# NetIQ Identity Manager

## Einrichtungshandbuch

**Februar 2017**

## Rechtliche Hinweise

Informationen zu rechtlichen Hinweisen, Haftungsausschlüssen, Gewährleistungen, Ausfuhrbeschränkungen und sonstigen Nutzungseinschränkungen für NetIQ, Patentrichtlinien und Einschränkungen von Rechten der US-Regierung und Erfüllung von FIPS finden Sie unter https://www.netiq.com/company/legal/.

# 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.

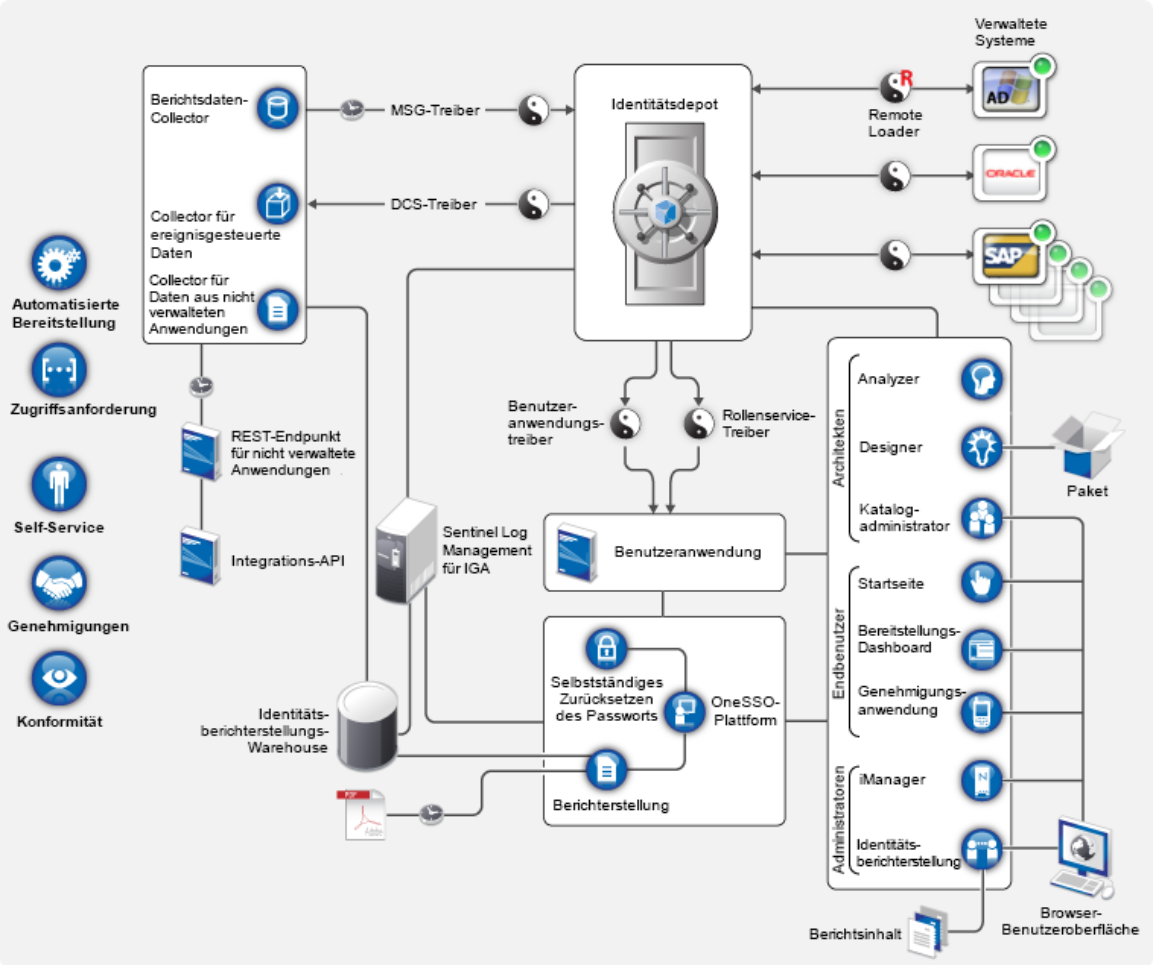
Im Allgemeinen lassen sich die Komponenten von Identity Manager in die folgenden Bereiche gliedern:

- Identity Manager-Umgebung erstellen und pflegen. Weitere Informationen finden Sie unter Kapitel 2, „Erstellen und Pflegen der Identity Manager-Umgebung“, auf Seite 27.
- Identity Manager-Umgebung überwachen (z. B. Benutzerbereitstellungsaktivitätiten 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 31.
- 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 35.

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 25.

# 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 27
- Abschnitt 2.2, „Analyzer für Identity Manager“, auf Seite 28
- Abschnitt 2.3, „Rollenverwaltung“, auf Seite 28
- Abschnitt 2.4, „iManager“, auf Seite 29


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 Rollenverwaltung

In Identity Manager definiert eine **Rolle** eine Reihe von Berechtigungen, die in Beziehung zu einem oder mehreren Zielsystemen oder Anwendungen stehen. Entsprechend dem Berechtigungsmodell erfassen die Identity Manager-Treiber die Konto-IDs und die Berechtigungszuweisungen von den verbundenen Systemen. Identity Manager nennt diese Berechtigungszuweisungen **Berechtigungen**. Anhand dieser Berechtigungen erteilt Identity Manager den Benutzern den Zugriff auf Ressourcen in den verbundenen Systemen. Das Identity Manager-Rollensystem umfasst verschiedene vordefinierte Rollen mit unterschiedlichen Zugriffsrechten auf das rollenbasierte Bereitstellungssystem. Ein Benutzer, der als Administrator des Rollenmoduls benannt wurde, besitzt beispielsweise uneingeschränkte Rechte im Rollensystem, während ein Benutzer, dem lediglich die Verwaltung der Rollen gestattet wurde, auf die explizit angebenen Benutzer, Gruppen und Rollen beschränkt ist.

Unternehmensanalytiker können im **Katalogadministrator in NetIQ Identity Manager** (Katalogadministrator) die Berechtigungen verwalten, ohne mit der zugrunde liegenden IT-Infrastruktur vertraut sein zu müssen. Mit diesen Komponenten können Sie Rollen, zusammengefasste Rollen und Profile (gemeinsam als **Autorisierungen** bezeichnet) zentral ermitteln und den Identity Manager-Rollen auf verschiedenen Systemen zuweisen. Die Autorisierungen können aus Unternehmensrollen, zusammengefassten Rollen und Profilen bestehen. Wenn Sie beispielsweise einem Benutzer eine Identity Manager-Rolle im rollenbasierten Bereitstellungsmodul zuweisen, erhält dieser Benutzer alle Autorisierungen, die dieser Rolle zugeordnet sind.

Der Katalogadministrator ruft die Rolleninformationen vom Benutzeranwendungstreiber ab und benötigt für die Identitätsanwendungen Zugriff auf das Identitätsdepot und das Dashboard. Weitere Informationen finden Sie in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen).

## 2.4 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
- 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 8.8-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. Zur Erleichterung der Auslastung und der Konfiguration der Umgebung können Sie den Remote Loader auf einem separaten Server installieren, also nicht auf demselben Server wie Tomcat und den Identity Manager-Server.

Weitere Informationen zum Remote Loader finden Sie in Abschnitt 18.2, „Erläuterungen zum Remote Loader“, auf Seite 167.

### 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 33
- „Datenerfassungsdienst“, auf Seite 34
- „Treiber „Verwaltetes System - Gateway““, auf Seite 34

#### Identitätsberichterstellung für Identity Manager

Das Identity Information Warehouse speichert die Daten in der SIEM-Datenbank von Sentinel Log Management für 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
- Katalogadministrator
- 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:

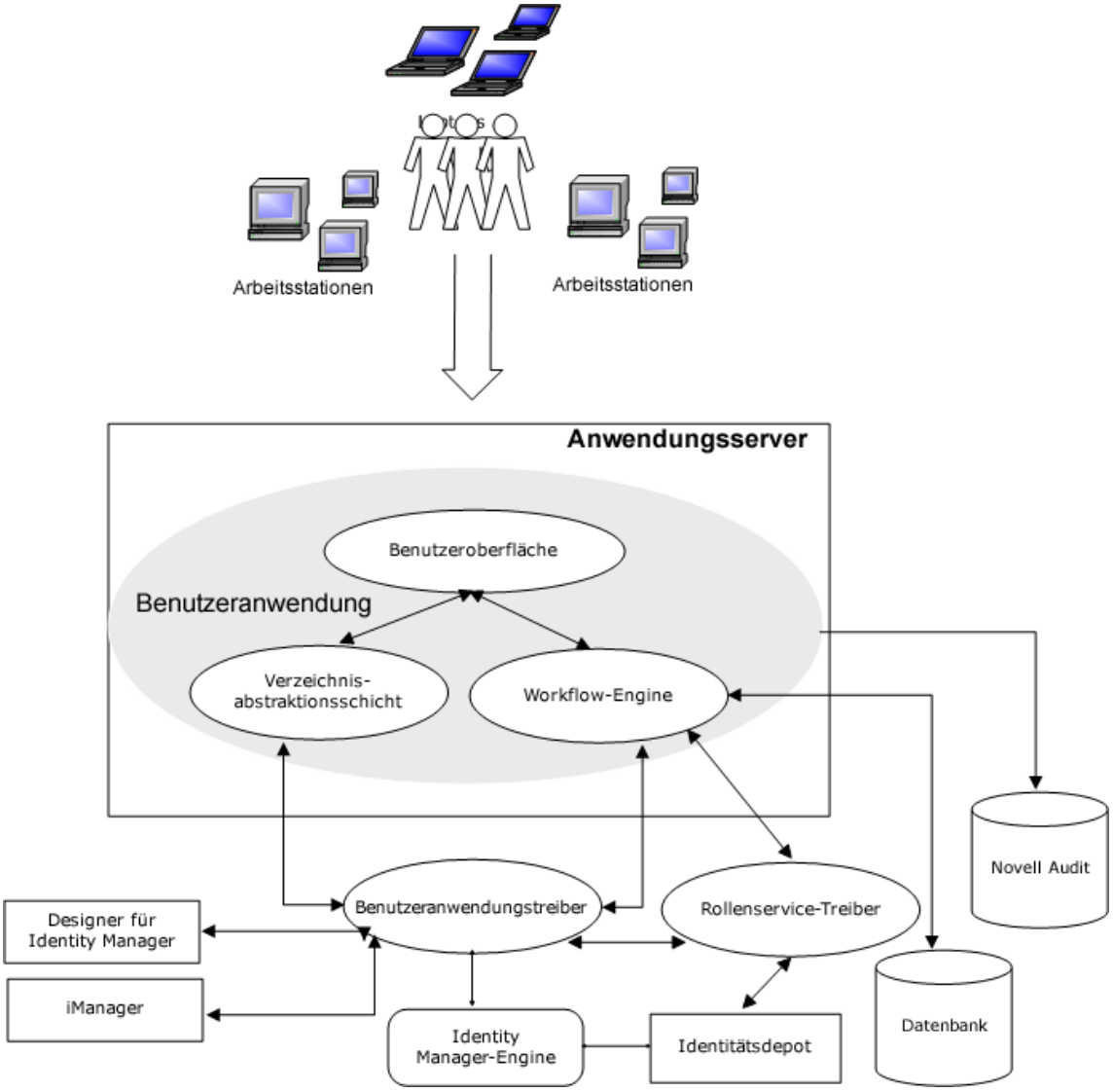

- Abschnitt 4.3.1, „Benutzeranwendung und rollenbasiertes Bereitstellungsmodul“, auf Seite 37
- Abschnitt 4.3.2, „Identity Manager-Dashboard“, auf Seite 39


### 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 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).

## 4.4 Verwenden von Self-Service Password Management in Identity Manager

Identity Manager umfasst die Komponente NetIQ Self Service Password Reset (SSPR), mit der Benutzer, die Zugriff auf die Identitätsanwendungen besitzen, ihr Passwort ohne Administratoreingriff zurücksetzen können. Bei der Installation bzw. einem Upgrade auf die neueste Version von Identity Manager wird SSPR standardmäßig aktiviert. In einer Neuinstallation verwendet SSPR ein systemeigenes Protokoll zur Verwaltung der Authentifizierungsmethoden. Bei einem Upgrade können Sie SSPR allerdings auch anweisen, die NetIQ Modular Authentication Services (NMAS) zu verwenden, die von Identity Manager bisher als Passwortverwaltungsprogramm eingesetzt wurden.

Sie können einen der folgenden Anbieter konfigurieren, abhängig davon, ob die komplexe Passwortverwaltung genutzt werden soll:

**SSPR**

NetIQ-SSPR (Self Service Password Reset, Zurücksetzen von Passwörtern per Selbstbedienung) ist die Standardoption beim Installieren oder Aufrüsten von Identity Manager. Weitere Informationen finden Sie unter Abschnitt 4.4.1, „Erläuterungen zum standardmäßigen Self-Service-Vorgang“, auf Seite 40.

**Bisheriger Anbieter für die Passwortverwaltung**

Übernimmt den Passwortverwaltungsvorgang aus Identity Manager 4.0.2, der die Verwendung mehrerer Passwortrichtlinien unterstützt. Weitere Informationen finden Sie unter Abschnitt 4.4.2, „Erläuterungen zum bisherigen Anbieter für die Passwortverwaltung“, auf Seite 41.

**Drittanbieter-Passwortverwaltung**

Sie können vergessene Passwörter mit einem Programm eines Drittanbieters verwalten. Hierbei müssen Sie jedoch einige Konfigurationseinstellungen für Identity Manager ändern. Weitere Informationen finden Sie unter Abschnitt 39.6.3, „Verwenden eines externen Systems für die „Passwort vergessen“-Verwaltung“, auf Seite 363.

### 4.4.1 Erläuterungen zum standardmäßigen Self-Service-Vorgang

SSPR integriert sich automatisch in den von Identity Reporting und den Identitätsanwendungen verwendeten Single Sign-On-Prozess. SSPR ist selbst dann das standardmäßige Passwortverwaltungsprogramm für Identity Manager, wenn Sie SSPR gar nicht installieren. Wenn ein Benutzer eine Passwortzurücksetzung anfordert, fragt SSPR den Benutzer nach den Antworten auf seine persönliche Sicherheitsabfrage. Werden die Antworten korrekt eingegeben, reagiert SSPR auf eine der folgenden Weisen:

- Erlaubt dem Benutzer das Erstellen eines neuen Passworts
- Erstellt ein neues Passwort und sendet es dem Benutzer zu
- Erstellt ein neues Passwort, sendet es dem Benutzer zu und markiert das alte Passwort als abgelaufen

Die Reaktion von SSPR können Sie im SSPR-Konfigurationseditor festlegen. Nach einem Upgrade auf eine neue Version von Identity Manager können Sie SSPR so konfigurieren, dass Identity Manager weiterhin NMAS, die bisherige Methode der Passwortverwaltung, verwendet. Ihre bisherigen Passwortrichtlinien für die Verwaltung vergessener Passwörter erkennt SSPR allerdings nicht. Weitere Informationen zur fortgesetzten Verwendung der Richtlinien finden Sie in Abschnitt 4.4.2, „Erläuterungen zum bisherigen Anbieter für die Passwortverwaltung“, auf Seite 41.

Sie können SSPR auch so konfigurieren, dass es statt NMAS sein proprietäres Protokoll verwendet. Wenn Sie diese Änderung vornehmen, können Sie allerdings nicht mehr ohne Zurücksetzung Ihrer Passwortrichtlinien zu NMAS zurückkehren.

| Weitere Informationen zum... | Erklärt in... |
|---|---|
| Installieren von SSPR | Kapitel 32, „Installieren der Passwortverwaltung für Identity Manager“, auf Seite 285 |
| Konfigurieren der Passwortverwaltung für die Identitätsanwendungen | Abschnitt 39.6.1, „Verwenden der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung für die „Passwort vergessen“-Verwaltung“, auf Seite 359 |
| Verwalten und Konfigurieren von SSPR | *NetIQ Self Service Password Reset Administration Guide* (NetIQ-Administrationshandbuch für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung) |

Das `.iso`-Image für Identity Manager und das integrierte Identity Manager-Installationsprogramm enthalten das Installationsprogramm für SSPR.

## 4.4.2 Erläuterungen zum bisherigen Anbieter für die Passwortverwaltung

**HINWEIS:** Die bisherige Selbstbedienungsfunktion für Passwörter wird mit dieser Version eingestellt. NetIQ empfiehlt dringend, alle passwortspezifischen Aufgaben auf SSPR umzustellen. Im Installationsvorgang wird SSPR standardmäßig aktiviert. Weitere Informationen finden Sie unter Abschnitt 4.2, „Erläuterungen zum Self-Service-Prozess in Identity Manager“, auf Seite 36.

Wenn Sie eine ältere Identity Manager-Version aufrüsten, greifen die Identitätsanwendungen standardmäßig auf SSPR als Passwortverwaltungsprogramm zurück. SSPR kann die NMAS-Methode verwenden, mit der die Passwortverwaltung in Identity Manager bislang vorgenommen wurde. Ihre bisherigen Passwortrichtlinien für die Verwaltung vergessener Passwörter erkennt SSPR allerdings nicht. Sie können SSPR umgehen und den bisherigen Anbieter für die Passwortverwaltung nutzen.

Wenn ein Benutzer das Zurücksetzen eines Passworts anfordert, vergleicht der bisherige Anbieter den Berechtigungsnachweis des Benutzers mit den festgelegten Passwortrichtlinien. Der Benutzer muss dann beispielsweise eine persönliche Sicherheitsabfrage beantworten. Je nach der gültigen Richtlinie für den Benutzer reagiert das Programm wie folgt:

- Setzt das Passwort zurück
- Zeigt den Passworthinweis an
- Sendet den Passworthinweis per Email an den Benutzer
- Sendet ein neues Passwort per Email an den Benutzer

Nutzen Sie den bisherigen Anbieter, wenn in Ihrem Unternehmen mehrere oder komplexe Passwortrichtlinien zum Einsatz kommen. Dies ist beispielsweise der Fall, wenn Ihre Passwortrichtlinien auf Benutzerrollen beruhen. Für einen Praktikanten reicht ein automatisch erzeugtes Passwort ohne Challenge-Response-Verfahren. Bei einem Manager, der auf sichere Daten zugreifen kann, gelten dagegen strengere Anforderungen. Dieser Benutzer muss das Passwort ggf. regelmäßig zurücksetzen. In beiden Fällen sollen die Benutzer ihr Passwort per Self-Service zurücksetzen können.

Wenn der bisherige Anbieter verwendet werden soll, bearbeiten Sie nach dem Installieren oder Aufrüsten von Identity Manager die Konfigurationseinstellungen für die Identitätsanwendungen. Die Passwortrichtlinien müssen nach dem Aufrüsten nicht erneut konfiguriert werden.

| Weitere Informationen zum... | Erklärt in... |
|---|---|
| Konfigurieren von Identity Manager für das Verwenden des bisherigen Anbieters | Abschnitt 39.6.2, „Verwenden des bisherigen Anbieters für die „Passwort vergessen“-Verwaltung“, auf Seite 361 |
| Verwenden des bisherigen Anbieters für die Passwortverwaltung | *NetIQ Identity Manager Password Management Guide* (Handbuch zur Passwortverwaltung in NetIQ Identity Manager) |

## 4.5 Verwenden des Single-Sign-On-Zugriffs in Identity Manager

Der Single-Sign-On-Zugriff (SSO-Zugriff) in Identity Manager erfolgt mit dem Authentifizierungsdienst NetIQ One SSO Provider (OSP). Für die folgenden Komponenten müssen Sie OSP verwenden:

- Katalogadministrator
- Identity Manager-Dashboard
- Identitätsberichterstellung
- Self-Service Password Reset
- Benutzeranwendung

Sowohl das `.iso`-Image für Identity Manager als auch das integrierte Identity Manager-Installationsprogramm enthält eine Option zum Installieren des OSP. Weitere Informationen zum Installieren des OSP finden Sie in Kapitel 32, „Installieren der Passwortverwaltung für Identity Manager“, auf Seite 285.

### 4.5.1 Erläuterungen zur Authentifizierung mit One SSO Provider (OSP)

Der OSP unterstützt die OAuth2-Spezifikation und erfordert einen LDAP-Authentifizierungsserver, der die Authentifizierung mit dem OAuth2-Protokoll vornimmt. Standardmäßig verwendet Identity Manager das Identitätsdepot (eDirectory). OSP kommuniziert auch andere Typen von **Authentifizierungsquellen** (oder **Identitätsdepots**), um Authentifizierungsanforderungen zu verarbeiten. Der spezifische Ursprung muss jedoch das OAuth-Protokoll verwenden. Es ist möglich, die vom OSP zu verwendende Authentifizierungsart zu konfigurieren: Benutzer-ID und Passwort, Kerberos oder SAML. Der OSP unterstützt allerdings keine MIT-Anmeldetickets aus Kerberos oder SAP.

**Wie funktionieren der OSP und SSO?**

Wenn Sie das Identitätsdepot als Authentifizierungsdienst verwenden und die angegebenen Container im Identitätsdepot CNs und Passwörter aufweisen, melden sich autorisierte Benutzer sofort nach der Installation bei Identity Manager an. Ohne diese Anmeldekonten kann sich nur der Administrator, der während der Installation angegeben wurde, sofort anmelden.

Wenn sich ein Benutzer bei einer der browsergestützten Komponenten anmeldet, leitet der Prozess den Namen und das Passwort des Benutzers an den OSP-Dienst weiter, der dann den Authentifizierungsserver abfragt. Der Server validiert den Benutzer-Berechtigungsnachweis.

Anschließend gibt der OSP ein OAuth2-Zugriffstoken an die Komponente und den Browser aus. Anhand des Tokens erteilt der Browser dem Benutzer während seiner Sitzung den SSO-Zugriff auf alle browsergestützten Komponenten.

Wenn Sie Kerberos oder SAML verwenden, akzeptiert der OSP die Authentifizierung durch den Kerberos-Ticketserver oder den SAML-IDP. Anschließend gibt der OSP ein OAuth2-Zugriffstoken an die Komponente aus, bei der sich der Benutzer angemeldet hat.

**Wie arbeitet der OSP mit Kerberos zusammen?**

OSP und Kerberos sorgen dafür, dass die Benutzer sich einmalig anmelden und so eine Sitzung bei einer der Identitätsanwendungen und der Identitätsberichterstellung anlegen können. Wenn die Gültigkeitsdauer der Benutzersitzung abläuft, erfolgt die Autorisierung automatisch und ohne Eingreifen des Benutzers. Nach dem Abmelden sollten die Benutzer den Browser in jedem Fall schließen, sodass die jeweilige Sitzung beendet wird. Ansonsten leitet die Anwendung den Benutzer zum Anmeldefenster weiter, und der OSP autorisiert die Benutzersitzung erneut.

**Wie richte ich die Authentifizierung und den Single-Sign-On-Zugriff ein?**

Sie müssen den OSP installieren, damit der OSP und SSO funktionsfähig sind. Geben Sie anschließend die URLs für den Client-Zugriff auf die einzelnen Komponenten, die URL für die Weiterleitung der Validierungsanforderungen an den OSP sowie die Einstellungen für den Authentifizierungsserver an. Diese Angaben können Sie wahlweise während der Installation oder zu einem späteren Zeitpunkt mit dem RBPM-Konfigurationsprogramm festlegen. Darüber hinaus können Sie die Einstellungen für den Kerberos-Ticketserver oder den SAML-IDP angeben.

Weitere Informationen zum Konfigurieren der Authentifizierung und des Single-Sign-On-Zugriffs finden Sie in Teil XV, „Konfiguration des Single-Sign-On-Zugriffs in Identity Manager“, auf Seite 443. In einem Cluster müssen die Konfigurationseinstellungen für alle Clustermitglieder identisch sein.

## 4.5.2 Erläuterungen zum Keystore für One SSO Provider (OSP)

Der Keystore in Identity Manager unterstützt die HTTP- und die HTTPS-Kommunikation zwischen dem OSP-Dienst und dem Authentifizierungsserver. Dieser Keystore wird beim Installieren des OSP erstellt. Außerdem legen Sie ein Passwort an, das der OSP für die autorisierten Interaktionen mit dem Authentifizierungsserver heranzieht. Weitere Informationen finden Sie unter Kapitel 32, „Installieren der Passwortverwaltung für Identity Manager“, auf Seite 285.

## 4.5.3 Erläuterungen zu den Revisionsereignissen für One SSO Provider (OSP)

OSP erzeugt ein einzelnes Ereignis, sobald sich ein Benutzer bei der Benutzeranwendung oder der Identitätsberichterstellung an- oder abmeldet:

- 003E0204 für die Anmeldung
- 003E0201 für die Abmeldung

Die XDAS-Taxonomie interpretiert diese OSP-Ereignisse dann entweder als erfolgreiche An-/Abmeldung, als SOAP-Aufruf der Benutzeranmeldung oder als „anderes Ereignis als Erfolg“.

# 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 47
- Kapitel 6, „Überlegungen und Voraussetzungen für die Installation“, auf Seite 61

# 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 23. |
| ❑ | 2. Wählen Sie das gewünschte Installationsprogramm aus. Weitere Informationen finden Sie in Abschnitt 5.2, „Erläuterungen zur integrierten Installation und zur Standalone-Installation“, auf Seite 49. |
| ❑ | 3. Ermitteln Sie die optimalen Betriebssystemplattformen für Ihre Installation. Weitere Informationen finden Sie in Abschnitt 5.3.5, „Auswählen einer Betriebssystemplattform für Identity Manager“, auf Seite 54.<br><br>**HINWEIS:** Sentinel Log Management für IGA kann nur auf einem Linux-Server installiert werden. Wenn Ihre Identitätslösung ausschließlich unter Windows läuft, können Sie jedoch einen anderen Revisionsdienst nutzen. |
| ❑ | 4. (Bedingt) Stellen Sie beim Installieren von Komponenten in einer Umgebung mit Red Hat Enterprise Linux 6.*x*- oder 7.*x* sicher, dass die richtigen Bibliotheken auf dem Server vorliegen. Weitere Informationen finden Sie in Abschnitt 6.4, „Installieren von Identity Manager auf einem RHEL 6.*x- oder 7.x-Server“, auf Seite 63* |
| ❑ | 5. Legen Sie die Installationsreihenfolge und den Installationsort der einzelnen Komponenten fest. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |

| | Checkliste |
|---|---|
| ❑ | 6. Stellen Sie sicher, dass eine Lizenz für die Ausführung von Identity Manager vorliegt. Weitere Informationen finden Sie in Abschnitt 5.4, „Erläuterungen zur Lizenzierung und zur Aktivierung“, auf Seite 56. |
| ❑ | 7. 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 5.5, „Erläuterungen zur Identity Manager-Kommunikation“, auf Seite 56. |
| ❑ | 8. Stellen Sie fest, ob die Installationsprogramme in Ihrer bevorzugten Sprache ausgeführt werden können. Weitere Informationen finden Sie in Abschnitt 5.6, „Erläuterungen zur Sprachunterstützung“, auf Seite 58. |
| ❑ | 9. Stellen Sie sicher, dass die erforderlichen Dateien für die Installation von Identity Manager vorliegen. Weitere Informationen finden Sie in Abschnitt 5.7, „Herunterladen der Installationsdateien“, auf Seite 60.<br><br>**WICHTIG:** Zur Erleichterung der Installation führen Sie keine CPU-intensiven Anwendungen aus, während die Identity Manager-Komponenten installiert werden. |
| ❑ | 10. (Bedingt) Wenn Identity Manager in einem Cluster installiert werden soll, überprüfen Sie, ob Ihre Umgebung den Anforderungen entspricht. Weitere Informationen finden Sie in Abschnitt 6.1, „Sicherstellen der Hochverfügbarkeit von Identity Manager“, auf Seite 61. |
| ❑ | 11. 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. |

| | Checkliste |
|---|---|
| ❑ | 12. Stellen Sie sicher, dass die Computer, auf denen die Identity Manager-Komponenten installiert werden sollen, den angegebenen Anforderungen entsprechen. Weitere Informationen finden Sie in den folgenden Abschnitten:<br>◆ **Analyzer:** (Optional) „Planen der Installation von Analyzer“, auf Seite 435<br>◆ **Designer:** „Planen der Installation von Designer“, auf Seite 247<br>◆ **Sentinel Log Management für IGA**: „Installieren und Verwalten von Sentinel for Log Management für Identity Governance and Administration“, auf Seite 129<br>◆ **Identitätsanwendungen für Rollen- und Ressourcenverwaltung:** „Planen der Installation der Identitätsanwendungen“, auf Seite 297<br>◆ **Identity Manager-Engine:** „Planen der Installation der Engine, der Treiber und der Plugins“, auf Seite 141<br>◆ **Identitätsdepot:** „Installieren des Identitätsdepots“, auf Seite 67<br>◆ **iManager:** (Optional) „Planen der Installation von iManager“, auf Seite 217<br>◆ **Passwortrücksetzung (SSPR):** „Planen der Installation der Passwortverwaltung für Identity Manager“, auf Seite 281<br>◆ **PostgreSQL:** „Planen der Installation von PostgreSQL und Tomcat“, auf Seite 257<br>◆ **Remote Loader:** „Planen der Installation der Engine, der Treiber und der Plugins“, auf Seite 141<br>◆ **Berichterstellung**: „Planen der Installation der Identitätsberichterstellung“, auf Seite 393<br>◆ **Single-Sign-On-Zugriff (OSP):** „Planen der Installation der Passwortverwaltung für Identity Manager“, auf Seite 281<br>◆ **TomCat:** „Planen der Installation von PostgreSQL und Tomcat“, auf Seite 257<br>**HINWEIS:** NetIQ empfiehlt, die Konten zu notieren, die Sie während des Installationsvorgangs erstellen. |
| ❑ | 13. Weitere Informationen zum Installieren von Identity Manager mit den Standardeinstellungen finden Sie im *NetIQ Identity Manager Integrated Installation Guide* (Handbuch zur integrierten Installation von NetIQ Identity Manager). |
| ❑ | 14. Aktivieren Sie die Identity Manager-Komponenten. Weitere Informationen finden Sie in Abschnitt 53.7, „Aktivieren von Identity Manager“, auf Seite 486. |

## 5.2 Erläuterungen zur integrierten Installation und zur Standalone-Installation

Mit dem Programm für die integrierte Installation und dem Programm für die Standalone-Installation bietet NetIQ zwei Möglichkeiten, wie Sie Identity Manager in Ihrer Umgebung installieren und konfigurieren. Anhand der Informationen in diesem Abschnitt ermitteln Sie das geeignete Verfahren für Ihre Umgebung.

