auf **Eigenschaften**.
6. Navigieren Sie auf der Seite **Eigenschaften** zur Registerkarte **Pakete**.
7. Klicken Sie oben rechts auf das Symbol **Paket hinzufügen (+)**.
8. Wählen Sie das Paket aus, und klicken Sie auf **OK**.
9. Wiederholen Sie dieses Verfahren und rüsten Sie das Paket für den Rollen- und Ressourcenservice-Treiber auf.

HINWEIS: Der Benutzeranwendungstreiber und der Rollen- und Ressourcenservice-Treiber müssen mit der aufgerüsteten Version von Identity Manager verbunden sein.

26.5.6 Aufrüsten der Identitätsanwendungen

HINWEIS: Wenn die Identitätsanwendungen und SSPR auf unterschiedlichen Servern installiert sind, müssen Sie SSPR manuell aufrüsten. Weitere Informationen finden Sie unter „Aufrüsten von SSPR“, auf Seite 274.

Aufrüsten der Identitätsanwendungen

Im nachfolgenden Verfahren erfahren Sie, wie Sie die Identitätsanwendungen aufrüsten.

1. Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` von der NetIQ Downloads-Website herunter.
2. Hängen Sie die heruntergeladene `.iso`-Datei ein.
3. Führen Sie den folgenden Befehl aus:

   ```
   ./install.sh
   ```

4. Lesen Sie die Lizenzvereinbarung.
5. Akzeptieren Sie die Lizenzvereinbarung mit `j`.
6. Geben Sie an, ob die Identity Manager-Komponenten aufgerüstet werden sollen. Die verfügbaren Optionen lauten **j** und **n**.
7. Wählen Sie die Identitätsanwendungen aus und setzen Sie die Aufrüstung fort.
8. Geben Sie die folgenden Informationen ein:

   SSPR-Installationsordner: Geben Sie den SSPR-Installationsordner an.

   Benutzeranwendungsordner: Geben Sie den Benutzeranwendungsordner an.

   One SSO-Dienstpasswort für Identitätsanwendungen: Geben Sie das One SSO-Passwort an.

   JDBC-jar-Datei für Identitätsanwendungs-Datenbank: Geben Sie die JAR-Datei für die Datenbank an. Der Standardspeicherort der vorhandenen Datenbank-jar-Datei lautet `/opt/netiq/idm/apps/postgres/postgresql-9.4.1212.jar`.

   Schema für Identitätsanwendungen erstellen: Gibt den Zeitpunkt an, zu dem das Datenbankschema erstellt werden soll. Verfügbare Optionen: **Jetzt**, **Start** und **Datei**.

Aufrüsten von SSPR

HINWEIS: Wenn SSPR nicht auf demselben Server wie die Identitätsanwendungen und OSP installiert ist, müssen Sie SSPR separat aufrüsten.

1. Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` gemäß den Anweisungen unter Abschnitt 5.11, „Herunterladen der Installationsdateien“, auf Seite 50 herunter.
2. Hängen Sie die heruntergeladene `.iso`-Datei ein.
3. Navigieren Sie im Stammverzeichnis der `.iso`-Datei zum Verzeichnis `SSPR`.
4. Führen Sie den folgenden Befehl aus:

   ```
   ./install.sh
   ```

5 Lesen Sie die Lizenzvereinbarung.

6 Akzeptieren Sie die Lizenzvereinbarung mit `j`.

26.5.7 Aufgaben nach der Aufrüstung

- Prüfen Sie, ob der Parameter **RBPM-zu-eDirectory-SAML-Konfiguration** im configupdate-Dienstprogramm auf **Auto** eingestellt ist.
  1. Starten Sie das Dienstprogramm configupdate.
  2. Navigieren Sie zu **SSO-Clients** > **RBPM** und legen Sie unter **RBPM-zu-eDirectory-SAML-Konfiguration** die Option `Auto` fest.
  3. Speichern Sie die Änderungen.
  4. Starten Sie Tomcat.
- Ändern Sie die Berechtigung und das Eigentum für das OSP-Verzeichnis:

  ```
  chmod +x novlua:novlua /opt/netiq/idm/apps/osp
  ```
- Löschen Sie die bisherige Version des Tomcat- und des ActiveMQ-Diensts manuell.

  ```
  /etc/init.d/idmapps_tomcat_init
  /etc/init.d/idmapps_activemq_init
  ```

Sie müssen außerdem die benutzerdefinierten Einstellungen für Tomcat, SSPR, OSP oder die Identitätsanwendungen manuell wiederherstellen.

- „Java“, auf Seite 275
- „Tomcat“, auf Seite 276
- „Identitätsanwendungen“, auf Seite 277
- „One SSO-Anbieter“, auf Seite 278
- „Kerberos“, auf Seite 278

Java

Prüfen Sie, ob der aufgerüstete JRE-Speicherort (`jre/lib/security/cacerts`) alle Zertifikate aus dem bisherigen JRE-Speicherort enthält. Falls ein Zertifikat fehlt, importieren Sie dieses Zertifikat manuell in die `cacerts` der aufgerüsteten JRE.

1 Importieren Sie `java cacerts` mit dem Befehl `keytool`:

```
keytool -import -trustcacerts -file Cerificate_Path -alias ALIAS_NAME -keystore
cacerts
```

HINWEIS: Nach der Aufrüstung ist JRE im Installationsverzeichnis der Identitätsanwendungen gespeichert. Beispiel: `/opt/netiq/idm/apps/jre`.

---

2 Prüfen Sie den JRE-Speicherort.

```
tomcat/bin/setenv.sh
```

3 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 die benutzerdefinierten 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 `osp.jks` auf alle Knoten vom ersten Knoten unter `/opt/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 Identitätsanwendungen in das Identitätsdepot unter `/opt/novell/eDirectory/lib64/nds-modules/jre/lib/security/cacerts`.

  Sie können die Zertifikate beispielsweise mit dem folgenden „keytool“-Befehl in das Identitätsdepot importieren:

  ```
  keytool -importkeystore -alias <keyalias> -srckeystore  <backup cacert> -
  srcstorepass changeit -destkeystore /opt/novell/eDirectory/lib64/nds-
  modules/jre/lib/security/cacerts
   -deststorepass changeit
  ```

2 (Bedingt) Navigieren Sie zur Benutzeranwendung und stellen Sie die benutzerdefinierten Einstellungen manuell wieder her. Lesen Sie hierzu die gesicherte Konfiguration wieder ein.

Identitätsanwendungen

Stellen Sie die benutzerdefinierten Konfigurationen der Identitätsanwendungen anhand der Sicherung wieder her, die im Rahmen des Aufrüstungsvorgangs erstellt wurde.

Wenn Sie den benutzerdefinierten Kontextordner vor dem Ausführen des Aufrüstungsprogramms in `IDMProv` umbenannt haben, stellen Sie den ursprünglichen Kontextnamen mit dem Dienstprogramm `configupdate` wieder her. Der ursprüngliche benutzerdefinierte Kontextname lautet beispielsweise `IDMDev` und wurde in `IDMProv` umbenannt.

Stellen Sie den ursprünglichen Kontextnamen mit den folgenden Schritten wieder her:

1. Navigieren Sie zum Benutzeranwendungsverzeichnis unter `/opt/netiq/idm/apps/UserApplication`.
2. (Optional) Möchten Sie das configupdate-Dienstprogramm über die Benutzeroberfläche starten, stellen Sie sicher, dass die Option `use_console` in der Datei `configupdate.sh.properties` auf `false` festgelegt wurde.

   Dieser Schritt ist erforderlich, da das Aufrüstdienstprogramm den Wert dieser Option in `true` ändert.

   Alternativ starten Sie das configupdate-Dienstprogramm und übergeben Sie ein zusätzliches Befehlszeilenargument unter Linux.

   ```
   ./configupdate.sh use_console=false
   ```

3. Starten Sie das Dienstprogramm `configupdate`.

   ```
   configupdate.sh
   ```

4. Klicken Sie auf der Registerkarte **Benutzeranwendung** auf **Erweiterte Optionen anzeigen** und führen Sie die folgenden Schritte aus:

   4a Aktivieren Sie das Kontrollkästchen **Namen des RBPM-Kontexts ändern**.

   4b Geben Sie den ursprünglichen RBPM-Kontextnamen ein.

   4c Wählen Sie den zugehörigen **Rollentreiber-DN** aus, und klicken Sie auf **OK**.

   4d Ändern Sie die Berechtigung und das Eigentum für die `WAR`-Datei mit dem folgenden Befehl.

   ```
   chmod 755 <Original_Context_Name>.war; chown -R novlua:novlua
   <Original_Context_Name>.war
   ```

   Der ursprüngliche benutzerdefinierte Kontextname lautet beispielsweise `IDMDev`:

   ```
   chmod 755 IDMDev.war; chown -R novlua:novlua IDMDev.war
   ```

5. (Bedingt) Sobald Sie alle Aufgaben nach der Aufrüstung beendet haben, starten Sie den Tomcat-Dienst für die Identitätsanwendungen.

One SSO-Anbieter

Wenn OSP und die Benutzeranwendung auf verschiedenen Servern installiert sind, aktualisieren Sie den SSO-Client-Parameter mit dem Konfigurationsaktualisierungsprogramm. Weitere Informationen hierzu finden Sie in „IDM-Dashboard“, auf Seite 160 in Abschnitt 11.6.5, „Parameter für SSO-Clients“, auf Seite 160.

Standardmäßig ist der Eintrag `LogHost` in der Datei `/etc/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.

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.

26.6 Aufrüsten der Identitätsberichterstellung

Die Identitätsberichterstellung umfasst zwei Treiber. Nehmen Sie die Aufrüstung in der nachstehenden Reihenfolge vor:

HINWEIS: Die Datenbank muss auf eine unterstützte Version aufgerüstet sein.

---

1. Rüsten Sie die Datenbank auf eine unterstützte Version auf. Weitere Informationen zum Aufrüsten der PostgreSQL-Datenbank finden Sie unter Abschnitt 26.5.4, „Aufrüsten der PostgreSQL-Datenbank“, auf Seite 270.
2. Rüsten Sie die Treiberpakete auf. Weitere Informationen finden Sie unter Abschnitt 26.6.2, „Aufrüsten der Treiberpakete für die Identitätsberichterstellung“, auf Seite 279.
3. Rüsten Sie auf Sentinel Log Management für IGA auf (oder führen Sie die Migration durch).

   Wenn Sie von Identity Reporting 4.6.x aufrüsten, rüsten Sie Sentinel Log Management für IGA auf die Version 4.7 auf. Weitere Informationen finden Sie unter Abschnitt 26.6.3, „Aufrüsten von Sentinel Log Management für IGA“, auf Seite 279.

   Wenn Sie von Identity Reporting 4.5.x migrieren, migrieren Sie von EAS zu Sentinel Log Management für IGA. Weitere Informationen finden Sie unter Abschnitt 29.8.1, „Migrieren des Ereignisrevisionsdiensts in Sentinel for Log Management für IGA“, auf Seite 302.
4. Rüsten Sie die Identitätsberichterstellung auf. Weitere Informationen finden Sie unter Abschnitt 26.6.5, „Aufrüsten der Identitätsberichterstellung“, auf Seite 280.

26.6.1 Voraussetzungen und Überlegungen für die Aufrüstung

Vor einer Aufrüstung gelten die folgenden Überlegungen:

- Bei der Aufrüstung müssen Sie den richtigen Speicherort für die Datei `postgresql-9.4.1212.jar` angeben. Der Standardspeicherort lautet `/opt/netiq/idm/postgres/`. In den folgenden Szenarien schlägt die Datenbankverbindung fehl:
  - wenn Sie den falschen Pfad angeben
  - wenn Sie die falsche jar-Datei angeben

- wenn die Firewall aktiviert ist
- wenn die Datenbank keine Verbindungen von entfernten Computern akzeptiert

- Wenn die Datenbank über SSL konfiguriert ist, entfernen Sie `ssl=true` aus der Datei `server.xml` in PATH unter:

  ```
  /opt/netiq/idm/apps/tomcat/conf/
  ```

  Ändern Sie beispielsweise

  ```
  jdbc:postgresql://<postgres db>:5432/idmuserappdb?ssl=true
  ```

  in

  ```
  jdbc:postgresql://<postgres db>:5432/idmuserappdb
  ```

26.6.2 Aufrüsten der Treiberpakete für die Identitätsberichterstellung

In diesem Abschnitt wird die Aktualisierung der Pakete für den MSGW-Treiber und den DCS-Treiber auf die aktuelle Version beschrieben. Sie müssen diese Aufgabe vor der Aufrüstung der Identitätsberichterstellung ausführen.

1. Öffnen Sie Ihr aktuelles Projekt in Designer.
2. Klicken Sie mit der rechten Maustaste auf **Paketkatalog**, und wählen Sie „Paket importieren“.
3. Wählen Sie das gewünschte Paket aus. Beispiel: **Managed System Gateway-Basispaket**.
4. Klicken Sie auf **OK**.
5. Klicken Sie in der Entwickler-Ansicht mit der rechten Maustaste auf den Treiber, und klicken Sie auf **Eigenschaften**.
6. Navigieren Sie auf der Seite **Eigenschaften** zur Registerkarte **Pakete**.
7. Klicken Sie oben rechts auf das Symbol **Paket hinzufügen (+)**.
8. Wählen Sie das Paket aus, und klicken Sie auf **OK**.
9. Wiederholen Sie dieses Verfahren und rüsten Sie das Paket für den Datenerfassungsdiensttreiber auf.

HINWEIS: Überprüfen Sie, ob der MSGW-Treiber und der DCS-Treiber mit der aufgerüsteten Version von Identity Manager verbunden sind.

26.6.3 Aufrüsten von Sentinel Log Management für IGA

1. Laden Sie die Datei `SentinelLogManagementForIGA8.1.1.0.tar.gz` von der NetIQ Downloads-Website herunter.
2. Navigieren Sie zu dem Verzeichnis, in dem die Datei extrahiert werden soll.
3. Extrahieren Sie die Datei mit dem folgenden Befehl:

   ```
   tar -zxvf SentinelLogManagementForIGA8.1.1.0.tar.gz
   ```

4. Navigieren Sie zum Verzeichnis `SentinelLogManagementforIGA`.
5. Installieren Sie SLM für IGA mit dem folgenden Befehl:

   ```
   ./install.sh
   ```

6 Geben Sie die Sprache an, die für die Installation verwendet werden soll. Drücken Sie dann die `Eingabetaste`.

7 Akzeptieren Sie die Lizenzvereinbarung mit `j`.

HINWEIS: Nach dem Aufrüsten von SLM für IGA müssen Sie die aktuellen Kollektoren manuell importieren.

1. Navigieren Sie zur NetIQ Downloads-Website.
2. Laden Sie die Datei `SentinelLogManagementForIGA8.1.1.0.tar.gz` herunter.
3. Extrahieren Sie die Datei und navigieren Sie zum Verzeichnis `/content/`.
4. Importieren Sie den Identity Manager-Kollektor.

26.6.4 Aufrüsten des Betriebssystems

Wenn Sie das Betriebssystem von SLES 11 auf SLES 12 aufrüsten, werden beim Aufrüstungsverfahren für das Betriebssystem einige SLM für IGA-RPMs gelöscht.

Die nachfolgenden Befehle sorgen dafür, dass SLM für IGA nach dem Aufrüsten des Betriebssystems ordnungsgemäß arbeitet.

HINWEIS: Rüsten Sie zunächst SLM für IGA auf, bevor Sie das Betriebssystem aufrüsten.

So rüsten Sie Ihr Betriebssystem auf:

1 Navigieren Sie zu dem Verzeichnis, in das die Sentinel-Installationsdatei extrahiert wurde.

2 Stoppen Sie die Sentinel-Dienste:

```
rcsentinel stop
```

3 Führen Sie den folgenden Befehl aus:

```
./install.sh --preosupgrade
```

4 Rüsten Sie Ihr Betriebssystem auf.

5 Führen Sie den folgenden Befehl aus:

```
./install.sh --postosupgrade
```

6 Starten Sie den Sentinel-Dienst neu:

```
rcsentinel restart
```

26.6.5 Aufrüsten der Identitätsberichterstellung

1 Laden Sie die Datei `Identity_Manager_4.7_Linux.iso` von der NetIQ Downloads-Website herunter.

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

3 Führen Sie den folgenden Befehl aus:

```
./install.sh
```

4 Lesen Sie die Lizenzvereinbarung.

5 Akzeptieren Sie die Lizenzvereinbarung mit `j`.

6 Geben Sie an, ob die Identity Manager-Komponenten aufgerüstet werden sollen. Die verfügbaren Optionen lauten **j** und **n**.

7 Wählen Sie Identity Reporting aus und setzen Sie die Aufrüstung fort.

8 Geben Sie die folgenden Informationen ein:

OSP installiert: Geben Sie an, ob OSP installiert ist.

Berichterstellungs-Installationsordner für Sicherung: Geben Sie den Berichterstellungs-Installationsordner an.

Schema für Identity Reporting erstellen: Geben Sie den Zeitpunkt an, zu dem das Schema für die Datenbank erstellt werden soll.

JDBC-jar-Datei für Identity Reporting-Datenbank: Geben Sie die Datenbank-jar-Datei für Identity Reporting an. Der Standardspeicherort der vorhandenen Datenbank-jar-Datei lautet `/opt/netiq/idm/apps/postgres/postgresql-9.4.1212.jar`.

Identity Reporting-Datenbankbenutzer: Geben Sie den Namen des Berichterstellungsdatenbank-Benutzers an.

Passwort für Identity Reporting-Datenbankkonto: Geben Sie das Passwort für die Berichterstellungsdatenbank an.

26.6.6 Schritte nach der Aufrüstung für Reporting

HINWEIS: Die Identity Manager 4.6.1-Berichte sind nach einer Aufrüstung nicht mehr nutzbar. Sie können lediglich die Identity Manager 4.7-Berichte nutzen.

Wenn Sie bei der Aufrüstung für die Erstellung des **Datenbankschemas** die Option **Start** oder **Datei** gewählt haben, gehen Sie wie folgt vor:

1. Melden Sie sich bei Identity Reporting an.
2. Löschen Sie die vorhandenen Datenquellen- und Berichtdefinitionen aus dem Identity Reporting-Repository.
3. Tragen Sie die neue Identity Manager-Datenerfassungsdienst-Datenquelle ein.

26.6.7 Überprüfen der Aufrüstung für die Identitätsberichterstellung

1 Starten Sie die Identitätsberichterstellung.

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.

26.7 Aufrüsten von Analyzer

Für die Aufrüstung von Analyzer stellt NetIQ 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.

1. Laden Sie die Datei `Identity_Manager_4.7_Linux_Analyzer.tar.gz` von der NetIQ Downloads-Website 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** Prüfen Sie, ob die neue Version im Programm angezeigt wird.

26.8 Hinzufügen von neuen Servern zum Treibersatz

Beim Aufrüsten oder Migrieren von 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 iManager aktualisieren.

26.8.1 Hinzufügen des neuen Servers zum Treibersatz

Wenn Sie iManager verwenden, müssen Sie den neuen Server zum Treibersatz hinzufügen. Designer enthält einen Migrationsassistenten für den Server, der diesen Schritt für Sie durchführt. Wenn Sie iManager verwenden, führen Sie die folgenden Schritte durch:

1. Klicken Sie in iManager auf , um die Identity Manager-Verwaltungsseite anzuzeigen.
2. Klicken Sie auf **Identity Manager-Überblick**.
3. Suchen Sie den Container, der den Treibersatz enthält, und wählen Sie ihn aus.
4. Klicken Sie auf den Treibersatznamen, um auf die Seite „Treibersatz-Überblick“ zuzugreifen.
5. Klicken Sie auf **Server > Server hinzufügen**.
6. Suchen Sie den neuen Identity Manager -Server, wählen Sie ihn aus, und klicken Sie anschließend auf **OK**.

26.8.2 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 283
- „Mithilfe von iManager den alten Server aus dem Treibersatz entfernen“, auf Seite 283
- „Stilllegen des alten Servers“, auf Seite 283

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 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 „Deploying a Driver Set to an Identity Vault“ (Bereitstellen eines Treibersatzes in einem Identitätsdepot) im *NetIQ Designer for Identity Manager Administration Guide* (Administrationshandbuch zu NetIQ Designer für Identity Manager).

Mithilfe von iManager den alten Server aus dem Treibersatz entfernen

1 Klicken Sie in iManager auf , um die Identity Manager-Verwaltungsseite anzuzeigen.

2 Klicken Sie auf **Identity Manager-Überblick**.

3 Suchen Sie den Container, der den Treibersatz enthält, und wählen Sie ihn aus.

4 Klicken Sie auf den Treibersatznamen, um auf die Seite „Treibersatz-Überblick“ zuzugreifen.

5 Klicken Sie auf **Server > Server entfernen**.

6 Wählen Sie den alten Identity Manager-Server 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 eDirectory-Reproduktionen von diesem Server.

   Weitere Informationen finden Sie unter Löschen von Reproduktionen im *Novell eDirectory - Administrationshandbuch*.

2 Entfernen Sie eDirectory von diesem Server.

   Weitere Informationen finden Sie in TID 10056593, „Removing a Server From an NDS Tree Permanently“.

26.9 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.

- Abschnitt 26.9.1, „Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von Designer“, auf Seite 284
- Abschnitt 26.9.2, „Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von iManager“, auf Seite 285

26.9.1 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 in Abschnitt 23.1.2, „Starten der Treiber“, auf Seite 242. Weitere Informationen zum Testen des Treibers finden Sie unter „Testing Policies with Policy Simulator“ (Testen von Richtlinien mit den Richtliniensimulator) im Handbuch *NetIQ Identity Manager Using Designer to Create Policies* (NetIQ Identity Manager-Verwenden von Richtlinien in Designer).
9. Wenn Sie überprüft haben, dass die Richtlinien funktionieren, können Sie den Treiber in der Produktionsumgebung einsetzen.

26.9.2 Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von iManager

Führen Sie diese Schritte in einer Testumgebung durch, bevor Sie den aktualisierten Treiber in Ihre Produktionsumgebung verschieben.

1. Klicken Sie in iManager auf **Identity Manager > Identity Manager-Überblick**.
2. Wählen Sie in der Baumstruktur den Speicherort aus, in dem nach Treibersatzobjekten gesucht werden soll, und klicken Sie dann auf das Suchsymbol ▸.
3. Klicken Sie auf das Treibersatzobjekt, das den aufgerüsteten Treiber enthält.
4. Klicken Sie auf das Treibersymbol und wählen Sie dann den Richtliniensatz, dessen benutzerdefinierte Richtlinie wiederhergestellt werden soll.
5. Klicken Sie auf **Einfügen**.
6. Wählen Sie **Vorhandene Richtlinie verwenden**. Wechseln Sie anschließend zur benutzerdefinierten Richtlinie und wählen Sie sie aus.
7. Klicken Sie auf **OK** und anschließend auf **Schließen**.
8. Wiederholen Sie Schritt 3 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 in Abschnitt 23.1.2, „Starten der Treiber“, auf Seite 242. In iManager 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.

27 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 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 Identitätsdepot-Verzeichnis `dib`.

     `/var/opt/novell/eDirectory/data/dib`
   - **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 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 die folgenden WAR-Dateien und Webapps-Ordner aus dem Verzeichnis `/opt/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 `<Installationsordner>/tomcat/conf` in ein Sicherungsverzeichnis.
8. Installieren Sie die Identitätsberichterstellung von den Medien für Identity Manager 4.6.
9. Starten Sie `configupdate.sh` 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. `192.168.0.1`
  - **TCP-Port für OAuth-Server**
  - **OAuth-Server verwendet TLS/SSL**
- Authentifizierungskonfiguration
  - **OAuth-Keystore-Datei**. Beispiel: `/opt/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://192.168.0.1:8180/sspr/public/oauth`

Weitere Informationen zum Konfigurationsprogramm finden Sie in „Ausführen des Konfigurationsprogramms der Identitätsanwendungen“, auf Seite 144.

10 Speichern Sie die Änderungen und schließen Sie das Konfigurationsprogramm.

11 Starten Sie Tomcat.

X Migrieren der Identity Manager-Daten in eine neue Installation

In diesem Abschnitt wird die Migration vorhandener Daten aus den Identity Manager-Komponenten in eine neue Installation beschrieben. Der Großteil der Migrationsaufgaben befasst sich mit Identitätsanwendungen. Anweisungen zum Aufrüsten der Identity Manager-Komponenten finden Sie unter Teil IX, „Aufrüsten von Identity Manager“, auf Seite 249. Weitere Informationen zum Unterschied zwischen Aufrüstung und Migration finden Sie in Abschnitt 25.2, „Erläuterungen zum Aufrüstungsvorgang“, auf Seite 253.

28 Vorbereiten der Migration von Identity Manager

In diesem Abschnitt wird die Vorbereitung Ihrer Identity Manager-Lösung auf die Migration in die neue Installation beschrieben.

28.1 Checkliste für die Migration

NetIQ empfiehlt, die Schritte in der nachfolgenden Checkliste für die Migration auszuführen.

	Checkliste
❑	1. Entscheiden Sie sich, ob eine Aufrüstung oder eine Migration vorgenommen werden soll. Weitere Informationen finden Sie in Abschnitt 25.2, „Erläuterungen zum Aufrüstungsvorgang“, auf Seite 253.
❑	2. Stellen Sie sicher, dass das aktuelle Installations-Kit für die Migration der Identity Manager-Daten vorliegt.
❑	3. Informieren Sie sich über die Interaktion zwischen den Identity Manager-Komponenten. Weitere Informationen finden Sie in Teil I, „Einführung“, auf Seite 15.
❑	4. Stellen Sie sicher, dass die Computer die Hardware- und Software-Anforderungen für eine höhere Version von Identity Manager erfüllen. Weitere Informationen finden Sie in Abschnitt 5.9, „Vorbereitung der Installation“, auf Seite 43 sowie in den Versionshinweisen zur Version, auf die Sie aufrüsten möchten.
❑	5. Rüsten Sie eDirectory auf die aktuelle unterstützte Version für das Identitätsdepot auf. Weitere Informationen finden Sie in Abschnitt 26.3.1, „Aufrüsten des Identitätsdepots“, auf Seite 262.
❑	6. Fügen Sie dem neuen Server die eDirectory-Reproduktionen hinzu, die sich auf dem aktuellen Identity Manager-Server befinden. Weitere Informationen finden Sie in Abschnitt 29.4, „Migrieren der Identity Manager-Engine auf einen neuen Server“, auf Seite 297.
❑	7. Installieren Sie Identity Manager auf dem neuen Server. Weitere Informationen finden Sie in „Planen der Installation von Identity Manager“, auf Seite 31.
❑	8. (Bedingt) Wenn der Treibersatz einen Remote Loader-Treiber enthält, rüsten Sie den Remote Loader-Server für jeden Treiber auf. Weitere Informationen finden Sie in Abschnitt 26.3.3, „Aufrüstung von Remote Loader“, auf Seite 263.
❑	9. (Bedingt) Wenn die Benutzeranwendung auf dem bisherigen Server ausgeführt wird, aktualisieren Sie diese Komponente und die zugehörigen Treiber. Weitere Informationen finden Sie in Abschnitt 29.1, „Checkliste für die Migration von Identity Manager“, auf Seite 293.
❑	10. Ändern Sie die serverspezifischen Informationen für jeden Treiber. Weitere Informationen finden Sie in Abschnitt 29.3.1, „Kopieren der serverspezifischen Informationen in Designer“, auf Seite 295.

	Checkliste
❑	11. (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 Abschnitt 29.3, „Kopieren von serverspezifischen Informationen für den Treibersatz“, auf Seite 295.
❑	12. Aktualisieren Sie die Treiber auf das Paketformat. Weitere Informationen finden Sie in Abschnitt 26.4, „Aufrüsten der Identity Manager-Treiber“, auf Seite 266.
❑	13. (Bedingt) Wenn Sie benutzerdefinierte Richtlinien und Regeln verwenden, stellen Sie die angepassten Einstellungen wieder her. Weitere Informationen finden Sie in Abschnitt 26.9, „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“, auf Seite 284.
❑	14. Installieren Sie Identity Reporting und die zugehörigen Treiber. Weitere Informationen finden Sie in Abschnitt 29.8, „Migrieren von Identity Reporting“, auf Seite 301.
❑	15. Entfernen Sie den alten Server aus dem Treibersatz. Weitere Informationen finden Sie in Abschnitt 26.8.2, „Entfernen des alten Servers aus dem Treibersatz“, auf Seite 282.
❑	16. Aktivieren Sie die aufgerüstete Identity Manager-Lösung. Weitere Informationen finden Sie in Abschnitt 24, „Aktivieren von Identity Manager“, auf Seite 245.

28.2 Anhalten und Starten der Identity Manager-Treiber während der Migration

Beim Aufrüsten oder Migrieren von Identity Manager müssen Sie die Treiber starten und anhalten, damit die richtigen Dateien geändert oder ersetzt werden können. Dieser Abschnitt enthält die nachfolgenden Verfahren. Weitere Informationen finden Sie in den folgenden Abschnitten:

- Abschnitt 23.1.1, „Anhalten der Treiber“, auf Seite 241
- Abschnitt 23.1.2, „Starten der Treiber“, auf Seite 242

29 Migrieren von Identity Manager auf einen neuen Server

In diesem Abschnitt wird die Migration von der Benutzeranwendung auf die Identitätsanwendungen 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:

29.1 Checkliste für die Migration von Identity Manager

NetIQ empfiehlt, die Schritte in der nachfolgenden Checkliste auszuführen.