- Abschnitt 5.2.1, „Erläuterungen zur integrierten Installation“, auf Seite 50
- Abschnitt 5.2.2, „Erläuterungen zur Standalone-Installation“, auf Seite 50

### 5.2.1 Erläuterungen zur integrierten Installation

NetIQ empfiehlt dieses Verfahren, wenn Sie Identity Manager testen oder eine Testumgebung erstellen möchten. Das Programm für die integrierte Installation fasst alle erforderlichen Komponenten in einem einzigen Installationsvorgang zusammen. Dieser Vorgang bietet folgende Funktionen:

- Wendet die Standardwerte für die meisten Einstellungen an, z. B. eine vordefinierte Baumstruktur für das Identitätsdepot
- Installiert alle Komponenten auf einem einzigen Computer oder in einer kleinen dezentralen Umgebung
- Installiert alle Treiber und erstellt den Treibersatz als separate Partition, wenn Sie Einstellungen für die Identity Manager-Engine festlegen
- Installiert alle iManager-Plugins
- Verwendet PostgreSQL für alle Datenbanken
- Verwendet Apache Tomcat als Anwendungsserver
- Prüft die Plattform des Servers und ermittelt, ob eine unterstützte Version vorliegt
- Kann auf Plattformen mit Red Hat Enterprise Linux (RHEL) 7.3 (oder höher), SUSE Linux Enterprise Server (SLES) 12 SP1 (oder höher) oder Windows 2012 R2 ausgeführt werden
- Kann nicht zur Installation von Identity Manager auf den folgenden Betriebssystemen verwendet werden:
  - Open Enterprise Server 2015
  - Open Enterprise Server 11 SP2
  - RedHat Enterprise Linux 6.x
  - SUSE Linux Enterprise Server 11
- Kann nicht zur Installation der Identity Manager Standard Edition verwendet werden
- Kann nicht in einer Cluster-Umgebung verwendet werden
- Kann nicht in einer Produktionsumgebung verwendet werden
- Kann nicht zum Aufrüsten einer früheren Version von Identity Manager verwendet werden

Weitere Informationen finden Sie im *NetIQ Identity Manager Integrated Installation Guide* (Handbuch zur integrierten Installation von NetIQ Identity Manager).

### 5.2.2 Erläuterungen zur Standalone-Installation

NetIQ empfiehlt diese Option für die Staging- und Produktionsumgebung Ihrer Identitätsmanagement-Lösung. Mit dem Programm für die Standalone-Installation können Sie Ihre Umgebung flexibler einrichten. Zahlreiche Identity Manager-Komponenten (z. B. das Identitätsdepot) sind datenintensiv und sollten daher auf separaten Servern installiert werden.

Das Programm für die Standalone-Installation weist die folgenden neuen Fähigkeiten auf:

- Möglichkeit zum Anpassen der Einstellungen für die Komponenten, z. B. die Baumstruktur im Identitätsdepot
- Möglichkeit zum Installieren in dezentralen Umgebungen und Cluster-Umgebungen
- Möglichkeit zum Auswählen der Treiber und zum Erstellen von Treibersätzen, die zur Identitätsmanagement-Lösung hinzugefügt werden sollen

- Möglichkeit zum Auswählen der iManager-Plugins, die zur Identitätsmanagement-Lösung hinzugefügt werden sollen
- Möglichkeit zum Installieren bestimmter Komponenten mit einem Nicht-`Root`-Konto
- Unterstützt mehrere Datenbankplattformen
- Verwendet Apache Tomcat für alle unterstützten Betriebssysteme
- Erstellt eine unterstützte Produktionsumgebung
- Kann zum Aufrüsten einer früheren Version von Identity Manager verwendet werden

Führen Sie die Programme zur Standalone-Installation nach Möglichkeit in der Reihenfolge aus, die durch Ihre Identitätsmanagement-Lösung vorgegeben ist. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51.

## 5.3 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.



### 5.3.1 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. Identitätsdepot
3. Identity Manager-Engine, Treiber und iManager-Plugins
4. (Optional) iManager
5. Designer
6. Tomcat und PostgreSQL
7. OSP
8. SSPR

9. Identitätsanwendungen
10. (Optional) Analyzer

### 5.3.2 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. Identitätsdepot
2. Sentinel Log Management für IGA
3. Identity Manager-Engine, Treiber und iManager-Plugins
4. (Optional) iManager
5. Designer
6. Tomcat und PostgreSQL
7. OSP
8. SSPR
9. Identitätsanwendungen
10. Identitätsberichterstellung
11. (Optional) Analyzer

### 5.3.3 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. Identitätsdepot
3. Identity Manager-Engine, Treiber und iManager-Plugins
4. (Optional) iManager
5. Designer
6. Tomcat und PostgreSQL
7. OSP
8. SSPR
9. Identitätsanwendungen
10. Identitätsberichterstellung
11. (Optional) Analyzer

## 5.3.4 Empfohlene Servereinrichtung

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

| Einzurichtende(r) Computer | Einzurichtende Komponente(n) |
|---|---|
| Server 1 und 2 (Verzeichnisreproduktion auf zwei Servern) | ◆ Identitätsdepot<br>◆ Identity Manager-Engine |
| Server 3 und 4 (Cluster mit zwei Servern) | ◆ Identitätsanwendungen<br>◆ iManager<br>◆ Ein SSO-Anbieter<br>◆ Remote Loader<br>◆ Zurücksetzen von Passwörtern per Selbstbedienung |
| Server 5 (oder ein Server-Cluster) | Identity Manager-Datenbanken:<br>◆ Identitätsanwendungen<br>◆ Identitätsberichterstellung |
| Server 6 (nicht in einem Cluster) | Identitätsberichterstellung |
| Server 7 | Sentinel Log Management für IGA |
| Client-Arbeitsstationen (mindestens 1) | ◆ Designer<br>◆ iManager Workstation<br>◆ Internetbrowserzugriff auf die Identitätsanwendungen und die Identitätsberichterstellung |

## 5.3.5 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 |
|---|---|
| Open Enterprise Server (OES) | Identitätsanwendungen |
| | Identity Manager-Engine |
| | Identitätsberichterstellung |
| | Identitätsdepot |
| | iManager (Server) |
| | Ein SSO-Anbieter |
| | PostgreSQL |
| | Remote Loader |
| | Zurücksetzen von Passwörtern per Selbstbedienung |
| | Tomcat |
| | **HINWEIS:** Auf einem System mit Open Enterprise Server 11 SP2 oder Open Enterprise Server 2015 ist der integrierte Installationsvorgang nicht möglich. |
| openSUSE | Analyzer |
| | Designer |
| | iManager -Arbeitsstation (Client) |
| Red Hat Linux Server (RHEL) | Identitätsanwendungen |
| | Identity Manager-Engine |
| | Identitätsberichterstellung |
| | Identitätsdepot |
| | iManager (Server) |
| | Ein SSO-Anbieter |
| | PostgreSQL |
| | Remote Loader |
| | Zurücksetzen von Passwörtern per Selbstbedienung |
| | Sentinel Log Management für IGA |
| | Tomcat |
| SUSE Linux Enterprise Desktop (SLED) | Designer |

| Plattform | Komponente |
|---|---|
| SUSE Linux Enterprise Server (SLES) | Analyzer |
| | Designer |
| | Identitätsanwendungen |
| | Identity Manager-Engine |
| | Identitätsberichterstellung |
| | Identitätsdepot |
| | iManager (Server) |
| | Ein SSO-Anbieter |
| | PostgreSQL |
| | Remote Loader |
| | Zurücksetzen von Passwörtern per Selbstbedienung |
| | Sentinel Log Management für IGA |
| | Tomcat |
| Windows Desktop | Designer |
| | iManager Workstation (Client) |
| | Browserzugriff auf die Identitätsanwendungen und die Identitätsberichterstellung |
| Windows Server | Analyzer |
| | Designer |
| | Identitätsanwendungen |
| | Identity Manager-Engine |
| | Identitätsberichterstellung |
| | Identitätsdepot |
| | iManager (Server) |
| | .NET Remote Loader |
| | Ein SSO-Anbieter |
| | PostgreSQL |
| | Remote Loader |
| | Zurücksetzen von Passwörtern per Selbstbedienung |
| | Tomcat |

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

- „Planen der Installation von Analyzer“, auf Seite 435
- „Planen der Installation von Designer“, auf Seite 247

- „Planen der Installation von iManager“, auf Seite 217
- „Installieren des Identitätsdepots“, auf Seite 67
- „Planen der Installation der Engine, der Treiber und der Plugins“, auf Seite 141
- „Planen der Installation der Identitätsanwendungen“, auf Seite 297
- „Planen der Installation der Passwortverwaltung für Identity Manager“, auf Seite 281
- „Planen der Installation von PostgreSQL und Tomcat“, auf Seite 257

## 5.4 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.

Vor Identity Manager 4.6 wurden die Identity Manager Advanced Edition und Standard Edition jeweils in separaten ISO-Dateien bereitgestellt. In Identity Manager 4.6 vereint NetIQ diese beiden Editions 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 53.7, „Aktivieren von Identity Manager“, auf Seite 486.

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.

## 5.5 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.

---

| Portnummer | Komponente auf dem Computer | Verwendung durch den Port |
|---|---|---|
| 389 | Identitätsdepot | Für die LDAP-Kommunikation in Klartext mit Identity Manager-Komponenten |
| 435 | 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 |
| 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<br>**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<br>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<br>**HINWEIS:** Jeder Instanz des Remote Loader muss ein eindeutiger Port zugewiesen werden. |
| 8109 | Identitätsanwendungen | Nur bei Verwendung der integrierten Installation<br>Wird von Tomcat für die Kommunikation mit einem Web-Connector über das AJP-Protokoll anstatt über HTTP verwendet |
| 8180 | Identitätsanwendungen | Wird vom Anwendungsserver (z. B. Tomcat), auf dem die Identitätsanwendungen ausgeführt werden, für die HTTP-Kommunikation verwendet |
| 8443 | Identitätsanwendungen<br>iManager | Wird von Tomcat für die HTTPS-Kommunikation (SSL-Kommunikation) oder zum Umleiten von Anforderungen für die SSL-Kommunikation verwendet |

| Portnummer | Komponente auf dem Computer | Verwendung durch den Port |
|---|---|---|
| 8543 | Identitätsanwendungen | *Standardmäßig keine Überwachung*<br>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 PostgreSQL-Datenbank-Sentinel 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 |

## 5.6 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, ändern Sie die Ländereinstellung in Windows mit der Option **Ländereinstellungen**. Unter Linux legen Sie die LANG-Variable im Profil oder über die Befehlszeile fest.

### 5.6.1 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.

| Ländereinstellung | Designer | Identity Manager-Engine | iManager | iManager-Plugins | Identitätsan-wendungen |
|---|---|---|---|---|---|
| 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 |

| Ländereinstellung | Designer | Identity Manager-Engine | iManager | iManager-Plugins | Identitätsanwendungen |
|---|---|---|---|---|---|
| Italienisch | Ja | – | Ja | – | Ja |
| Japanisch | Ja | Ja | Ja | Ja | Ja |
| Portugiesisch (Brasilien | Ja | – | Ja | – | Ja |
| Russisch | – | – | Ja | – | Ja |
| Spanisch | Ja | – | Ja | – | Ja |
| Schwedisch | – | – | – | – | Ja |

Identitätsanwendungen umfassen das Dashboard, den Katalogadministrator, die Identitätsberichterstellung, die Identitätsgenehmigungen und die Benutzeranwendung.

## 5.6.2 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.
- Wenn Sie Designer auf Computern mit Linux-Betriebssystem installieren, müssen Sie auch 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.

# 5.7 Herunterladen der Installationsdateien

NetIQ stellt ISO-Dateien mit allen Komponenten für die vollständige Identity Manager-Installation bereit. Jede Datei enthält die Versionen des Produkts. Aus dem Namen der ISO-Datei ist die jeweilige Plattform ersichtlich. Beispiel: `Identity_Manager_`*`Version`*`_Linux.iso`.

---

**HINWEIS:** Die ISO-Image-Dateien sind sehr groß. Laden Sie sie auf ein Volume oder eine DVD herunter, auf die die Dateigröße passt.

---

**So laden Sie die Installationsdateien für Identity Manager herunter:**

1. Gehen Sie zur NetIQ Downloads-Website.
2. Wählen Sie im Menü **Produkt oder Technologie** den Eintrag **Identity Manager** aus, und klicken Sie auf **Suchen**.
3. Klicken Sie auf der Download-Website von NetIQ Identity Manager auf die Schaltfläche **Download** neben der herunterzuladenden ISO-Datei.
4. Befolgen Sie die Bildschirmanweisungen, um die Datei in einen Ordner auf Ihrem Computer herunterzuladen.
5. Mounten Sie die heruntergeladene `.iso`-Datei als Volume oder verwenden Sie die `.iso`-Datei zum Erstellen einer DVD der Software.

# 6 Überlegungen und Voraussetzungen für die 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.



## 6.1 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:
  - Identitätsdepot
  - Identity Manager-Engine
  - Remote Loader
  - Identitätsanwendungen mit Ausnahme der Identitätsberichterstellung
- Verwalten Sie die Verfügbarkeit Ihrer Netzwerkressourcen für die Identity Manager-Umgebung, indem Sie die SUSE Linux Enterprise High Availability Extension des SUSE Linux Enterprise Servers (SLES) 11 SP4 oder höher mit den neuesten Patches verwenden.
- 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 5.3.4, „Empfohlene Servereinrichtung“, auf Seite 53 |
| Konfigurieren der SLES High Availability Extension | *SUSE Linux Enterprise High Availability Extention 11.SP4* |
| Einrichten einer Hochverfügbarkeitsumgebung unter SLES | Anhang A, „Beispiellösung für eine Identity Manager-Clusterbereitstellung“, auf Seite 575 |

| Weitere Informationen zum... | Erklärt in... |
|---|---|
| Ausführen des Identitätsdepots in einem Cluster | Abschnitt 7.2.4, „Voraussetzungen für die Installation des Identitätsdepots in einer Cluster-Umgebung“, auf Seite 74<br><br>Bereitstellen von eDirectory in Hochverfügbarkeits-Clustern im *NetIQ eDirectory-Installationshandbuch* |
| Ausführen der Identitätsanwendungen in einem Cluster | Abschnitt 32.5, „Konfigurieren von OSP und SSPR für Clustering“, auf Seite 291<br><br>Abschnitt 33.3.4, „Voraussetzungen für die Installation der Identitätsanwendungen in einer Cluster-Umgebung“, auf Seite 305<br><br>Abschnitt 36.2, „Aktivieren des Berechtigungsindex für das Clustering“, auf Seite 320<br><br>Abschnitt 36.4, „Vorbereiten eines Clusters für die Identitätsanwendungen“, auf Seite 322<br><br>Abschnitt 38.2, „Konfigurieren des Benutzeranwendungstreibers für das Clustering“, auf Seite 352<br><br>Abschnitt 39.6.4, „Aktualisieren der SSPR-Links im Dashboard für eine dezentrale Umgebung oder eine Cluster-Umgebung“, auf Seite 364 |
| Einrichten der Identitätsanwendungen in einem Cluster unter SLES/RHEL | Anhang C, „Beispiel einer Bereitstellungslösung für Identitätsanwendungen in einem Cluster auf einem Tomcat-Anwendungsserver“, auf Seite 589 |

## 6.2 Mindestspeicheranforderungen auf Linux-Servern

Die Identity Manager-Komponenten haben Mindestspeicheranforderungen

In Tabelle 6-1 auf Seite 62 sehen Sie, wie viel sicherer Speicherplatz mindestens für die verschiedenen Komponenten erforderlich ist:

***Tabelle 6-1*** *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 |

Stellen Sie bei der Installation sicher, dass für den `/temp`-Ordner 5 GB freier Speicherplatz zur Verfügung stehen.

## 6.3 Installieren von Identity Manager auf Servern mit SLES 12 SP1 (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 SP1 (oder höher) installiert sein.

- `libXtst6-32bit-1.2.1-4.4.1.x86_64`
- `libXrender-32bit`
- `libXi6-32bit`

Im Allgemeinen können Sie die `.rpm`-Dateien von einer Website herunterladen, beispielsweise von http://rpmfind.net/linux. `libXtst6-32bit-1.2.1-4.4.1.x86_64.rpm` steht beispielsweise auf dieser Webseite zum Herunterladen bereit.

## 6.4 Installieren von Identity Manager auf einem RHEL 6.*x*- oder 7.*x*-Server

Wenn Identity Manager auf einem Server mit dem Betriebssystem Red Hat Enterprise Linux 6.*x*- oder 7.*x* installiert werden soll, muss der Server bestimmte Voraussetzungen erfüllen.


- Abschnitt 6.4.1, „Voraussetzungen für die Installation unter RHEL 6.*x* oder 7.*x*“, auf Seite 63
- Abschnitt 6.4.2, „Überprüfen der Voraussetzungen“, auf Seite 64
- Abschnitt 6.4.3, „Prüfen der abhängigen Bibliotheken für den Server“, auf Seite 64
- Abschnitt 6.4.4, „Erstellen eines Repository für die Installationsmedien“, auf Seite 65


### 6.4.1 Voraussetzungen für die Installation unter RHEL 6.*x* oder 7.*x*

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:

  ```
  127.0.0.1 test-system localhost.localdomain localhost
  ```

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

  ```
  127.0.0.1 localhost.localdomain localhost
  10.77.11.10 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 Abschnitt 6.4.3, „Prüfen der abhängigen Bibliotheken für den Server“, auf Seite 64.

## 6.4.2 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.

## 6.4.3 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
```

---

- **Geführte Installation (Benutzeroberfläche):**
  - `libXau-*.i686.rpm`
  - `libxcb-*.i686.rpm`
  - `libX11-*.i686.rpm`
  - `libXext-*.i686.rpm`
  - `libXi-*.i686.rpm`
  - `libXtst-*.i686.rpm`
  - `glibc-*.i686.rpm`
  - `libstdc++-*.i686.rpm`
  - `libgcc-*.i686.rpm`
  - `compat-libstdc++-33-*.x86_64.rpm`
  - `compat-libstdc++-33-*.i686.rpm`
  - `libXrender-*.i686.rpm`
- **Installation über Befehlszeile (Konsole oder automatisch):**
  - `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`

## 6.4.4 Erstellen eines Repository für die Installationsmedien

Wenn auf dem RHEL 6.x- oder 7.x-Server ein Repository für die Installationsmedien benötigt wird, 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 Abschnitt 6.4.3, „Prüfen der abhängigen Bibliotheken für den Server“, auf Seite 64.
- 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 RHEL 6.x- oder 7.x-ISO 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 6. 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 compat-libstdc++-33.x86_64"

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

---

**HINWEIS:** Das Skript findet die libstdc++.i686-Bibliothek im 64-Bit-Repository nicht – es sei denn, Sie haben das 64-Bit-Repository zu einem 32-Bit-Repository geändert (siehe Schritt 6).

---

7 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 RHEL-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
```

---

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

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

10 Installieren Sie Identity Manager 4.6.

# II Installieren des Identitätsdepots

In diesem Abschnitt finden Sie die Schritte für die Installation der erforderlichen Komponenten für das Identitätsdepot, in dem Informationen zu Identity Manager gespeichert werden, beispielsweise Treiberkonfigurationen, Parameter und Richtlinien.

Die Installationsdateien befinden sich im Verzeichnis `products/eDirectory/`*`Prozessortyp`*`/` in der `.iso`-Image-Datei des Identity Manager-Installationspakets. Standardmäßig installiert das Installationsprogramm das Identitätsdepot in den folgenden Speicherorten:

- **Linux:** `/opt/novell/eDirectory`
- **Windows:** `C:\Novell\Directory`

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie in Kapitel 7, „Planen der Installation des Identitätsdepots“, auf Seite 69.

# 7 Planen der Installation des Identitätsdepots

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.



## 7.1 Checkliste für die Installation des Identitätsdepots

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 3.3.1, „Identitätsdepot“, auf Seite 32. |
| ❑ | 2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.3.4, „Empfohlene Servereinrichtung“, auf Seite 53. |
| ❑ | 3. Legen Sie fest, ob ein Sentinel vor der Installation des Identitätsdepots installiert werden soll. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |
| ❑ | 4. Lesen Sie die Überlegungen zur Installation des Identitätsdepots, und prüfen Sie, ob die Computer den Voraussetzungen entsprechen. Weitere Informationen finden Sie in Abschnitt 7.2, „Voraussetzungen und Überlegungen für die Installation des Identitätsdepots“, auf Seite 71. |
| ❑ | 5. Prüfen Sie die Hardware- und Software-Voraussetzungen der Computer, auf denen das Identitätsdepot gehostet werden soll. Weitere Informationen finden Sie in Abschnitt 7.7, „Systemanforderungen für das Identitätsdepot“, auf Seite 81. |
| ❑ | 6. Informieren Sie sich, wie Sie Escape-Zeichen im Namen eines Containers im Identitätsdepot nutzen, der einen Punkt („.“) enthält. Weitere Informationen finden Sie in Abschnitt 8.1, „Verwenden von Escape-Zeichen im Namen eines Containers, der einen Punkt („.“) enthält“, auf Seite 83. |

| | Checkliste |
|---|---|
| ❑ | 7. Informieren Sie sich, wie Sie das Identitätsdepot in einer Umgebung verwenden, in der IPv6-Adressen genutzt werden. Weitere Informationen finden Sie in Abschnitt 8.4, „Verwenden von IPv6-Adressen auf dem Identitätsdepot-Server“, auf Seite 89. |
| ❑ | 8. Informieren Sie sich über die erforderlichen Ports für die LDAP-Kommunikation. Weitere Informationen finden Sie in Abschnitt 8.5, „Kommunizieren mit dem Identitätsdepot über LDAP“, auf Seite 91. |
| ❑ | 9. Stellen Sie sicher, dass ein SLP-Dienst (Service Location Protocol) installiert ist und dass die SLPDAs stabil sind bzw. dass die Datei `hosts.nds` konfiguriert ist. Weitere Informationen finden Sie in Abschnitt 8.2, „Auflösen von Baumnamen mit OpenSLP oder hosts.nds“, auf Seite 84. |
| ❑ | 10. (Bedingt) Wenn Sie das Identitätsdepot als Nicht-Root-Benutzer installieren möchten, stellen Sie sicher, dass Ihre Umgebung die Bedingungen für die Installation erfüllt. Weitere Informationen finden Sie in Abschnitt 7.2.2, „Voraussetzungen für die Installation des Identitätsdepots als Nicht-Root-Benutzer“, auf Seite 73. |
| ❑ | 11. (Bedingt) Bei der Installation auf einem Linux-Server befolgen Sie die Anweisungen in einem der folgenden Abschnitte:<br>◆ Anweisungen zum Installieren als `Root` finden Sie in Abschnitt 9.1, „Installieren des Identitätsdepots als Root“, auf Seite 99.<br>◆ Anweisungen zum Installieren als Nicht-`Root`-Benutzer finden Sie in Abschnitt 9.2, „Installieren des Identitätsdepots als Nicht-Root-Benutzer“, auf Seite 101. |
| ❑ | 12. (Bedingt) Bei der Installation auf einem Windows-Server befolgen Sie die Anweisungen in einem der folgenden Abschnitte:<br>◆ Anweisungen zur geführten Installation (Assistent) finden Sie in Abschnitt 10.1, „Installieren des Identitätsdepots mit dem Assistenten auf einem Windows-Server“, auf Seite 105.<br>◆ Anweisungen zur automatischen (unbeaufsichtigten) Installation finden Sie in Abschnitt 10.2, „Automatische Installation und Konfiguration des Identitätsdepots auf einem Windows-Server“, auf Seite 107. |
| ❑ | 13. Wenden Sie Hotfix 2 auf das Identitätsdepot an. Weitere Informationen finden Sie in Kapitel 11, „Anwenden von HotFix 2 auf das Identitätsdepot“, auf Seite 115. |
| ❑ | 14. Konfigurieren Sie NetIQ Secret Store. Weitere Informationen finden Sie in Abschnitt 12.1.2, „Hinzufügen von SecretStore zum Identitätsdepotschema“, auf Seite 123. |
| ❑ | 15. (Optional) Schließen Sie das DIB-Verzeichnis auf dem eDirectory-Server von allen Antiviren- und Sicherungssoftware-Verfahren aus. |
| ❑ | 16. (Optional) Sichern Sie das DIB-Verzeichnis Weitere Informationen finden Sie unter „Backing Up and Restoring NetIQ eDirectory“ (Sichern und Wiederherstellen von NetIQ eDirectory) im *NetIQ eDirectory -Administrationshandbuch*. |
| ❑ | 17. Installieren Sie die Identity Manager-Engine. Weitere Informationen finden Sie in Kapitel 16, „Vorbereiten der Installation der Engine, der Treiber und der Plugins“, auf Seite 147. |

## 7.2 Voraussetzungen und Überlegungen für die Installation des Identitätsdepots

Das Identitätsdepot nutzt ein Verzeichnis, in dem die Objekte gespeichert werden, die anhand der Identity Manager-Lösung synchronisiert werden. In den nachfolgenden Abschnitten finden Sie Hinweise, mit denen Sie die Bereitstellung von NetIQ eDirectory als Rahmenwerk für das Identitätsdepot planen können.



### 7.2.1 Voraussetzungen für die Installation des Identitätsdepots

NetIQ empfiehlt, vor der Installation von eDirectory als Rahmenwerk für das Identitätsdepot die folgenden Überlegungen zu lesen:

- Vor dem Installieren von eDirectory muss eine Methode vorliegen, mit der die Baumnamen in Serververweisadressen aufgelöst werden. NetIQ empfiehlt die Verwendung von SLP-Diensten (Service Location Protocol). Bei älteren Versionen von NetIQ eDirectory (vor Version 8.8) wurde SLP während der Installation mitinstalliert. Ab Version 8.8 muss SLP jedoch separat installiert werden. Alternativ können Sie die Baumnamen mithilfe des Flatfiles `hosts.nds` auflösen. Weitere Informationen finden Sie in Abschnitt 8.2, „Auflösen von Baumnamen mit OpenSLP oder hosts.nds“, auf Seite 84.
- (Bedingt) Bei der Installation auf einem Linux-Server müssen Sie Multicast-Routing für den Host mit 224.0.0.0 in der Routing-Tabelle aktivieren. Geben Sie beispielsweise den folgenden Befehl ein:

  ```
  route add -net 224.0.0.0 netmask 240.0.0.0 dev interface
  ```

  Hierbei gilt: *interface* steht für einen Wert wie eth0, hme0, hme1 oder hme2, abhängig von der Netzwerkschnittstellenkarte.
- (Bedingt) Zur geführten Installation auf einem Server mit SLES 12 SP1 (oder höher) müssen die Bibliotheken `libXtst6-32bit-1.2.1-4.4.1.x86_64`, `libXrender-32bit` und `libXi6-32bit` auf dem Server installiert sein.
- Damit die eDirectory-Infrastruktur effizient funktioniert, müssen Sie eine statische IP-Adresse auf dem Server konfigurieren. Wenn Sie DHCP-Adressen auf dem Server verwenden, liefert eDirectory unter Umständen unvorhersehbare Ergebnisse.
- Synchronisieren Sie die Uhrzeit auf allen Netzwerkservern. NetIQ empfiehlt die Option `ntp` von NTP (Network Time Protocol).
- (Bedingt) Wenn ein Sekundärserver installiert werden soll, müssen alle Reproduktionen in der Partition, auf der Sie das Produkt installieren, den Status ON aufweisen.
- (Bedingt) Soll ein Sekundärserver in einem vorhandenen Baum als Nicht-Administrator-Benutzer installiert werden, erstellen Sie einen Container, und partitionieren Sie ihn. Vergewissern Sie sich, dass Sie die folgenden Rechte besitzen:
  - Supervisor-Rechte für die Partition, der der Server hinzugefügt werden soll.
  - (Windows) Supervisor-Rechte für den Container, dem der Server hinzugefügt werden soll.

- Alle Attributrechte: Rechte zum Lesen, Vergleichen und Schreiben für das Objekt W0.KAP.Security.
- Attributrechte: Rechte zum Lesen und Vergleichen für das Security-Containerobjekt.
- Eingaberechte: Rechte zum Durchsuchen für das Security-Containerobjekt.

Diese Rechte sind für das Hinzufügen der Reproduktion erforderlich, wenn weniger als drei Reproduktionen vorhanden sind.

- (Bedingt) Soll ein Sekundärserver in einem vorhandenen Baum als Nicht-Administrator-Benutzer installiert werden, muss mindestens einer der Server im Baum dieselbe oder eine höhere eDirectory-Version aufweisen als der Sekundärserver, der als Container-Admin hinzugefügt werden soll. Wenn der hinzuzufügende Sekundärserver eine höhere Version aufweist, muss der Administrator des Baums das Schema erweitern, bevor der Sekundärserver über den Container-Admin hinzugefügt wird.
- Beim Konfigurieren von eDirectory müssen Sie einen NCP-Port (NetWare Core Protocol) in der Firewall aktivieren (standardmäßig 524), um das Hinzufügen des Sekundärservers zu ermöglichen. Abhängig von Ihren Anforderungen können Sie außerdem die folgenden standardmäßigen Dienstports aktivieren:
  - LDAP-Klartext – 389
  - LDAP-Klartext – 636
  - HTTP-Klartext – 8028
  - HTTP-Klartext – 8030
- Novell International Cryptographic Infrastructure (NICI) muss auf jeder Arbeitsstation installiert werden, auf der Verwaltungsdienstprogramme für eDirectory (z. B. iManager) verwendet werden. NICI und eDirectory unterstützen Schlüsselgrößen bis 4096 Bit.

  Unter Linux wird NICI mit dem Installationsprogramm `nds-install` für das Identitätsdepot automatisch installiert. Sie können NICI jedoch auch manuell installieren. Weitere Informationen finden Sie unter „Installieren von NICI“ im *NetIQ eDirectory-Installationshandbuch*.
- (Bedingt) NICI 2.7 und eDirectory 8.8.x unterstützen Schlüsselgrößen bis 4096 Bit. Soll ein Schlüssel mit 4 KB verwendet werden, müssen Sie alle Server auf die unterstützte Version von eDirectory aufrüsten. Außerdem muss NICI 2.7 auf jeder Arbeitsstation installiert werden, auf der Verwaltungsdienstprogramme (z. B. iManager oder ConsoleOne) verwendet werden.

  Wenn Sie den Zertifizierungsstellen-Server (CA-Server) auf eine unterstützte Version von eDirectory aufrüsten, bleibt die Schlüsselgröße unverändert bei 2 KB. Soll ein Schlüssel mit 4 KB erstellt werden, müssen Sie die CA auf dem aufgerüsteten eDirectory-Server erneut erstellen. Beim Erstellen der CA müssen Sie außerdem die standardmäßige Schlüsselgröße von 2 KB auf 4 KB erhöhen.
- (Bedingt) Wenn der Name eines Containers im eDirectory-Baum einen Punkt enthält, müssen Sie die Parameter für den Admin-Namen, den Admin-Kontext und den Serverkontext während der Installation und auch beim Hinzufügen eines Servers zu einem vorhandenen Baum mithilfe von Escape-Zeichen angeben. Weitere Informationen finden Sie in Abschnitt 8.1, „Verwenden von Escape-Zeichen im Namen eines Containers, der einen Punkt („.“) enthält“, auf Seite 83.
- Wenden Sie zur Unterstützung der LDAP-Suche mit Virtual List View(VLV)- und Server Side Sort(SSS)-Steuerelementen Hotfix 2 unter eDirectory 9.0.2 oder eDirectory 8.8.8 Patch 9 an. Weitere Informationen finden Sie unter Kapitel 11, „Anwenden von HotFix 2 auf das Identitätsdepot“, auf Seite 115.

  Wenn Sie eDirectory mit dem integrierten Installationsprogramm installiert haben, ist dieser Hotfix nicht erforderlich. Das integrierte Installationsprogramm installiert eine aktualisierte Version von eDirectory, auf die dieser Hotfix bereits angewendet wurde.

## 7.2.2 Voraussetzungen für die Installation des Identitätsdepots als Nicht-Root-Benutzer

Zur Installation des Identitätsdepots als Nicht-Root-Benutzer muss die Umgebung die folgenden Bedingungen erfüllen:

- Es ist nicht möglich, das Identitätsdepot als Nicht-Root-Benutzer in einer Cluster-Umgebung zu installieren.
- Ein Root-Benutzer muss den SNMP-Subagenten (NOVsubag) auf dem Server installieren und konfigurieren.

  **So installieren SieNovsubag:**

  Geben Sie den folgenden Befehl ein: `rpm -ivh --nodeps NOVLsubag_RPM_Dateiname_mit_Pfad`.

  **So konfigurieren Sie SNMP:**

  Exportieren Sie die Pfade für die Umgebungsvariablen manuell mit dem folgenden Befehl:

  ```
  export LD_LIBRARY_PATH=custom_location/opt/novell/eDirectory/lib64:/opt/
  novell/eDirectory/lib64/nds-modules:/opt/novell/lib64:$LD_LIBRARY_PATH
  export PATH=/opt/novell/eDirectory/bin:$PATH
  export MANPATH=/opt/novell/man:$MANPATH
  ```

  Beispiel:

  ```
  rpm -ivh --nodeps novell-NOVLsubag-8.8.1-5.i386.rpm
  ```

- (Bedingt) Wenn SLP und SNMP für den Identitätsdepot-Server verwendet werden sollen, müssen Sie diese Dienste als Root installieren.
- Das Nicht-Root-Benutzerkonto, mit dem das Identitätsdepot installiert wird, muss Schreibrechte auf das Verzeichnis besitzen, in dem die Installation erfolgen soll.

## 7.2.3 Voraussetzungen für die Installation des Identitätsdepots auf einem Windows-Server

NetIQ empfiehlt, vor der Installation des Identitätsdepots auf einem Windows-Server die folgenden Überlegungen zu lesen:

- Sie müssen Administratorrechte für den Windows-Server und alle Bereiche des eDirectory-Baums besitzen, die domänenfähige Benutzerobjekte enthalten. Bei der Installation in einem vorhandenen Baum benötigen Sie Verwaltungsrechte für das Baumobjekt, um das Schema zu erweitern und Objekte zu erzeugen.
- (Bedingt) Vor einer automatischen (unbeaufsichtigten) Installation müssen Sie die folgende Software auf dem Zielserver installieren:
  - Microsoft Visual C++ 2005 und Microsoft Visual C++ 2012 Redistributable Packages. Standardmäßig befinden sich die Installationsdateien `vcredist_x86.exe` und `vcredist_x64.exe` im Ordner `eDirectory\Windows\x64\redist_pkg`.
  - NICI (Novell International Cryptographic Infrastructure), sowohl für 32 Bit als auch für 64 Bit. Standardmäßig befinden sich die Installationsdateien im Ordner `eDirectory/Windows/`*`Prozessortyp`*`/nici`.

- Da NTFS einen sichereren Transaktionsprozess bietet als ein Dateisystem mit FAT, können Sie eDirectory nur in einer NTFS-Partition installieren. Wenn Sie nur Dateisysteme mit FAT haben, führen Sie daher einen der folgenden Punkte aus:
  - Verwenden Sie den Festplatten-Manager. Weitere Informationen hierzu finden Sie in der Dokumentation zu Windows Server.
  - Erzeugen Sie eine neue Partition und formatieren Sie sie als NTFS.
  - Wandeln Sie ein vorhandenes FAT-Dateisystem mit dem Befehl CONVERT in NTFS um.
  - Weitere Informationen hierzu finden Sie in der Dokumentation zu Windows Server.

  Wenn Ihr Server nur ein FAT-Dateisystem hat und Sie es versäumen, diesen Prozess zu überwachen, fordert Sie das Installationsprogramm auf, eine NTFS-Partition bereitzustellen.
- Die aktuelle Version des Windows-SNMP-Dienstes muss ausgeführt werden.
- Vor Beginn des Installationsvorgangs muss das Windows-Betriebssystem mit den aktuellen Service Packs aufgerüstet werden.
- Bei der Installation auf einem virtuellen Computer, der eine DHCP-Adresse aufweist, oder auf einem physischen oder virtuellen Computer, auf dem SLP nicht übertragen wird, muss der Verzeichnisagent im Netzwerk konfiguriert werden. Weitere Informationen finden Sie in Abschnitt 8.2.2, „Erläuterungen zu OpenSLP“, auf Seite 85.

### 7.2.4 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:

- Es müssen mindestens zwei Windows- oder Linux-Server mit Clustersoftware vorhanden sein.
- Die Clustersoftware muss externen gemeinsam genutzten Speicher unterstützen, wobei ausreichend Speicherplatz für alle Identitätsdepot- und NICI-Daten vorhanden sein muss:
  - Die Identitätsdepot-DIB muss sich im gemeinsam genutzten Clusterspeicher befinden. Die Zustandsdaten für das Identitätsdepot müssen sich im gemeinsam genutzten Speicher befinden, damit sie für den Clusterknoten verfügbar sind, der zurzeit die Dienste ausführt.
  - Die Root-Identitätsdepot-Instanz auf den Clusterknoten muss so konfiguriert sein, dass sie die DIB des gemeinsamen Speichers verwendet.
  - Auch die NICI-Daten (NetIQ International Cryptographic Infrastructure) müssen gemeinsam genutzt werden, damit serverspezifische Schlüssel zwischen den Clusterknoten reproduziert werden. Die von allen Clusterknoten verwendeten NICI-Daten müssen sich im gemeinsam genutzten Clusterspeicher befinden.
  - 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*.

## 7.3 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.

## 7.4 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 77.
  - **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.

## 7.5 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.

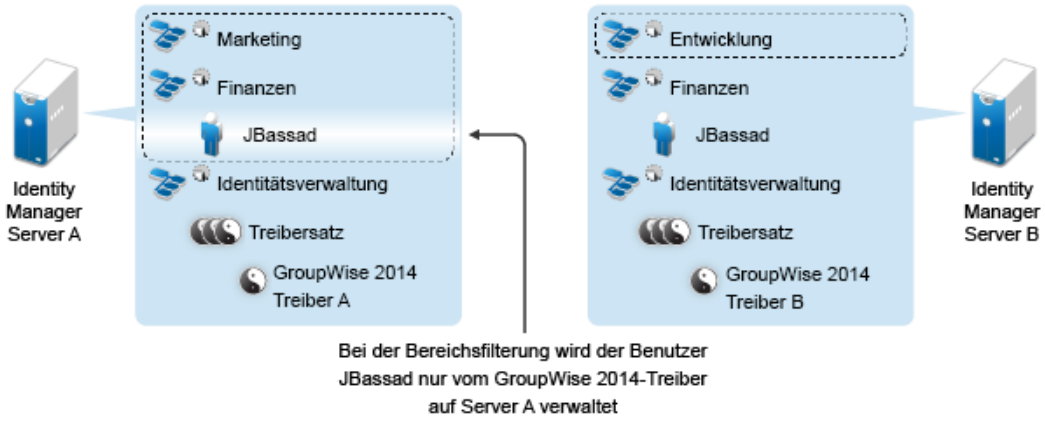
---

**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 7-1 auf Seite 78 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 7-1*** *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“.

## 7.6 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.<br>Dieses Paket enthält folgende Elemente:<br>◆ Beglaubigungswerkzeuge, die auch die für eDirectory benötigte RSA-Beglaubigung enthalten.<br>◆ Plattformunabhängige Systemabstraktions-Bibliothek, Bibliothek mit allen definierten Funktionen des Directory User Agent und Schemaerweiterungs-Bibliothek.<br>◆ Kombiniertes Konfigurations- und Testprogramm für Directory User Agent.<br>◆ 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. |
| `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:<br>◆ 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.<br>◆ eDirectory-Server-Daemon.<br>◆ Binärdatei für DNS und Binärdatei zum Laden und Entladen von LDAP.<br>◆ 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.<br>◆ Start-Scripts für DNS, NDSD und NLDAP.<br>◆ Handbuchseiten. |

| Paket | Beschreibung |
|---|---|
| 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:<br>◆ ldapdelete<br>◆ ldapmodify<br>◆ ldapmodrdn<br>◆ ldapsearch<br>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. |
| 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. |

# 7.7 Systemanforderungen für das Identitätsdepot

In diesem Abschnitt finden Sie die Mindestanforderungen für die Server, auf denen das Identitätsdepot installiert werden soll. Überprüfen Sie die Voraussetzungen und Überlegungen zur Installation, insbesondere im Zusammenhang mit dem Betriebssystem.

| Kategorie | Anforderung |
|---|---|
| Prozessor | 1 GHz |
| Festplattenspeicher | ◆ 300 MB für das Identitätsdepot<br>◆ 150 MB zusätzlicher Festplattenspeicher pro 50.000 Benutzer |
| Arbeitsspeicher | 2 GB |
| Betriebssystem (zertifiziert) | Eines der folgenden 64-Bit-Betriebssysteme:<br>◆ Open Enterprise Server 2015 SP1<br>◆ Open Enterprise Server 11 SP2<br>◆ Red Hat Enterprise Linux 7.3<br>◆ Red Hat Enterprise Linux 6.8<br>◆ SUSE Linux Enterprise Server 12 SP1<br>◆ SUSE Linux Enterprise Server 11 SP4<br>◆ Windows Server 2012 R2<br>◆ Windows Server 2012<br>NetIQ empfiehlt, vor der Installation von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden.<br>**HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird. |
| Betriebssystem (unterstützt) | Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme<br>**HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert. |
| Virtualisierungssystem | ◆ Hyper-V Server 2012 R2<br>◆ VMWare ESX 5.0 und höher<br>◆ Windows Server 2012 R2-Virtualisierung mit Hyper-V (unterstützt)<br>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 |
| --- | --- |
| Verzeichnisservices | NetIQ eDirectory 8.8.8 Patch 9 Hotfix 2 (wird mit iManager 2.7.7 Patch 9 oder höher ausgeführt)<br><br>Alternativ:<br><br>NetIQ eDirectory 9.0.2 Hotfix 2 (wird mit iManager 3.0.2 Patch 1 oder höher ausgeführt)<br><br>**HINWEIS:** NetIQ hat einige Beschränkungen für die Installation von eDirectory 9.0.2 als Identitätsdepot festgelegt. Weitere Informationen finden Sie unter Abschnitt 8.8, „Arbeiten mit eDirectory 9.0.2 oder höher“, auf Seite 96. |
| Webbrowser | Einer der folgenden Browser (ggf. höhere Version):<br><br>◆ Google Chrome 51<br>◆ Microsoft Internet Explorer 11<br>◆ Mozilla Firefox 46 |

# 8 Vorbereiten der Installation des Identitätsdepots

Die Umgebung für das Identitätsdepot muss entsprechend konfiguriert werden. Der Server muss beispielsweise mit einer Methode (einem Dienst oder einer bestimmten Datei) konfiguriert werden, mit der die Baumnamen im Identitätsdepot in Serververweisadressen aufgelöst werden können. In diesem Abschnitt erfahren Sie, wie Sie Ihre Umgebung auf die Installation des Identitätsdepots vorbereiten.

## 8.1 Verwenden von Escape-Zeichen im Namen eines Containers, der einen Punkt („.“) enthält

Sie können einen Windows- oder Linux-Server, dessen Name einen Punkt enthält, in einen Verzeichnisbaum aufnehmen. Beispiel: `O=netiq.com` oder `C=u.s.a`. Wenn der Name eines Containers im Baum einen Punkt („.“) enthält, müssen Sie jedoch ein Escape-Zeichen verwenden. Beachten Sie die folgenden Überlegungen:

- **Linux:**
  - Beim Angeben der Parameter für Admin-Name, Admin-Kontext und Serverkontext schließen Sie die Parameter jeweils in Anführungszeichen ein.
  - Stellen Sie dem Punkt im Containernamen einen umgekehrten Schrägstrich („\“) voran.
  - Beim Installieren des Identitätsdepots geben Sie beispielsweise den folgenden Installationsbefehl ein:

    ```
    ndsconfig new -a 'admin.netiq.com' -t netiq_tree -n
    'OU=servers.O=netiq\.com'
    ```

- **Windows:**
  - Ein Servername darf nicht mit einem Punkt beginnen. Beispiel: `.netiq`.
  - Stellen Sie dem Punkt im Containernamen einen umgekehrten Schrägstrich („\“) voran. Beispiel:

    ```
    O=novell\.com
    ```

    Alternativ:

    ```
    C=a\.b\.c
    ```

Wenn Sie Admin-Namen und Admin-Kontexte, die einen Punkt enthalten, für Dienstprogramme wie iMonitor, iManager, DHost iConsole, DSRepair, Backup, DSMerge, DSLogin oder ldapconfig eingeben, verwenden Sie jeweils ein Escape-Zeichen. Wenn Sie sich beispielsweise bei iMonitor anmelden und der Organisationsname im Baum `netiq.com` lautet, geben Sie entsprechend `'admin.netiq\.com'` oder `admin.netiq\.com` ein.

## 8.2 Auflösen von Baumnamen mit OpenSLP oder hosts.nds

Vor dem Installieren der Identitätsdepot-Infrastruktur muss der Server eine Methode (ein Dienst oder eine bestimmte Datei) aufweisen, mit der die Baumnamen im Identitätsdepot in Serververweisadressen aufgelöst werden können. NetIQ empfiehlt die Auflösung der Baumnamen mit SLP-Diensten (Service Location Protocol). Bei älteren Versionen von eDirectory wurde OpenSLP während der Installation mitinstalliert. Ab eDirectory 8.8 ist OpenSLP jedoch nicht mehr in der Installation enthalten. Sie müssen einen SLP-Dienst separat installieren oder eine `hosts.nds`-Datei verwenden. Wenn Sie einen SLP-Dienst nutzen, müssen die Verzeichnisagenten für den Dienst (SLPDAs) stabil sein.

Dieser Abschnitt enthält die folgenden Informationen:



### 8.2.1 Auflösen von Baumnamen mit einer hosts.nds-Datei

Die Datei `hosts.nds` enthält eine statische Suchtabelle, in denen die Identitätsdepot-Anwendungen die Identitätsdepot-Partitionen und -Server suchen. Hiermit können Sie SLP-Multicast-Verzögerungen vermeiden, wenn kein SLP-DA im Netzwerk vorhanden ist. Geben Sie die folgenden Informationen für jeden Baum oder Server jeweils in einer eigenen Zeile in der Datei `hosts.nds` ein:

- **Servername oder Baumname:** Die Baumnamen müssen mit einem Punkt (.) enden.
- **Internetadresse:** Dies kann ein DNS-Name oder eine IP-Adresse sein. Verwenden Sie nicht `localhost`.
- **Serverport:** Optional; hängen Sie die Portnummer bei Bedarf mit einem Doppelpunkt (:) an die Internetadresse an.

Für den lokalen Server müssen Sie nur dann einen Eintrag in die Datei vornehmen, wenn der Server einen nicht standardmäßigen NCP-Port überwacht.

**So konfigurieren Sie eine hosts.nds-Datei:**

1. Erstellen Sie eine neue `hosts.nds`-Datei, oder öffnen Sie eine bereits vorhandene Datei.
2. Fügen Sie die folgenden Informationen hinzu:

   *partition_name.tree_name. host_name/ip-addr:port server_name dns-addr/ip-addr:port*

   Beispiel:

   ```
   # This is an example of a hosts.nds file:
   # Tree name Internet address/DNS Resolvable Name
     CORPORATE. myserver.mycompany.com
     novell.CORPORATE. 1.2.3.4:524

   # Server name Internet address
     CORPSERVER myserver.mycompany.com:524
   ```

3. (Optional) Wenn Sie sich später entscheiden, den Baumnamen mit SLP aufzulösen und die Verfügbarkeit des Identitätsdepots im Netzwerk sicherzustellen, ergänzen Sie die Datei `hosts.nds` mit dem folgenden Text:

```
/usr/bin/slptool findattrs services:ndap.novell///(svcname-ws==[treename or *])"
```

Soll beispielsweise nach Diensten gesucht werden, deren Attribut `svcname-ws` mit dem Wert `SAMPLE_TREE` übereinstimmt, geben Sie den folgenden Befehl ein:

```
/usr/bin/slptool findattrs services:ndap.novell///(svcname-ws==SAMPLE_TREE)"
```

---

**HINWEIS:** Führen Sie diesen Vorgang aus, sobald SLP und das Identitätsdepot installiert wurden.

---

Wenn ein Dienst mit dem Wert `SAMPLE_TREE` für das Attribut `svcname-ws` registriert ist, erhalten Sie die Ausgabe `service:ndap.novell:///SAMPLE_TREE` (Beispiel). Ansonsten erfolgt keine Ausgabe.

## 8.2.2 Erläuterungen zu OpenSLP

OpenSLP ist eine Open-Source-Implementierung des Standards IETF Service Location Protocol Version 2.0 (dokumentiert in IETF Request-For-Comments (RFC) 2608).

Die Schnittstelle des OpenSLP-Quellcodes ist eine Implementierung eines weiteren IETF-Standards für den programmtechnischen Zugriff auf die SLP-Funktionen (dokumentiert in RFC 2614).

In diesen Dokumenten wird die Funktionsweise von SLP umfassend erläutert. Lesen Sie daher die Dokumente, und machen Sie sich mit den Funktionen vertraut. Die Dokumente sind relativ komplex, sind jedoch für die richtige Konfiguration von SLP in einem Intranet unerlässlich.

Weitere Informationen zum OpenSLP-Projekt finden Sie auf den Websites von OpenSLP und SourceForge. Auf der OpenSLP-Website finden Sie mehrere Dokumente mit nützlichen Tipps für die Konfiguration. Zum Zeitpunkt der Veröffentlichung dieses Dokuments ist der Großteil der Dokumente auf der Website noch unvollständig.

Dieser Abschnitt umfasst die folgenden Diskussionen über die Verwendung von SLP und das Verhältnis zum Identitätsdepot:


- „NetIQ Service Location Providers“, auf Seite 85
- „Benutzeragenten“, auf Seite 86
- „Service-Agenten“, auf Seite 86
- „Verzeichnisagenten“, auf Seite 87


### NetIQ Service Location Providers

Die NetIQ-Version von SLP nimmt es nicht so genau mit dem SLP-Standard, damit eine robustere Umgebung für die Dienstbekanntgabe erstellt werden kann; dies geht allerdings zu Lasten der Skalierbarkeit.

Soll die Skalierbarkeit für ein Dienstbekanntgabe-Netzwerk erhöht werden, können Sie beispielsweise die Anzahl der Pakete begrenzen, die über ein Teilnetz per Rundsendung oder Multicast verteilt werden. In der SLP-Spezifikation werden hierzu die Verzeichnisagentenabfragen durch die Service- und Benutzeragenten eingeschränkt. Hierbei wird der zuerst ermittelte Verzeichnisagent, der für den gewünschten Bereich zuständig ist, für alle nachfolgenden Abfragen eines Service-Agenten (und damit auch der lokalen Benutzeragenten) zu diesem Bereich herangezogen.

Die NetIQ SLP-Implementierung durchsucht alle bekannten Verzeichnisagenten nach Abfrageinformationen. Eine Laufzeit von 300 Millisekunden gilt dabei als zu lang; somit können 10 Server in etwa 3 bis 5 Sekunden durchsucht werden. Dies ist nicht erforderlich, wenn SLP ordnungsgemäß im Netzwerk konfiguriert ist. (OpenSLP geht davon aus, dass das Netzwerk ordnungsgemäß für den SLP-Verkehr konfiguriert ist.) Die Zeitüberschreitungswerte für Antworten sind bei OpenSLP höher als beim SLP-Dienstanbieter von NetIQ, und die Anzahl der Verzeichnisagenten ist auf den zuerst antwortenden Agenten beschränkt, unabhängig davon, ob die Angaben dieses Agenten richtig und vollständig sind oder nicht.

## Benutzeragenten

Benutzeragenten (UA) treten physisch als statische oder dynamische Bibliothek auf, die mit einer Anwendung verknüpft ist. Die Anwendung kann dabei die SLP-Dienste abfragen. Der Benutzeragent bildet eine programmtechnische Schnittstelle, über die die Clients die Dienste abfragen und die Dienste sich selbst bekanntgeben. Ein Benutzeragent stellt eine Verbindung zu einem Verzeichnisagenten her und fragt registrierte Dienste einer bestimmten Dienstklasse in einem bestimmten Bereich ab.

Die Benutzeragenten ermitteln die Adresse des Verzeichnisagenten, an den die Abfragen gesendet werden sollen, mithilfe eines bestimmten Algorithmus. Sobald sie die Adresse eines Verzeichnisagenten (DA) für einen bestimmten Bereich erhalten, nutzen sie diese Adresse so lange für den entsprechenden Bereich, bis der Verzeichnisagent nicht mehr antwortet; anschließend ermitteln sie eine andere DA-Adresse für den Bereich. Die Benutzeragenten suchen wie folgt die Adresse eines Verzeichnisagenten für einen bestimmten Bereich:

1. Der Agent prüft, ob die Socket-Zugriffsnummer der aktuellen Anforderung mit einem DA für den angegebenen Bereich verbunden ist. Bei einer mehrteiligen Anforderung ist ggf. bereits eine Cache-Verbindung in der Anforderung vorhanden.
2. Der Agent prüft, ob sich im lokalen Cache der bekannten DAs ein DA befindet, der mit dem angegebenen Bereich übereinstimmt.
3. Der Agent sucht beim lokalen Service-Agenten (SA) nach einem DA mit dem angegebenen Bereich (und fügt neue Adressen zum Cache hinzu).
4. Der Agent fragt DHCP nach im Netzwerk konfigurierten DA-Adressen ab, die mit dem angegebenen Bereich übereinstimmen (und fügt neue Adressen zum Cache hinzu).
5. Der Agent sendet eine DA-Ermittlungsanforderung per Multicast über einen bereits bekannten Port (und fügt neue Adressen zum Cache hinzu).

Soweit nicht anders angegeben, gilt der Bereich „Standard“. Wenn also weder statisch in der SLP-Konfigurationsdatei noch in der Abfrage ein Bereich definiert ist, wird der Wert „Standard“ für den Bereich verwendet. Beachten Sie außerdem, dass das Identitätsdepot unter keinen Umständen einen Bereich in den Registrierungen angibt. Ist ein statisch konfigurierter Bereich vorhanden, so wird dieser Bereich als Standardbereich für alle lokalen UA-Anforderungen und SA-Registrierungen übernommen, wenn anderweitig kein Bereich angegeben ist.

## Service-Agenten

Service-Agenten treten physisch als separater Prozess auf dem Hostcomputer auf. Unter Windows wird `slpd.exe` als Dienst auf dem lokalen Computer ausgeführt. Die Benutzeragenten senden Nachrichten an die Loopback-Adresse eines bekannten Ports und fragen so den lokalen Service-Agenten ab.

Der Service-Agent stellt permanenten Speicher und Wartungspunkte für lokale Dienste bereit, die sich bei SLP registriert haben. Der Service-Agent pflegt im Wesentlichen eine speicherinterne Datenbank der registrierten lokalen Dienste. Ein Dienst kann sich dabei nur dann bei SLP

registrieren, wenn ein lokaler SA vorhanden ist. Die Clients können Dienste durchaus nur mit einer UA-Bibliothek ermitteln. Für die Registrierung ist jedoch ein SA erforderlich, hauptsächlich weil der SA regelmäßig prüfen muss, ob die registrierten Dienste vorhanden sind, damit die Registrierung bei überwachenden Agenten aufrechterhalten werden kann.

Um die Verzeichnisagenten und ihre jeweils unterstützte Bereichsliste zu suchen und im Cache zu speichern, sendet ein Service-Agent wie folgt eine DA-Ermittlungsanforderung direkt an potenzielle DA-Adressen:

1. Der Agent prüft alle statisch konfigurierten DA-Adressen (und fügt neue DAs zum Cache des SA mit den bekannten DAs hinzu).
2. Der Agent fordert eine Liste der DAs und ihrer Bereiche von DHCP an (und fügt neue DAs zum Cache des SA mit den bekannten DA hinzu).
3. Der Agent sendet eine DA-Ermittlungsanforderung per Multicast über einen bereits bekannten Port (und fügt neue DAs zum Cache des SA mit den bekannten DA hinzu).
4. Der Agent empfängt DA-Bekanntgabepakete, die die DAs in regelmäßigen Abständen per Rundsendung übermitteln (und fügt neue DAs zum Cache des SA mit den bekannten DA hinzu).

Dies ist wichtig, weil ein Benutzeragent stets zuerst den lokalen Service-Agenten abfragt: Die Antwort des lokalen Service-Agenten bestimmt, ob der Benutzeragent zur nächsten Ermittlungsphase übergeht oder nicht (in diesem Fall DHCP; siehe Schritt 3 und Schritt 4 in „Benutzeragenten“, auf Seite 86).

## Verzeichnisagenten

Der Verzeichnisagent stellt einen langfristig permanenten Cache für bekannt gegebene Dienste bereit und fungiert als Zugriffspunkt für die Suche nach Diensten durch die Benutzeragenten. Der DA überwacht die SAs, ob neue Dienste bekannt gegeben werden, und speichert diese Benachrichtigungen im Cache. In kurzer Zeit wird der Cache eines DA voller oder vollständiger. Mithilfe eines Ablaufalgorithmus werden die Einträge im Cache der Verzeichnisagenten außer Kraft gesetzt. Beim Starten liest der Verzeichnisagent den Cache aus dem permanenten Speicher aus (in der Regel eine Festplatte), und anschließend werden die Einträge gemäß dem Algorithmus außer Kraft gesetzt. Wenn ein neuer DA gestartet wird oder der Cache gelöscht wurde, erkennt der DA diesen Zustand, und er sendet eine besondere Benachrichtigung an alle empfangenden SAs, ihre lokalen Datenbanken zu übermitteln, sodass der DA den Cache rasch aufbauen kann.

Falls keine Verzeichnisagenten vorhanden sind, sendet der UA eine allgemeine Multicast-Abfrage, auf die die SAs antworten können. So entsteht eine Liste der angeforderten Dienste, ähnlich wie beim Aufbauen des Cache durch die DAs. Die durch diese Abfrage zurückgegebene Diensteliste ist unvollständig und stärker lokal konzentriert als die Liste eines DA, insbesondere wenn eine Multicast-Filterung erfolgt. Diese Filterung wird von zahlreichen Netzwerkadministratoren vorgenommen, damit die Rundsendungen und Multicasts ausschließlich auf das lokale Teilnetz beschränkt werden.

Fazit: Alles hängt von dem Verzeichnisagent ab, den ein Benutzeragent für einen bestimmten Bereich auffindet.

## 8.2.3 Konfigurieren von SLP für das Identitätsdepot

Die folgenden Parameter in der Datei `%systemroot%/slp.conf` steuern die Ermittlung der Verzeichnisagenten:

```
net.slp.useScopes = comma-delimited scope list
net.slp.DAAddresses = comma-delimited address list
net.slp.passiveDADetection = <"true" or "false">
net.slp.activeDADetection = <"true" or "false">
net.slp.DAActiveDiscoveryInterval = <0, 1, or a number of seconds>
```

**useScopes**

Gibt die Bereiche an, in denen der SA die Bekanntgabe vornimmt, außerdem die Bereiche, die abgefragt werden sollen, wenn kein bestimmter Bereich in der Registrierung oder Abfrage des Dienstes oder der Client-Anwendung festgelegt ist. Da das Identitätsdepot Bekanntgaben und Abfragen stets im Standardbereich vornimmt, wird diese Liste zur Standardbereichsliste für alle Registrierungen und Abfragen des Identitätsdepots.

**DAAddresses**

Enthält eine durch Komma getrennte Liste mit dezimalen IP-Adressen der DAs (mit Punkten), die Vorrang vor allen anderen Adressen erhalten sollen. Falls diese Liste der konfigurierten DAs den Bereich einer Registrierung oder Abfrage nicht unterstützt, senden die SAs und UAs ein Multicast für die DA-Ermittlung, sofern diese Art der Ermittlung nicht deaktiviert ist.

**passiveDADetection**

Weist standardmäßig den Wert `Wahr` auf. Wenn die Verzeichnisagenten entsprechend konfiguriert sind, übermitteln sie ihre Existenz in regelmäßigen Abständen per Rundsendung im Teilnetz über einen bekannten Port. Diese Pakete werden als DAAdvert-Pakete bezeichnet. Ist diese Option auf „Falsch“ eingestellt, ignoriert der SA alle rundgesendeten DAAdvert-Pakete.

**activeDADetection**

Weist standardmäßig den Wert `Wahr` auf. Damit kann der SA in regelmäßigen Abständen per Rundsendung eine Anforderung an alle DAs übermitteln, mit einem zielgerichteten DAAdvert-Paket zu antworten. Ein zielgerichtetes Paket wird nicht rundgesendet, sondern direkt als Antwort auf diese Anforderungen an den SA gesendet. Ist diese Option auf „Falsch“ eingestellt, übermittelt der SA keine DA-Ermittlungsanforderung in regelmäßigen Abständen per Rundsendung.

**DAActiveDirectoryInterval**

Parameter mit drei möglichen Zuständen. Der Standardwert lautet `1`. Dieser Wert bedeutet, dass der SA nur bei der Initialisierung eine einzige DA-Ermittlungsanforderung senden soll. Wenn Sie diese Option auf 0 einstellen, hat dies dieselbe Wirkung, als wenn Sie die Option activeDADetection auf „Falsch“ einstellen. Jeder andere Wert bezeichnet den Zeitraum (in Sekunden) zwischen den Ermittlungsrundsendungen.

Mithilfe dieser Optionen können Sie die Nutzung der Netzwerkbandbreite für die Dienstbekanntgabe ausgewogen gestalten. Die Standardeinstellungen sind so gewählt, dass die Skalierbarkeit in einem durchschnittlichen Netzwerk optimiert wird.

## 8.3 Erhöhen der Leistung des Identitätsdepots

eDirectory, die zugrunde liegende Infrastruktur des Identitätsdepots, ist eher eine E/A-intensive als eine prozessorintensive Anwendung. Zwei Faktoren steigern die Leistung des Identitätsdepots: ein größerer Cache-Speicher und schnellere Prozessoren. Um optimale Ergebnisse zu erzielen, sollten Sie so viele Teile des DIB-Satzes (Directory Information Base, Verzeichnisinformationsdatenbank), wie es die Hardware erlaubt, im Cache-Speicher ablegen.

eDirectory lässt sich schon auf einem einzelnen Prozessor gut skalieren; unter Umständen sollten Sie jedoch den Einsatz mehrerer Prozessoren erwägen. Eine höhere Prozessoranzahl erhöht die Leistung in Bereichen wie die Benutzeranmeldung. Auch die Verwendung mehrerer aktiver Threads auf mehreren Prozessoren trägt zur Leistungssteigerung bei.

Die nachfolgende Tabelle zeigt allgemeine Anhaltspunkte für die Servereinstellungen, die auf der erwarteten Anzahl der Objekte in eDirectory beruhen.

| Objekte | Arbeitsspeicher | Festplatte |
|---|---|---|
| 100.000 | mindestens 2 GB (Linux) | 300 MB (Linux) |
| | 384 MB (Windows) | 144 MB (Windows) |
| 1 Millionen | 4 GB (Linux) | 1,5 GB |
| | 4 GB (Windows) | |
| 10 Millionen | mindestens 4 GB (Linux) | 15 GB |
| | mindestens 2 GB (Windows) | |

Eine Basis-Installation von eDirectory mit dem Standardschema erfordert zum Beispiel ungefähr 74 MB Festplattenpeicher pro 50.000 Benutzer. Wenn Sie jedoch einen neuen Satz von Attributen hinzufügen oder alle vorhandenen Attribute komplett ausfüllen, steigt die Objektgröße. Dies wirkt sich auf den erforderlichen Festplattenspeicher, Prozessor und Arbeitsspeicher aus. Die Anforderungen an die Prozessoren sind zudem abhängig von den verfügbaren zusätzlichen Diensten auf dem Computer und der Anzahl der Beglaubigungen und Lese- und Schreibvorgänge, die der Computer verarbeitet. Prozesse wie die Verschlüsselung und die Indizierung können prozessorintensiv sein.

## 8.4 Verwenden von IPv6-Adressen auf dem Identitätsdepot-Server

Das Identitätsdepot unterstützt sowohl IPv4-Adressen als auch IPv6-Adressen. Beim Installieren des Identitätsdepots können Sie IPv6-Adressen aktivieren. Wenn Sie eine frühere Version aufrüsten, müssen Sie die IPv6-Adressen manuell aktivieren.

Das Identitätsdepot unterstützt außerdem die IPv6-Übergangsmethoden Dual-IP-Stack, Tunneling und Pure. Es werden lediglich die globalen IP-Adressen unterstützt. Beispiel:

- `[::]`
- `[::1]`
- `[2015::12]`
- `[2015::12]:524`

IPv6-Adressen müssen in eckigen Klammern [ ] angegeben werden. Soll der Hostname statt der IP-Adresse verwendet werden, müssen Sie den Namen in der Datei `etc\hosts` angeben und mit der IPv6-Adresse verknüpfen.

## 8.4.1 Verwenden von IPv6-Adressen auf Linux-Servern

Mit dem ndsconfig-Dienstprogramm können Sie Bäume mit einer IPv6-Adresse erstellen, Server mit IPv6-Adressen zu vorhandenen Bäumen hinzufügen und LDAP-URLs für IPv6 festlegen. Weitere Informationen zur Verwendung des Dienstprogramms finden Sie in Abschnitt 12.1, „Ändern des eDirectory-Baums und des Reproduktionsservers mit dem ndsconfig-Dienstprogramm“, auf Seite 119.

Neben dem ndsconfig-Dienstprogramm stehen weitere Schritte zur Auswahl, mit denen Sie das Identitätsdepot auf einem Linux-Computer konfigurieren, der bereits IPv6-Adressen unterstützt:

- „Aktivieren von IPv6-Adressen auf vorhandenen oder aufgerüsteten eDirectory-Servern“, auf Seite 90
- „Hinzufügen von LDAP-URLS für IPv6 auf dem LDAP-Serverobjekt“, auf Seite 90

### Aktivieren von IPv6-Adressen auf vorhandenen oder aufgerüsteten eDirectory-Servern

---

**HINWEIS:** Wenn auf dem Computer mehrere Instanzen konfiguriert sind, müssen Sie die IPv6-Adresse in jede Konfigurationsdatei eintragen.

---

1. Öffnen Sie die Datei `nds.conf` (standardmäßig im Verzeichnis `/etc/opt/novell/eDirectory/conf/`).
2. Tragen Sie die IPv6-Schnittstellenadresse mit der Portnummer in die Datei ein. Beispiel:

   ```
   n4u.server.interfaces=164.99.90.148@524,[2015::4]@524,[2015:1234:2345:3456:abcd:bcde:cdef:aaaa]@524

   http.server.interfaces=164.99.90.148@8028,[2015::4]@8028,[2015:1234:2345:3456:abcd:bcde:cdef:aaaa]@8028

   https.server.interfaces=164.99.90.148@8030,[2015::4]@8030,[2015:1234:2345:3456:abcd:bcde:cdef:aaaa]@8030
   ```

3. Starten Sie `ndsd` mit den folgenden Befehlen neu:

   ```
   ndsmanage stopall
   ndsmanage startall
   ```

### Hinzufügen von LDAP-URLS für IPv6 auf dem LDAP-Serverobjekt

Wenn Sie die LDAP-URLs beim ersten Konfigurieren des Identitätsdepots nicht angeben, können Sie sie mit dem Befehl `ldapconfig` oder mit iManager zum Attribut `ldapInterfaces` hinzufügen.

**So fügen Sie LDAP-URLs über die Befehlszeile hinzu:**

Verwenden Sie wahlweise den Befehl `ldapconfig set` oder den Befehl `ldapconfig -s`. Geben Sie Text wie in den folgenden Beispielen ein:

```
ldapconfig set "ldapInterfaces=ldap://[2015::3]:389,ldaps://[2015::3]:636"
```

```
ldapconfig -s
"ldapInterfaces=ldap://[2015::3]:389,ldapInterfaces=ldaps://[2015::3]:636"
```

**So fügen Sie LDAP-URLs in iManager hinzu:**

1. Klicken Sie in iManager auf **Rollen und Aufgaben**.
2. Klicken Sie auf **LDAP** > **LDAP-Optionen**.
3. Klicken Sie auf **LDAP-Server anzeigen** und dann auf den Namen des zu konfigurierenden LDAP-Serverobjekts.
4. Klicken Sie unter **LDAP-Schnittstellen** auf **Verbindungen** und dann auf **LDAP-URLS hinzufügen**.
5. Klicken Sie auf **Anwenden** und anschließend auf **OK**.

### 8.4.2 Verwenden von IPv6-Adressen auf Windows-Servern

Sollen IPv6-Adressen auf einem Windows-Server verwendet werden, müssen Sie während der Installation das Kontrollkästchen **IPv6 aktivieren** unter **IPv6-Einstellungen** aktivieren. Mit dieser Option werden das NCP-, das HTTP- und das HTTPS-Protokoll für die IPv6-Adressen aktiviert. Wenn Sie die IPv6-Adressen nicht während des Installationsvorgangs aktivieren und sich erst später für die Nutzung dieser Adressen entscheiden, müssen Sie das Setup-Programm erneut ausführen. Weitere Informationen finden Sie in Kapitel 10, „Installieren des Identitätsdepots auf einem Windows-Server“, auf Seite 105.

Unter dem folgenden Link können Sie auf iMonitor über IPv6-Adressen zugreifen:`http://[2015::3]:8028/nds`.

## 8.5 Kommunizieren mit dem Identitätsdepot über LDAP

Beim Installieren des Identitätsdepots müssen Sie die Ports angeben, die der LDAP-Server überwachen soll, sodass LDAP-Anforderungen verarbeitet werden können. Im Rahmen der standardmäßigen Konfiguration werden die Portnummern für Klartext und SSL/TLS auf 389 bzw. 636 festgelegt.

Für eine einfache LDAP-Bindung ist lediglich ein DN und ein Passwort erforderlich. Das Passwort liegt in Klartext vor. Wenn Sie Port 389 verwenden, ist das gesamte Paket in Klartext verfügbar. Da der Port 389 die Verwendung von Klartext zulässt, verarbeitet der LDAP-Server die Lese- und Schreibanforderungen an das Verzeichnis über diesen Port. Diese Offenheit eignet sich für vertrauenswürdige Umgebungen, in denen kein Spoofing auftritt und die Benutzer nicht unbefugt Pakete abfangen. Standardmäßig ist diese Option bei der Installation deaktiviert.

Die Verbindung über Port 636 ist verschlüsselt. Die Verschlüsselung wird von TLS (früher SSL) verwaltet. Bei einer Verbindung mit Port 636 wird automatisch ein Handshake instanziiert. Falls ein Fehler beim Handshake auftritt, wird die Verbindung abgelehnt.

---

**HINWEIS:** Im Installationsprogramm wird Port 636 standardmäßig für die TLS/SSL-Kommunikation ausgewählt. Diese Standardauswahl kann auf Ihrem LDAP-Server ein Problem darstellen. Wenn ein Dienst, der bereits vor der Installation von eDirectory auf dem Hostserver geladen war, den Port 636 nutzt, müssen Sie einen anderen Port angeben. Bei Installationen vor eDirectory 8.7 wurde dieser Konflikt als schwerwiegender Fehler behandelt, und `nldap` wurde entladen. Ab eDirectory 8.7.3 wird `nldap` durch das Installationsprogramm geladen, in die Datei `dstrace.log` wird eine Fehlermeldung eingetragen, und das Programm wird ohne den sicheren Port ausgeführt.

---

Während des Installationsvorgangs können Sie das Identitätsdepot so konfigurieren, dass Passwörter und andere Daten in Klartext nicht zulässig sind. Die Option **TLS für einfache Bindung mit Passwort erforderlich** hält die Benutzer davon ab, erkennbare Passwörter zu senden. Wenn Sie diese Einstellung nicht auswählen, ist es für die Benutzer nicht ersichtlich, dass andere Benutzer ihre Passwörter mitlesen können. Diese Option, mit der die Verbindung nicht zugelassen wird, gilt lediglich für den Klartext-Port. Wenn Sie eine sichere Verbindung mit Port 636 herstellen und eine einfache Bindung vorliegt, ist die Verbindung bereits verschlüsselt. Die Passwörter, Datenpakete und Bindungsanforderungen sind nicht einsehbar.

Betrachten Sie die folgenden Szenarien:

**Option „TLS für einfache Bindung mit Passwort erforderlich“ ist aktiviert**

Frau Lehmann nutzt einen Client, der ein Passwort anfordert. Sobald Frau Lehmann das Passwort eingibt, stellt der Client eine Verbindung zum Server her. Der LDAP-Server lässt jedoch nicht zu, dass die Verbindung über den Klartext-Port eine Bindung zum Server vornimmt. Alle Benutzer können Frau Lehmanns Passwort einsehen, während sie selbst keine gebundene Verbindung erhält.

**Port 636 wird bereits verwendet**

Auf dem Server wird Active Directory ausgeführt. Active Directory führt ein LDAP-Programm aus, das auf den Port 636 zugreift. Sie installieren eDirectory. Das Installationsprogramm erkennt, dass der Port 636 bereits verwendet wird, und weist dem NetIQ-LDAP-Server keine Portnummer zu. Der LDAP-Server wird geladen und wird scheinbar ausgeführt. Da der LDAP-Server einen bereits geöffneten Port nicht duplizieren und nicht verwenden kann, verarbeitet der LDAP-Server jedoch keine Anforderungen über duplizierte Ports.

Mit dem ICE-Dienstprogramm stellen Sie fest, ob dem NetIQ-LDAP-Server der Port 389 oder 636 zugewiesen ist. Wenn im Feld *Herstellerversion* nicht NetIQ angegeben ist, müssen Sie den LDAP-Server für eDirectory neu konfigurieren und einen anderen Port auswählen. Weitere Informationen finden Sie unter „Verifying That the LDAP Server is Running“ (Überprüfen, ob der LDAP-Server ausgeführt wird) im *NetIQ eDirectory -Administrationshandbuch*.

**Active Directory wird ausgeführt**

Wenn Active Directory ausgeführt wird und der Klartext-Port 389 geöffnet ist, können Sie den ICE-Befehl für Port 389 ausführen und die Herstellerversion abfragen. Im Bericht wird **Microsoft*** angezeigt. Anschließend konfigurieren Sie den NetIQ-LDAP-Server neu. Wählen Sie hierzu einen anderen Port aus, sodass der eDirectory-LDAP-Server die LDAP-Anforderungen verarbeiten kann.

iMonitor kann außerdem melden, ob der Port 389 oder 636 bereits geöffnet ist. Wenn der LDAP-Server nicht funktioniert, erhalten Sie mit iMonitor nähere Details. Weitere Informationen finden Sie unter „Verifying That the LDAP Server is Running“ (Überprüfen, ob der LDAP-Server ausgeführt wird) im *NetIQ eDirectory -Administrationshandbuch*.

## 8.6 Manuelle Installation von NICI auf Arbeitsstationen, auf denen Verwaltungsfunktionen vorliegen

NICI muss auf allen Arbeitsstationen installiert werden, auf denen Verwaltungsfunktionen (z. B. iManager) verwendet werden. Weitere Informationen zum Verwenden von NICI mit dem Identitätsdepot finden Sie in Abschnitt 7.2.1, „Voraussetzungen für die Installation des Identitätsdepots“, auf Seite 71.

### 8.6.1 Installieren von NICI auf einem Linux-Server

Verwenden Sie `nds-install`, und wählen Sie die Option für NICI. Standardmäßig befindet sich die Installationsdatei im Verzeichnis `products\eDirectory\`*`Prozessortyp`*`\setup\`. NetIQ empfiehlt, NICI als `Root` zu installieren, da die erforderlichen NICI-Pakete systemweit genutzt werden. Bei Bedarf können Sie jedoch den Zugriff mit `sudo` an ein anderes Konto delegieren und die NICI-Pakete über dieses Konto installieren.

---

**HINWEIS:** Ab eDirectory 8.8 Service Pack 3 können Sie mit NetIQ sowohl die 32-Bit-Version als auch die 64-Bit-Version von eDirectory auf einem einzigen System installieren. Wenn Sie beide Versionen auf einem Server installieren, müssen Sie auch die 32-Bit- und die 64-Bit-Version von NICI installieren.

---

In diesem Abschnitt werden die folgenden Vorgänge beschrieben:

- „Installieren von NICI als Root-Benutzer“, auf Seite 93
- „Installieren von NICI mit einem Nicht-Root-Benutzer“, auf Seite 94

#### Installieren von NICI als Root-Benutzer

Führen Sie zur Installation von NICI folgende Schritte durch:

1. Führen Sie die beiden folgenden Befehle aus:

   ```
   32-bit: rpm -ivh NICI_rpm_absolute_path/nici-2.7.7-0.02.i586.rpm
   64-bit: rpm -ivh NICI_rpm_absolute_path/nici64-2.7.7-0.02.x86_64.rpm
   ```

   ---

   **HINWEIS:** Ab eDirectory 8.8 Service Pack 3 können Sie mit NetIQ sowohl die 32-Bit-Version als auch die 64-Bit-Version von eDirectory auf einem einzigen System installieren. Wenn Sie beide Versionen auf einem Server installieren, müssen Sie auch die 32-Bit- und die 64-Bit-Version von NICI installieren.

   ---

2. 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 eDirectory-Konfiguration nicht fehlschlägt.

### Installieren von NICI mit einem Nicht-Root-Benutzer

Nicht-Root-Benutzer können NICI mit dem Dienstprogramm sudo installieren. Mit sudo (superuser do) kann ein Root-Benutzer bestimmte Benutzer in die Lage versetzen, einige Befehle als Root auszuführen. Hierzu fügt der Root-Benutzer die entsprechenden Einträge zur Konfigurationsdatei /etc/sudoers hinzu.

**WARNUNG:** Mit sudo erteilen Sie Nicht-Root-Benutzern eingeschränkte Root-Berechtigungen.

1. Melden Sie sich mit einem sudo-Konto bei dem Server an, auf dem NICI installiert werden soll.
2. Führen Sie den folgenden Befehl aus:

   ```
   sudo rpm -ivh nici_rpm_file_name_with_path
   ```

3. Initialisieren Sie NICI mit dem folgenden Befehl:

   ```
   ln -sf /var/opt/novell/nici /var/novell/nici
   ```

4. (Optional) Überprüfen Sie mit dem folgenden Befehl, ob sich NICI im Servermodus befindet:

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

## 8.6.2 Installieren von NICI auf einem Windows-Server

Zum Installieren von NICI auf einem Windows-Server verwenden Sie die Datei NICI_wx64.msi (standardmäßig im Ordner products\eDirectory*Prozessortyp*\windows*Prozessortyp*\nici). Sie können die Datei wahlweise als geführten Vorgang (Assistent) oder als automatische Installation ausführen.

# 8.7 Installieren der NMAS-Client-Software

Die NMAS-Client-Software (NetIQ Modular Authentication Service) muss auf jeder Client-Arbeitsstation installiert werden, auf der die NMAS-Anmeldemethoden verwendet werden sollen. Die Anmeldemethoden legen Sie beim Installieren des Identitätsdepots fest.

## 8.7.1 Installieren und Konfigurieren der NMAS-Client-Software auf einem Linux-Server

Das Installationsprogramm des Identitätsdepots (nds-install) umfasst NMAS als Installationskomponente. Zum Konfigurieren von NMAS bietet NetIQ zwei Dienstprogramme:

**ndsconfig-Dienstprogramm**

Mit diesem Dienstprogramm konfigurieren Sie sowohl das Identitätsdepot als auch NMAS nach der Installation des Identitätsdepots. Dieses Dienstprogramm installiert nicht die NMAS-Anmeldemethoden.

**nmasinst-Dienstprogramm**

Dieses Dienstprogramm kommt zum Einsatz, wenn Sie das Identitätsdepot bereits konfiguriert haben und lediglich NMAS konfiguriert werden soll. Dieses Dienstprogramm installiert die NMAS-Anmeldemethoden.

---

**HINWEIS:** Vor dem Installieren der NMAS-Anmeldemethoden müssen Sie das Identitätsdepot mit dem ndsconfig-Dienstprogramm konfigurieren. Außerdem benötigen Sie Administratorrechte für den Baum.

---

### Konfigurieren von NMAS

Mit diesem Vorgang werden die erforderlichen Objekte für NMAS im Sicherheitscontainer erstellt, und die LDAP-Erweiterungen für NMAS werden im LDAP-Serverobjekt in eDirectory installiert.

Beim ersten Installieren von NMAS in einem Baum müssen Sie sich mit Rechten zum Erstellen von Objekten im Sicherheitscontainer anmelden. Nachfolgende Installationen können dann von Containeradministratoren vorgenommen werden, die lediglich Nur-Lese-Rechte auf den Sicherheitscontainer besitzen. nmasinst überprüft zunächst, ob die NMAS-Objekte bereits im Sicherheitscontainer vorhanden sind; nur wenn die Objekte fehlen, werden sie erstellt.

Das nmasinst-Dienstprogramm erweitert nicht das Schema. Stattdessen umfasst das Identitätsdepot das NMAS-Schema als Teil des grundlegenden eDirectory-Schemas.

**So können Sie NMAS konfigurieren und NMAS-Objekte in eDirectory erstellen:**

1. Geben Sie in der Befehlszeile der Serverkonsole Folgendes ein:

   ```
   nmasinst -i admin.context tree_name
   ```

2. Geben Sie das Passwort ein.

### Installieren der NMAS-Anmeldemethoden

Mit dem nmasinst-Dienstprogramm können Sie die NMAS-Anmeldemethoden installieren. Hierbei müssen Sie die Datei `config.txt` für die zu installierende Anmeldemethode angeben. Für jede Anmeldemethode gibt es eine eigene Datei `config.txt`.

Geben Sie in der Befehlszeile der Serverkonsole den folgenden Befehl ein:

`nmasinst -addmethod` *`admin`*`.context` *`tree_name config.txt_path`*

Soll beispielsweise der Befehl `-addmethod` verwendet werden, geben Sie Folgendes ein:

```
nmasinst -addmethod admin.netiq MY_TREE ./nmas-methods/novell/Simple Password/
config.txt
```

Wenn die Anmeldemethode bereits vorhanden ist, wird sie durch das nmasinst-Dienstprogramm aktualisiert.

Weitere Informationen finden Sie unter „Verwalten von Anmelde- und Post-Login-Methoden und -Sequenzen“ im *NetIQ eDirectory-Administrationshandbuch*.

### 8.7.2 Installieren der NMAS-Client-Software auf einem Windows-Server

1. Melden Sie sich mit einem Administratorkonto bei der Windows-Client-Arbeitsstation an.
2. Führen Sie das Programm `nmasinstall.exe` im Installationsverzeichnis aus (standardmäßig `IDM4.5_Win:\products\eDirectory\`*`Prozessortyp`*`\nmas\`).
3. Klicken Sie auf **NMAS-Client-Komponenten**.
4. (Optional) Wählen Sie die Option für NICI, wenn die NICI-Komponente installiert werden soll.
5. Klicken Sie auf **OK**.
6. Starten Sie nach Abschluss der Installation die Arbeitsstation neu.

## 8.8 Arbeiten mit eDirectory 9.0.2 oder höher

Zusätzlich zu eDirectory 8.8.8 Patch 3 können Sie eDirectory 9.0.2 oder höher als Identitätsdepot und als verbundenes System mit Identity Manager 4.6 installieren. NetIQ empfiehlt, sich vor Verwendung von eDirectory 9.0.2 oder höher als Identitätsdepot die folgenden Abschnitte genau anzusehen:

- Abschnitt 8.8.1, „Funktionen, die zur Aktivierung auf dem Identitätsdepot-Server verfügbar sind“, auf Seite 96
- Abschnitt 8.8.2, „Ändern der NICI-Konfiguration in einen Nicht-FIPS-Modus in eDirectory“, auf Seite 97

### 8.8.1 Funktionen, die zur Aktivierung auf dem Identitätsdepot-Server verfügbar sind

Sehen Sie sich die folgende Tabelle an, um zu verstehen, welche Funktionen von eDirectory 9.0.1 oder höher mit Identity Manager aktiviert werden. Diese Einschränkungen gelten nicht, wenn eDirectory 9.0.1 oder höher als verbundenes System verwendet wird.

| Funktion | Kann aktiviert werden (Ja/Nein) | Beschreibung |
|---|---|---|
| TLS 1.2 | Ja | Kann die gesamte TCP-Kommunikation mit dem TLS 1.2-Protokoll aktivieren. |
| Suite B-Konfiguration | Ja | Kann stärkere Verschlüsselungen für die SSL-Kommunikation verwenden wie von Suite B angegeben. |
| AES-256-Bit-SDI-Schlüssel | Ja | Ohne Einfluss auf Identity Manager |
| LDAP- und HTTP-Services | Ja | Die Identity Manager-Services verwenden weiterhin das RSA-Zertifikat. |
| Authentifizierung | Ja | Ohne Einfluss auf Identity Manager |

| Funktion | Kann aktiviert werden (Ja/Nein) | Beschreibung |
|---|---|---|
| NPKI (NetIQ-Zertifikatsserver) | Ja | Ohne Einfluss auf Identity Manager |
| NICI im FIPS-Modus | Nein | NICI ist standardmäßig im FIPS-Modus deaktiviert. Wenn Sie es aktivieren, startet die Identity Manager-Engine nicht und meldet einen Fehler. Informationen zum Ändern der NICI-Konfiguration in einen Nicht-FIPS-Modus finden Sie in Abschnitt 8.8.2, „Ändern der NICI-Konfiguration in einen Nicht-FIPS-Modus in eDirectory“, auf Seite 97. |
| Besserer Umgang mit Containern | Ja | Ohne Einfluss auf Identity Manager |
| Verbesserungen bei verschachtelten Gruppen | Ja | Von der Identity Manager-Engine und den Treibern nicht unterstützt |
| Steuerung der Proxyautorisierung | Ja | Ohne Einfluss auf Identity Manager |
| Überwachung | Ja | Support nicht erweitert auf die Überwachung von Identity Manager-Komponenten |
| Optimierte Datenreproduktion | Ja | Ohne Einfluss auf Identity Manager |
| Bessere Datensynchronisierung | Ja | Ohne Einfluss auf Identity Manager |
| Optimierter Janitor-Thread für die Berechnung vererbter ACLs | Ja | Ohne Einfluss auf Identity Manager |

Weitere Informationen zu den neuen Funktionen von eDirectory 9.0.1 und 9.0.2 finden Sie in den entsprechenden Versionshinweisen auf der Website der eDirectory-Dokumentation.

## 8.8.2 Ändern der NICI-Konfiguration in einen Nicht-FIPS-Modus in eDirectory

Identity Manager 4.6 unterstützt nicht eDirectory 9.0.1 oder höher, wenn NICI im FIPS-Modus aktiviert ist. Für eine ordnungsgemäße Funktionsweise von Identity Manager müssen Sie den FIPS-Modus für NICI in der NICI-Konfiguration anhand einer der folgenden Methoden ändern:

- **Linux:** Navigieren Sie zu `/etc/opt/novell/nici64.cfg` und ändern Sie **RestrictionLevel** zu **0**.
- **Windows:** Navigieren Sie zur `HKLM\SOFTWARE\Novell\Windows`-Registrierung und ändern Sie die Einstellungen im `nici_x64`-Schlüssel zu **0**. Nehmen Sie diese Änderung am `nici_x64`-Schlüssel für jeden Server im Baum vor.

# 9 Installieren des Identitätsdepots auf einem Linux-Server

Das Installationsprogramm führt Sie durch die Konfigurationseinstellungen für das Identitätsdepot. Führen Sie die Installation entsprechend der geplanten Methode, mit der später die Identity Manager-Engine installiert werden soll, als `Root`-Benutzer oder mit einem Nicht-`Root`-Benutzer aus. Weitere Informationen zu den zusätzlichen Paketen, mit denen eDirectory auf einem Linux-Server installiert wird, finden Sie unter Linux-Pakete für NetIQ eDirectory im *NetIQ eDirectory 9.0 SP2-Installationshandbuch*.

---

**WARNUNG:** Das Verzeichnis *`install_location`*`/etc/opt/novell/eDirectory/conf` enthält wichtige Konfigurationsinformationen für das Nachverfolgen und Verwalten der eDirectory-Instanzen, die auf dem Server ausgeführt werden. Entfernen Sie keine Inhalte aus diesem Verzeichnis.

---

Falls Sie eDirectory 9.0 oder eine neuere Version installieren, wenn der neueste 64-Bit Remote Loader bereits installiert ist, wird die eDirectory-Installation nicht durchgeführt und der Remote Loader funktioniert nicht mehr. Führen Sie vor der Installation von eDirectory 9.0 oder höher die folgenden Schritte durch, um sicherzustellen, dass der Remote Loader ordnungsgemäß funktioniert:

1. Stoppen Sie den Remote Loader und seine Instanzen.
2. Deinstallieren Sie die `novell-DXMLopensslx`-RPM.
3. Installieren Sie eDirectory.

## 9.1 Installieren des Identitätsdepots als Root

In diesem Abschnitt wird die Installation des Identitätsdepots als `Root`-Benutzer mit dem Dienstprogramm nds-install beschrieben. Das Dienstprogramm fügt auf der Basis der Komponenten, die Sie für die Installation ausgewählt haben, die erforderlichen Pakete hinzu.

---

**HINWEIS:** Wenn Sie die Installation als `Nicht-Root`-Benutzer vornehmen und einen benutzerdefinierten Installationspfad angeben möchten, sollten Sie ggf. das tarball-Format für die Installation verwenden. Weitere Informationen finden Sie in Abschnitt 9.2, „Installieren des Identitätsdepots als Nicht-Root-Benutzer“, auf Seite 101.

---

**So installieren Sie das Identitätsdepot als `Root`:**

1. Melden Sie sich als `Root` an dem Computer an, auf dem das Identitätsdepot installiert werden soll.
2. Führen Sie den folgenden Befehl in dem Verzeichnis aus, in dem sich das Dienstprogramm `nds-install` befindet (standardmäßig im Verzeichnis `products/eDirectory/`*`Prozessortyp`*`/setup`):

   `./nds-install` *`parameters`*

   Die folgenden Parameter stehen in der Befehlszeile zur Auswahl:

**-h oder --help**

Zeigt die Hilfe für nds-install an.

**-i**

Verhindert, dass das Skript von nds-install den Befehl `ndsconfig upgrade` aufruft, wenn eine DIB während der Aktualisierung gefunden wird.

**-j**

Überspringt die Option zur Prüfung der Funktionsfähigkeit vor dem Installieren von eDirectory oder setzt diese Option außer Kraft. Weitere Informationen zu den Prüfungen der Funktionsfähigkeit finden Sie unter „Keeping eDirectory Healthy“ (Funktionsfähigkeit von eDirectory aufrechterhalten) im *NetIQ eDirectory -Administrationshandbuch*.

**-m *Modulname***

Gibt den Namen des Moduls an, das installiert und konfiguriert werden soll.

Während ein neuer Baum konfiguriert wird, können Sie nur das Modul DS konfigurieren. Fügen Sie nach dem Konfigurieren des DS-Moduls die NMAS-, LDAP-, SAS-, SNMP- und HTTP-Services hinzu. Wenn Sie den Modulnamen nicht angeben, werden alle Module installiert.

---

**HINWEIS:** Sie müssen NetIQ SecreStore (`ss`) installieren und konfigurieren. Weitere Informationen finden Sie unter Abschnitt 12.1.2, „Hinzufügen von SecretStore zum Identitätsdepotschema“, auf Seite 123.

---

**-u**

Gibt an, dass die Installation unbeaufsichtigt (automatisch) ausgeführt werden soll.

3 (Optional) Wenn sich die Lizenzdatei nicht im Standardverzeichnis befindet, geben Sie an der Eingabeaufforderung den vollständigen Pfad zur Lizenzdatei ein.

4 Bearbeiten Sie alle Eingabeaufforderungen, bis der Installationsvorgang abgeschlossen ist.

5 (Bedingt) Sollen die nachfolgenden Umgebungsvariablen manuell aktualisiert und exportiert werden, geben Sie den folgenden Befehl ein:

```
export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib64:/opt/novell/
eDirectory/lib64/nds-modules:/opt/novell/lib64:$LD_LIBRARY_PATH

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

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

6 (Bedingt) Wenn die nachfolgenden Umgebungsvariablen mit dem ndspath-Skript aktualisiert und ihre Pfade 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/` mit dem folgenden Befehl aus:

```
eDirectory installation/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
```

---

**HINWEIS:** Wenn Sie das ndspath-Skript den Befehlen mit Argumenten voranstellen, geben Sie die Argumente in doppelten Anführungszeichen an.

Beispiel:

```
/opt/novell/eDirectory/bin/ndspath ldapconfig "-s ldapTLSRequired=yes"
```

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

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

**6d** Führen Sie die Dienstprogramme wie gewohnt aus.

**6e** 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** Wenden Sie zur Unterstützung der LDAP-Suche mit VLV(Virtual List View)- und SSS(Server Side Sort)-Steuerelementen Hotfix 2 auf das Identitätsdepot an. Weitere Informationen finden Sie unter Kapitel 11, „Anwenden von HotFix 2 auf das Identitätsdepot“, auf Seite 115.

## 9.2 Installieren des Identitätsdepots als Nicht-Root-Benutzer

In diesem Abschnitt wird beschrieben, wie Sie das Identitätsdepot mit tarball statt mit dem Dienstprogramm nds-install installieren. Beim Entpacken der tar-Datei erstellt das System die Verzeichnisse `etc`, `opt` und `var`.

Weitere Informationen zu den Voraussetzungen für die Installation als Nicht-Root-Benutzer finden Sie in Abschnitt 7.2.2, „Voraussetzungen für die Installation des Identitätsdepots als Nicht-Root-Benutzer“, auf Seite 73.

---

**HINWEIS:** Mit diesem Vorgang können Sie außerdem einen benutzerdefinierten Pfad angeben, wenn Sie die Installation als `Root`-Benutzer vornehmen.

---

**So installieren Sie das Identitätsdepot als Nicht-`Root`-Benutzer:**

**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** Entpacken Sie die tar-Datei in dem Verzeichnis, in dem das Identitätsdepot installiert werden soll, mit dem folgenden Befehl:

```
tar -xvf /tar_file_name
```

**3** (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
```

**4** (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:

**4a** 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
```

**4b** Exportieren Sie die Pfade in der aktuellen Shell mit dem folgenden Befehl:

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

**4c** Führen Sie die Dienstprogramme wie gewohnt aus.

**4d** 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.

**5** Wenden Sie zur Unterstützung der LDAP-Suche mit VLV(Virtual List View)- und SSS(Server Side Sort)-Steuerelementen Hotfix 2 auf das Identitätsdepot an. Weitere Informationen finden Sie unter Kapitel 11, „Anwenden von HotFix 2 auf das Identitätsdepot“, auf Seite 115.

**6** Konfigurieren Sie das Identitätsdepot mit einem der folgenden Schritte:

**6a** 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**

- Weitere Informationen zu den verfügbaren Parametern für das ndsconfig-Dienstprogramm finden Sie in Abschnitt 12.1.1, „Erläuterungen zu den Parametern des ndsconfig-Dienstprogramms“, auf Seite 120.

- 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`.
- Sie müssen NetIQ SecreStore (`ss`) installieren und konfigurieren. Weitere Informationen finden Sie unter Abschnitt 12.1.2, „Hinzufügen von SecretStore zum Identitätsdepotschema“, auf Seite 123.

---

**6b** Mit dem ndsmanage-Dienstprogramm konfigurieren Sie eine neue Instanz. Weitere Informationen finden Sie in Abschnitt 12.2.2, „Erstellen einer neuen Instanz im Identitätsdepot“, auf Seite 127.

# 10 Installieren des Identitätsdepots auf einem Windows-Server

Das Installationsprogramm (Assistent) führt Sie durch die Konfigurationseinstellungen für das Identitätsdepot. Das Installationsprogramm geht automatisch in den Assistenten-Modus über. Die automatische Installation ist jedoch auch möglich.

In diesem Abschnitt wird vorausgesetzt, dass Sie eDirectory als Grundstruktur für das Identitätsdepot verwenden möchten.

Wenn Sie das Installationsprogramm starten, sucht es nach NICI (Novell International Cryptographic Infrastructure) und dem Novell-Client für Windows. Je nach Bedarf werden diese Komponenten durch das Installationsprogramm installiert oder aktualisiert. Wenn Sie das Identitätsdepot auf einem Computer installieren, auf dem der Novell-Client bereits vorliegt, nutzt eDirectory den vorhandenen Novell-Client. Sie können das Identitätsdepot für Windows auch ohne den Novell-Client installieren.

Weitere Informationen zu NICI finden Sie im *Novell International Cryptographic Infrastructure - Administrationshandbuch*. Weitere Informationen zum Client finden Sie in der Dokumentation über den Novell-Client für Windows.

Das Installationsprogramm kann die Serverkomponenten für NMAS (NetIQ Module Authentication Service) installieren. Während der Installation müssen Sie die Anmeldemethoden für NMAS festlegen. Außerdem muss die NMAS-Client-Software auf jeder Client-Arbeitsstation installiert werden, auf der die NMAS-Anmeldemethoden verwendet werden sollen.

---

**HINWEIS**

- Ab eDirectory 8.8 können Sie für alle Dienstprogramme Passwörter angeben, bei denen zwischen Groß- und Kleinschreibung unterschieden wird.
- Die Containernamen dürfen einen Punkt (.) enthalten. Weitere Informationen zum Verwenden von Punkten in Containernamen finden Sie in Abschnitt 7.2.3, „Voraussetzungen für die Installation des Identitätsdepots auf einem Windows-Server“, auf Seite 73.

---

## 10.1 Installieren des Identitätsdepots mit dem Assistenten auf einem Windows-Server

1. Melden Sie sich an dem Computer, auf dem eDirectory installiert werden soll, als Administratorbenutzer an.
2. Wechseln Sie zum Programm `Setup.exe` im Installationsverzeichnis (standardmäßig `IDM`*`Version`*`_Win:\products\eDirectory\`*`Prozessortyp`*`\windows\`).
3. Führen Sie das Programm `Setup.exe` aus.
4. Befolgen Sie die Anweisungen im Installationsassistenten.

5 (Bedingt) Wenn NICI oder der Novell-Client für Windows nicht bereits auf dem Computer installiert ist, werden Sie vom Installationsprogramm aufgefordert, diese Komponenten zu installieren.

   Nach der Installation von NICI wird der Computer neu gestartet. Der Assistent für die Installation des Identitätsdepots wird im Normalfall nach dem Neustart des Computers erneut geöffnet. Ist dies nicht der Fall, führen Sie das Programm `Setup.exe` aus.

6 Beachten Sie bei den Anweisungen des Assistenten im Installationsprogramm für das Identitätsdepot die folgenden Überlegungen:

   - (Optional) Sollen IPv6-Adressen auf dem Identitätsdepot-Server verwendet werden, klicken Sie auf **IPv6 aktivieren** unter **IPv6-Einstellungen**.

     ---

     **HINWEIS:** NetIQ empfiehlt, diese Option zu aktivieren. Wenn die IPv6-Adressen nach erfolgter Installation aktiviert werden sollen, müssen Sie das Setup-Programm erneut ausführen.

     ---

   - Die Ports für den HTTP-Stack dürfen nicht mit den HTTP-Stack-Ports identisch sein, die für NetIQ iManager verwendet wurden oder noch verwendet werden sollen. Weitere Informationen finden Sie im *iManager-Administrationshandbuch*.
   - (Bedingt) Wenn ein Dienst, der bereits vor der Installation von eDirectory auf dem Hostserver geladen war, den Port 636 nutzt, müssen Sie einen anderen Port für SSL/TLS angeben.
   - (Optional) Wenn Passwörter und andere Daten im Klartext nicht zulässig sein sollen, wählen Sie beim Angeben der LDAP-Ports die Option **TLS für einfache Bindung mit Passwort erforderlich**. Weitere Informationen finden Sie in Abschnitt 8.5, „Kommunizieren mit dem Identitätsdepot über LDAP“, auf Seite 91.
   - Geben Sie die Anmeldemethoden an, die für NMAS (NetIQ Module Authentication Service) installiert werden sollen. Weitere Informationen finden Sie unter „Verwalten von Anmelde- und Post-Login-Methoden und -Sequenzen“ im *NetIQ eDirectory-Administrationshandbuch*.
   - Sie müssen NetIQ SecreStore (`ss`) installieren und konfigurieren. Weitere Informationen finden Sie unter Abschnitt 12.1.2, „Hinzufügen von SecretStore zum Identitätsdepotschema“, auf Seite 123.

7 Befolgen Sie die Anweisungen im Installationsassistenten, bis die Installation des Identitätsdepots abgeschlossen ist.

8 Wenden Sie zur Unterstützung der LDAP-Suche mit VLV(Virtual List View)- und SSS(Server Side Sort)-Steuerelementen Hotfix 2 auf das Identitätsdepot an. Weitere Informationen finden Sie unter Kapitel 11, „Anwenden von HotFix 2 auf das Identitätsdepot“, auf Seite 115.

9 Sollen die NMAS-Anmeldemethoden verwendet werden, installieren Sie die NMAS-Client-Software auf jeder Client-Arbeitsstation. Weitere Informationen finden Sie unter „Überlegungen zu NMAS“ im *NetIQ eDirectory-Administrationshandbuch*.

10 (Optional) Schließen Sie das DIB-Verzeichnis auf dem eDirectory-Server von allen Antiviren- und Sicherungssoftware-Verfahren aus. Sichern Sie das DIB-Verzeichnis mit dem eDirectory - Sicherungswerkzeug. Weitere Informationen zum Sichern von eDirectory finden Sie unter „Backing Up and Restoring NetIQ eDirectory“ (Sichern und Wiederherstellen von NetIQ eDirectory) im *NetIQ eDirectory -Administrationshandbuch*.

## 10.2 Automatische Installation und Konfiguration des Identitätsdepots auf einem Windows-Server

Wenn das Identitätsdepot automatisch (unbeaufsichtigt) installiert oder konfiguriert werden soll, können Sie eine Datei `response.ni` verwenden, die Abschnitte und Schlüssel enthält (ähnlich wie eine Datei `Windows.ini`).

---

**HINWEIS:** Sie müssen NetIQ SecreStore (`ss`) installieren und konfigurieren. Weitere Informationen finden Sie unter Abschnitt 12.1.2, „Hinzufügen von SecretStore zum Identitätsdepotschema“, auf Seite 123.

---

### 10.2.1 Bearbeiten der Datei response.ni

Die Datei `response.ni` kann mit einem ASCII-Texteditor erstellt und bearbeitet werden. Die Antwortdatei ermöglicht Folgendes:

- Ausführen einer vollständigen unbeaufsichtigten Installation mit sämtlichen erforderlichen Benutzereingaben.
- Definieren der Standardkonfiguration für die Komponenten.
- Umgehen aller Eingabeaufforderungen während der Installation.

NetIQ stellt eine Datei `response.ni` im Ordner `products\eDirectory\x64\windows\x64\NDSonNT` des Installations-Kits bereit. Die Datei enthält Standardeinstellungen für unerlässliche Parameter. Sie müssen die Werte für die eDirectory-Instanz im Abschnitt NWI:NDS bearbeiten.

---

**HINWEIS:** Geben Sie beim Bearbeiten der Datei `response.ni` in den Schlüssel-Wert-Paaren keine Leerzeichen zusätzlich zum Gleichheitszeichen („=“) zwischen dem Schlüssel und dem Wert ein.

---

---

**WARNUNG:** In der Datei `response.ni` geben Sie den Administrator-Berechtigungsnachweis für eine unbeaufsichtigte Installation an. Damit der Administrator-Berechtigungsnachweis nicht missbraucht werden kann, sollten Sie die Datei nach der Installation oder Konfiguration dauerhaft löschen.

---

In den folgenden Abschnitten werden die erforderlichen Abschnitte und Schlüssel für die Datei `response.ni` beschrieben:


- „NWI:NDS“, auf Seite 108
- „NWI:NMAS (NMAS-Methoden)“, auf Seite 110
- „eDir:HTTP (Ports)“, auf Seite 110
- „Novell:Languages:1.0.0 (Spracheinstellungen)“, auf Seite 111
- „Initialisierung“, auf Seite 111
- „NWI:SNMP“, auf Seite 112
- „EDIR:SLP“, auf Seite 112
- „Novell:ExistingTree:1.0.0“, auf Seite 112
- „Ausgewählte Knoten“, auf Seite 113
- „Novell:NOVELL_ROOT:1.0.0“, auf Seite 113

## NWI:NDS

**Aufrüstungsmodus**

Gibt an, ob das Installationsprogramm als Aufrüstung ausgeführt werden soll. Gültige Werte sind `Falsch`, `Wahr` und `Kopieren`.

**Modus**

Gibt den Typ der auszuführenden Installation an:

- Mit **Vollständig** wird das Identitätsdepot sowohl installiert als auch konfiguriert. Geben Sie diesen Wert an, wenn Sie das Identitätsdepot völlig neu installieren und konfigurieren oder lediglich die erforderlichen Dateien aufrüsten und konfigurieren möchten.
- Mit **Installieren** können Sie das Identitätsdepot neu installieren bzw. die erforderlichen Dateien aufrüsten.
- Mit **Konfigurieren** können Sie die Einstellungen für das Identitätsdepot bearbeiten. Wenn lediglich die erforderlichen Dateien aufgerüstet werden, konfiguriert das Installationsprogramm entsprechend nur die aufgerüsteten Dateien.

---

**HINWEIS**

- Wenn Sie *Konfigurieren* angeben, darf der Wert für `RestrictNodeRemove` im Schlüssel `ConfigurationMode` im Abschnitt [Initialisierung] nicht geändert werden.
- Wenn Sie *Vollständig* angeben, erhalten Sie beim Deinstallieren des Identitätsdepots keine individuellen Optionen für die Dekonfiguration und die Deinstallation.

---

**Neuer Baum**

Gibt an, ob diese Installation für einen neuen Baum oder einen Sekundärserver erfolgt. Zulässige Werte sind `Ja` und `Nein`. Wenn Sie beispielsweise einen neuen Baum installieren möchten, geben Sie `Ja` an. Weitere Informationen zum Festlegen von Werten für einen vorhandenen Baum finden Sie in „Novell:ExistingTree:1.0.0“, auf Seite 112.

**Baumname**

Bei einer Neuinstallation geben Sie den Namen des zu installierenden Baums an. Wird ein Sekundärserver installiert, geben Sie den Baum an, dem der Server hinzugefügt werden soll.

**Servername**

Gibt den Namen des Servers an, der im Identitätsdepot installiert werden soll.

**Servercontainer**

Gibt das Containerobjekt im Baum an, dem das Serverobjekt hinzugefügt werden soll. Das Serverobjekt enthält alle Konfigurationsdaten für den Identitätsdepot-Server. Wenn Sie das Identitätsdepot neu installieren, erstellt das Installationsprogramm diesen Container mit dem Serverobjekt.

**Serverkontext**

Gibt den vollständigen eindeutigen Name (DN) des Serverobjekts (Servername) sowie das Containerobjekt an. Wenn beispielsweise EDIR-TEST-SERVER als Identitätsdepot-Server fungiert und der Container Netiq verwendet wird, geben Sie `EDIR-TEST-SERVER.Netiq` an.

**Admin-Kontext**

Gibt das Containerobjekt im Baum an, dem das Administratorobjekt hinzugefügt werden soll. Beispiel: `Netiq`. Jeder Benutzer, der einem Baum hinzugefügt wird, besitzt ein Benutzerobjekt mit allen benutzerspezifischen Details. Wenn Sie das Identitätsdepot neu installieren, erstellt das Installationsprogramm diesen Container mit dem Serverobjekt.

**Admin-Anmeldename**

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). Beispiel: `Admin`. Mit diesem Konto führt das Installationsprogramm alle Vorgänge im Baum aus.

**Admin-Passwort**

Geben Sie das Passwort für das Administratorobjekt an. Beispiel: `netiq123`. Wenn Sie das Identitätsdepot neu installieren, konfiguriert das Installationsprogramm ein Passwort für das Administratorobjekt.

**NDS-Speicherort**

Gibt den Pfad im lokalen System an, in dem die Bibliotheksdateien und die Binärdateien für das Identitätsdepot installiert werden sollen. Wenn Sie die Komponenten des Identitätsdepots konfigurieren, suchen diese die relevanten Dateien an diesem Speicherort. Standardmäßig legt das Installationsprogramm die Dateien unter `C:\Novell\NDS` ab.

**DataDir**

Gibt den Pfad im lokalen System an, in dem die DIB-Dateien installiert werden sollen. Standardmäßig legt das Installationsprogramm die Dateien unter `C:\Novell\NDS\DIBFiles` ab.

Wenn die DIB-Datendateien mehr Speicherplatz benötigen als im Standardspeicherort verfügbar ist, sollten Sie einen anderen Pfad angeben.

**Installationsort**

(Optional) Geben Sie den Pfad an, den das Installationsprogramm beim Kopieren von Dateien in den NDS-Speicherort verwenden soll. Beispiel: `[Novell:DST:1.0.0_Location]` oder `Path=file://C:\Novell\NDS`. Der Standardwert lautet `C:\Novell\NDS` (wie beim NDS-Speicherort). Das Installationsprogramm nutzt diesen Pfad, wenn Dateien in die angegebenen NDS- und DataDir-Speicherorte kopiert werden sollen.

**Systemstandort**

(Optional) Gibt den Pfad zum Systemordner des Computers an, auf dem der Identitätsdepot-Server installiert werden soll. Beispiel: `[Novell:SYS32_DST:1.0.0_Location]` oder `Path=file:/C:\Windows\system32`. Das Installationsprogramm benötigt den Zugriff auf den Systemordner, damit während der Installation DLLs kopiert und systemspezifische Dateien abgerufen werden können.

**TLS erforderlich**

(Optional) Gibt an, ob das Identitätsdepot das TLS-Protokoll (Transport Layer Security) für den Empfang von LDAP-Anforderungen im Klartext benötigt.

**LDAP TLS-Port**

(Optional) Gibt den Port an, den das Identitätsdepot auf LDAP-Anforderungen im Klartext überwachen soll.

**LDAP SSL-Port**

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

**Installation als Dienst**

Weist das Installationsprogramm an, eDirectory als Dienst in Windows zu installieren. Hier müssen Sie `Ja` angeben.

**Eingabeaufforderung**

Gibt an, ob das Installationsprogramm bei bestimmten Entscheidungen (z. B. Baum- oder Servername) eine Eingabeaufforderung anzeigen soll. Für eine automatische oder unbeaufsichtigte Installation geben Sie beispielsweise `Falsch` an.

## NWI:NMAS (NMAS-Methoden)

Das Identitätsdepot unterstützt mehrere NMAS-Methoden, sowohl beim Installieren als auch beim Aufrüsten. Sie müssen die NDS-NMAS-Methode in der Datei `response.ni` angeben. Falls Sie keine NMAS-Methoden angeben, installiert das Installationsprogramm standardmäßig die NDS-Methode. Wenn Sie jedoch eine explizite Liste erstellen, müssen Sie NDS aufführen.

**Optionen**

Gibt die Anzahl der zu installierenden NMAS-Methoden an. Beispiel: `5`.

**Methodik**

Gibt die Typen der zu installierenden NMAS-Methoden an. Trennen Sie mehrere Typen jeweils mit Kommas voneinander ab. Beispiel: `CertMutual,Challenge Response,DIGEST-MD5,NDS`.

Das Installationsprogramm bestimmt die zu installierenden NMAS-Methoden nach der exakten Zeichenfolge, wobei zwischen Groß- und Kleinschreibung unterschieden wird. Sie müssen die Werte also genau wie aufgelistet angeben:

- `CertMutual`
- `Challenge-Response` – Die NMAS-Methode der NetIQ-Challenge-Response.
- `DIGEST-MD5`
- `Erweitertes Passwort`
- `Entrust`
- `GSSAPI` – Der SASL-GSSAPI-Mechanismus für eDirectory. Die Authentifizierung beim Identitätsdepot erfolgt durch LDAP über ein Kerberos-Ticket.
- `NDS` – Die standardmäßige Anmeldemethode. ERFORDERLICH.
- `NDS-Passwortänderung`
- `Einfaches Passwort`
- `Universelle Smartcard`
- `Erweitertes X.509-Zertifikat`
- `X.509-Zertifikat`

Wenn Sie die NMAS-Methoden in der Antwortdatei angeben, zeigt das Identitätsdepot während der Installation eine Statusmeldung an, ohne dass eine Benutzereingabe angefordert wird.

## eDir:HTTP (Ports)

Das Identitätsdepot überwacht die vorkonfigurierten HTTP-Ports auf Zugriffe über das Web. iMonitor greift beispielsweise über Webschnittstellen auf das Identitätsdepot zu. Diese müssen bestimmte Ports angeben, damit sie auf die entsprechenden Anwendungen zugreifen können. Mit den folgenden Optionen können Sie das Identitätsdepot für bestimmte Ports konfigurieren:

**Klartext-HTTP-Port**

Gibt die Nummer des Ports für HTTP-Vorgänge im Klartext an.

**SSL-HTTP-Port**

Gibt die Nummer des Ports für HTTP-Vorgänge mit dem SSL-Protokoll an.

## Novell:Languages:1.0.0 (Spracheinstellungen)

Bei der Installation können Sie das Gebietsschema und die angezeigte Sprache für das Identitätsdepot festlegen: Englisch, Französisch oder Japanisch. Die Werte schließen sich gegenseitig aus.

**LangID4**

Steht für Englisch. Beispiel: `LangID4=true`.

**LangID6**

Steht für Französisch.

**LangID9**

Steht für Japanisch.

---

**HINWEIS**

- Geben Sie den Wert `Wahr` nur für eine einzige Sprache an, nicht für mehrere Sprachen gleichzeitig.
- Sie können auch die Sprache festlegen, in der das Installationsprogramm die Meldungen während der Installation anzeigen soll. Weitere Informationen finden Sie in „Initialisierung“, auf Seite 111.

---

## Initialisierung

Der Abschnitt `[Initialisierung]` der Datei `response.ni` enthält die Einstellungen für den Installationsvorgang.

**DisplayLanguage**

Gibt die Sprache an, in der die Meldungen während des Installationsvorgangs angezeigt werden sollen. Beispiel: `DisplayLanguage=en_US`.

**InstallationMode**

Gibt an, wie der Installationsvorgang ausgeführt werden soll. Für eine automatische oder unbeaufsichtigte Installation geben Sie beispielsweise `Automatisch` an.

**SummaryPrompt**

Gibt an, ob das Installationsprogramm eine Eingabeaufforderung anzeigt, mit der Sie aufgefordert werden, die Übersicht der Installationseinstellungen zu prüfen. Für eine automatische oder unbeaufsichtigte Installation geben Sie beispielsweise `Falsch` an.

**Eingabeaufforderung**

Gibt an, ob das Installationsprogramm bei Entscheidungen eine Eingabeaufforderung anzeigen soll. Für eine automatische oder unbeaufsichtigte Installation geben Sie beispielsweise `Falsch` an.

## NWI:SNMP

SNMP ist auf den meisten Windows-Servern konfiguriert und wird dort ausgeführt. Wenn Sie das Identitätsdepot installieren, müssen Sie die SNMP-Dienste anhalten und nach Abschluss der Installation neu starten. Während der manuellen Installation werden Sie durch das Programm aufgefordert, die SNMP-Dienste anzuhalten, bevor die Installation fortgesetzt werden kann.

Zum Anhalten der SNMP-Dienste ohne Eingabeaufforderung bei einer automatischen oder unbeaufsichtigten Installation geben Sie im Abschnitt `[NWI:SNMP]` in der Datei `response.ni` den Eintrag `Stop Service=yes` ein.