	Checkliste
❑	1. Sichern Sie die Verzeichnisse und Datenbanken in Ihrer Identity Manager-Lösung.
❑	2. Stellen Sie sicher, dass jeweils die aktuelle Version der Identity Manager-Komponenten installiert ist (außer die Identitätsanwendungen). Weitere Informationen finden Sie in Abschnitt 5.7.4, „Empfohlene Servereinrichtung“, auf Seite 40 sowie in den aktuellen Versionshinweisen für die Komponenten. **HINWEIS:** Soll die aktuelle Datenbank der Benutzeranwendung weiterhin genutzt werden, wählen Sie im Installationsprogramm die Option **Vorhandene Datenbank**. Weitere Informationen finden Sie in Kapitel 9, „Installieren der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting“, auf Seite 91.
❑	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 in Abschnitt 29.2, „Vorbereiten des Designer-Projekts auf die Migration“, auf Seite 294.

	Checkliste
❑	6. (Bedingt) Soll die Identity Manager-Engine auf einen neuen Server migriert werden, kopieren Sie die eDirectory-Reproduktionen auf den neuen Server. Weitere Informationen finden Sie in Abschnitt 29.4, „Migrieren der Identity Manager-Engine auf einen neuen Server“, auf Seite 297.
❑	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 in Abschnitt 29.5, „Migrieren des Benutzeranwendungstreibers“, auf Seite 297.
❑	9. Rüsten Sie die Identitätsanwendungen auf. Weitere Informationen finden Sie in Abschnitt 26.5, „Aufrüsten der Identitätsanwendungen“, auf Seite 268.
❑	10. (Bedingt) Soll eine Oracle-Datenbank mit einer SQL-Datei aufgerüstet werden, die im Rahmen des Installationsvorgangs erstellt wurde, bereiten Sie die Oracle-Umgebung entsprechend vor. Weitere Informationen finden Sie in Abschnitt 29.7.1, „Vorbereiten einer Oracle-Datenbank für die SQL-Datei“, auf Seite 299.
❑	11. Stellen Sie sicher, dass die Browser keine Inhalte aus früheren Versionen von Identity Manager enthalten. Weitere Informationen finden Sie in Abschnitt 29.7.2, „Leeren des Browsercache“, auf Seite 300.
❑	12. (Bedingt) Stellen Sie Ihre benutzerdefinierten Einstellungen für das SharedPagePortlet wieder her. Weitere Informationen finden Sie in Abschnitt 29.7.3, „Aktualisieren der Einstellung für die maximale Zeitüberschreitung für das SharedPagePortlet“, auf Seite 300.
❑	13. Stellen Sie sicher, dass mit der Suchoption für Gruppen erst dann Informationen angezeigt werden, wenn der Benutzer Filterparameter festlegt. Weitere Informationen finden Sie in Abschnitt 29.7.4, „Deaktivieren der Einstellung für automatische Abfragen für Gruppen“, auf Seite 301.

29.2 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 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.

29.3 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 iManager. Wenn Sie Designer verwenden, ist es ein automatisierter Prozess. Wenn Sie iManager verwenden, ist es ein manueller Prozess. Die Migration eines Identity Manager-Servers vor Version 3.5 auf einen Identity Manager-Server mit Version 3.5 oder höher sollten Sie mit iManager vornehmen. Bei allen anderen unterstützten Migrationspfaden können Sie Designer verwenden.

- Abschnitt 29.3.1, „Kopieren der serverspezifischen Informationen in Designer“, auf Seite 295
- Abschnitt 29.3.2, „Ändern der serverspezifischen Informationen in iManager“, auf Seite 296
- Abschnitt 29.3.3, „Ändern der serverspezifischen Informationen für die Benutzeranwendung“, auf Seite 297

29.3.1 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 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. NetIQ empfiehlt, diese Option zu verwenden.
- **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 „Deploying a Driver to an Identity Vault“ (Bereitstellen eines Treibersatzes in einem Identitätsdepot) im *NetIQ Designer for Identity Manager Administration Guide* (Administrationshandbuch zu NetIQ Designer für Identity Manager).

8 Starten Sie die Treiber.

Weitere Informationen finden Sie in Abschnitt 23.1.2, „Starten der Treiber“, auf Seite 242.

29.3.2 Ändern der serverspezifischen Informationen in iManager

1 Klicken Sie in iManager auf , um die Identity Manager-Verwaltungsseite anzuzeigen.

2 Klicken Sie auf **Identity Manager-Überblick**.

3 Suchen Sie den Container, der den Treibersatz enthält, und wählen Sie ihn aus.

4 Klicken Sie auf den Treibersatznamen, um auf die Seite „Treibersatz-Überblick“ zuzugreifen.

5 Klicken Sie auf die obere rechte Ecke des Treibers und klicken Sie anschließend auf **Treiber anhalten**.

6 Klicken Sie auf die obere rechte Ecke des Treibers und klicken Sie anschließend auf **Eigenschaften bearbeiten**.

7 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.

8 Klicken Sie zum Speichern aller Änderungen auf **OK**.

9 Klicken Sie auf die obere rechte Ecke des Treibers, um ihn zu starten.

10 Wiederholen Sie Schritt 5 bis Schritt 9 für jeden Treiber im Treibersatz.

29.3.3 Ändern der serverspezifischen Informationen für die Benutzeranwendung

Sie müssen die Benutzeranwendung neu konfigurieren, damit der neue Server erkannt wird. Führen Sie `configupdate.sh` aus.

1. Navigieren Sie zum Konfigurationsprogramm für die Aktualisierung (standardmäßig im Installationsunterverzeichnis der Benutzeranwendung).
2. Starten Sie das Konfigurationsprogramm für die Aktualisierung über die Befehlszeile:

   ```
   configupdate.sh
   ```

3. Geben Sie die Werte aus Kapitel 11.6, „Konfigurieren der Einstellungen für die Identitätsanwendungen“, auf Seite 143 an.

29.4 Migrieren der Identity Manager-Engine auf einen neuen Server

Wenn Sie die Identity Manager-Engine auf einen neuen Server migrieren, können Sie die eDirectory-Reproduktionen beibehalten, die derzeit auf dem bisherigen Identity Manager-Server verwendet werden.

1. Installieren Sie eine unterstützte Version von eDirectory auf dem neuen Server.
2. Kopieren Sie die eDirectory-Reproduktionen, die sich auf dem aktuellen Identity Manager-Server befinden, auf den neuen Server.

   Weitere Informationen finden Sie unter „Administering Replicas“ (Verwalten von Reproduktionen) im *NetIQ eDirectory Administration Guide* (NetIQ eDirectory-Verwaltungshandbuch).
3. Installieren Sie die Identity Manager-Engine auf dem neuen Server.

   Weitere Informationen finden Sie in Kapitel 9, „Installieren der Identity Manager-Engine, der Identitätsanwendungen und von Identity Reporting“, auf Seite 91.

29.5 Migrieren des Benutzeranwendungstreibers

Beim Aufrüsten auf eine neue Version von 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 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.

29.5.1 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**.

29.5.2 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**.

29.5.3 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 *NetIQ Identity Manager – Administratorhandbuch zur Entwicklung der Identitätsanwendungen*. 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.

29.6 Aufrüsten der Identitätsanwendungen

Wenn Sie das Aufrüstungsprogramm für die Identitätsanwendungen 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**.
- (Bedingt) Wenn die vorhandene Datenbank unter Oracle ausgeführt wird und Sie das Installationsprogramm anweisen, eine SQL-Datei zum Aktualisieren des Schemas zu schreiben, fallen zusätzliche Schritte an. Weitere Informationen finden Sie in Abschnitt 29.7.1, „Vorbereiten einer Oracle-Datenbank für die SQL-Datei“, auf Seite 299.
- 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.
- Geben Sie für die Sortierung der Datenbank an, dass nach Groß-/Kleinschreibung unterschieden werden soll. Die Sortierung ohne Berücksichtigung der Groß-/Kleinschreibung wird nicht unterstützt. Wenn Sie die Sortierung ohne Berücksichtigung der Groß-/Kleinschreibung verwenden, treten bei der Migration möglicherweise Fehler durch doppelte Schlüssel auf. Wenn ein Fehler durch doppelte Schlüssel auftritt, müssen Sie die Sortierung überprüfen und korrigieren. Installieren Sie anschließend die Identitätsanwendungen erneut.
- Informieren Sie sich über die Unterschiede der Anbieter für die Passwortverwaltung. Der standardmäßige Anbieter ist SSPR. Soll der bisherige Identity Manager-Anbieter oder ein externer Anbieter verwendet werden, müssen Sie die Konfiguration der Identitätsanwendungen nach dem Aufrüsten aktualisieren.

Weitere Informationen zum Aufrüsten der Identitätsanwendungen finden Sie in Abschnitt 26.5, „Aufrüsten der Identitätsanwendungen“, auf Seite 268.

29.7 Abschließen der Migration der Identitätsanwendungen

Nach dem Aufrüsten oder Migrieren der Identitätsanwendungen schließen Sie den Migrationsvorgang ab.

29.7.1 Vorbereiten einer Oracle-Datenbank für die SQL-Datei

Während des Installationsvorgangs haben Sie ggf. angegeben, dass eine SQL-Datei zum Aktualisieren der Datenbank der Identitätsanwendungen 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:

```
/opt/novell/idm/jre/bin/java -Xms256m -Xmx256m  -Dwar.context.name=IDMProv
-jar /opt/novell/idm/liquibase.jar
--databaseClass=com.novell.soa.persist.liquibase.OracleUnicodeDatabase
--driver=oracle.jdbc.driver.OracleDriver
--classpath=/root/ojdbc8.jar:/opt/novell/idm/tomcat/server/IDMProv/deploy/
IDMProv.war
--changeLogFile=DatabaseChangeLog.xml
--url="jdbcURL" --logLevel=debug
--logFile=/opt/novell/idm/db.out --contexts="prov,updatedb" --username=xxxx
--password=xxxx updateSQL  > /opt/novell/idm/db.sql
```

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.

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

29.7.2 Leeren des Browsercache

Bevor Sie sich bei den Identitätsanwendungen anmelden, leeren Sie den Cache des Browsers. Wenn Sie den Cache nicht leeren, können einige Laufzeitfehler auftreten.

29.7.3 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**.

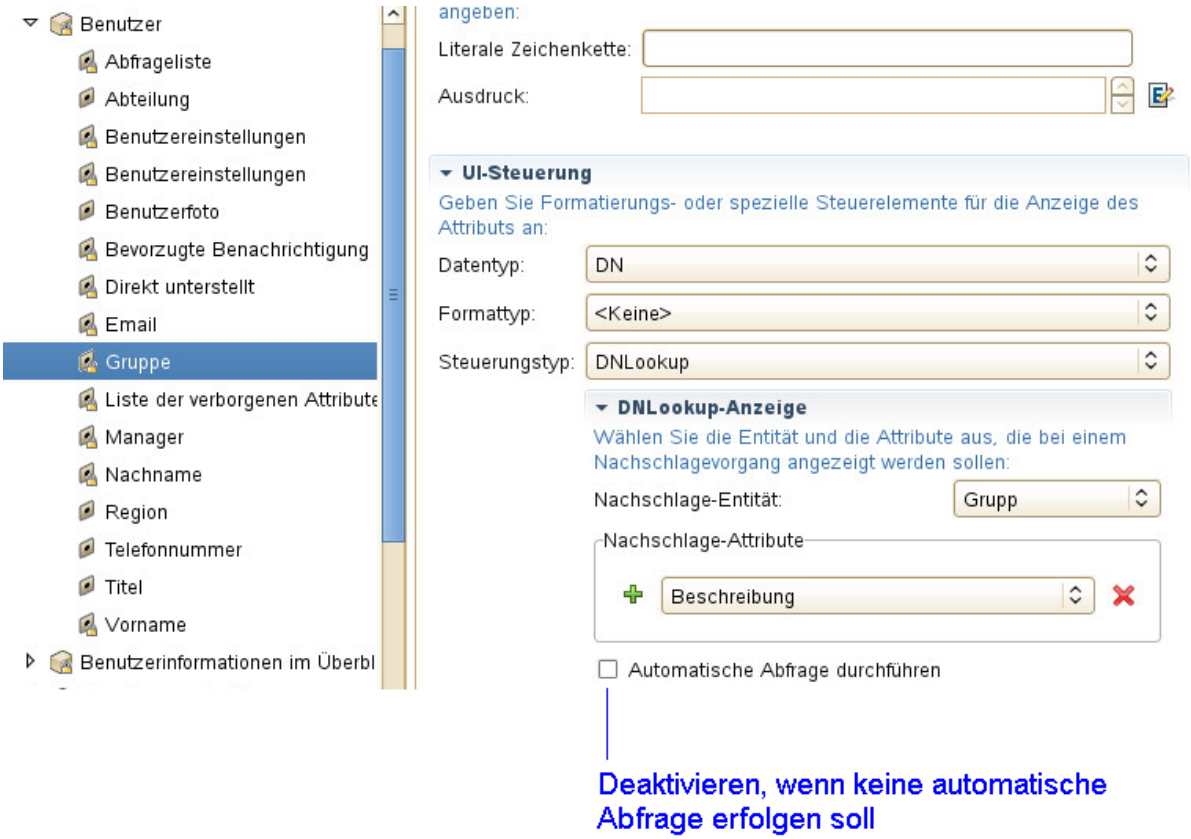
6 Die Einstellung **Maximale Zeitüberschreitung** muss 0 lauten.

7 Klicken Sie auf **Einstellungen speichern**.

29.7.4 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**:



29.8 Migrieren von Identity Reporting

Beim Migrieren von einer früheren Version von Identity Manager muss auch Identity Reporting migriert werden. Beachten Sie die folgenden Überlegungen:

- Migrieren Sie die Ereignisrevisionsdienst-Daten manuell zur PostgreSQL-Datenbank.
- Bereinigen Sie die vorhandene Berichterstellungsinstallation.

- Führen Sie eine Neuinstallation von Identity Reporting 4.7 auf dem neuen Server durch.
- Geben Sie den Installationsort des vorhandenen Authentifizierungsdiensts und Identitätsdepots für die soeben installierte Identity Reporting-Version an.

29.8.1 Migrieren des Ereignisrevisionsdiensts in Sentinel for Log Management für IGA

In diesem Abschnitt finden Sie Informationen zum Migrieren der SIEM-Daten aus der EAS-Datenbank zu einer unterstützten PostgreSQL-Datenbank.

Sie müssen die erforderlichen Rollen und Tablespaces erstellen, damit keine Fehler bei der Migration auftreten.

Vorbereiten der neuen PostgreSQL-Datenbank

1. Halten Sie EAS an, damit keine Ereignisse an den EAS-Server gesendet werden.
2. Halten Sie den DCS-Treiber mit iManager an:
   - **2a** Melden Sie sich bei iManager an.
   - **2b** Halten Sie den DCS-Treiber an.
   - **2c** Stellen Sie die Startoption in den Treibereigenschaften auf **Manuell** ein.

     Dieser Schritt sorgt dafür, dass der Treiber nicht automatisch gestartet wird.
3. Erstellen Sie die erforderlichen Rollen, die Tablespaces und die Datenbank mit den nachfolgenden SQL-Befehlen mithilfe von `PGAdmin`.

   Dieser Schritt sorgt dafür, dass bei der Migration keine Fehler auftreten.

   - **3a** Erstellen Sie die erforderlichen Rollen mit den folgenden Befehlen:

```
CREATE ROLE esec_app
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE esec_user
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE admin LOGIN
  ENCRYPTED PASSWORD '<specify the password for admin>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO admin;

CREATE ROLE appuser LOGIN
  ENCRYPTED PASSWORD '<specify the password for appuser>'
  NOSUPERUSER INHERIT NOCREATEDB CREATEROLE;
GRANT esec_app TO appuser;

CREATE ROLE dbauser LOGIN
  ENCRYPTED PASSWORD '<specify the password for dbauser>'
  SUPERUSER INHERIT CREATEDB CREATEROLE;
```

```
CREATE ROLE idmrptsrv LOGIN
  ENCRYPTED PASSWORD '<specify the password for idmrptsrv>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO idmrptsrv;

CREATE ROLE idmrptuser LOGIN
  ENCRYPTED PASSWORD '<specify the password for idmrptuser>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE rptuser LOGIN
  ENCRYPTED PASSWORD '<specify the password for rptuser>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO rptuser;
```

3b Erstellen Sie die Tablespaces mit den folgenden Befehlen:

```
 CREATE TABLESPACE sendata1
  OWNER dbauser
  LOCATION '<provide the location where table space has to be created>';
```

Beispiel:

```
CREATE TABLESPACE sendata1
  OWNER dbauser
  LOCATION '</opt/netiq/idm/apps/postgres/data>';
```

3c Erstellen Sie eine SIEM-Datenbank mit dem folgenden Befehl:

```
CREATE DATABASE "SIEM"
  WITH OWNER = dbauser
       ENCODING = 'UTF8'
       TABLESPACE = sendata1
       CONNECTION LIMIT = -1;
```

Exportieren der Daten aus EAS

1. Halten Sie EAS an, damit keine Ereignisse an den EAS-Server gesendet werden.
2. Halten Sie den DCS-Treiber mit iManager an:
   - **2a** Melden Sie sich bei iManager an.
   - **2b** Halten Sie den DCS-Treiber an.
   - **2c** Stellen Sie die Startoption in den Treibereigenschaften auf **Manuell** ein.

     Dieser Schritt sorgt dafür, dass der Treiber nicht automatisch gestartet wird.
3. Exportieren Sie die Daten aus der EAS-Datenbank in eine Datei:
   - **3a** Melden Sie sich beim EAS-Benutzerkonto an:

     ```
     # su - novleas
     ```
   - **3b** Geben Sie einen Speicherort an, auf den der EAS-Benutzer uneingeschränkt zugreifen kann, beispielsweise `/home/novleas`.
   - **3c** Navigieren Sie zum PostgreSQL-Installationsverzeichnis und führen Sie die folgenden Befehle aus:

     Beispiel:

     ```
     export PATH=/opt/novell/sentinel_eas/3rdparty/postgresql/bin/:$PATH
     ```

     ```
     export LD_LIBRARY_PATH=/opt/novell/sentinel_eas/3rdparty/postgresql/lib/
     :$LD_LIBRARY_PATH
     ```

3d Exportieren Sie die Daten mit dem folgenden Befehl in eine `.sql`-Datei:

```
./pg_dump -p <Portnummer> -U <Benutzername> -d <Datenbankname> -f
<Exportspeicherort>
```

Beispiel:

```
./pg_dump -p 15432 -U dbauser SIEM -f /home/novleas/SIEM.sql
```

Importieren der Daten in die neue PostgreSQL-Datenbank

1. Halten Sie EAS an, damit keine Ereignisse an den EAS-Server gesendet werden.
2. Halten Sie den DCS-Treiber mit iManager an:
   - **2a** Melden Sie sich bei iManager an.
   - **2b** Halten Sie den DCS-Treiber an.
   - **2c** Stellen Sie die Startoption in den Treibereigenschaften auf **Manuell** ein.

     Dieser Schritt sorgt dafür, dass der Treiber nicht automatisch gestartet wird.
3. Importieren Sie die Daten in die neue PostgreSQL-Datenbank:
   - **3a** (Bedingt) Erstellen Sie einen `postgres`-Benutzer.

     Dies gilt lediglich für Windows. Unter Linux wird automatisch ein Benutzer erstellt.
   - **3b** Kopieren Sie die in Schritt 3d exportierte Datei in einen Speicherort, auf den der Postgres-Benutzer uneingeschränkt zugreifen kann. Beispiel: `/opt/netiq/idm/postgres`
   - **3c** Importieren Sie die Daten mit dem folgenden Befehl in die PostgreSQL-Datenbank.

     ```
     psql -d <Datenbankname> -U <Benutzername> -f <vollständiger Pfad der
     exportierten Datei>
     ```

     Beispiel:

     ```
     psql -d SIEM -U postgres -f /opt/netiq/idm/apps/postgres/SIEM.sql
     ```
4. Prüfen Sie, ob im Migrationsprotokoll Fehler vorhanden sind, und beheben Sie diese.

HINWEIS: Für die Identity Manager 4.7-Berichte werden keine Revisionsdaten verwendet, die aus EAS in SLM für IGA migriert werden. Stattdessen werden für diese Berichte die Revisionsdaten verwendet, die direkt von SLM für IGA synchronisiert werden.

29.8.2 Einrichten des neuen Berichterstellungsservers

Nach dem Importieren der EAS-Daten in die neue PostgreSQL-Datenbank installieren Sie eine neue Reporting-Anwendung auf einem anderen Server und verweisen Sie auf das Identitätsdepot und den vorhandenen Authentifizierungsdienst.

1. Halten Sie den vorhandenen Tomcat-Dienst an (also die Ausführung der vorhandenen Reporting-Anwendung).
2. Erstellen Sie eine Sicherung der vorhandenen Identity Reporting-WAR-Dateien im Verzeichnis `tomcat/webapps` und des `Reporting`-Basisverzeichnisses im Verzeichnis `/opt/netiq/idm/apps/` außerhalb des `Tomcat`-Installationspfads.
3. Entfernen Sie die EAS-Einträge aus der vorhandenen Datei `server.xml`.
4. Erstellen Sie eine neue Datenbank in derselben PostgreSQL-Datenbank, in die die EAS-Daten migriert werden.

5 Installieren und konfigurieren Sie Identity Reporting auf dem neuen Server und verweisen Sie auf den vorhandenen Single-Sign-On-Dienst und das vorhandene Identitätsdepot. Weitere Informationen finden Sie unter Kapitel 10, „Konfigurieren der installierten Komponenten“, auf Seite 101.

6 Zum Verweisen des vorhandenen Single-Sign-On-Diensts auf die soeben installierte Identity Reporting-Version bearbeiten Sie die Identity Reporting-Konfigurationseinträge mit dem Konfigurationsaktualisierungsprogramm.

7 Starten Sie den Tomcat-Server neu, auf dem der vorhandene Single-Sign-On-Dienst ausgeführt wird.

29.8.3 Erstellen der Datensynchronisierungsrichtlinie

Nach der Konfiguration des Berichterstellungsservers müssen Sie die Datensynchronisierungsrichtlinie erstellen, mit der Ereignisse von SLM für IGA an die Berichterstellungsdatenbank weitergeleitet werden. Beim Aufrüsten auf Identity Reporting 4.7 gelten die nachfolgenden Überlegungen.

HINWEIS

- Wenn Sie von Identity Reporting 4.5.6 auf Identity Reporting 4.7 aufrüsten, müssen Sie eine neue Richtlinie auf der Seite der Identity Manager-Datenerfassungsdienste erstellen. Weitere Informationen finden Sie unter About the Data Sync Policies tab (Informationen zur Registerkarte „Datensynchronisierungsrichtlinie“) im Administrator Guide to NetIQ Identity Reporting (Administratorhandbuch für die NetIQ-Identitätsberichterstellung).
- Wenn·Sie·von·Identity·Reporting¬4.6.x·auf·Identity·Reporting¬4.7·aufrüsten,·beachten·Sie·die·Anweisungen·unter·Probleme beim Aufrüsten von Identity Manager in den Versionshinweisen zu NetIQ Identity Manager 4.7.

---

30 Deinstallieren der Identity Manager-Komponenten

In diesem Abschnitt wird die Deinstallation der 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 Identity Manager-Komponenten müssen Sie alle Dienste anhalten, beispielsweise Tomcat, PostgreSQL und ActiveMQ.

30.1 Entfernen von Objekten aus dem Identitätsdepot

Im ersten Schritt der Deinstallation von Identity Manager müssen alle 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“ (Funktionsfähigkeit von eDirectory aufrechterhalten) im *NetIQ eDirectory -Administrationshandbuch*.

2. Melden Sie sich bei iManager als Administrator mit vollständigen Berechtigungen für den eDirectory-Baum an.
3. Wählen Sie für Partitionen und Reproduktionen die Option zum Zusammenführen von Partitionen aus.
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.

30.2 Deinstallieren der Identity Manager-Engine

Das Installationsprogramm umfasst ein Deinstallationsskript für Identity Manager. Mithilfe dieses Skripts können Sie alle Dienste, Pakete und Verzeichnisse entfernen, die während der Installation erstellt wurden.

HINWEIS: Bevor Sie die Identity Manager-Engine deinstallieren können, muss zunächst das Identitätsdepot entsprechend vorbereitet werden. Weitere Informationen finden Sie in Abschnitt 30.1, „Entfernen von Objekten aus dem Identitätsdepot“, auf Seite 307.

So deinstallieren Sie die Identity Manager-Engine:

1. Navigieren Sie zu dem Speicherort, an dem Sie die .iso-Datei zur Installation eingehängt haben.
2. Führen Sie im Stammverzeichnis der `.iso`-Datei den folgenden Befehl aus:

   ```
   ./uninstall.sh
   ```

3. Geben Sie die zu deinstallierenden Komponenten an.

   Mit *1* wird beispielsweise die Identity Manager-Engine deinstalliert. Sie können auch mehrere Komponenten gleichzeitig deinstallieren. Mit *1, 2, 3* werden beispielsweise die Identity Manager-Engine, der Remote Loader sowie der Fan-out-Agent deinstalliert.

30.3 Deinstallieren der Identitätsanwendungen

1. Navigieren Sie zu dem Speicherort, an dem Sie die `.iso`-Datei zur Installation eingehängt haben.
2. Führen Sie im Stammverzeichnis der `.iso`-Datei den folgenden Befehl aus:

   ```
   ./uninstall.sh
   ```

3. Geben Sie die zu deinstallierenden Komponenten an.

   Mit *1* werden beispielsweise die Identitätsanwendungen deinstalliert.

30.4 Deinstallieren der Identity Reporting-Komponenten

Die Komponenten der Identitätsberichterstellung müssen in der nachstehenden Reihenfolge deinstalliert werden:

1. Löschen Sie die Treiber. Weitere Informationen finden Sie in Abschnitt 30.4.1, „Löschen der Berichterstellungstreiber“, auf Seite 309.
2. Löschen Sie die Identitätsberichterstellung. Weitere Informationen finden Sie in Abschnitt 30.4.2, „Deinstallieren der Identitätsberichterstellung“, auf Seite 309.
3. Löschen Sie Sentinel. Weitere Informationen finden Sie unter Abschnitt 30.4.3, „Deinstallieren von Sentinel“, auf Seite 309.

HINWEIS: Um Speicherplatz einzusparen, wird mit den Installationsprogrammen für die Identitätsberichterstellung 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.

30.4.1 Löschen der Berichterstellungstreiber

Sie können den DCS-Treiber und den MSGW-Treiber wahlweise in Designer oder iManager 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**.
   - **iManager:** 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**.
   - **iManager:** Klicken Sie auf der Seite „Treibersatz-Überblick“ auf **Treiber > Treiber löschen** und dann auf den zu löschenden Treiber.

30.4.2 Deinstallieren der Identitätsberichterstellung

Vor dem Löschen der Identitätsberichterstellung müssen zunächst der DCS-Treiber und der MSGW-Treiber gelöscht werden. Weitere Informationen finden Sie in Abschnitt 30.4.1, „Löschen der Berichterstellungstreiber“, auf Seite 309.

1. Navigieren Sie zu dem Speicherort, an dem Sie die `.iso`-Datei zur Installation eingehängt haben.
2. Führen Sie im Stammverzeichnis der `.iso`-Datei den folgenden Befehl aus:

   ```
   ./uninstall.sh
   ```
3. Geben Sie die zu deinstallierenden Komponenten an.

   Mit *1* wird beispielsweise Identity Reporting deinstalliert.

30.4.3 Deinstallieren von Sentinel

1. Melden Sie sich beim Sentinel-Server an.
2. Navigieren Sie zu dem Verzeichnis mit dem Deinstallationsskript:

   ```
   /opt/novell/sentinel/setup/
   ```
3. Führen Sie den folgenden Befehl aus:

   ```
   ./uninstall.sh
   ```
4. Wenn Sie aufgefordert werden, zu bestätigen, dass Sie mit der Deinstallation fortfahren möchten, drücken Sie `j`.

   Das Skript stoppt den Service zunächst und entfernt ihn dann vollständig.

30.5 Deinstallation von Designer

1. Schließen Sie Designer.
2. Deinstallieren Sie Designer.

   Navigieren Sie zum Verzeichnis, in dem sich das Deinstallationsskript befindet (standardmäßig `<Installationsverzeichnis>/designer/UninstallDesigner/Uninstall Designer for Identity Manager`).

   Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./uninstall`

30.6 Deinstallation von Analyzer

1. Schließen Sie Analyzer.
2. Deinstallieren Sie Analyzer mit dem entsprechenden Verfahren für Ihr Betriebssystem:

   Navigieren Sie zum Skript `Uninstall Analyzer for Identity Manager` (standardmäßig im Verzeichnis `<Installationsverzeichnis>/analyzer/UninstallAnalyzer`).

   Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./Deinstallieren`

31 Fehlersuche

In diesem Abschnitt finden Sie nützliche Hinweise für die Fehlersuche, wenn Probleme beim Installieren von Identity Manager auftreten. Weitere Informationen zur Fehlersuche für Identity Manager finden Sie im Handbuch der entsprechenden Komponente.

31.1 Fehlersuche bei der Installation der Benutzeranwendung und des RBPMs

Die nachfolgende Tabelle enthält die möglichen Probleme und Vorschläge für Gegenmaßnahmen. Falls das Problem weiterhin auftritt, wenden Sie sich an Ihren zuständigen NetIQ-Ansprechpartner.

Problem	Empfohlene Vorgehensweise
Wenn Sie die CEF-Revision für OSP über das configupdate-Dienstprogramm (`configupdate.sh`) aktivieren, schlagen die Anmeldeversuche bei IDMRPT fehl.	Als Behelfslösung führen Sie die folgenden Schritte aus: 1. Navigieren Sie zu den Dateien `ism-configuration.properties` und `idmrptcore_logging.xml` im Verzeichnis `/opt/netiq/idm/apps/tomcat/conf`. 2. Bearbeiten Sie die Dateien `ism-configuration.properties` und `idmrptcore_logging.xml`. 3. Ersetzen Sie den Wert **tcp** für **com.netiq.ism.audit.cef.protocol** und **<Protokoll>** in den Dateien `ism-configuration.properties` und `idmrptcore_logging.xml` durch **TCP**. 4. Starten Sie Tomcat neu.
Wenn die Identitätsanwendungen und Identity Reporting auf demselben Server installiert sind und Sie für das Erstellen der Datenbank die Option **Start** wählen, enthält das Protokoll einige Ausnahmen.	Zum Löschen der Ausnahmen starten Sie Tomcat manuell neu.
Sie möchten eine oder mehrere Konfigurationseinstellungen für die Benutzeranwendung ändern, die Sie während der Installation vorgenommen haben: ◆ Identitätsdepot-Verbindungen und -Zertifikate ◆ Email-Einstellungen ◆ Benutzeridentität und Benutzergruppen in der Identity Manager-Engine ◆ Access Manager- oder iChain-Einstellungen	Das Dienstprogramm für die Konfiguration kann unabhängig vom Installationsprogramm ausgeführt werden. **Linux:** Führen Sie im Installationsverzeichnis (standardmäßig `/opt/netiq/idm/apps/configupdate/`) den folgenden Befehl aus: `./configupdate.sh`

Problem	Empfohlene Vorgehensweise
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 der Benutzeranwendung angegeben wurde.
Die Anmeldung bei der Portaladministratorseite ist nicht möglich.	Überprüfen Sie, ob ein Konto für den Benutzeranwendungsadministrator vorhanden ist. Dieses Konto ist nicht mit dem iManager-Administratorkonto identisch.
Auch mit einem Administratorkonto können keine neuen Benutzer angelegt werden.	Der Benutzeranwendungsadministrator muss ein Trustee des Containers der obersten Ebene sein und sollte über Supervisor-Rechte verfügen. Sie können versuchen, die Rechte des Administrators der Benutzeranwendung mit denen des LDAP-Administrators gleichzusetzen (in iManager).
Beim Starten des Anwendungsservers treten Keystore-Fehler auf.	Ihr Anwendungsserver verwendet nicht das bei der Installation der Benutzeranwendung 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).
Es werden keine Email-Benachrichtigungen gesendet.	Überprüfen Sie mit dem `configupdate`-Dienstprogramm, ob Sie Werte für die Benutzeranwendungs-Konfigurationsparameter **Email-Von** und **Email-Host** angegeben haben. **Linux:** Führen Sie im Installationsverzeichnis (standardmäßig `/opt/netiq/idm/apps/UserApplication/`) den folgenden Befehl aus: `./configupdate.sh`

31.2 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 NetIQ-Ansprechpartner.

Problem	Empfohlene Vorgehensweise
Der Benutzer kann sich in einer großen Umgebung (> 2 Millionen Objekte) nicht anmelden	Ergänzen Sie sowohl den 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 Identitätsanwendungen 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 Identitätsanwendungen werden keine Challenge-Response-Fragen angezeigt	1. Prüfen Sie, ob der SSPR-Server ein mit FQDN erstelltes Zertifikat enthält. 2. Melden Sie sich beim Benutzeranwendungsserver an und starten Sie das ConfigUpdate-Dienstprogramm (`/opt/netiq/idm/apps/configupdate/`). 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 Benutzeranwendungsserver unter `/opt/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 Benutzeranwendungsserver 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.
Fehler beim Starten des ConfigUpdate-Dienstprogramms aus einem anderen Verzeichnis heraus	Das ConfigUpdate-Dienstprogramm meldet Fehler. Änderungen werden nicht gespeichert. Wenn Sie beispielsweise das configupdate-Dienstprogramm mit dem Befehl `/opt/netiq/idm/apps/configupdate/configupdate.sh` starten, wird es nicht gestartet. Navigieren Sie stattdessen zum Verzeichnis `/opt/netiq/idm/apps/configupdate/` und führen Sie dann den Befehl `./configupdate.sh` aus.

31.3 Fehlersuche bei der Deinstallation

Die nachfolgende Tabelle enthält die möglichen Probleme und Vorschläge für Gegenmaßnahmen. Falls das Problem weiterhin auftritt, wenden Sie sich an Ihren zuständigen NetIQ-Ansprechpartner.

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.

A Arbeiten mit mehreren Identitätsdepot-Instanzen

In diesem Abschnitt finden Sie die Voraussetzungen, die Überlegungen und die notwendige Systemeinrichtung für die Installation des Identitätsdepots. Informieren Sie sich zunächst anhand der Checkliste über den Installationsvorgang.

A.1 Erläuterungen zu Identity Manager-Objekten in eDirectory

Die folgende Liste enthält die wesentlichen Identity Manager-Objekte, die in eDirectory gespeichert sind, und deren Verhalten zueinander. Während der Installation werden keine Projekte erstellt. Stattdessen legen Sie die Identity Manager-Objekte an, wenn Sie die Identity Manager-Lösung konfigurieren.

- **Treibersatz:** Ein Treibersatz ist ein Container, der Identity Manager-Treiber und Bibliotheksobjekte enthält. Auf einem Server kann immer nur ein Treibersatz aktiv sein. Sie können einen Treibersatz jedoch mit mehreren Servern verknüpfen. Ein Treiber kann auch mehreren Servern gleichzeitig zugeordnet werden. Er sollte jedoch immer nur auf einem Server gleichzeitig ausgeführt werden. Auf den anderen Servern muss der Treiber deaktiviert sein. Auf jedem mit einem Treibersatz verknüpften Server muss der Identity Manager-Server installiert sein.
- **Bibliothek:** Das Bibliotheksobjekt ist ein Repository mit häufig verwendeten Richtlinien, das von mehreren Positionen aus referenziert werden kann. Die Bibliothek wird im Treibersatz gespeichert. Sie können eine Richtlinie in die Bibliothek stellen, damit jeder Treiber im Treibersatz auf sie verwiesen werden kann.
- **Treiber:** Ein Treiber stellt die Verbindung zwischen einer Anwendung und dem Identitätsdepot her. Er ermöglicht darüber hinaus die Datensynchronisierung und Datenfreigabe zwischen Systemen. Der Treiber wird im Treibersatz abgelegt.
- **Auftrag:** Ein Auftrag automatisiert eine wiederkehrende Aufgabe. Ein Auftrag kann beispielsweise ein System konfigurieren, um ein Konto an einem bestimmten Tag zu deaktivieren oder um einen Workflow zu starten, mit dem eine Erweiterung der Zugriffsrechte einer Person auf eine Unternehmensressource angefordert wird. Der Auftrag wird im Treibersatz abgelegt.

A.2 Reproduktion der von Identity Manager auf dem Server benötigten Objekte

Wenn in Ihrer Identity Manager-Umgebung mehrere Server benötigt werden, damit mehrere Identity Manager-Treiber ausgeführt werden können, sollten Sie dies in Ihrem Plan berücksichtigen und sicherstellen, dass bestimmte eDirectory-Objekte auf Servern reproduziert werden, auf denen die Identity Manager-Treiber ausgeführt werden sollen.

Sie können gefilterte Reproduktionen verwenden, sofern alle Objekte und Attribute, die der Treiber lesen oder synchronisieren muss, Teil der gefilterten Reproduktion sind.

Denken Sie daran, dem Identity Manager-Treiberobjekt ausreichende eDirectory-Rechte für die zu synchronisierenden Objekte zu erteilen. Gewähren Sie diese Rechte entweder explizit oder definieren Sie das Treiberobjekt als sicherheitsäquivalent mit einem Objekt, das über die gewünschten Rechte verfügt.

Ein eDirectory-Server, auf dem ein Identity Manager-Treiber ausgeführt wird (oder auf den der Treiber verweist, falls Sie den Remote Loader verwenden), muss eine Masterreproduktion oder eine Lese-/Schreibreproduktion der folgenden Elemente enthalten:

- Das Treibersatzobjekt für den Server.

  Für jeden Server, auf dem Identity Manager läuft, muss ein Treibersatzobjekt vorhanden sein. Sofern Sie keine speziellen Anforderungen haben, ordnen Sie nicht mehrere Server demselben Treibersatzobjekt zu.

  HINWEIS: Beim Erstellen eines Treibersatzobjekts wird standardmäßig eine separate Partition erstellt. NetIQ empfiehlt, für das Treibersatzobjekt eine separate Partition zu erstellen. Damit Identity Manager funktioniert, muss der Server eine vollständige Reproduktion des Treibersatzobjekts enthalten. Wenn dem Server eine vollständige Reproduktion des Speicherorts zur Verfügung steht, an dem das Treibersatzobjekt installiert ist, wird keine Partition benötigt.

- Das Serverobjekt für den Treiber.

  Das Serverobjekt wird benötigt, damit der Treiber Schlüsselpaare für Objekte erstellen kann. Außerdem ist es wichtig für die Authentifizierung des Remote Loaders.

- Die Objekte, die diese Instanz des Treibers synchronisieren soll.

  Der Treiber kann nur Objekte synchronisieren, sofern sich eine Reproduktion dieser Objekte auf demselben Server befindet wie der Treiber. Der Identity Manager-Treiber synchronisiert die Objekte in *allen* Containern, die auf dem betreffenden Server reproduziert sind, sofern Sie keine anderen Regeln für die Bereichsfilterung festgelegt haben.

  Wenn ein Treiber beispielsweise alle Benutzerobjekte synchronisieren soll, geschieht dies am einfachsten durch die Instanz eines Treibers auf dem Server, auf dem sich eine Lese-/Schreibreproduktion aller Benutzer befindet.

  In vielen Umgebungen gibt es jedoch keinen Einzelserver, der eine Reproduktion aller Benutzer enthält. Stattdessen sind die Benutzer-Datensätze auf mehrere Server verteilt. In diesem Fall stehen Ihnen drei Möglichkeiten zur Auswahl:

  - **Kumulierung aller Benutzer auf einem Server.** Sie können einen Server erstellen, der alle Benutzer enthält, indem Sie zu einem vorhandenen Server Reproduktionen hinzufügen. Sofern erforderlich können gefilterte Reproduktionen verwendet werden, was die Größe der eDirectory-Datenbank verringert. Die erforderlichen Benutzerobjekte und -attribute müssen jedoch Teil der gefilterten Reproduktion sein.

- **Verwendung mehrerer Instanzen des Treibers auf mehreren Servern mit Bereichsfilterung.** Wenn Sie die Benutzer nicht auf einem Server kumulieren möchten, müssen Sie festlegen, welche Server alle Benutzer enthalten, und anschließend auf jedem dieser Treiber eine Instanz des Identity Manager-Treibers einrichten.

  Damit keine separaten Instanzen eines Treibers versuchen, dieselben Benutzer zu synchronisieren, müssen Sie in der Bereichsfilterung definieren, welche Benutzer von den einzelnen Instanzen des Treibers synchronisiert werden sollen. Mithilfe der Bereichsfilterung können Sie jedem Treiber Regeln hinzufügen, damit die Aktionen des Treibers auf bestimmte Container beschränkt werden. Siehe „Verwendung der Bereichsfilterung zum Verwalten von Benutzern auf verschiedenen Servern“, auf Seite 319.

- **Verwendung mehrerer Instanzen des Treibers auf mehreren Servern ohne Bereichsfilterung.** Wenn mehrere Instanzen eines Treibers auf mehreren Servern ohne die Verwendung gefilterter Reproduktionen laufen sollen, müssen Sie für die verschiedenen Treiberinstanzen Richtlinien definieren, auf deren Basis der Treiber im selben Identitätsdepot unterschiedliche Objektsätze verarbeiten kann.

- Die Schablonenobjekte, die vom Treiber bei der Erstellung von Benutzern verwendet werden sollen, sofern die Verwendung von Schablonen ausgewählt ist.

  Identity Manager-Treiber erfordern nicht, dass eDirectory-Schablonenobjekte für die Benutzererstellung festgelegt werden. Wenn Sie jedoch festlegen, dass ein Treiber eine Schablone für die Erstellung von Benutzern in eDirectory verwenden soll, muss das Schablonenobjekt auf dem Server reproduziert werden, auf dem der Treiber läuft.

- Alle Container, die der Identity Manager-Treiber zur Benutzerverwaltung verwenden soll.

  Wenn Sie beispielweise einen Container namens „Inaktive Benutzer“ erstellt haben, der deaktivierte Benutzerkonten enthält, benötigen Sie eine Master- oder eine Lese-/Schreibreproduktion (vorzugsweise eine Masterreproduktion) für diesen Container auf dem Server, auf dem der Treiber läuft.

- Alle anderen Objekte, auf die sich der Treiber beziehen muss (z. B. Auftragsobjekte für den Treiber).

  Wenn die anderen Objekte vom Treiber nur gelesen und nicht geändert werden müssen, ist für diese Objekte auf dem Server eine Lesereproduktion ausreichend.

A.3 Verwendung der Bereichsfilterung zum Verwalten von Benutzern auf verschiedenen Servern

Mithilfe der Bereichsfilterung können Sie jedem Treiber Regeln hinzufügen, wodurch die Aktionen des Treibers auf bestimmte Container beschränkt werden. Die Bereichsfilterung sollte beispielsweise in den folgenden Situationen verwendet werden:

- Der Treiber soll nur die Benutzer in einem bestimmten Container synchronisieren.

  In der Standardeinstellung synchronisiert der Identity Manager-Treiber die Objekte in allen Containern, die auf dem Server reproduziert sind, auf denen er läuft. Sie können diesen Bereich einschränken, indem Sie Regeln für die Bereichsfilterung erstellen.

- Ein Identity Manager-Treiber soll alle Benutzer synchronisieren, aber Sie möchten nicht, dass alle Benutzer auf demselben Server reproduziert werden.

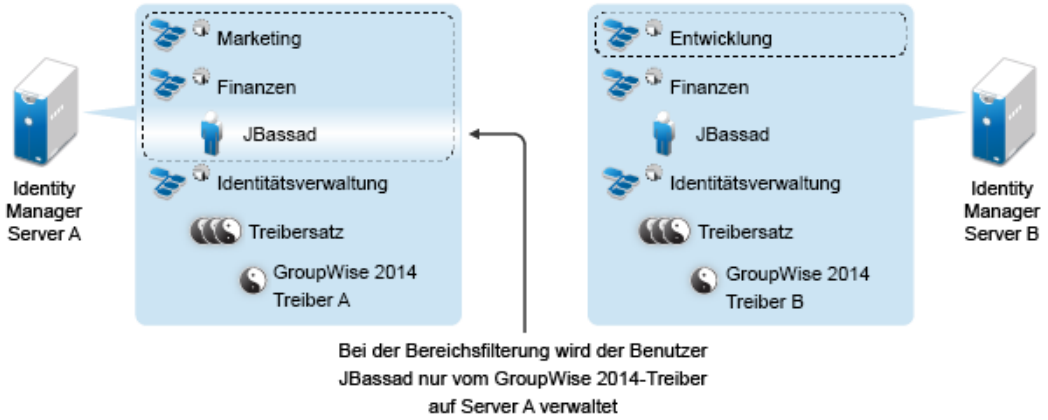
  Zur Synchronisierung von Benutzern, die nicht auf einem einzelnen Server reproduziert sind, müssen Sie die Server festlegen, die alle Benutzer enthalten. Anschließend müssen Sie auf jedem dieser Server eine Instanz des Identity Manager-Treibers erstellen. Damit nicht zwei

Instanzen eines Treibers versuchen, dieselben Benutzer zu synchronisieren, müssen Sie in der Bereichsfilterung definieren, welche Benutzer von den einzelnen Instanzen des Treibers synchronisiert werden sollen.

HINWEIS: Sie sollten die Bereichsfilterung auch dann verwenden, wenn sich die Reproduktionen der Server gegenwärtig nicht überschneiden. Es könnte sein, dass zu einem späteren Zeitpunkt Reproduktionen auf die Server übertragen werden, sodass eine unbeabsichtigte Überschneidung entsteht. Bei Verwendung der Bereichsfilterung versuchen die Identity Manager-Treiber nicht, dieselben Benutzer zu synchronisieren, selbst wenn zu einem späteren Zeitpunkt Reproduktionen auf die Server übertragen werden.

Abbildung A-1 auf Seite 320 zeigt ein Beispiel für ein Identitätsdepot mit drei Containern, in denen folgende Benutzer gespeichert sind: „Marketing“, „Finanzen“ und „Entwicklung“. Sie zeigt auch einen Identitätsmanagement-Container, in dem die Treibersätze gespeichert sind. Jeder dieser Container ist eine separate Partition. In diesem Beispiel verfügt der Identity Manager-Administrator über zwei Identitätsdepot-Server, Server A und Server B. Auf keinem der Server befindet sich eine Kopie aller Benutzer. Jeder Server enthält zwei der drei Partitionen, sodass sich die auf den Servern gespeicherten Bereiche überschneiden.

Abbildung A-1 *Die Bereichsfilterung definiert, welche Treiber die einzelnen Container synchronisieren*



Der Administrator möchte, dass alle Benutzer im Baum vom GroupWise 2014-Treiber synchronisiert werden, aber es sollen keine Reproduktionen der Benutzer auf einem einzelnen Server zusammengefasst werden. Stattdessen verwendet er zwei Instanzen des GroupWise 2014-Treibers, von denen sich eine auf Server A und die andere auf Server B befindet. Er installiert Identity Manager und richtet auf beiden Identity Manager-Servern den GroupWise 2014-Treiber ein.

Server A enthält Reproduktionen der Container „Marketing“ und „Finanzen“. Außerdem befindet sich auf dem Server eine Reproduktion des Identity Management-Containers, der den Treibersatz für Server A und das GroupWise 2014-Treiberobjekt für Server A enthält.

Auf Server B befinden sich Reproduktionen der Container "Entwicklung" und "Finanzen" sowie der Identity Manager-Container, in dem sich der Treibersatz für Server B und das GroupWise 2014-Treiberobjekt für Server B befinden.

Da sich sowohl auf Server A als auch auf Server B eine Reproduktion des Containers „Finanzen“ befindet, ist auf beiden Servern der Benutzer „JBassad“ gespeichert, der sich im Container „Finanzen“ befindet. Ohne Bereichsfilterung nimmt sowohl GroupWise 2014-Treiber A als auch

GroupWise 2014-Treiber B die Synchronisierung von "JBassad" vor. Durch die Bereichsfilterung wird verhindert, dass beide Instanzen des Treibers denselben Benutzer verwalten, weil definiert wird, welche Treiber die einzelnen Container synchronisieren.

In Identity Manager sind vordefinierte Regeln enthalten. Für die Bereichsfilterung stehen zwei Regeln bereit: **Ereignistransformation – Bereichsfilterung – Teilbäume einbeziehen** und **Ereignistransformation – Bereichsfilterung – Teilbäume ausschließen**. Weitere Informationen finden Sie im *NetIQ Identity Manager Understanding Policies Guide* (Handbuch über Richtlinien in NetIQ Identity Manager).

Für dieses Beispiel sollte die vordefinierte Regel „Teilbäume einbeziehen“ für Server A und Server B verwendet werden. Der Bereich muss für jeden Treiber unterschiedlich definiert sein, sodass sie nur die Benutzer in den angegebenen Containern synchronisieren. Server A würde die Container „Marketing“ und „Finanzen“ synchronisieren und Server B den Container „Entwicklung“.

A.4 Erläuterungen zu den Linux-Paketen im Installations-Kit des Identitätsdepots

NetIQ eDirectory enthält ein Linux-Paketsystem mit einer Sammlung aus Werkzeugen, mit denen die Installation und die Deinstallation verschiedener eDirectory-Komponenten vereinfacht wird. Die Pakete enthalten Dateien (`makefiles`), die die Anforderungen für das Erstellen einer bestimmten Komponente von eDirectory enthalten. Die Pakete enthalten außerdem Konfigurationsdateien, Dienstprogramme, Bibliotheken, Daemon-Programme und man-Seiten, die die mit dem Betriebssystem installierten Linux-Standardwerkzeuge verwenden.

Bestimmte Pakete sind von anderen Paketen oder Identity Manager-Komponenten abhängig, beispielsweise NICI. Damit die Funktionsfähigkeit gewährleistet ist, müssen alle abhängigen Pakete installiert werden.

Die nachfolgende Tabelle liefert Informationen über die Linux-Pakete, die in eDirectory enthalten sind. Alle Pakete weisen das Präfix *novell-* auf. Beispiel: NDSserv ist nun `novell-NDSserv`.

Paket	Beschreibung
`NOVLice`	Enthält das NetIQ Import Convert Export-Programm. Dieses Paket ist abhängig von den Paketen `NOVLmgnt`, `NOVLxis` und `NLDAPbase`.
`NOVbase`	Stellt den Directory User Agent dar. Dieses Paket ist abhängig vom NICI-Paket. Dieses Paket enthält folgende Elemente: ◆ Beglaubigungswerkzeuge, die auch die für eDirectory benötigte RSA-Beglaubigung enthalten. ◆ Plattformunabhängige Systemabstraktions-Bibliothek, Bibliothek mit allen definierten Funktionen des Directory User Agent und Schemaerweiterungs-Bibliothek. ◆ Kombiniertes Konfigurations- und Testprogramm für Directory User Agent. ◆ Konfigurationsdatei und man-Seiten zu eDirectory.
`NDScommon`	Enthält die man-Seiten für die eDirectory-Konfigurationsdatei, Installations- und Deinstallationsprogramme. Dieses Paket ist abhängig vom NDSbase-Paket.

Paket	Beschreibung
NDSmasv	Enthält die erforderlichen Bibliotheken für die obligatorische Zugriffssteuerung (MASV).
NDSserv	Enthält alle Binärdateien und Bibliotheken, die vom eDirectory-Server benötigt werden. Enthält außerdem die Dienstprogramme zur Verwaltung des eDirectory-Servers auf dem System. Dieses Paket ist abhängig von den Paketen NDSbase, NDScommon, NDSmasv, NLDAPsdk, NOVLpkia und NOVLpkit. Enthält außerdem folgende Elemente: ◆ NDS-Installations-Bibliothek, FLAIM-Bibliothek, Verfolgungs-Bibliothek, NDS-Bibliothek, LDAP-Server-Bibliothek, LDAP-Installations-Bibliothek, Index-Editor-Bibliothek, DNS-Bibliothek, Zusammenführungs-Bibliothek und LDAP Erweiterungs-Bibliothek für LDAP SDK. ◆ eDirectory-Server-Daemon. ◆ Binärdatei für DNS und Binärdatei zum Laden und Entladen von LDAP. ◆ Dienstprogramm zum Erstellen der MAC-Adresse, Dienstprogramm zur Verfolgung des Servers und zur Änderung einiger der globalen Variablen des Servers, Dienstprogramm zum Sichern und Wiederherstellen von eDirectory und Dienstprogramm zum Zusammenführen von eDirectory-Bäumen. ◆ Start-Scripts für DNS, NDSD und NLDAP. ◆ Handbuchseiten.
NDSrepair	Enthält die Laufzeitbibliotheken und das Dienstprogramm zum Beheben von Problemen in der eDirectory-Datenbank. Dieses Paket ist abhängig vom NDSbase-Paket.
NLDAPbase	Enthält LDAP-Bibliotheken, Erweiterungen von LDAP-Bibliotheken und die folgenden LDAP-Werkzeuge: ◆ ldapdelete ◆ ldapmodify ◆ ldapmodrdn ◆ ldapsearch Dieses Paket ist abhängig vom NLDAPsdk-Paket.
NOVLnmas	Enthält alle NMAS-Bibliotheken und die erforderlichen nmasinst-Binärdateien für den NMAS-Server. Dieses Paket ist abhängig von den Paketen NICI und NDSmasv.
NLDAPsdk	Enthält NetIQ-Erweiterungen zu den LDAP-Laufzeit- und Sicherheitsbibliotheken (Client-NICI).
NOVLsubag	Enthält die Laufzeitbibliotheken und die Dienstprogramme für den eDirectory-SNMP-Subagenten. Dieses Paket ist abhängig von den Paketen NICI, NDSbase und NLDAPbase.
NOVLpkit	Enthält PKI-Dienste, für die eDirectory nicht benötigt wird. Dieses Paket ist abhängig von den Paketen NICI und NLDAPsdk.
NOVLpkis	Enthält den PKI-Server-Dienst. Dieses Paket ist abhängig von den Paketen NICI, NDSbase und NLDAPsdk.

Paket	Beschreibung
NOVLsnmp	Enthält die Laufzeitbibliotheken und Dienstprogramme für SNMP. Dieses Paket ist abhängig vom NICI-Paket.
NDSdexvnt	Enthält die Bibliothek, die die in NetIQ eDirectory generierten Ereignisse gegenüber anderen Datenbanken verwaltet.
NOVLpkia	Enthält PKI-Dienste. Dieses Paket ist abhängig von den Paketen NICI, NDSbase und NLDAPsdk.
NOVLembox	Enthält die eMBox-Infrastruktur und eMTools.
NOVLlmgnt	Enthält die Laufzeitbibliotheken für NetIQ Language Management.
NOVLxis	Enthält die Laufzeitbibliotheken für NetIQ XIS.
NOVLsas	Enthält die NetIQ SAS-Bibliotheken.
NOVLntls	Enthält die NetIQ TLS-Bibliothek. Dieses Paket wird auch als ntls bezeichnet.
NOVLldif2	Enthält das NetIQ Offline Bulkload-Dienstprogramm und ist abhängig von den Paketen NDSbase, NDSserv, NOVLntls, NOVLlmgnt und NICI.
NOVLncp	Enthält die NetIQ Encrypted NCP Services für Linux. Dieses Paket ist abhängig vom NDScommon-Paket.

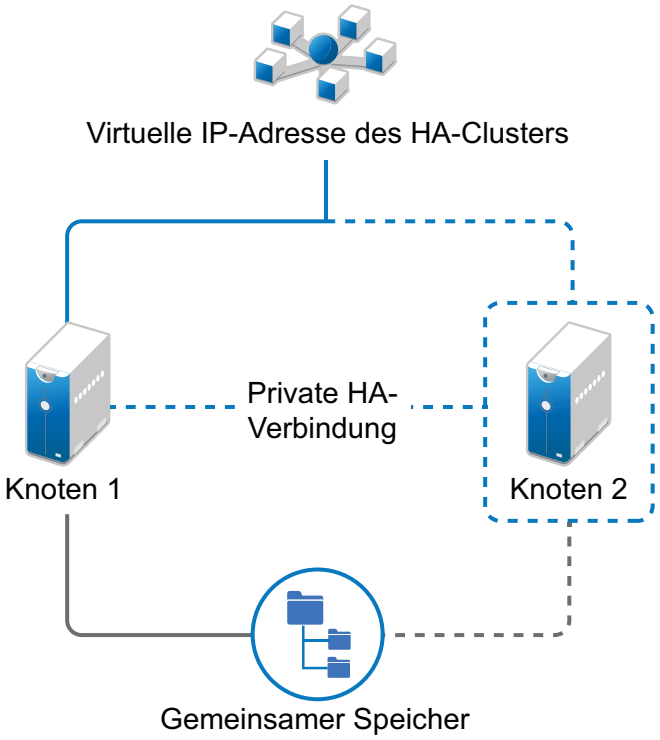
B Beispiellösung für die Bereitstellung eines Identity Manager-Clusters unter SLES 12 SP2

In diesem Anhang finden Sie schrittweise Anweisungen zum Konfigurieren von eDirectory und Identity Manager in einer unterstützten SLES-Cluster-Umgebung (SUSE Linux Enterprise Server) mit freigegebenem Speicher sowie ein Beispiel für eine Identity Manager-Bereitstellung in einem Cluster.

Für eine Linux-Hochverfügbarkeitslösung (HA-Lösung) mit freigegebenem Speicher auf Produktionsebene wird die Implementierung eines Fencing-Mechanismus im Cluster empfohlen. Hierfür stehen verschiedene Alternativen zur Auswahl. Im folgenden Beispiel wird eine STONITH-Ressource mit Systemspaltungsdetektor (SBD) verwendet.

Abbildung B-1 auf Seite 325 zeigt eine Beispiellösung für die Clusterbereitstellung.

Abbildung B-1 *Beispiellösung für eine Clusterbereitstellung*



B.1 Voraussetzungen

- Zwei Server mit SLES 12 SP2 (64 Bit) für Knoten
- Ein Server mit SLES 12 SP2 (64 Bit) für iSCSI-Server
- ISO-Image zur HA-Erweiterung für SLES12 SP2 (64 Bit)
- Sechs statische IP-Adressen:
  - Je zwei statische IP-Adressen pro Knoten.
  - Eine statische IP-Adresse für den Cluster. Diese IP-Adresse wird dynamisch dem Knoten zugewiesen, auf dem derzeit eDirectory ausgeführt wird.
  - Eine IP-Adresse für den iSCSI-Server.

B.2 Installationsvorgang

In diesem Abschnitt wird die Installation und Konfiguration der nachfolgenden Elemente beim Einrichten der Cluster-Umgebung beschrieben. Weitere Informationen zum Konfigurieren der SLES High Availability Extension finden Sie im Handbuch SUSE Linux Enterprise High Availability Extension.

B.2.1 Konfigurieren des iSCSI-Servers

Ein iSCSI-Ziel ist ein Gerät, das als freigegebener Speicher für alle Knoten in einem Cluster konfiguriert ist. Dieser virtuelle Datenträger wird auf dem Linux-Server erstellt und ermöglicht den Remote-Zugriff eines iSCSI-Initiators über eine Ethernet-Verbindung. Ein iSCSI-Initiator ist ein beliebiger Knoten im Cluster, der für das Herstellen einer Verbindung zum Ziel (iSCSI) zur Erbringung von Diensten konfiguriert ist. Das iSCSI-Ziel sollte ununterbrochen ausgeführt werden, damit jeder Host, der als Initiator auftritt, das Ziel ansprechen kann. Bevor Sie das iSCSI-Ziel auf dem iSCSI-Server installieren, überprüfen Sie, ob auf dem iSCSI-Ziel ausreichend Speicherplatz für den freigegebenen Speicher verfügbar ist. Installieren Sie die iSCSI-Initiatorpakete nach der Installation von SLES 12 SP2 auf den beiden anderen Knoten.

Beachten Sie Folgendes während der Installation von SLES 12 SP2:

1. Erstellen Sie eine separate Partition, und legen Sie den Partitionspfad als Partition mit dem freigegebenen iSCSI-Speicher fest.
2. Installieren Sie die iSCSI-Zielpakete.

So konfigurieren Sie den iSCSI-Server:

1. Erstellen Sie ein Blockgerät auf dem Zielserver.
2. Geben Sie im Terminal den Befehl `yast2 disk` ein.
3. Erstellen Sie eine neue Linux-Partition, und wählen Sie **Nicht formatieren**.
4. Wählen Sie **Partition nicht einhängen**.
5. Legen Sie die Partitionsgröße fest.
6. Geben Sie am Terminal den Befehl `yast2 iscsi-server` oder `yast2 iscsi-lio-server` ein.
7. Klicken Sie auf die Registerkarte **Dienst** und wählen Sie **Beim Booten** in **Dienst starten**.
8. Klicken Sie auf der Registerkarte **Ziele** auf **Hinzufügen**, und geben Sie den Partitionspfad ein (während der SLES-Installation erstellt).

9 Geben Sie auf der Seite **iSCSI-Ziel-Initiator-Einrichtung bearbeiten** die iSCSI-Client-Initiator-Hostnamen für den Zielserver an und klicken Sie auf **Weiter**.

   Beispiel: *iqn.sles12sp2node2.com* und *iqn.sles12sp2node3.com*.

10 Klicken Sie auf **Fertig stellen**.

11 Überprüfen Sie, ob das iSCSI-Ziel installiert wurde. Geben Sie hierzu den Befehl `cat /proc/net/iet/volume` im Terminal ein.

B.2.2 Konfigurieren des iSCSI-Initiators auf allen Knoten

Sie müssen den iSCSI-Initiator auf allen Clusterknoten konfigurieren, die eine Verbindung zum iSCSI-Ziel herstellen.

So konfigurieren Sie den iSCSI-Initiator:

1 Installieren Sie die iSCSI-Initiatorpakete.

2 Führen Sie im Terminal den Befehl `yast2 iscsi-client` aus.

3 Klicken Sie auf die Registerkarte **Dienst** und wählen Sie **Beim Booten** in **Dienst starten**.

4 Klicken Sie auf die Registerkarte **Verbundene Ziele**, klicken Sie auf **Hinzufügen**, und geben Sie die IP-Adresse des iSCSI-Zielservers ein.

5 Wählen Sie **Keine Authentifizierung**.

6 Klicken Sie auf **Weiter** und dann auf **Verbinden**.

7 Klicken Sie auf **Start umschalten**, ändern Sie die Startoption von „Manuell“ in „Automatisch“, und klicken Sie auf **Weiter**.

8 Klicken Sie auf **Weiter** und anschließend auf **OK**.

9 Überprüfen Sie den Status des verbundenen Zielservers. Führen Sie hierzu den Befehl `cat /proc/net/iet/session` auf dem Zielserver aus. Die Liste der Initiatoren, die mit dem iSCSI-Server verbunden sind, wird angezeigt.

B.2.3 Partitionieren des freigegebenen Speichers

Erstellen Sie im freigegebenen Speicher je eine Partition für SBD und für Cluster File System.

So partitionieren Sie den freigegebenen Speicher:

1 Führen Sie im Terminal den Befehl `yast2 disk` aus.

2 Wählen Sie im Dialogfeld **Partitionierungsexperte** das freigegebene Volume aus. In diesem Beispiel wählen Sie im Dialogfeld **Partitionierungsexperte** den Eintrag **sdb**.

3 Klicken Sie auf **Hinzufügen**, wählen Sie **Primäre Partition**, und klicken Sie auf **Weiter**.

4 Wählen Sie **Benutzerdefinierte Größe**, und klicken Sie auf **Weiter**. In diesem Beispiel beträgt die benutzerdefinierte Größe 100 MB.

5 Wählen Sie unter **Formatierungsoptionen** die Option **Partition nicht formatieren**. In diesem Beispiel lautet die Dateisystem-ID „0x83 Linux“.

6 Wählen Sie unter **Einhängeoptionen** die Option **Partition nicht einhängen**, und klicken Sie auf **Fertig stellen**.

7 Klicken Sie auf **Hinzufügen**, und wählen Sie **Primäre Partition**.

8 Klicken Sie auf **Weiter**, wählen Sie **Max. Größe**, und klicken Sie auf **Weiter**.

9 Wählen Sie unter **Formatierungsoptionen** die Option **Partition nicht formatieren**. In diesem Beispiel geben Sie die Dateisystem-ID „0x83 Linux“ an.

10 Wählen Sie unter **Einhängeoptionen** die Option **Partition nicht einhängen**, und klicken Sie auf **Fertig stellen**.

B.2.4 Installieren der HA-Erweiterung

So installieren Sie die HA-Erweiterung:

1 Gehen Sie zur SUSE Downloads-Website.

Die SUSE Linux Enterprise High Availability Extension (SLE HA) steht für die verfügbaren Plattformen als je zwei ISO-Images zum Herunterladen bereit. Medium 1 enthält die Binärpakete und Medium 2 den Quellcode.

HINWEIS: Wählen Sie die entsprechende ISO-Datei mit der HA-Erweiterung für Ihre Systemarchitektur aus.

---

2 Laden Sie die ISO-Datei für Medium 1 auf die einzelnen Server herunter.

3 Öffnen Sie das Dialogfeld **YaST-Kontrollzentrum**, und klicken Sie auf **Zusatzprodukte > Hinzufügen**.

4 Klicken Sie auf **Durchsuchen**, wählen Sie die DVD oder das lokale ISO-Image aus und klicken Sie auf **Weiter**.

5 Wählen Sie auf der Registerkarte **Muster** die Option **Hochverfügbarkeit** unter **Primäre Funktionen**.

Prüfen Sie, ob alle Komponenten mit hoher Verfügbarkeit installiert wurden.

6 Klicken Sie auf **Akzeptieren**.

B.2.5 Einrichten des softdog-Watchdog

In der SLES-HA-Erweiterung ist die Unterstützung für die Überwachung im Kernel standardmäßig aktiviert. Die Erweiterung umfasst einige Kernelmodule mit hardwarespezifischen Überwachungstreibern. Der entsprechende Überwachungstreiber für Ihre Hardware wird automatisch beim Booten des Systems geladen.

1 Aktivieren Sie den softdog-Watchdog:

```
echo softdog > /etc/modules-load.d/watchdog.conf
```

```
systemctl restart systemd-modules-load
```

2 Testen Sie, ob das softdog-Modul richtig geladen wurde:

```
lsmod | grep dog
```

B.2.6 Konfigurieren des HA-Clusters

In diesem Beispiel wird vorausgesetzt, dass Sie zwei Knoten in einem Cluster konfigurieren.

Einrichtung des ersten Knotens:

1 Melden Sie sich als root an dem physischen oder virtuellen Rechner an, den Sie als Cluster-Knoten verwenden möchten.

2 Führen Sie den folgenden Befehl aus:

`ha-cluster-init`

Der Befehl führt eine Prüfung im Hinblick auf die NTP-Konfiguration und einen Hardware-Watchdog-Service durch. Es generiert die öffentlichen und privaten SSH-Schlüssel, die für den SSH-Zugriff und die Csync2-Synchronisierung verwendet werden, und startet die entsprechenden Services.

3 Konfigurieren Sie die Cluster-Kommunikationsschicht:

   3a Geben Sie eine Netzwerkadresse ein, an die eine Bindung erfolgen soll.

   3b Geben Sie eine Multicast-Adresse ein. Das Skript schlägt eine Zufallsadresse vor, die Sie als Standard verwenden können.

   3c Geben Sie einen Multicast-Port ein. Standardmäßig lautet die Portnummer 5405.

4 Richten Sie SBD als Fencing-Mechanismus für Knoten ein:

   4a Mit *j* geben Sie an, dass SBD verwendet werden soll.

   4b Geben Sie einen persistenten Pfad zu der Partition Ihres Blockgeräts ein, die Sie für SBD verwenden möchten. Der Pfad muss bei beiden Knoten im Cluster konsistent sein.

5 Konfigurieren Sie eine virtuelle IP-Adresse für die Cluster-Verwaltung:

   5a Mit *j* geben Sie an, dass eine virtuelle IP-Adresse konfiguriert werden soll.

   5b Geben Sie eine nicht verwendete IP-Adresse ein, die Sie als Verwaltungs-IP für die SUSE Hawk-Benutzeroberfläche verwenden möchten. Beispiel: *192.168.1.3*.

   Sie können auch eine Verbindung mit der virtuellen IP-Adresse herstellen, statt sich an einem einzelnen Cluster-Knoten anzumelden.

Sobald der erste Knoten ausgeführt wird, fügen Sie den zweiten Cluster-Knoten mit dem Befehl `ha-cluster-join` hinzu.

Einrichtung des zweiten Knotens:

1 Melden Sie sich als Root-Benutzer bei dem physischen oder virtuellen Computer an, der mit dem Cluster verbunden werden soll.

2 Führen Sie den folgenden Befehl aus:

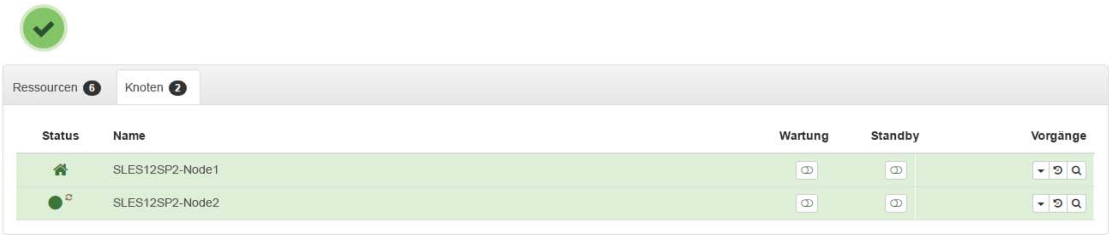
   `ha-cluster-join`

   Wenn NTP nicht konfiguriert ist, wird eine Meldung angezeigt. Der Befehl prüft, ob ein Hardware-Watchdog-Gerät vorhanden ist, und gibt eine Benachrichtigung aus, wenn ein solches Gerät fehlt.

3 Geben Sie die IP-Adresse des ersten Knotens ein.

4 Geben Sie das Root-Passwort des ersten Knotens ein.

5 Melden Sie sich bei der SUSE Hawk-Benutzeroberfläche an und klicken Sie auf **Status** > **Knoten**. Beispiel: `https://192.168.1.3:7630/cib/live`.



B.2.7 Installieren und Konfigurieren von eDirectory und Identity Manager auf Clusterknoten

1 So installieren Sie eDirectory auf Clusterknoten:

Installieren Sie eine unterstützte Version von eDirectory. Schrittweise Anweisungen zum Konfigurieren von eDirectory in einem HA-Cluster finden Sie unter „Deploying eDirectory on High Availability Clusters“ (Bereitstellen von eDirectory in Hochverfügbarkeitsclustern) im *eDirectory-Installationshandbuch*.

WICHTIG: Die virtuelle IP-Adresse muss auf Knoten1 konfiguriert sein, bevor Sie eDirectory auf Knoten1 installieren.

---

2 Installieren Sie Identity Manager mit der Metaverzeichnis-Server-Option auf Knoten1.

3 Installieren Sie die Identity Manager-Engine mit der Option `DCLUSTER_INSTALL` auf Knoten2.

Führen Sie das Kommando `./install.bin -DCLUSTER_INSTALL="true"` im Terminal aus.

Die Identity Manager-Dateien werden ohne Interaktion mit eDirectory installiert.

B.2.8 Konfigurieren der eDirectory-Ressource

1 Melden Sie sich bei der SUSE Hawk-Benutzeroberfläche an.

2 Klicken Sie auf **Ressource hinzufügen** und erstellen Sie eine neue Gruppe.

2a Klicken Sie auf ⊕ neben der **Gruppe**.

2b Geben Sie eine Gruppen-ID an. Beispiel: *Group-1*.

Beim Erstellen einer Gruppe müssen die folgenden untergeordneten Ressourcen ausgewählt werden:

- *stonith-sbd*
- *admin_addr (Cluster-IP-Adresse)*

3 Wählen Sie auf der Registerkarte **Meta-Attribute** im Feld **target-role** die Option *Gestartet* und im Feld **is-managed** die Option *Ja*.

4 Klicken Sie auf **Konfiguration bearbeiten** und klicken Sie dann auf ✎ neben der Gruppe, die Sie in Schritt 2 erstellt haben.

5 Tragen Sie die folgenden untergeordneten Ressourcen in das Feld **Untergeordnete Elemente** ein:

- *shared-storage*
- *eDirectory-resource*

Fügen Sie die Ressourcen beispielsweise in der nachstehenden Reihenfolge in die Gruppe ein:

- *stonith-sbd*
- *admin_addr (Cluster-IP-Adresse)*
- *shared-storage*
- *eDirectory-resource*

Sie können die Ressourcennamen gegebenenfalls ändern. Jede Ressource umfasst einen Satz mit Parametern, die definiert werden müssen. Weitere Informationen zu Beispielen für shared-storage- und eDirectory-Ressourcen finden Sie unter Stammfunktionen für untergeordnete eDirectory- und shared-storage-Ressourcen.

B.2.9 Stammfunktionen für untergeordnete eDirectory- und shared-storage-Ressourcen

Die Ressourcen *stonith-sbd* und admin_addr werden standardmäßig mit HA-Cluster-Befehlen beim Initialisieren des Cluster-Knotens konfiguriert.

Tabelle B-1 *Beispiel für shared-storage*

Ressourcen-ID	Name der shared-storage-Ressource
Klasse	ocf
Anbieter	heartbeat
Typ	Dateisystem
Gerät	/dev/sdc1
Verzeichnis	/freigegeben
fstype	XFS
operations	◆ start (60, 0) ◆ stop (60, 0) ◆ monitor (40, 20)
is-managed	Ja
resource-stickiness	100
target-role	Angefangen

Tabelle B-2 *Beispiel für eDirectory-Ressource*

Ressourcen-ID	Name der eDirectory-Ressource
Klasse	systemd
Typ	ndsdtmpl-shared-conf-nds.conf@-shared-conf-env
operations	◆ start (100, 0) ◆ stop (100, 0) ◆ monitor (100, 60)
target-role	Angefangen
is-managed	Ja
resource-stickiness	100
failure-timeout	125
migration-threshold	0

B.2.10 Ändern des Ortseinschränkungs-Scores

Ändern Sie den Ortseinschränkungs-Score zu dem Wert 0.

1. Melden Sie sich bei der SUSE Hawk-Benutzeroberfläche an.
2. Klicken Sie auf **Konfiguration bearbeiten**.
3. Klicken Sie auf der Registerkarte **Einschränkungen** auf ✎ neben Knoten 1 im Cluster.
4. Stellen Sie den Score auf der Registerkarte **Einfach** auf den Wert *0* ein.
5. Klicken Sie auf **Anwenden**.

Der Score muss für alle Knoten im Cluster auf *0* festgelegt sein.

HINWEIS: Wenn Sie die Ressourcen über die SUSE Hawk-Benutzeroberfläche mit der Option **Status** > **Ressourcen** > **Migrieren** von einem Knoten zu einen anderen Knoten migrieren, ändert sich der Ortseinschränkungs-Score zu *Unendlich* oder *–Unendlich*. Damit erhält nur ein Knoten im Cluster den Vorrang, sodass die eDirectory-Vorgänge verzögert werden.

C Beispiel einer Bereitstellungslösung für Identitätsanwendungen in einem Cluster auf einem Tomcat-Anwendungsserver

Im Anhang finden Sie Anweisungen zum Konfigurieren der Identitätsanwendungen in einer Clusterumgebung auf einem Tomcat-Anwendungsserver mit einer Beispielbereitstellung.

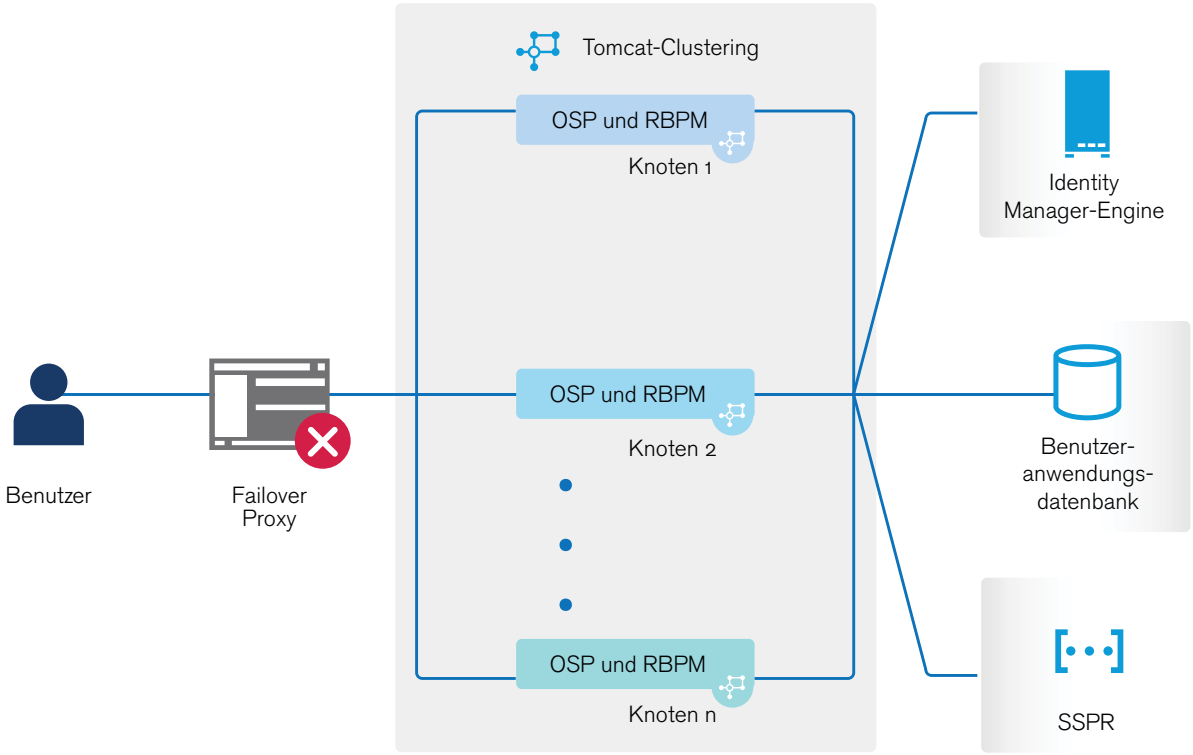
Durch das Clustering ist es möglich, Identitätsanwendungen auf verschiedenen parallelen Servern (Clusterknoten) auszuführen und dadurch hohe Verfügbarkeit zu erzielen. Zum Aufbau eines Clusters müssen verschiedene Tomcat-Instanzen (Knoten) gruppiert werden. Die Last wird auf verschiedene Server verteilt. Auch wenn einer der Server ausfällt, ist der Zugriff auf die Identitätsanwendungen weiterhin über andere Clusterknoten möglich. Für ein Failover erstellen Sie einen Cluster der Identitätsanwendungen und konfigurieren diese so, dass sie als einzelner Server fungieren. Diese Konfiguration enthält jedoch nicht die Identitätsberichterstellung.

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 C-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. Diese Vorgehensweise wird für Bereitstellungen auf Produktionsebene empfohlen.
- Sie sind bereits mit dem Installationsverfahren für eDirectory, die Identity Manager-Engine, die Identitätsanwendungen, den Tomcat-Anwendungsserver und die Datenbanken für die Benutzeranwendung vertraut.
- 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 unterstützt werden – wie Oracle oder MsSQL – eignen sich jedoch genauso gut dafür.
- Alle Benutzeranwendungsknoten kommunizieren mit derselben Instanz von eDirectory und der Datenbank mit der Benutzeranwendung. Die Anzahl der Benutzeranwendungsinstanzen kann je nach Bedarf erhöht werden.

Abbildung C-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.

C.1 Voraussetzungen

- Zwei Server, auf denen SUSE Linux Enterprise Server () 12 2 (), SLES SP (64-Bit) oder RedHat Enterprise Linux (RHEL) 7.3 (64-Bit) für die Knoten ausgeführt werden, auf denen alle abhängigen Bibliotheken installiert sind. Weitere Informationen finden Sie im Abschnitt zu RHEL.
- Die Identity Manager 4.7-Komponenten sind installiert.
- 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.

C.2 Installationsvorgang

In diesem Abschnitt finden Sie schrittweise Anleitungen zum Installieren einer neuen Instanz der Identitätsanwendungen auf Tomcat und der anschließenden Konfiguration für ein Clustering.

1. Installieren Sie die Identity Manager 4.7-Engine. Schrittweise Anleitungen finden Sie unter Abschnitt 9.1, „Installieren der Identity Manager-Engine“, auf Seite 91. Für eine Bereitstellung auf Produktionsebene empfiehlt es sich, die Identity Manager-Engine auf einem separaten Server zu installieren.
2. Installieren Sie die Datenbank für die Identitätsanwendungen. Sie können die PostgreSQL-Datenbank verwenden, die zusammen mit den Identitätsanwendungen installiert wird. Es wird jedoch empfohlen, die Datenbank auf einem separaten Server zu installieren.
3. Installieren und konfigurieren Sie die Identitätsanwendungen auf Knoten1.

   Bei der Installation müssen Sie:

   - die Option für eine neue Datenbank wählen
   - eine eindeutige Workflow-Engine-ID angeben. Beispiel: `Knoten1`.
   - die Datenbank-jar-Datei in allen Benutzeranwendungsknoten im Cluster bereitstellen. Für PostgreSQL befindet sich die Datei `postgresql-9.4.1212.jar` im Verzeichnis `/opt/netiq/idm/postgres`.

   Die Identitätsanwendungen verschlüsseln vertrauliche Daten mit einem Master-Schlüssel. Das Installationsprogramm erstellt bei der Konfiguration der Identitätsanwendungen einen neuen Master-Schlüssel. In einem Cluster muss für das Benutzeranwendungs-Clustering jede Instanz der Benutzeranwendung denselben Master-Schlüssel verwenden. Der Master-Schlüssel wird in der Eigenschaft `com.novell.idm.masterkey` in der Datei `ism-configuration.properties` im Verzeichnis `/opt/netiq/idm/apps/tomcat/conf/` gespeichert.

   Weitere Anweisungen finden Sie unter Abschnitt 9.3, „Installieren von Identitätsanwendungen“, auf Seite 97.
4. Installieren und konfigurieren Sie die Identitätsanwendungen auf Knoten2.

   Bei der Installation müssen Sie:

   - die Option für eine vorhandene Datenbank wählen
   - eine eindeutige Workflow-Engine-ID angeben. Beispiel: `Knoten2`.
   - die Datenbank-jar-Datei in allen Benutzeranwendungsknoten im Cluster bereitstellen. Für PostgreSQL befindet sich die Datei `postgresql-9.4.1212.jar` im Verzeichnis `/opt/netiq/idm/postgres`.

   Sobald Sie die Konfiguration der Benutzeranwendung auf Knoten2 abgeschlossen haben, kopieren Sie den Wert des Master-Schlüssels aus der Datei „ism-configuration.properties“ in Knoten1 und ersetzen Sie den entsprechenden Wert für den Master-Schlüssel in der Datei „ism-configuration.properties“ in Knoten2. Der Master-Schlüssel ist in der Eigenschaft „com.novell.idm.masterkey“ in der Datei „ism-configuration.properties“ („/opt/netiq/idm/apps/tomcat/conf/“) gespeichert.
5. Installieren Sie SSPR auf einem separaten Computer.

   Notieren Sie sich vor der Installation die folgenden Einstellungen und geben Sie diese während des Installationsvorgangs an:

   Starten Sie Tomcat nach der Installation von SSPR. Starten Sie dann SSPR (`http://<IP>:<Port>/sspr/private/config/ConfigEditor`) und melden Sie sich an. Klicken Sie auf **Konfigurationseditor** > **Einstellungen** > **Sicherheit** > **Whitelist-URL für die Umleitung**.

   a. Klicken Sie auf **Wert hinzufügen** und geben Sie die folgende URL an:

      OSP: `http://<DNS_für_Failover>:<Port>/osp`

b. Speichern Sie die Änderungen.

c. 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.

d. 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.

e. Starten Sie zur Aktualisierung der SSPR-Informationen auf Knoten1 das Konfigurationsprogramm unter `/opt/netiq/idm/apps/UserApplication/configupdate.sh`.

f. Klicken Sie auf **SSO-Clients > Self Service Password Reset** und geben Sie die Werte für die Parameter **Client-ID**, **Passwort** und **URL zur Umleitung der OSP-Authentifizierung** ein. Weitere Informationen finden Sie unter Abschnitt 22.3, „Aktualisieren der SSPR-Links im Dashboard für eine dezentrale Umgebung oder eine Cluster-Umgebung“, auf Seite 239.

HINWEIS: Vergewissern Sie sich, dass die Werte für diese Parameter in Knoten2 aktualisiert werden.

---

6. 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:

```
/opt/netiq/idm/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: `/opt/netiq/idm/jre/bin/keytool -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.

---

7. (Bedingt) Führen Sie folgenden Befehl aus, um zu überprüfen, ob die `osp.jks`-Datei mit den Änderungen aktualisiert wurde:

```
/opt/netiq/idm/jre/bin/keytool -list -v -keystore osp.jks -storepass changeit
```

8. Sichern Sie die ursprüngliche `osp.jks`-Datei, die sich unter `/opt/netiq/idm/apps/osp_sspr/osp/` befindet, und kopieren Sie die neue `osp.jks`-Datei an diesen Speicherort.

9. Kopieren Sie die neue `osp.jks`-Datei, die sich unter `/opt/netiq/idm/apps/osp_sspr/osp/` befindet, von Knoten1 in alle anderen Benutzeranwendungsknoten im Cluster.

10. 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.

    b. Kopieren Sie die Datei `ism-configuration.properties` unter `/TOMCAT_INSTALLED_HOME/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.

---

11. 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 der `setenv.sh`-Datei in Knoten1 `-Dcom.novell.afw.wf.Engine-id="Engine1"` 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.
12. 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 die Registerkarte **Administration**.

       Die Benutzeranwendung zeigt das Portal zur Anwendungskonfiguration an.
    d. Klicken Sie auf **Caching**.

       Die Benutzeranwendung zeigt die Seite "Cache-Management" an.
    e. Wählen Sie **True** für die Eigenschaft **Cluster aktiviert** aus.
    f. Klicken Sie auf **Speichern**.
    g. 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. Soll dieses Protokoll auf TCP umgestellt werden, befolgen Sie die Anweisungen unter Portal Configuration Tasks (Portalkonfigurationsaufgaben) in NetIQ Analyzer for Identity Manager Administration Guide (Administratorhandbuch zu NetIQ Analyzer für Identity Manager).

---

13. Aktivieren Sie den Berechtigungsindex für das Clustering.
    a. Melden Sie sich bei iManager auf Knoten1 an und navigieren Sie zu **Objekte anzeigen**.
    b. Navigieren Sie unter **System** zum Treibersatz mit dem Benutzeranwendungstreiber.
    c. Wählen Sie **AppConfig > AppDefs > Konfiguration** aus.
    d. Wählen Sie das XMLData-Attribut aus, 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>
```

e. Klicken Sie auf **OK**.

14. 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"/>
    ```

    Befolgen Sie für die erweiterte Tomcat-Clustering-Konfiguration die Schritte unter https://tomcat.apache.org/tomcat-8.5-doc/cluster-howto.html.

15. Starten Sie Tomcat in allen Knoten neu.

16. Konfigurieren Sie den Benutzeranwendungstreiber für das Clustering.

    In einem Cluster muss der Benutzeranwendungstreiber so konfiguriert sein, dass er den DNS-Namen des lokalen Lastausgleichprogramms für den Cluster verwendet. Sie konfigurieren den Benutzeranwendungstreiber mit iManager.

    a. Melden Sie sich bei iManager an, der Ihre Identity Manager-Engine verwaltet.

    b. Klicken Sie im Navigationsrahmen von iManager auf **Identity Manager**-Knoten.

    c. Klicken Sie auf **Identity Manager-Überblick.**

    d. Zeigen Sie auf der Seite "Suche" den Identity Manager-Überblick für den Treibersatz an, der Ihren Benutzeranwendungstreiber und den Rollen- und Ressourcenservice-Treiber enthält.

    e. Klicken Sie auf den runden Statusindikator in der rechten oberen Ecke des Treibersymbols:

       Es wird ein Menü mit Befehlen zum Starten und Stoppen des Treibers und zum Bearbeiten der Treibereigenschaften angezeigt.

    f. Wählen Sie **Eigenschaften bearbeiten** aus.

    g. Ändern Sie im Abschnitt "Treiberparameter" **Host** zum Hostnamen oder der IP-Adresse des Dispatchers.

    h. Klicken Sie auf **OK**.

    i. Starten Sie den Treiber neu.

17. Wiederholen Sie zum Ändern der URL des Rollen- und Ressourcenservice-Treibers die Schritte 18a bis 18f und klicken Sie auf **Treiberkonfiguration**. Aktualisieren Sie die **Benutzeranwendungs-URL** mit dem DNS-Namen des Lastausgleichprogramms.

18. Vergewissern Sie sich, dass die Sitzungstreue für den Cluster aktiviert ist, der in der Lastausgleichsoftware für die Benutzeranwendungsknoten erstellt wurde.

19. Konfigurieren Sie die Client-Einstellungen im Identity Manager-Dashboard. Weitere Informationen finden Sie unter Modus zur Konfiguration der Client-Einstellungen im NetIQ Identity Manager – Administratorhandbuch für die Identitätsanwendungen.