## EDIR:SLP

Während der Installation oder Aufrüstung ermittelt das Identitätsdepot mithilfe von SLP-Diensten (Service Location Protocol) andere Server oder Bäume im Teilnetz. Wenn die SLP-Dienste bereits auf dem Server installiert sind, können Sie diese durch die Version ersetzen, die in der aktuellen Version des Identitätsdepots inbegriffen sind, oder auch eigene SLP-Dienste verwenden.

**Deinstallation von Diensten erforderlich**

Gibt an, ob die bereits auf dem Server installierten SLP-Dienste deinstalliert werden sollen. Der Standardwert ist `Wahr`.

**Entfernen von Dateien erforderlich**

Gibt an, ob die Dateien für die bereits auf dem Server installierten SLP-Dienste entfernt werden sollen. Der Standardwert ist `Wahr`.

## Novell:ExistingTree:1.0.0

Das Installationsprogramm bietet Optionen für die unbeaufsichtigte Installation eines Primär- oder Sekundärservers im Netzwerk. Das Installationsprogramm entscheidet anhand von drei verschiedenen Schlüsseln, ob ein neuer Baum oder aber ein Sekundärserver in einem vorhandenen Baum installiert werden soll.

---

**HINWEIS:** Der Schlüssel `Neuer Baum` befindet sich im Abschnitt `NWI:NDS`. Weitere Informationen finden Sie in „NWI:NDS“, auf Seite 108.

---

**ExistingTreeYes**

Gültige Werte sind `Wahr` und `Falsch`. Wenn Sie beispielsweise einen neuen Baum installieren möchten, geben Sie `Falsch` an.

**ExistingTreeNo**

Gültige Werte sind `Wahr` und `Falsch`. Wenn Sie beispielsweise einen neuen Baum installieren möchten, geben Sie `True` an.

Soll eine automatische oder unbeaufsichtigte Installation ausgeführt werden, bei der keine Eingabeaufforderungen für Entscheidungen zur Installation eines Primär- oder Sekundärserver angezeigt werden, geben Sie im Abschnitt `Vorhandener Baum` in der Datei `response.ni` den Wert `prompt=false` an.

### Ausgewählte Knoten

Dieser Abschnitt in der Datei `response.ni` enthält die Komponenten, die im Identitätsdepot installiert sind, außerdem Informationen in der Profildatenbank, die weitere Details zur Komponente enthält (z. B. Quellspeicherort, Kopierzielort und Version der Komponente). Diese Angaben in der Profildatenbank werden in einer `.db`-Datei zusammengefasst, die in der Identitätsdepot-Version bereitgestellt wird.

Soll eine automatische oder unbeaufsichtigte Installation ausgeführt werden, bei der keine Eingabeaufforderungen für Entscheidungen angezeigt werden (z. B. zum Kopierzielort oder zu den Versionsdetails), geben Sie im Abschnitt `[Ausgewählte Knoten]` in der Datei `response.ni` den Wert `prompt=false` an.

Die Antwortdatei muss diesen Abschnitt enthalten. Verwenden Sie die Schlüssel und Werte aus der Beispieldatei `response.ni`.

### Novell:NOVELL_ROOT:1.0.0

Dieser Abschnitt in der Datei `response.ni` enthält die Einstellungen für die Bilder und Statusangaben, die während des Installationsvorgangs angezeigt werden. Hier können Sie beispielsweise festlegen, wie das Installationsprogramm auf bestimmte Szenarien (z. B. Probleme beim Schreiben in Dateien oder Entscheidungen für das Kopieren von Dateien) reagieren soll. Außerdem können Sie festlegen, ob Bilder angezeigt werden. Die meisten Bilder enthalten Informationen über die zu installierende Version des Identitätsdepots, die zu installierenden Komponenten, einen Begrüßungsbildschirm, Lizenzdateien, Optionen für die benutzerdefinierte Anpassung, eine Statusmeldung mit der derzeit installierten Komponente, eine Fortschrittsanzeige in Prozent und vieles mehr. Bei einigen Anwendungen, in denen eDirectory eingebettet werden soll, sollen diese Bilder nicht in eDirectory angezeigt werden.

Soll eine automatische oder unbeaufsichtigte Installation ausgeführt werden, bei der keine Eingabeaufforderungen für Entscheidungen angezeigt werden (z. B. zum Kopierzielort oder zu den Versionsdetails), geben Sie in der Datei `response.ni` den Wert `prompt=false` an.

Die Antwortdatei muss diesen Abschnitt enthalten. Verwenden Sie die Schlüssel und Werte aus der Beispieldatei `response.ni`.

## 10.2.2 Ausführen einer automatischen oder unbeaufsichtigten Installation

Prüfen Sie zunächst die Voraussetzungen für eine automatische oder unbeaufsichtigte Installation auf einem Windows-Server. Weitere Informationen finden Sie in Abschnitt 7.2.3, „Voraussetzungen für die Installation des Identitätsdepots auf einem Windows-Server“, auf Seite 73. Erstellen Sie außerdem die Datei `response.ni` als Schablone für die Installation. Weitere Informationen finden Sie in Abschnitt 10.2.1, „Bearbeiten der Datei response.ni“, auf Seite 107.

---

**HINWEIS:** Mit der Option `nopleasewait` im Befehl legen Sie fest, dass das Betriebssystem kein Statusfenster für die Installation, Aufrüstung oder Konfiguration anzeigt.

---

1. Erstellen Sie eine neue Datei `response.ni`, oder bearbeiten Sie eine vorhandene Antwortdatei. Weitere Informationen zu den Werten in der Antwortdatei finden Sie in Abschnitt 10.2.1, „Bearbeiten der Datei response.ni“, auf Seite 107.
2. Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem das Identitätsdepot installiert werden soll.

3 Öffnen Sie eine Eingabeaufforderung mit der Option **Als Administrator ausführen**.

4 Geben Sie an der Befehlszeile den folgenden Befehl ein:

```
path_to_installation_files\windows\eDirectory\x64\NDSonNT>install.exe /silent
/nopleasewait /template=Response file
```

Beispiel:

```
D:\builds\eDirectory\windows\eDirectory\x64\NDSonNT>install.exe /silent /
nopleasewait /template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
```

## 10.2.3 Ausführen einer automatischen Konfiguration

1 Erstellen Sie eine neue Datei `response.ni`, oder bearbeiten Sie eine vorhandene Antwortdatei. Weitere Informationen zu den Werten in der Antwortdatei finden Sie in Abschnitt 10.2.1, „Bearbeiten der Datei response.ni“, auf Seite 107.

2 Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem das Identitätsdepot installiert werden soll.

3 Öffnen Sie eine Eingabeaufforderung mit der Option **Als Administrator ausführen**.

4 Geben Sie an der Befehlszeile den folgenden Befehl ein:

```
Windows Drive\Program Files\Common Files\novell>install.exe /silent /
restrictnoderemove /nopleasewait /template=Response file
```

Beispiel:

```
c:\Program Files\Common Files\novell>install.exe /silent /restrictnoderemove /
nopleasewait /template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
```

## 10.2.4 Ausführen einer automatischen Installation mit nachfolgender Konfiguration

Prüfen Sie zunächst die Voraussetzungen für eine automatische oder unbeaufsichtigte Installation auf einem Windows-Server. Weitere Informationen finden Sie in Abschnitt 7.2.3, „Voraussetzungen für die Installation des Identitätsdepots auf einem Windows-Server“, auf Seite 73. Erstellen Sie außerdem die Datei `response.ni` als Schablone für die Installation.

1 Erstellen Sie eine neue Datei `response.ni`, oder bearbeiten Sie eine vorhandene Antwortdatei. Weitere Informationen zu den Werten in der Antwortdatei finden Sie in Abschnitt 10.2.1, „Bearbeiten der Datei response.ni“, auf Seite 107.

2 Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem das Identitätsdepot installiert werden soll.

3 Öffnen Sie eine Eingabeaufforderung mit der Option **Als Administrator ausführen**.

4 Geben Sie an der Befehlszeile den folgenden Befehl ein:

```
Unzipped Location\windows\eDirectory\x64\NDSonNT>install.exe /silent /
nopleasewait /template=Response file
```

Beispiel:

```
D:\builds\eDirectory\windows\eDirectory\x64\NDSonNT>install.exe /silent /
nopleasewait /template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
```

# 11 Anwenden von HotFix 2 auf das Identitätsdepot

Das Identity Manager-Installationspaket enthält die Dateien zum Anwenden des Hotfix 2 auf das Identitätsdepot für eDirectory 8.8.8 Patch 9 und eDirectory 9.0.2. Sie können den HotFix als Root-Benutzer, Administrator oder Nicht-Root-Benutzer installieren.

## 11.1 Voraussetzungen für die Installation des Hotfix

Führen Sie vor der Installation des Hotfix die folgenden Schritte durch:

- Halten Sie das Identitätsdepot an.
- (Bedingt) Unter Windows halten Sie das Identitätsdepot und die SNMP-Dienste an.

## 11.2 Installieren des Hotfix als Root-Benutzer oder Administrator

Installieren Sie den Hotfix mit den folgenden Schritten als Root-Benutzer im Identitätsdepot:

1. Vergewissern Sie sich, dass Sie die Voraussetzungen zur Installation des Hotfix erfüllen.
2. Melden Sie sich am Server, auf dem Sie den Hotfix ausführen möchten, als `Root`-Benutzer oder Administrator an.
3. Navigieren Sie zum Verzeichnis mit den Hotfix-Installationsdateien der `ISO`-Image-Datei.
   - **eDirectory 9.0.2 Hotfix 2:** `products/eDirectory/eDir902_HF2`
   - **eDirectory 8.8.8 Patch 9 Hotfix 2:** `products/eDirectory-888x/eDir8889_HF2`
4. Führen Sie den entsprechenden Befehl für Ihre Plattform aus:
   - **Linux:** Führen Sie die folgenden Befehle in einem Terminal-Fenster aus:
     - **eDirectory 9.0.2:** Führen Sie folgende Befehle aus:

       ```
       rpm -Uvh novell-NDSserv-9.0.2-2.x86_64.rpm

       rpm -Uvh novell-AUDTplatformagent-2.0.2-80.x86_64.rpm

       rpm -Uvh novell-AUDTedirinst-9.0.2-2.x86_64.rpm

       rpm -Uvh novell-eba-9.0.2-2.x86_64.rpm

       rpm -Uvh novell-nmas-server-9.0.2-2.x86_64.rpm
       ```

     - **eDirectory 8.8.8 Patch 9**: Führen Sie folgende Befehle aus:

       ```
       rpm -Uvh  novell-NDSserv-8.8.8.9-2.x86_64.rpm

       rpm -Uvh novell-AUDTedirinst-8.8.8.9-62.x86_64.rpm

       rpm -Uvh novell-AUDTplatformagent-2.0.2-80.x86_64.rpm

       rpm -Uvh novell-nmas-8.8.8.9-20170112.x86_64.rpm
       ```

- **Windows:** Führen Sie die folgenden Schritte aus:
  1. Kopieren Sie die folgenden Dateien vom Hotfix-Verzeichnis in Ihr aktuelles Verzeichnis. Beispiel: `C:\Novell\Directory`:
     - `nldap.dlm`
     - `ebasrv.dlm`
     - `nauditds.dlm`
     - `nmas.dlm`
  2. Installieren Sie die Datei `Novell_Audit_PlatformAgent_Win64.exe`.

**5** Starten Sie die eDirectory-Instanz.

- **Linux:** Geben Sie zum Starten aller Instanzen das folgende Kommando in der Kommandozeile ein:

  ```
  ndsmanage startall
  ```

  Geben Sie zum Starten einer einzelnen Instanz das folgende Kommando ein:

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

- **Windows:** Öffnen Sie ein Terminal und navigieren Sie zum Dienstprogramm `NDSCons.exe`, das sich standardmäßig im eDirectory-Installationsordner befindet:
  1. Führen Sie den folgenden Befehl aus:

     ```
     NDSCons.exe
     ```

  2. Klicken Sie im NDSCons-Dienstprogramm auf **Start**, damit alle eDirectory-Services gestartet werden.
  3. Klicken Sie zur Bestätigung auf **Ja**.
  4. Überprüfen Sie, ob alle eDirectory-Services ausgeführt werden, und schließen Sie dann das NDSCons-Dienstprogramm.

  Klicken Sie alternativ auf **Start > Systemsteuerung > Novell eDirectory Services**.

**6** (Bedingt) Zur Überprüfung, ob der Hotfix erfolgreich angewendet wurde, prüfen Sie das Änderungsdatum für die Dateien, die vom Hotfix-Installationsprogramm aktualisiert wurden.

- **Linux:** Führen Sie je nach eDirectory-Version die folgenden Kommandos aus:
  - **eDirectory 9.0.2:** Führen Sie folgende Befehle aus:

    ```
    rpm -qa | grep -i novell-NDSserv
    ```

    ```
    rpm -qa | grep -i novell-AUDTedirinst
    ```

    ```
    rpm -qa | grep -i novell-AUDTplatformagent
    ```

    ```
    rpm -qa | grep -i novell-eba
    ```

    ```
    rpm –qa | grep –i nmas
    ```

  - **eDirectory 8.8.8 Patch 9:** Führen Sie folgende Befehle aus:

    ```
    rpm -qa | grep -i novell-NDSserv
    ```

    ```
    rpm -qa | grep -i novell-AUDTedirinst
    ```

    ```
    rpm -qa | grep -i novell-AUDTplatformagent
    ```

    ```
    rpm -qa | grep -i nmas
    ```

- **Windows:** Führen Sie die folgenden Schritte aus:
  1. Klicken Sie im eDirectory-Installationsordner mit der rechten Maustaste auf die Datei `nldap.dlm`.
  2. Wählen Sie im Fenster „Eigenschaften“ die Registerkarte `Details` aus.
  3. Überprüfen Sie den Wert in der Version für die aktualisierten Komponenten.
     - `nmas` und `EBAServ` ist `9.0.2.2`
     - nldap ist 4.4.56.0

# 11.3 Installieren des Hotfix als Nicht-Root-Benutzer

Führen Sie die folgenden Schritte durch, um den Hotfix im Identitätsdepot als Nicht-Root-Benutzer zu installieren:

1. Vergewissern Sie sich, dass Sie die Voraussetzungen zur Installation des Hotfix erfüllen.
2. Melden Sie sich am Server, auf dem der Hotfix ausgeführt werden soll, als Nicht-Root-Benutzer an.
3. Navigieren Sie zum Verzeichnis mit den Hotfix-Installationsdateien der `ISO`-Image-Datei.
   - **eDirectory 9.0.2 Hotfix 2:** `products/eDirectory/eDir902_HF2`
   - **eDirectory 8.8.8 Patch 9 Hotfix 2:** `products/eDirectory-888x/eDir8889_HF2`
4. Erstellen Sie auf Ihrem Linux-Rechner ein temporäres Verzeichnis und extrahieren Sie die Dateien aus `nonroot.tar.gz` in dieses Verzeichnis.
5. Kopieren Sie mit dem folgenden Kommando das `opt`-Verzeichnis von diesem temporären Verzeichnisspeicherort an einen Installationsspeicherort von eDirectory:

   ```
   cp –rp opt/
   ```

   Beispiel eines eDirectory-Installationsspeicherorts: `/home/user/eDirectory`
6. Erstellen Sie ein anderes temporäres Verzeichnis, um Dateien von RPM zu extrahieren.
7. Navigieren Sie zum temporären Verzeichnis und führen Sie die folgenden Befehle basierend auf Ihrer aktuellen eDirectory-Version aus:
   - **eDirectory 9.0.2 Hotfix 2:** Führen Sie folgende Befehle aus:

     ```
     rpm2cpio ../novell-AUDTedirinst-9.0.2-2.x86_64.rpm | cpio –idmv
     ```
   - **eDirectory 8.8.8 Patch 9 Hotfix 2:** Führen Sie folgende Befehle aus:

     ```
     rpm2cpio ../novell-AUDTedirinst-8.8.8.9-62.x86_64.rpm | cpio –idmv
     ```
8. Kopieren Sie mit dem folgenden Befehl das `opt`-Verzeichnis vom temporären Verzeichnisspeicherort an einen Installationsspeicherort von eDirectory:

   ```
   cp –rp opt/
   ```

   Beispiel eines eDirectory-Installationsspeicherorts: `/home/user/eDirectory`
9. Starten Sie eDirectory.
   - Geben Sie zum Starten aller Instanzen das folgende Kommando in der Kommandozeile ein:

     ```
     ndsmanage startall
     ```
   - Geben Sie zum Starten einer einzelnen Instanz das folgende Kommando ein:

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

10 Rüsten Sie mit dem folgenden Befehl Ihre Baumkonfiguration auf:

```
ndsconfig upgrade
```

11 Starten Sie eDirectory neu.

- Geben Sie zum Starten aller Instanzen das folgende Kommando in der Kommandozeile ein:

  ```
  ndsmanage startall
  ```

- Geben Sie zum Starten einer einzelnen Instanz das folgende Kommando ein:

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

12 (Bedingt) Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Hotfix erfolgreich angewendet wurde:

```
strings <installed location>/opt/novell/eDirectory/lib64/nds-modules/
libnldap.so | grep –i version
```

Überprüfen Sie, ob der Wert in der Version `40004.56.5` für eDirectory 9.0.2 und `20810.25.5` für eDirectory 8.8.8 Patch 9 lautet.

# 12 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.

## 12.1 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 12, „Konfigurieren des Identitätsdepots nach der Installation“, auf Seite 119.

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*.

### 12.1.1 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.

**-S *Servername***

Gibt den Servernamen an. Punkte im Servernamen sind zulässig (beispielsweise netiq.com). Den Punkten muss jedoch jeweils ein Escape-Zeichen vorangestellt werden. Weitere Informationen zur Verwendung von Escape-Zeichen finden Sie in Abschnitt 8.1, „Verwenden von Escape-Zeichen im Namen eines Containers, der einen Punkt („.“) enthält“, auf Seite 83.

**-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. Weitere Informationen finden Sie in „Hinzufügen von LDAP-URLS für IPv6 auf dem LDAP-Serverobjekt“, auf Seite 90.

---

**-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.

## 12.1.2 Hinzufügen von SecretStore zum Identitätsdepotschema

Zur Unterstützung der SecretStore-Funktion müssen Sie das Identitätsdepotschema erweitern. Die Identitätsanwendungen benötigen SecretStore zur Verbindung mit dem Depot.

1. Geben Sie folgenden Befehl ein, um das Schema für das Identitätsdepot zu erweitern:

   ```
   ice -S SCH -f /installation_path/eDirectory/lib/nds-schema/sssv3.sch -D LDAP -
   s serverIP -d adminDN
   ```

   Beispiel:

   ```
   ice -S SCH -f /var/opt/novell/eDirectory/lib/nds-schema/sssv3.sch -D LDAP -s
   192.0.2.1 -d cn=admin,o=administrators
   ```

2. (Bedingt) Führen Sie die folgenden Schritte durch, um SecretStore auf einem Linux-Server zu konfigurieren:

   **2a** Navigieren Sie zum `conf`-Verzeichnis – standardmäßig unter `/opt/novell/eDirectory/bin`.

   **2b** Geben Sie `ssscfg -c` ein, um die Konfigurationsdatei auszuführen.

   **2c** Geben Sie die Konfigurationseinstellungen für SecretStore an und schließen Sie anschließend das Dienstprogramm.

   **2d** Öffnen Sie `ndsmodules.conf` in einem Texteditor.

   **2e** Fügen Sie der Datei den folgenden Eintrag hinzu:

```
ssncp
```

Durch diesen Eintrag wird das SecretStore-Modul geladen, wenn eDirectory startet.

3 (Bedingt) Führen Sie die folgenden Schritte durch, um SecretStore auf einem Windows-Server zu konfigurieren:

**3a** Navigieren Sie zum `conf`-Verzeichnis – standardmäßig unter `Programme/novell/eDirectory/conf`.

**3b** Geben Sie den folgenden Befehl ein:

```
ssscfg.exe -c
```

**3c** Geben Sie die Konfigurationseinstellungen für SecretStore an und schließen Sie anschließend das Dienstprogramm.

**3d** Führen Sie NDSCons.exe aus.

**3e** Geben Sie im Dienstprogramm `auto` für das `ssncp.dlm`-Modul an.

**3f** Schließen Sie das Dienstprogramm.

Weitere Informationen finden Sie unter SecretStore Configuration for eDirectory Server (SecretStore-Konfiguration für den eDirectory-Server) im *NetIQ eDirectory Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html) (NetIQ eDirectory-Verwaltungshandbuch).

## 12.1.3 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
```

## 12.1.4 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]
```

## 12.1.5 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
```

## 12.1.6 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]
```

## 12.1.7 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
```

### 12.1.8 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).

---

## 12.2 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.

### 12.2.1 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.

## 12.2.2 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.

## 12.2.3 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.

## 12.2.4 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 164.99.146.109:1524
```

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

## 12.2.5 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
   ```

# IV Installieren und Verwalten von Sentinel for Log Management für Identity Governance and Administration

In diesem Abschnitt werden Sie durch die Installation von Sentinel Log Management für IGA (Sentinel) geführt, dem Standard-Revisionsdienst für Identity Manager. Für die Berichterstellung ist diese Sentinel-Version oder ein Drittanbieter-Revisionsdienst wie NetIQ Sentinel erforderlich.

Die Installationsdateien befinden sich im Verzeichnis `products/Sentinel` in der `.iso`-Image-Datei des Identity Manager-Installationspakets. Standardmäßig installiert das Installationsprogramm die Komponenten in den Speicherort `/opt/novell/sentinel`.

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie in Kapitel 13, „Planen der Installation von Sentinel Log Management für IGA“, auf Seite 131.

# 13 Planen der Installation von Sentinel Log Management für IGA

In diesem Abschnitt finden Sie Anweisungen zum Vorbereiten der Installation von Sentinel Log Management für IGA (Sentinel), dem Standard-Revisionsdienst für Identity Manager.



## 13.1 Checkliste für die Installation von Sentinel

NetIQ empfiehlt, die Schritte in der nachfolgenden Checkliste auszuführen.

| | **Checkliste** |
|---|---|
| ❑ | 1. Informieren Sie sich über den Zeitpunkt für die Installation von Sentinel Log Management für IGA. Weitere Informationen finden Sie in Abschnitt 13.2, „Festlegen des Zeitpunkts für die Installation von Sentinel“, auf Seite 132. |
| ❑ | 2. Überprüfen Sie die Systemvoraussetzungen vor der Installation. Weitere Informationen finden Sie in Abschnitt 13.5, „Systemanforderungen“, auf Seite 133. |
| ❑ | 3. (Bedingt) Zur geführten Installation auf Computern mit dem Betriebssystem SLES 12 SP1 (oder höher) müssen die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in Abschnitt 6.3, „Installieren von Identity Manager auf Servern mit SLES 12 SP1 (oder höher)“, auf Seite 63. |
| ❑ | 4. (Bedingt) Stellen Sie bei Computern mit RHEL 6.x- oder Rhel 7.x-Betriebssystem sicher, dass die erforderlichen Bibliotheken installiert sind. Weitere Informationen finden Sie in Abschnitt 6.4, „Installieren von Identity Manager auf einem RHEL 6.*x- oder 7.x-Server“, auf Seite 63*. |
| ❑ | 5. Entscheiden Sie sich für einen Installationsmodus. Sentinel unterstützt die Installation im interaktiven Modus und im Automatikmodus. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |
| ❑ | 6. (Bedingt) Wenn Sie Ihre Daten von EAS zu Sentinel Log Management für IGA migrieren, beachten Sie Abschnitt 55.6.2, „Migrieren des Ereignisrevisionsdiensts in Sentinel for Log Management für IGA“, auf Seite 522. |
| ❑ | 7. (Bedingt) Richten Sie eine neue Datenbank für die Berichterstellung ein. Weitere Informationen finden Sie in „Einrichten des Berichterstellungsservers“, auf Seite 527. |
| ❑ | 8. Installieren Sie die Berichterstellung auf demselben Server, auf dem sich der migrierte Datenbankserver befindet. Weitere Informationen finden Sie in „Geführte Installation der Identitätsberichterstellung“, auf Seite 399. |

| | Checkliste |
|---|---|
| ❑ | 9. Führen Sie das Datensynchronisierungsprogramm aus, damit die Ereignisse von Sentinel an die Berichterstellungsdatenbank weitergeleitet werden. Weitere Informationen finden Sie in „Ausführen des Datensynchronisierungsprogramms“, auf Seite 527. |
| ❑ | 10. Legen Sie in der Datensynchronisierungsrichtlinie den richtigen Filter fest, damit Ereignisse nur von Identity Manager-Komponenten empfangen werden. Weitere Informationen finden Sie in „Filtern der Datensynchronisierungsrichtlinie“, auf Seite 530. |
| ❑ | 11. Melden Sie sich bei der Ereignisquellenverwaltung (Live-Ansicht) an und prüfen Sie, ob Sentinel Ereignisse empfängt. Weitere Informationen finden Sie in Abschnitt 53.6.1, „Prüfen auf Sentinel-Ereignisse“, auf Seite 484. |
| ❑ | 12. Konfigurieren Sie die iManager-, OSP- und SSPR-Collector-Instanzen. Weitere Informationen finden Sie in Abschnitt 53.6.2, „Konfigurieren der Collector-Instanzen in Sentinel“, auf Seite 484 |
| ❑ | 13. Konfigurieren Sie die Ereignisbeibehaltung und die Speicherplatznutzung. Weitere Informationen hierzu finden Sie in Abschnitt 53.6.3, „Konfigurieren der Ereignisdatenbeibehaltung“, auf Seite 484 und Abschnitt 53.6.4, „Konfigurieren der Speicherplatznutzung für Sentinel“, auf Seite 484. |
| ❑ | 14. Laden Sie die Berichte und Ansichten für Sentinel herunter. Weitere Informationen finden Sie unter Herstellen von Berichtsdefinitionen und Ansichten über die Download-Seite im Administratorhandbuch für die NetIQ-Identitätsberichterstellung. |
| ❑ | 15. (Bedingt) Konfigurieren Sie den Sentinel-Link, sodass Ereignisse von Sentinel über IGA an Sentinel Log Management weitergeleitet werden. Weitere Informationen finden Sie unter Abschnitt 53.6.6, „Konfigurieren der Sentinel-Link-Verbindung“, auf Seite 485. |

## 13.2 Festlegen des Zeitpunkts für die Installation von Sentinel

Wenn Sie bereits mit Sentinel oder mit einer Identity Tracking-Lösung arbeiten, können Sie die Revision von Ereignissen mithilfe der vorhandenen Sentinel-Installation vornehmen. Alternativ können Sie Sentinel Log Management für IGA installieren. Unabhängig von Ihrer Entscheidung müssen Sie das Datensynchronisierungsprogramm ausführen, mit dem eine Richtlinie in Sentinel für den Empfang von Ereignissen von den Identity Manager-Komponenten erstellt wird, die für die Revision konfiguriert sind. Weitere Informationen zum Ausführen des Datensynchronisierungsprogramms finden Sie unter „Ausführen des Datensynchronisierungsprogramms“, auf Seite 527.

## 13.3 Erläuterungen zum Installationsvorgang für Sentinel

Das Installationsprogramm für Sentinel führt folgende 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**)

## 13.4 Voraussetzungen für die Installation von Sentinel

Vergewissern Sie sich vor dem Beginn der Installation, dass folgende Aufgaben abgeschlossen sind:

- Vergewissern Sie sich, dass die Hardware und Software die in Abschnitt 13.5, „Systemanforderungen“, auf Seite 133 aufgeführten Systemanforderungen erfüllt.
- Wenn Sie mit Sentinel oder mit einer Identity Tracking-Lösung arbeiten und noch nicht auf Sentinel 8.0.0.1 aufgerüstet haben, müssen Sie den aktuellen JDBC-Patch anwenden:
  1. Halten Sie den Sentinel-Dienst an.

     ```
     rcsentinel stop
     ```

  2. Sichern Sie die Datei `postgresql-9.4-1201-jdbc4.jar` im Verzeichnis `$ESEC_HOME$/lib`.
  3. Navigieren Sie zum Verzeichnis `/products/SentinelLogManagementforIGA/patches` und kopieren Sie die Datei `postgresql-9.4-1212-jdbc4.jar` in das Verzeichnis `$ESEC_HOME$/lib`.
  4. Weisen Sie die erforderlichen Berechtigungen für die Datei `postgresql-9.4-1212-jdbc4.jar` zu:

     ```
     chown novell:novell postgresql-9.4-1212-jdbc4.jar
     ```

     ```
     chmod 600 postgresql-9.4-1212-jdbc4.jar
     ```

  5. Fügen Sie in die Datei `server.conf` einen Eintrag für `postgresql-9.4-1212-jdbc4.jar` ein:

     ```
     vi $ESEC_HOME$/config/server.conf
     ```

     ```
     wrapper.java.classpath.7=%ESEC_HOME%/lib/postgresql-9.4-1212-jdbc4.jar
     ```

  6. Starten Sie den Sentinel-Dienst.

     ```
     rcsentinel start
     ```

## 13.5 Systemanforderungen

Sentinel Log Management für IGA In diesem Abschnitt finden Sie die Mindestanforderungen für den oder die Server, auf dem bzw. 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 | 8 bis 15 GB |

| Kategorie | Anforderung |
| --- | --- |
| Betriebssystem (zertifiziert) | Eines der folgenden 64-Bit-Betriebssysteme:<br>◆ Red Hat Enterprise Linux 7.3<br>◆ Red Hat Enterprise Linux 7.2<br>◆ Red Hat Enterprise Linux 6.8<br>◆ Red Hat Enterprise Linux 6.7<br>◆ SUSE Linux Enterprise Server 12 SP1<br>◆ SUSE Linux Enterprise Server 11 SP4<br>NetIQ empfiehlt, vor der Installation von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden.<br>**HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird. |
| Betriebssystem (unterstützt) | Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme<br>**HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert. |

# 14 Installieren von Sentinel

Zur Installation von Sentinel können die folgenden Methoden angewendet werden:

- Durchführen einer interaktiven Installation
- Ausführen einer automatischen Installation

## 14.1 Durchführen einer interaktiven Installation

Sie können Sentinel wahlweise im interaktiven Modus oder im Automatikmodus installieren. Im interaktiven Modus haben Sie die Wahl zwischen der Standardinstallation und einer angepassten Installation. In der Standardinstallation installieren Sie Sentinel mit Standardwerten für die Ports, Lizenzen und Passwörter. Sollen die Portzuweisungen, Lizenzen und Passwörter während der Installation geändert werden, führen Sie die angepasste Installation aus.

Falls Sie auf Identity Manager 4.6 aufrüsten, migrieren Sie Ihre EAS-Daten nach der Installation zu Sentinel. Weitere Informationen finden Sie unter Abschnitt 55.6.2, „Migrieren des Ereignisrevisionsdiensts in Sentinel for Log Management für IGA“, auf Seite 522.

Im interaktiven Modus stehen zwei Möglichkeiten zur Installation von Sentinel zur Auswahl:

### 14.1.1 Standardinstallation

1. Melden Sie sich an dem Computer, auf dem Sentinel installiert werden soll, als Administratorbenutzer an.
2. Führen Sie im Verzeichnis mit den Installationsdateien den folgenden Befehl aus:

   ```
   ./install-logmanager
   ```

3. Geben Sie die Sprache an, die für die Installation verwendet werden soll. Drücken Sie dann die `Eingabetaste`.
4. Drücken Sie die `Leertaste` und lesen Sie die Lizenzvereinbarung.
5. Geben Sie `yes` bzw. `y` ein, um die Lizenzvereinbarung zu akzeptieren und mit der Installation fortzufahren.

   Das Laden der Installationspakete kann einige Sekunden in Anspruch nehmen.
6. Geben Sie bei der Eingabeaufforderung `1` an, um mit der Standardkonfiguration fortzufahren.

   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.
7. Geben Sie das Passwort für den Administratorbenutzer `admin` an.
8. 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 Server anmelden.

Geben Sie in einem Webbrowser folgende URL ein, um auf die Sentinel-Hauptoberfläche zuzugreifen:

`https://<IP_Address/DNS_Sentinel_server>:8443/sentinel/views/main.html`

<*IP_Address/DNS_Sentinel_server*> ist die IP-Adresse oder der DNS-Name des Sentinel-Servers. Der Standardport für den Sentinel-Server lautet *8443*.

## 14.1.2 Angepasste Installation

1. Melden Sie sich an dem Computer, auf dem Sentinel installiert werden soll, als Administratorbenutzer an.
2. Führen Sie im Verzeichnis mit den Installationsdateien den folgenden Befehl aus:

   ```
   ./install-logmanager
   ```

3. Geben Sie die Sprache an, die für die Installation verwendet werden soll. Drücken Sie dann die `Eingabetaste`.
4. Drücken Sie die `Leertaste` und lesen Sie die Lizenzvereinbarung.
5. Geben Sie `yes` bzw. `y` ein, um die Lizenzvereinbarung zu akzeptieren und mit der Installation fortzufahren.

   Das Laden der Installationspakete kann einige Sekunden in Anspruch nehmen.
6. Geben Sie `2` ein, um Sentinel benutzerdefiniert zu konfigurieren.
7. Geben Sie `1` ein, um den standardmäßigen Evaluierungslizenzschlüssel zu verwenden.

   Alternativ:

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

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

    Beispielsweise hat der Standardport für Datenbank-Services die Nummer 8443. Soll die Portnummer für die Datenbank-Services bearbeitet werden, geben Sie `4` an. Geben Sie den neuen Portwert für Datenbank-Services ein, beispielsweise „8643“.
12. Geben Sie nach dem Ändern der Ports „7“ ein, um den Änderungsvorgang abzuschließen.

13 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`.

14 Geben Sie `n` ein, wenn Sie aufgefordert werden, den FIPS 140-2-Modus zu aktivieren.

15 Geben Sie `n` ein, wenn Sie aufgefordert werden, den skalierbaren Speicher zu aktivieren.

Die Installation von Sentinel 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 Server anmelden.

Geben Sie in einem Webbrowser folgende URL ein, um auf die Sentinel-Hauptoberfläche zuzugreifen:

`https://<IP_Address/DNS_Sentinel_server>:<port>/sentinel/views/main.html`

*<IP_Address/DNS_Sentinel_server>* ist die IP-Adresse oder der DNS-Name des Sentinel-Servers und *<port>* ist der Standardport für den Sentinel-Server.

## 14.2 Ausführen einer automatischen Installation

Um eine automatische Installation von Sentinel durchführen zu lassen, erstellen Sie eine Eigenschaftendatei mit den für die Installation erforderlichen Parametern. In den Identity Manager-Medien befindet sich ein Beispiel für die `silent.properties`-Datei.

1 Erstellen Sie eine Eigenschaftendatei im Installationsverzeichnis, oder bearbeiten Sie die Beispieldatei `silent.properties`.

2 Tragen Sie in einem Texteditor die erforderlichen Parameter in die Datei ein.

3 Geben Sie folgenden Befehl ein, um Sentinel im Automatikmodus zu installieren:

```
./install-logmanager -u <full path of the silent.properties file>
```

## 14.3 Anpassen der Konfiguration

Wenn Sie nach der Installation von Sentinel einen gültigen Lizenzschlüssel eingeben möchten oder das Passwort oder die zugewiesenen Ports ändern möchten, können Sie hierzu das Skript `configure.sh` ausführen. Das Skript befindet sich im Ordner `/setup`.

1 Fahren Sie Sentinel mit dem folgenden Befehl herunter:

```
rcsentinel stop
```

2 Führen Sie das Skript `configure.sh` mit dem folgenden Befehl in der Befehlszeile aus:

```
./configure.sh
```

3 Geben Sie `1` ein, um die Standardkonfiguration durchzuführen, oder `2`, um Sentinel benutzerdefiniert zu konfigurieren.

4 Drücken Sie die `Leertaste` und lesen Sie die Lizenzvereinbarung.

5 Geben Sie `yes` bzw. `y` ein, um die Lizenzvereinbarung zu akzeptieren und mit der Installation fortzufahren.

   Das Laden der Installationspakete kann einige Sekunden in Anspruch nehmen.

6 Geben Sie `1` ein, um den standardmäßigen Evaluierungslizenzschlüssel zu verwenden.

   Alternativ:

   Geben Sie `2` ein, um einen erworbenen Lizenzschlüssel für Sentinel einzugeben.

7 Wählen Sie aus, ob Sie das vorhandene Passwort für den Administratorbenutzer `admin` beibehalten möchten.

   - Wenn Sie das vorhandene Passwort beibehalten möchten, geben Sie `1` ein.
   - Wenn Sie das Passwort ändern möchten, geben Sie `2` ein. Geben Sie dann das neue Passwort an und bestätigen Sie das Passwort.

   Der `admin`-Benutzer wird zum Ausführen von Verwaltungsaufgaben über die Sentinel-Hauptoberfläche verwendet. Dies umfasst auch die Erstellung weiterer Benutzerkonten.

8 Wählen Sie aus, ob Sie das vorhandene Passwort für den Datenbankbenutzer `dbauser` beibehalten möchten.

   - Wenn Sie das vorhandene Passwort beibehalten möchten, geben Sie `1` ein.
   - Wenn Sie das Passwort ändern möchten, geben Sie `2` ein. Geben Sie dann das neue Passwort an und bestätigen Sie das Passwort.

   Das `dbauser`-Konto wird von Sentinel zur Interaktion mit der Datenbank verwendet. Das hier eingegebene Passwort kann zum Ausführen von Datenbankwartungsaufgaben verwendet werden, unter anderem zum Zurücksetzen des Administratorpassworts, falls dieses vergessen wird bzw. nicht mehr auffindbar ist.

9 Geben Sie an, ob Sie das vorhandene Passwort für den Datenbankbenutzer `appuser` beibehalten möchten.

   - Wenn Sie das vorhandene Passwort beibehalten möchten, geben Sie `1` ein.
   - Wenn Sie das Passwort ändern möchten, geben Sie `2` ein. Geben Sie dann das neue Passwort an und bestätigen Sie das Passwort.

   Das `appuser`-Konto ist eine interne Identität, mit der der Java-Prozess von Sentinel eine Verbindung zur Datenbank herstellt und mit ihr interagiert. Das hier eingegebene Passwort wird zum Ausführen von Datenbankaufgaben verwendet.

10 Ändern Sie die Portzuweisungen für die Sentinel-Services, indem Sie die entsprechende Nummer und dann die neue Portnummer angeben.

11 Geben Sie nach dem Ändern der Ports `7` ein, um den Änderungsvorgang abzuschließen.

12 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`.

# V Installieren der Identity Manager-Engine, der Treiber und der iManager-Plugins

In diesem Abschnitt wird die Installation eines Teils des Basisrahmenwerks für den Identity Manager-Server beschrieben. Mit diesem Installationsprogramm können Sie die folgenden Komponenten installieren:

- Identity Manager-Treiber
- Identity Manager-Engine
- iManager-Plugins für Identity Manager

Als Arbeitserleichterung hat NetIQ die Komponenten zu einem einzigen Installationsprogramm zusammengefasst. Sie können diese Komponenten wahlweise allesamt auf demselben Server oder auch auf verschiedenen Servern installieren. Die Installationsdateien befinden sich im Verzeichnis `products/IDM/` im Identity Manager-Installationspaket. Standardmäßig installiert das Installationsprogramm die Komponenten in den folgenden Speicherorten:

- **Linux:** `/opt/netiq`
- **Windows:** `C:\netiq`

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie in Abschnitt 15.1, „Checkliste für die Installation der Identity Manager-Engine, der Treiber und der iManager-Plugins“, auf Seite 141.

---

**HINWEIS:** Mit diesem Installationsprogramm können Sie außerdem den Remote Loader installieren. Weitere Informationen finden Sie in Teil VI, „Installieren und Verwalten des Remote Loaders“, auf Seite 163.

---

# 15 Planen der Installation der Engine, der Treiber und der Plugins

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.



**HINWEIS:** Mit diesem Installationsprogramm können Sie außerdem den Remote Loader installieren. Weitere Informationen finden Sie in Teil VI, „Installieren und Verwalten des Remote Loaders“, auf Seite 163.

## 15.1 Checkliste für die Installation der Identity Manager-Engine, der Treiber und der iManager-Plugins

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 3.3.2, „Identity Manager-Engine“, auf Seite 32. |
| ❑ | 2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |
| ❑ | 3. Stellen Sie sicher, dass das Identitätsdepot installiert wurde und dass es einen Baum mit mindestens einer organisatorischen Einheit, einem Benutzer und einem iManager-Server enthält. Weitere Informationen finden Sie in Kapitel 9, „Installieren des Identitätsdepots auf einem Linux-Server“, auf Seite 99. |
| ❑ | 4. 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 15.3, „Voraussetzungen und Überlegungen für die Installation der Identity Manager-Engine“, auf Seite 143. |
| ❑ | 5. Prüfen Sie die Hardware- und Software-Voraussetzungen der Computer, auf denen die Identity Manager-Engine gehostet werden soll. Weitere Informationen hierzu finden Sie in Abschnitt 22.5, „Systemanforderungen für iManager Server“, auf Seite 224 und Abschnitt 22.6, „Systemanforderungen für iManager Workstation (Client-Version)“, auf Seite 225. |

| | Checkliste |
|---|---|
| ❑ | 6. Informieren Sie sich, welche Treiber nach der Installation der Identity Manager-Engine automatisch aktiviert werden. Weitere Informationen finden Sie in Abschnitt 15.3.2, „Überlegungen für die Installation von Treibern zusammen mit der Identity Manager-Engine“, auf Seite 144. |
| ❑ | 7. (Bedingt) Zur geführten Installation auf Computern mit dem Betriebssystem SLES 12 SP1 (oder höher) müssen die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in Abschnitt 6.3, „Installieren von Identity Manager auf Servern mit SLES 12 SP1 (oder höher)“, auf Seite 63. |
| ❑ | 8. (Bedingt) Stellen Sie bei Computern mit RHEL 6.x- oder Rhel 7.x-Betriebssystem sicher, dass die erforderlichen Bibliotheken installiert sind. Weitere Informationen finden Sie in Abschnitt 6.4, „Installieren von Identity Manager auf einem RHEL 6.*x- oder 7.x-Server“, auf Seite 63*. |
| ❑ | 9. Informieren Sie sich über die Optionen im Installationsprogramm. Weitere Informationen finden Sie in Abschnitt 15.2, „Erläuterungen zum Installationsprogramm“, auf Seite 142. |
| ❑ | 10. Überprüfen Sie, ob die UNIX/Linux-Umgebung den Voraussetzungen für die Identity Manager-Engine entspricht. Weitere Informationen finden Sie in Abschnitt 16.1, „Überprüfen der Umgebungsvariablen (UNIX/Linux) für die Identity Manager-Installation“, auf Seite 147. |
| ❑ | 11. (Bedingt) Befolgen Sie die Anweisungen für den geführten Installationsvorgang (Assistent) der Identity Manager-Engine in einem der folgenden Abschnitte:<br>◆ Abschnitt 17.1.1, „Installieren als Root-Benutzer oder als verwaltungsbefugter Benutzer“, auf Seite 151<br>◆ Abschnitt 17.1.2, „Installieren von mit einem Nicht-Root-Benutzer“, auf Seite 153 |
| ❑ | 12. (Bedingt) Sollen die Komponenten mit einem einzigen Befehl installiert werden, beachten Sie die Anweisungen in Abschnitt 17.2, „Ausführen einer automatischen Installation“, auf Seite 154. |
| ❑ | 13. (Bedingt) Soll der Remote Loader installiert werden, beachten Sie die Anweisungen in Teil VI, „Installieren und Verwalten des Remote Loaders“, auf Seite 163. |
| ❑ | 14. (Bedingt) Wenn Sie eine Nicht-Root-Installation durchführen, aktualisieren Sie den Treibersatz, um Grafiken in E-Mail-Benachrichtigungen zu unterstützen. Weitere Informationen finden Sie in Abschnitt 17.4.3, „Unterstützung für Grafiken in E-Mail-Benachrichtigungen“, auf Seite 161. |
| ❑ | 15. Starten Sie die Treiberinstanz im Remote Loader. Weitere Informationen finden Sie in Kapitel 20, „Konfigurieren des Remote Loaders und der Treiber“, auf Seite 181. |
| ❑ | 16. Installieren Sie die restlichen Identity Manager-Komponenten (z. B. Identitätsanwendungen und Identitätsberichterstellung). |

## 15.2 Erläuterungen zum Installationsprogramm

Als Arbeitserleichterung sind im Installationsprogramm mehrere Komponenten zusammengefasst, die gemeinsam das zugrunde liegende Rahmenwerk der Identity Manager-Lösung bilden. Sie können diese Komponenten wahlweise allesamt auf demselben Server oder auch auf verschiedenen Servern installieren. Weitere Informationen zu den Serveranforderungen finden Sie unter Planen der Installation der Engine, der Treiber und der Plugins für die einzelnen Komponenten, im Handbuch für die einzelnen Treiber sowie in den aktuellen Versionshinweisen.

Das Installationsprogramm bietet die folgenden Optionen zum Installieren der Komponenten:

**Identity Manager Server**

Installiert die Identity Manager-Engine, das Schema, den NetIQ Audit-Agenten sowie XDAS (Distributed Audit-Dienste).

**Server für verbundenes System**

Installiert den Remote Loader-Dienst und die Treiberinstanzen im 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.

Im Installationsprogramm können Sie die Treiber auswählen, die zusammen mit dem Remote Loader auf dem verbundenen System installiert werden sollen. Auf Linux-Servern können Sie wahlweise die 32-Bit-Version und/oder die 64-Bit-Version des Dienstes installieren. Auf Windows-Servern können Sie den .NET Remote Loader installieren.

**iManager-Plugins für Identity Manager**

Installiert die iManager-Plugins, mit denen Sie die Identity Manager-Treiber, die über strukturierte GCVs (Globalkonfigurationswerte) verfügen, in iManager verwalten können. Wählen Sie diese Option, wenn Sie iManager bereits auf dem Server installiert haben.

**Fan-out-Agent**

Installiert den Fan-out-Agenten für den JDBC-Fan-out-Treiber. Der JDBC-Fan-out-Treiber verwendet den Fan-out-Agenten, um mehrere JDBC-Fan-out-Treiberinstanzen zu erstellen. Der Fan-out-Agent lädt die JDBC-Treiberinstanzen basierend auf der Konfiguration der Verbindungsobjekte im Fan-out-Treiber. Weitere Informationen finden Sie im *Implementierungshandbuch zum NetIQ Identity Manager-Treiber für JDBC-Fan-out*.

**Treiber**

Die Identity Manager-Treiber synchronisieren die Identitätsdaten über verschiedene Verzeichnistypen, Datenbanken und Geschäftsanwendungen einerseits und dem Identitätsdepot andererseits hinweg. Sie können den Treiber so konfigurieren, dass die Daten nur in eine Richtung oder auch in beide Richtungen synchronisiert werden.

Im Installationsprogramm können Sie die Treiber auswählen, die zusammen mit den anderen Komponenten installiert werden sollen. Bei Bedarf können Sie einige Treiber auf einem Server installieren, auf dem die Identity Manager-Engine nicht gehostet wird. In diesem Fall muss auch der Remote Loader-Dienst auf diesem Server installiert werden.

## 15.3 Voraussetzungen und Überlegungen für die Installation der Identity Manager-Engine

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

- Abschnitt 15.3.1, „Überlegungen für die Installation der Identity Manager-Engine“, auf Seite 144
- Abschnitt 15.3.2, „Überlegungen für die Installation von Treibern zusammen mit der Identity Manager-Engine“, auf Seite 144

### 15.3.1 Überlegungen für die Installation der Identity Manager-Engine

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

- (Bedingt) Zur geführten Installation der Identity Manager-Engine auf einem Server mit SLES 12 SP1 (oder höher) müssen die Bibliotheken `libXtst6-32bit-1.2.1-4.4.1.x86_64`, `libXrender-32bit` und `libXi6-32bit` auf dem Server installiert sein.
- Bevor Sie die Identity Manager-Engine installieren können, muss zunächst das Identitätsdepot installiert werden. Das Identitätsdepot muss zudem einen Baum mit mindestens einer organisatorischen Einheit, einem Benutzer und einem iManager-Server enthalten.
- Installieren Sie die Identity Manager-Engine auf demselben Server, auf dem das Identitätsdepot gehostet wird. Je nach Version des Identitätsdepots installiert das Installationsprogramm die 32-Bit- oder 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 18.5, „Voraussetzungen und Überlegungen für die Installation des Remote Loaders“, auf Seite 169.
- (Bedingt) Wenn Sie die Identity Manager-Engine als Nicht-`Root`-Benutzer installieren, werden der NetIQ Sentinel-Plattformagent, der UNIX/Linux-Kontentreiber und der Remote Loader nicht durch das Installationsprogramm 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.

  ---

### 15.3.2 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 Abschnitt 53.7, „Aktivieren von Identity Manager“, auf Seite 486.

## 15.4 Systemanforderungen für die Identity Manager-Engine

In diesem Abschnitt finden Sie die Mindestanforderungen für die Server, auf denen die Identity Manager-Engine installiert werden soll. Überprüfen Sie die Voraussetzungen und Überlegungen zur Installation, insbesondere im Zusammenhang mit dem Betriebssystem.

| Kategorie | Anforderung |
|---|---|
| Prozessor | 1 GHz |
| Festplattenspeicher | ◆ 300 MB<br>◆ 150 MB zusätzlicher Festplattenspeicher pro 50.000 Benutzer |
| Arbeitsspeicher | ◆ 2048 MB für die Identity Manager-Engine<br>◆ 200 MB für Identity Manager-Treiber |
| Betriebssystem (zertifiziert) | Eines der folgenden 64-Bit-Betriebssysteme:<br>◆ Open Enterprise Server 2015 SP1<br>◆ Open Enterprise Server 11 SP2<br>◆ Red Hat Enterprise Linux 7.3<br>◆ Red Hat Enterprise Linux 6.8<br>◆ SUSE Linux Enterprise Server 12 SP1<br>◆ SUSE Linux Enterprise Server 11 SP4<br>◆ Windows Server 2012 R2<br>◆ Windows Server 2012<br>NetIQ empfiehlt, vor der Installation von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden.<br>**HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird. |
| Betriebssysteme (unterstützt) | Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme<br>**HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert. |
| Virtualisierungssystem | ◆ Hyper-V Server 2012 R2<br>◆ VMWare ESX 5.0 und höher<br>◆ Windows Server 2012 R2-Virtualisierung mit Hyper-V (unterstützt)<br>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 |
| --- | --- |
| Webbrowser | Einer der folgenden Browser (ggf. höhere Version):<br>◆ Google Chrome 51<br>◆ Microsoft Internet Explorer 11<br>◆ Mozilla Firefox 46 |
| Zusätzliche Software | ◆ NetIQ eDirectory 8.8.8 Patch 9 Hotfix 2<br>◆ NetIQ eDirectory 9.0.2 Hotfix 2<br>◆ iManager 2.7.7 Patch 9 (für eDirectory 8.8.8 Patch 9 oder höher)<br>◆ iManager 3.0.2 Patch 1 (für eDirectory 9.0.2 oder höher) |

# 16 Vorbereiten der Installation der Engine, der Treiber und der Plugins

Die Identity Manager-Engine verarbeitet die Datenänderungen, die im Identitätsdepot und in den verbundenen Anwendungen vorgenommen werden. Diese Engine wird auch als Metaverzeichnis-Engine bezeichnet. Die Identity Manager-Engine ist über Treiber mit den verbundenen Anwendungen verbunden. Der Remote Loader lädt die Treiber, die auf den Remote-Servern installiert sind, und kommuniziert an deren Stelle mit der Identity Manager-Engine.



## 16.1 Überprüfen der Umgebungsvariablen (UNIX/Linux) für die Identity Manager-Installation

Beim Installieren der Identity Manager-Engine auf einem Linux- oder UNIX-Server muss der Pfad für die Installation des Identitätsdepots in den Umgebungsvariablen des Systems festgelegt sein. Überprüfen Sie, ob die Umgebungsvariablen für eDirectory exportiert wurden. Geben Sie hierzu den folgenden Befehl an der Eingabeaufforderung ein:

```
set | grep $PATH
```

Wenn die Umgebungsvariablen festgelegt sind, gibt das System den Pfad für die Installation des Identitätsdepots zurück. Falls die Umgebungsvariablen noch nicht konfiguriert wurden, geben Sie den folgenden Befehl für Ihre aktuelle Shell ein:

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

Geben Sie unbedingt das Leerzeichen zwischen dem Punkt (.) und dem Schrägstrich (/) ein, damit der Befehl funktioniert. Weitere Informationen finden Sie unter Installation von eDirectory-Komponenten mithilfe des Dienstprogramms nds-install im *NetIQ eDirectory-Installationshandbuch*.

## 16.2 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:

## 16.2.1 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 148
- „Anhalten der Treiber mithilfe von iManager“, auf Seite 148

### 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.

## 16.2.2 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 149
- „Starten der Treiber mithilfe von iManager“, auf Seite 149

## 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.

# 17 Installieren der Engine, der Treiber und der iManager-Plugins

In diesem Abschnitt wird der Installationsvorgang für die Identity Manager-Engine, die Treiber, die iManager-Plugins und den Remote Loader beschrieben. Sie können diese Programme wahlweise allesamt auf demselben Server oder auch auf verschiedenen Servern installieren. Beispielsweise ist es möglich, einen Treiber auf einem verbundenen System zu installieren statt auf demselben Server wie die Identity Manager-Engine. In diesem Fall muss auch der Remote Loader auf diesem verbundenen System installiert werden.

NetIQ bietet sowohl eine geführte Installation als auch eine automatische Installation.



## 17.1 Installieren der Komponenten mit dem Assistenten

Das Installationsprogramm führt Sie durch die Konfigurationseinstellungen für die Identity Manager-Engine. Sie können die Installation an der Konsole oder auf der Benutzeroberfläche ausführen. Auf UNIX- und Windows-Computern geht das Installationsprogramm automatisch in den Assistenten-Modus über.

Anweisungen zum Vorbereiten der Installation finden Sie in Abschnitt 15.1, „Checkliste für die Installation der Identity Manager-Engine, der Treiber und der iManager-Plugins“, auf Seite 141. Beachten Sie auch die Versionshinweise zur betreffenden Version. Anweisungen für die unbeaufsichtigte Installation finden Sie in Abschnitt 17.2, „Ausführen einer automatischen Installation“, auf Seite 154.

---

**HINWEIS:** Führen Sie die Installation entsprechend der Methode, mit der Sie das Identitätsdepot installiert haben, als `Root`-Benutzer oder mit einem Nicht-`Root`-Benutzer aus.

---

### 17.1.1 Installieren als Root-Benutzer oder als verwaltungsbefugter Benutzer

In diesem Abschnitt wird die geführte Installation der Identity Manager-Engine als `Root`-Benutzer oder Administrator mit dem Assistenten oder der Konsole auf einem Windows-Computer beschrieben. Führen Sie das folgende Installationsprogramm für Ihre Plattform aus:

- **Linux:** `/products/IDM/install.bin`
- **Windows:** `\products\IDM\windows\setup\idm_install.exe`

**HINWEIS:** Wenn Sie auf einer Linux-Plattform die Identity Manager-Engine als `Root`-Benutzer installieren, befinden sich die Installationsdateien im `/tmp`-Verzeichnis. Wenn kein `/tmp`-Verzeichnis vorhanden ist, wird es vom Installationsprogramm erstellt. 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 `Root`-Benutzer oder als verwaltungsberechtigter Benutzer:**

1. Melden Sie sich als `Root` oder Administrator an dem Computer an, auf dem die Identity Manager-Engine installiert werden soll.
2. Führen Sie im Verzeichnis mit den Installationsdateien einen der folgenden Schritte aus:
   - **Linux (Konsole)** – Geben Sie Folgendes ein: `/install.bin -i console`
   - **Linux (Benutzeroberfläche)** – Geben Sie Folgendes ein: `/install.bin`
   - **Windows** – Führen Sie `idm_install.exe` aus.
3. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster „Komponenten auswählen“ die zu installierenden Komponenten aus.

   Weitere Informationen zu den Optionen finden Sie in Abschnitt 15.2, „Erläuterungen zum Installationsprogramm“, auf Seite 142.
5. (Optional) Wählen Sie mit den folgenden Schritten bestimmte Treiber für die einzelnen Komponenten aus:
   - **5a** Klicken Sie auf **Ausgewählte Komponenten anpassen** und dann auf **Weiter**.
   - **5b** Erweitern Sie den Eintrag **Treiber** unter der zu installierenden Komponente.
   - **5c** Wählen Sie die zu installierenden Treiber aus.
6. Klicken Sie auf **Weiter**.
7. Klicken Sie im Fenster mit dem Aktivierungshinweis auf **OK**. Weitere Informationen finden Sie in Abschnitt 53.7, „Aktivieren von Identity Manager“, auf Seite 486.
8. Geben Sie zur Authentifizierung ein Benutzerkonto und das zugehörige Passwort an, das über ausreichende Berechtigungen zum Erweitern des Schemas in eDirectory verfügt. Geben Sie den Benutzernamen im LDAP-Format an. Beispiel: `cn=Admin,o=Firma`.
9. Überprüfen Sie die Einstellungen auf der Seite zu den Aspekten vor der Installation.
10. Klicken Sie auf **Installieren**.
11. Aktivieren Sie Identity Manager. Weitere Informationen finden Sie in Abschnitt 53.7, „Aktivieren von Identity Manager“, auf Seite 486.
12. 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.
13. (Optional) Die Standardinstallationsverzeichnisse sind in der Datei `/tmp/idmInstall.log` aufgeführt.

## 17.1.2 Installieren von mit einem Nicht-Root-Benutzer

Die Installation von Identity Manager als Nicht-Root-Benutzer erhöht die Sicherheit des UNIX- oder Linux-Servers. Identity Manager kann nicht als Nicht-Root-Benutzer installiert werden, falls Sie das Identitätsdepot als Root-Benutzer installiert haben.

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 in Abschnitt 19.3, „Installieren des Java Remote Loaders unter Linux“, auf Seite 177.
- **UNIX/Linux-Kontentreiber:** Erfordert Root-Berechtigungen.

---

**HINWEIS:** Wenn Sie auf einer Linux-Plattform die Identity Manager-Engine als Nicht-Root-Benutzer installieren, befinden sich die Installationsdateien im Nicht-Root-Benutzer-Verzeichnis (Beispiel: /home/user, wobei „user“ für Nicht-Root-Benutzer steht). 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 (eDirectory) verfügen.

2. Führen Sie das Installationsprogramm aus:

   ```
   IDMversion_Lin/products/IDM/linux/setup/idm-nonroot-install
   ```

3. 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.

**Dienstprogramme**

(Optional) Wenn Sie ein Identity Manager-Treiberdienstprogramm für einen Windows-Server benötigen, müssen Sie die Dienstprogramme von den Datenträgern für die Identity Manager-Installation auf den Identity Manager-Server kopieren. Alle Dienstprogramme befinden sich im Verzeichnis `IDM`*`Version_Plattform`*`/product/IDM/`*`Plattform`*`/setup/utilities`.

4 Fahren Sie zum Abschließen des Installationsvorgangs mit Abschnitt 17.4, „Durchführen einer Nicht-Root-Installation“, auf Seite 157 fort.

5 Aktivieren Sie Identity Manager. Weitere Informationen finden Sie in Abschnitt 53.7, „Aktivieren von Identity Manager“, auf Seite 486.

6 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.

## 17.2 Ausführen einer automatischen Installation

Um eine automatische Installation von Identity Manager durchführen zu lassen, erstellen Sie eine Eigenschaftendatei mit den für die Installation erforderlichen Parametern. In den Identity Manager-Medien befindet sich ein Beispiel für eine Eigenschaftendatei:

- **Linux:** `/products/IDM/linux/setup/silent.properties`
- **Windows:** `\products\IDM\windows\setup\silent.properties`

**So lassen Sie eine automatische Installation ausführen:**

1 Erstellen Sie eine Eigenschaftendatei im Installationsverzeichnis, oder bearbeiten Sie die Beispieldatei `silent.properties`.

2 Tragen Sie in einem Texteditor die folgenden Parameter in die Datei ein:

**EDITION_INPUT_RESULTS**

Gibt die Edition des Identity Manager-Servers an. Beispiel: `Advanced Edition` oder `Standard Edition`. Anhand dieser Angaben konfiguriert das Installationsprogramm die angegebene Identity Manager-Edition.

**EDIR_USER_NAME**

Gibt den eindeutigen LDAP-Namen des Administratorkontos für das Identitätsdepot an. Beispiel: `c=Admin,o=netiq`. Über dieses Konto verbindet das Installationsprogramm die Identity Manager-Engine mit dem Identitätsdepot.

Unter Umständen müssen Sie diesen Parameter zur Beispieldatei `silent.properties` hinzufügen.

**EDIR_USER_PASSWORD**

Gibt das Passwort des Administratorkontos für das Identitätsdepot an. Beispiel: `netiq123`. Unter Umständen müssen Sie diesen Parameter zur Beispieldatei `silent.properties` hinzufügen.

Soll das Passwort nicht in der Datei gespeichert werden, lassen Sie dieses Feld leer. Das Installationsprogramm liest dann den Wert aus der Umgebungsvariablen `EDIR_USER_PASSWORD` aus. Stellen Sie sicher, dass die Umgebungsvariable `EDIR_USER_PASSWORD` vorhanden ist.

**METADIRECTORY_SERVER_SELECTED**

Gibt an, ob der Identity Manager-Server und die Treiber installiert werden sollen.

**CONNECTED_SYSTEM_SELECTED**

Gibt an, ob die 32-Bit-Version des Remote Loader-Dienstes und der Treiber installiert werden sollen. Sie können sowohl die 32-Bit-Version als auch die 64-Bit-Version auf demselben Server installieren.

**FANOUTAGENT_SELECTED**

Gibt an, ob der Fan-out-Agent für den JDBC-Treiber installiert werden soll.

**X64_CONNECTED_SYSTEM_SELECTED**

Gibt an, ob die 64-Bit-Version des Remote Loader-Dienstes und der Treiber installiert werden sollen. Sie können sowohl die 32-Bit-Version als auch die 64-Bit-Version auf demselben Server installieren.

**WEB_ADMIN_SELECTED**

*Gilt nur dann, wenn Sie iManager bereits installiert haben.*

Gibt an, ob die iManager-Plugins installiert werden sollen.

**UTLITIES_SELECTED**

Gibt an, ob die Dienstprogramme und die Systemkomponenten für den Remote Loader installiert werden sollen.

**DOT_NET_REMOTELOADER_SELECTED**

Gibt an, ob der .NET Remote Loader-Dienst und die Treiber auf dem Windows-Server installiert werden sollen.

**EDIR_NDS_CONF**

Gibt den Pfad zur Konfigurationsdatei `nds.conf` an, also zur Konfigurationsdatei für das Identitätsdepot. Beispiel: `/etc/opt/novell/eDirectory/nds.conf`.

Wenn Sie mehrere Instanzen des Identitätsdepots nutzen, geben Sie jeweils den entsprechenden Wert für die einzelnen Instanzen an.

**EDIR_IP_ADDRESS**

Gibt die IP-Adresse des Identitätsdepots an.

Wenn Sie mehrere Instanzen des Identitätsdepots nutzen, geben Sie jeweils die entsprechende Adresse für die einzelnen Instanzen an.

**EDIR_NCP_PORT**

Gibt die Portnummer des Identitätsdepots an.

Wenn Sie mehrere Instanzen des Identitätsdepots nutzen, geben Sie jeweils den entsprechenden Port für die einzelnen Instanzen an.

3 Für die automatische Installation geben Sie einen der folgenden Befehle im Verzeichnis der Eigenschaftsdatei ein:

- **Linux:** `install.bin -i silent -f` *`Dateiname`*`.properties`
- **Windows:** `install.exe -i silent -f` *`Dateiname`*`.properties`

4 (Optional) Die Standardinstallationsverzeichnisse sind in der Datei `/tmp/idmInstall.log` aufgeführt.

5 (Bedingt) Wenn Sie die Installation als Nicht-`Root`-Benutzer ausgeführt haben, fahren Sie mit Abschnitt 17.4, „Durchführen einer Nicht-Root-Installation“, auf Seite 157 fort.

## 17.3 Installieren auf einem Server mit mehreren Instanzen des Identitätsdepots

Identity Manager unterstützt diese Installation als Root-Benutzer und im Automatikmodus. Für diesen Vorgang müssen Sie eine `silent.properties`-Datei für jede Instanz des Identitätsdepots erstellen, in der Identity Manager installiert werden soll.

Führen Sie die folgenden Schritte durch, um Identity Manager im Automatikmodus zu installieren:

1. Die Voraussetzungen und Systemanforderungen finden Sie in Kapitel 15, „Planen der Installation der Engine, der Treiber und der Plugins“, auf Seite 141.
2. Befolgen Sie die Anleitungen in Abschnitt 17.2, „Ausführen einer automatischen Installation“, auf Seite 154.

   **2a** Die Datei silent.properties muss die folgenden Einstellungen enthalten:

   ```
   EDITION_INPUT_RESULTS=Advanced Edition
   EDIR_USER_NAME=cn=admin_name,o=organization_name
   EDIR_USER_PASSWORD=identity_vault_password
   METADIRECTORY_SERVER_SELECTED=true
   CONNECTED_SYSTEM_SELECTED=false
   X64_CONNECTED_SYSTEM_SELECTED=false
   WEB_ADMIN_SELECTED=false
   UTILITIES_SELECTED=false
   FANOUTAGENT_SELECTED=false
   EDIR_NCP_PORT=<ncp_port>
   EDIR_NDS_CONF=</path/to/edir/conf>
   EDIR_IP_ADDRESS=ip_address_for_identity_vault

   # For Customization use the following properties
   CUSTOM_SELECTED=true
   # engine custom list engine and drivers jdbc and delim
   CHOSEN_INSTALL_FEATURE_LIST_SERVER=ENGINE,JDBC,DELIM,additional_value
   ```

   **2b** Fügen Sie die folgenden zusätzlichen Werte hinzu, um die Liste der Engines anzupassen:

   - Server_DRIVERS
   - AD
   - EBSHR
   - EBSTCA
   - EBSUM
   - DELIM
   - EDIR
   - BIEDIR
   - JDBC
   - JMS
   - LDAP
   - NXSET
   - HINWEISE
   - PS
   - REMEDY
   - SAPUMJ

- SAPHR
- SAPBL
- SAPPORTAL
- SOAP
- REST
- SFORCE
- SENTREST
- BLACK
- BANNER
- GOOGLE
- AR
- NPUM
- TSS
- RACF
- AFC2
- UAD
- RRSD

3 (Bedingt) Suchen Sie die folgenden Zeilen in Datei `/tmp/idmInstall.log`, um zu überprüfen, ob die Installation erfolgreich war.

```
NDS schema extension complete.
exitValue=0
Schema extended
SCHEMA_EXTENDED=true
==== UpdateIDMConfigureStatus ==============================
stateFile: /root/idm/Uninstall_Identity_Manager/idmconfigure_state.conf
INSTALL_SUCCESS: SUCCESS
enter loop:
==== Complete ==============================================
INSTALL_SUCCESS=SUCCESS
```

# 17.4 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.


- Abschnitt 17.4.1, „Zuweisen des Passwortrichtlinienobjekts zu Treibersätzen“, auf Seite 158
- Abschnitt 17.4.2, „Erstellen des Standard-Benachrichtigungssammlungs-Objekts im Identitätsdepot“, auf Seite 160
- Abschnitt 17.4.3, „Unterstützung für Grafiken in E-Mail-Benachrichtigungen“, auf Seite 161

## 17.4.1 Zuweisen des Passwortrichtlinienobjekts 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 finden Sie unter „Erstellen einer benutzerdefinierten Passwortrichtlinie“, auf Seite 160.



### 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.
3. Erstellen Sie einen Container für Passwortrichtlinien.

   Weitere Informationen zum Erstellen eines Containers in eDirectory finden Sie im *eDirectory-Verwaltungshandbuch*.

### Erstellen des Passwortrichtlinienobjekts im Identitätsdepot

Nach der Erstellung des Containers für Passwortrichtlinien müssen Sie mit Designer oder dem ldapmodify-Dienstprogramm das `DirMXL-PasswordPolicy`-Objekt im Identitätsdepot erstellen. 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-Passwortrichtlinienobjekts im Identitätsdepot die Attribute aus der Datei; gehen Sie dazu folgendermaßen vor:

**Linux:**

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`.

**Windows:**

Führen Sie `ldapmodify.exe` im Verzeichnis `install/utilities` des Identity Manager-Installations-Kits aus.

## Zuweisen des Passwortrichtlinienobjekts

Sie müssen jedem Treibersatz in einem Baum das `DirMXL-Passwortrichtlinien`-Objekt hinzufügen.

1 Öffnen Sie Ihr Projekt in Designer.

2 Erweitern Sie Ihr Projekt im Bereich „Gliederung“.

3 Erweitern Sie **Paketkatalog > Allgemein > Allgemeine Einstellungen**, um zu überprüfen, ob das Standard-Universalpasswort-Richtlinienpaket vorhanden ist.

4 (Bedingt) Führen Sie folgende Schritte durch, wenn das Passwortrichtlinienpaket nicht bereits in Designer aufgelistet ist:

**4a** Klicken Sie mit der rechten Maustaste auf **Paketkatalog**.

**4b** Wählen Sie **Paket importieren** aus.

**4c** Wählen Sie **Standard-Universalpasswortrichtlinie für Identity Manager** aus, und klicken Sie anschließend auf **OK**.

Sie müssen möglicherweise die Option **Nur Basispaket anzeigen** deaktivieren, um sicherzustellen, dass in der Tabelle alle verfügbaren Pakete angezeigt werden.

5 Wählen Sie jeden Treibersatz aus, und weisen Sie ihm die Passwortrichtlinie zu.

### Erstellen 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 „Zuweisen des Passwortrichtlinienobjekts“, auf Seite 159.

---

## 17.4.2 Erstellen des Standard-Benachrichtigungssammlungs-Objekts im Identitätsdepot

Die Standard-Benachrichtigungssammlung ist ein Identitätsdepotobjekt, das einen Satz von Schablonen für E-Mail-Benachrichtigungen enthält, sowie ein Server, der zum Senden von aus Schablonen erstellten E-Mails verwendet wird. Der Nicht-`Root`-Installationsvorgang erstellt kein Standard-Benachrichtigungssammlungs-Objekt im Identitätsdepot. Sie müssen das Objekt mit Designer erstellen.



### Erstellen eines Containers für Benachrichtigungsschablonen

Identity Manager benötigt Schablonen für Standardbenachrichtigungen im Identitätsdepot. Der Nicht-`Root`-Installationsvorgang erstellt jedoch keinen Container für Benachrichtigungsschablonen.

1. Melden Sie sich im Identity Manager-Baum in iManager an.
2. Navigieren Sie zum Sicherheitscontainer in eDirectory.
3. Erstellen Sie einen Container für Benachrichtigungsschablonen.

   Weitere Informationen zum Erstellen eines Containers in eDirectory finden Sie im *eDirectory-Verwaltungshandbuch*.

### Erstellen des Standard-Benachrichtigungssammlungs-Objekts

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.

## 17.4.3 Unterstützung für Grafiken in E-Mail-Benachrichtigungen

Wenn Sie das Identitätsdepot und die Identity Manager-Engine als Nicht-`Root`-Benutzer installieren, sind in den E-Mail-Benachrichtigungen möglicherweise die in der E-Mail-Schablone enthaltenen Grafiken und Bilder nicht vorhanden. Wenn Sie beispielsweise `do-send-email-from-template` ausführen, wird die E-Mail 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 eDirectory neu.

# VI Installieren und Verwalten des Remote Loaders

In diesem Abschnitt erfahren Sie, wie Sie den Remote Loader, den .NET Remote Loader oder den Java Remote Loader installieren und Treiberinstanzen im Loader konfigurieren.

Das Installationsprogramm für den Remote Loader gehört zum Bundle der Identity Manager-Engine. Die Dateien befinden sich im Verzeichnis `products/IDM/` im Identity Manager-Installationspaket. Standardmäßig installiert das Installationsprogramm die Komponenten in den folgenden Speicherorten:

- **Linux:** `/opt/netiq`
- **Windows:** `C:\netiq`

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie in Abschnitt 18.1, „Checkliste für die Installation des Remote Loaders“, auf Seite 165.

# 18 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.



## 18.1 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 33. |
| ❑ | 2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |
| ❑ | 3. Stellen Sie sicher, dass die Identity Manager-Engine installiert ist. Weitere Informationen finden Sie in Teil V, „Installieren der Identity Manager-Engine, der Treiber und der iManager-Plugins“, auf Seite 139. |
| ❑ | 4. Lesen Sie die Überlegungen zur Installation des Remote Loaders, und prüfen Sie, ob die Computer den Voraussetzungen entsprechen. Weitere Informationen finden Sie in Abschnitt 18.5, „Voraussetzungen und Überlegungen für die Installation des Remote Loaders“, auf Seite 169. |
| ❑ | 5. Prüfen Sie die Hardware- und Software-Voraussetzungen der Computer, auf denen der Remote Loader gehostet werden soll. Weitere Informationen finden Sie in Abschnitt 18.6, „Systemanforderungen für den Remote Loader“, auf Seite 171. |
| ❑ | 6. (Bedingt) Zur geführten Installation auf Computern mit dem Betriebssystem SLES 12 SP1 (oder höher) müssen die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in Abschnitt 6.3, „Installieren von Identity Manager auf Servern mit SLES 12 SP1 (oder höher)“, auf Seite 63. |
| ❑ | 7. (Bedingt) Stellen Sie bei Computern mit RHEL 6.x- oder Rhel 7.x-Betriebssystem sicher, dass die erforderlichen Bibliotheken installiert sind. Weitere Informationen finden Sie in Abschnitt 6.4, „Installieren von Identity Manager auf einem RHEL 6.*x- oder 7.x-Server“, auf Seite 63*. |

| | Checkliste |
|---|---|
| ❑ | 8. (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 20.1, „Herstellen einer sicheren Verbindung zur Identity Manager-Engine“, auf Seite 181. |
| ❑ | 9. Entscheiden Sie, ob die 32-Bit- oder die 64-Bit-Version des Remote Loaders installiert werden soll. Weitere Informationen finden Sie in Abschnitt 18.4, „Verwenden des 32-Bit- und des 64-Bit-Remote Loaders auf demselben Computer“, auf Seite 169. |
| ❑ | 10. Entscheiden Sie, ob der Remote Loader oder der Java Remote Loader verwendet werden soll. Weitere Informationen finden Sie in Abschnitt 18.2.3, „Erläuterungen zum Java Remote Loader“, auf Seite 168. |
| ❑ | 11. Installieren Sie den Remote Loader:<br>◆ Anweisungen zur geführten Installation finden Sie in Abschnitt 19.1, „Installieren des Remote Loaders mit dem Assistenten“, auf Seite 175.<br>◆ Anweisungen zur automatischen Installation finden Sie in Abschnitt 19.2, „Ausführen einer automatischen Installation des Remote Loaders“, auf Seite 176. |
| ❑ | 12. (Bedingt) Soll der Java Remote Loader installiert werden, beachten Sie die Anweisungen in Abschnitt 19.3, „Installieren des Java Remote Loaders unter Linux“, auf Seite 177. |
| ❑ | 13. Prüfen Sie die Parameter zum Konfigurieren einer Treiberinstanz. Weitere Informationen finden Sie in Abschnitt 20.2, „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 185. |
| ❑ | 14. Befolgen Sie die Anweisungen zum Konfigurieren einer Treiberinstanz im Remote Loader in einem der folgenden Abschnitte:<br>◆ Abschnitt 20.3, „Konfigurieren des Remote Loaders für Treiberinstanzen unter UNIX oder Linux“, auf Seite 195<br>◆ Abschnitt 20.4, „Konfigurieren des Remote Loaders für Treiberinstanzen unter Windows“, auf Seite 196<br>◆ Abschnitt 20.5, „Konfigurieren des Java Remote Loaders für Treiberinstanzen“, auf Seite 199 |
| ❑ | 15. Bereiten Sie die Treiber für den Remote Loader vor. Weitere Informationen finden Sie in Abschnitt 20.6, „Konfigurieren von Identity Manager-Treibern für die Verwendung mit dem Remote Loader“, auf Seite 200. |
| ❑ | 16. Starten Sie die Treiberinstanz im Remote Loader. Weitere Informationen finden Sie in Abschnitt 21.1, „Starten einer Treiberinstanz im Remote Loader“, auf Seite 211. |
| ❑ | 17. (Bedingt) Weitere Informationen zum Konfigurieren der beiderseitigen Authentifizierung zwischen dem Remote Loader und der Identity Manager-Engine finden Sie in Abschnitt 20.7, „Konfigurieren der beiderseitigen Authentifizierung mit der Identity Manager-Engine“, auf Seite 201. |
| ❑ | 18. 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 20.8, „Überprüfen der Konfiguration“, auf Seite 209. |
| ❑ | 19. Installieren Sie die restlichen Identity Manager-Komponenten (z. B. Identitätsanwendungen und Identitätsberichterstellung). |

## 18.2 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 .NET Remote Loader eignet sich nur für Windows-Systeme.

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 `.so`-Dateien unter Linux/UNIX).

### 18.2.1 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 Loaders 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.

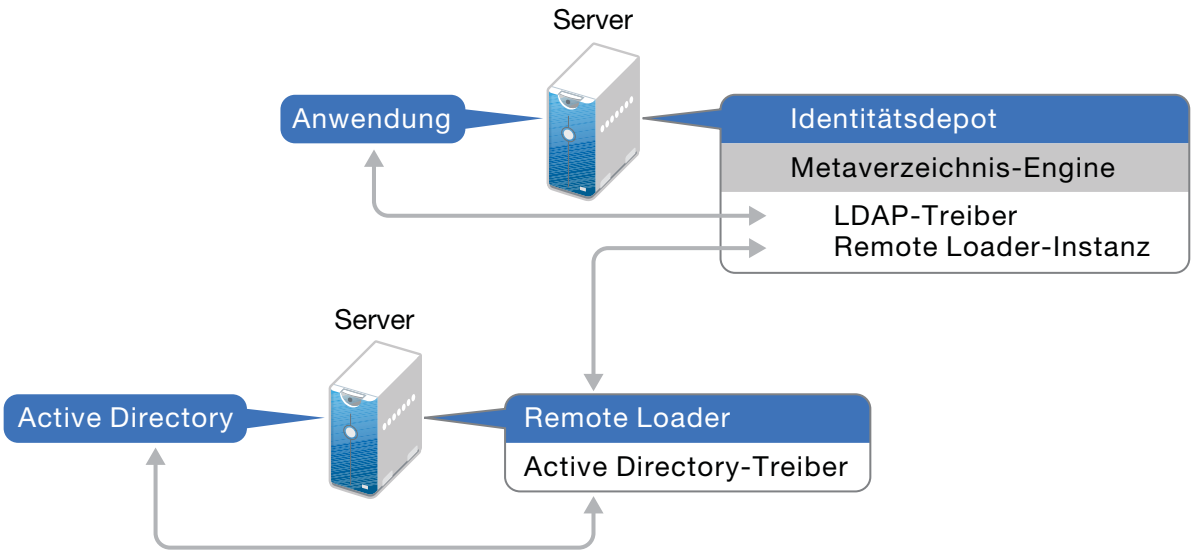
Weitere Informationen finden Sie in Kapitel 20, „Konfigurieren des Remote Loaders und der Treiber“, auf Seite 181.

### 18.2.2 Ermitteln des richtigen Zeitpunkts zum Verwenden des Remote Loaders

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.

### 18.2.3 Erläuterungen zum Java Remote Loader

Der Java Remote Loader bietet die Flexibilität zum Laden eines Treiberschnittstellenmoduls auf Computern mit UNIX- oder 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 20.5, „Konfigurieren des Java Remote Loaders für Treiberinstanzen“, auf Seite 199.

## 18.3 Erläuterungen zum Installationsprogramm

Als Arbeitserleichterung sind im Installationsprogramm mehrere Komponenten zusammengefasst, die gemeinsam das zugrunde liegende Rahmenwerk der Identity Manager-Lösung bilden. Sie können diese Komponenten wahlweise allesamt auf demselben Server oder auch auf verschiedenen Servern installieren. Neben dem Remote Loader können Sie im Installationsprogramm die Treiber auswählen, die auf dem verbundenen System installiert werden sollen. Das Installations-Kit umfasst die folgenden Installationsoptionen, abhängig vom Betriebssystem des Zielservers:

**Linux- oder UNIX-Server**

- Remote Loader als 32-Bit-Version, 64-Bit-Version oder beides
- Java Remote Loader

**Windows-Server**

.NET Remote Loader auf den unterstützten Betriebssystemen

## 18.4 Verwenden des 32-Bit- und des 64-Bit-Remote Loaders auf demselben Computer

Standardmäßig erkennt das Installationsprogramm die Betriebssystemversion und installiert anschließend die entsprechende Version des Remote Loaders. 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.

## 18.5 Voraussetzungen und Überlegungen für die Installation des Remote Loaders

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

- (Bedingt) Zur geführten Installation des Remote Loader auf einem Server mit SUSE Linux Enterprise Server (SLES) 12 SP1 (oder höher) müssen die Bibliotheken `libXtst6-32bit-1.2.1-4.4.1.x86_64`, `libXrender-32bit` und `libXi6-32bit` auf dem Server installiert sein.
- 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 18.6, „Systemanforderungen für den Remote Loader“, auf Seite 171.
- (Bedingt) Soll Identity Manager mit Active Directory verbunden werden, müssen Sie den Remote Loader und den Treiber für Active Directory auf einem Server installieren, der als Mitgliedserver oder Domänencontroller fungiert. Es ist nicht nötig, eDirectory und Identity Manager auf demselben Server wie das verbundene System zu installieren. Der Remote Loader sendet alle Ereignisse von Active Directory an den Identity Manager-Server. Der Remote Loader empfängt dann Informationen vom Identity Manager-Server und übergibt sie an die verbundene Anwendung.
- 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 eDirectory oder andere Treiber aus.
- eDirectory 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 Loaders:
  - Active Directory
  - Access Review
  - ACF2
  - Banner
  - Schwarzes Brett
  - Datenerfassungsdienste
  - Text mit Begrenzungszeichen
  - GoogleApps
  - REST
  - GroupWise 2014 (für den 32-Bit-Remote Loader)
  - JDBC
  - JMS
  - LDAP
  - Linux/UNIX-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 HR
  - SAP Portal
  - SAP-Benutzerverwaltung
  - 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

Weitere Informationen zum Remote Loader in Identity Manager finden Sie unter „Die zahlreichen Facetten des Remote Loaders in Identity Manager“.

## 18.6 Systemanforderungen für den Remote Loader

In diesem Abschnitt finden Sie die Mindestanforderungen für die Server, auf denen der Remote Loader, der .NET Remote Loader und der Java Remote Loader installiert werden sollen.

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

### 18.6.1 Remote Loader (32 Bit und 64 Bit)

| Kategorie | Anforderung |
|---|---|
| Prozessor | Pentium* III 600-MHz-Prozessor |
| Arbeitsspeicher | 512 MB |

| Kategorie | Anforderung |
|---|---|
| Betriebssystem (zertifiziert) | Eines der folgenden 64-Bit-Betriebssysteme:<br>◆ Open Enterprise Server 2015 SP1<br>◆ Open Enterprise Server 11 SP2<br>◆ Red Hat Enterprise Linux 7.3<br>◆ Red Hat Enterprise Linux 6.8<br>◆ SUSE Linux Enterprise Server 12 SP1<br>◆ SUSE Linux Enterprise Server 11 SP4<br>◆ Windows Server 2016<br>◆ Windows Server 2012 R2<br>◆ Windows Server 2012<br>◆ Windows Server 2008 R2<br>Für ein 32-Bit-Betriebssystem:<br>◆ Windows Server 2008 SP2<br>NetIQ empfiehlt, vor der Installation von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden.<br>**HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird. |
| Betriebssystem (unterstützt) | Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme<br>**HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert. |
| Virtualisierungssystem | ◆ Hyper-V Server 2012 R2<br>◆ VMWare ESX 5.0 und höher<br>◆ Windows Server 2012 R2-Virtualisierung mit Hyper-V (unterstützt)<br>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. |
| Webbrowser | Einer der folgenden Browser (ggf. höhere Version):<br>◆ Google Chrome 51<br>◆ Microsoft Internet Explorer 11<br>◆ Mozilla Firefox 46 |

## 18.6.2 .NET Remote Loader

Der .NET Remote Loader ist auf Windows-basierte Server ausgelegt.

| Kategorie | Anforderung |
|---|---|
| Prozessor | Pentium* III 600-MHz-Prozessor |
| Arbeitsspeicher | 512 MB |
| Betriebssystem (zertifiziert) | Eines der folgenden 64-Bit-Betriebssysteme:<br>◆ Windows Server 2015<br>◆ Windows Server 2012 R2<br>◆ Windows Server 2012<br>◆ Windows Server 2008 R2<br>Für ein 32-Bit-Betriebssystem:<br>◆ Windows Server 2008 SP2<br>NetIQ empfiehlt, vor der Installation von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden.<br>**HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird. |
| Betriebssystem (unterstützt) | Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme<br>**HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert. |
| Virtualisierungssystem | ◆ Hyper-V Server 2012 R2<br>◆ VMWare ESX 5.5<br>◆ Windows Server 2012 R2-Virtualisierung mit Hyper-V (unterstützt)<br>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. |
| .NET Framework | 4.x |

## 18.6.3 Java Remote Loader

Der Java Remote Loader kann auf jedem System mit kompatibler JRE und Java-Sockets ausgeführt werden.

| Kategorie | Anforderung |
|---|---|
| Prozessor | Pentium* III 600 MHz oder schneller |
| Arbeitsspeicher | 512 MB für den Remote Loader |
| JRE | Java8u112 oder höher<br>**HINWEIS:** Java Remote Loader funktioniert mit jeder öffentlich unterstützten Version von Java. |
| Plattformagent | Platform Agent 2011.1r5 |

# 19 Installation des Remote Loaders

Der Remote Loader kommuniziert über die folgenden Programme mit dem Server, auf dem die Identity Manager-Engine gehostet wird:

- **Linux und UNIX:** Die Programmdatei `rdxml` ermöglicht die Kommunikation der Identity Manager-Engine mit den in Solaris- oder Linux-Umgebungen ausgeführten Identity Manager-Treibern.
- **Windows:** Die Remote Loader-Konsole verwendet `rlconsole.exe` für die Kopplung mit `dirxml_remote.exe`. Dies ist eine Programmdatei, die die Kommunikation der Identity Manager-Engine mit den unter Windows ausgeführten Identity Manager-Treibern ermöglicht.



## 19.1 Installieren des Remote Loaders mit dem Assistenten

Das Installationsprogramm führt Sie durch die Konfigurationseinstellungen für den Remote Loader. Sie können die Installation an der Konsole oder auf der Benutzeroberfläche ausführen. Auf UNIX- und Windows-Computern geht das Installationsprogramm automatisch in den Assistenten-Modus über.

Anweisungen zum Vorbereiten der Installation finden Sie in Abschnitt 18.1, „Checkliste für die Installation des Remote Loaders“, auf Seite 165. Beachten Sie auch die Versionshinweise zur betreffenden Version. Anweisungen für die unbeaufsichtigte Installation finden Sie in Abschnitt 17.2, „Ausführen einer automatischen Installation“, auf Seite 154.

---

**HINWEIS:** Führen Sie die Installation entsprechend der Methode, mit der Sie das Identitätsdepot installiert haben, als `Root`-Benutzer oder mit einem Nicht-`Root`-Benutzer aus.

---

- **Linux:** `/products/IDM/install.bin`
- **Windows:** `\products\IDM\windows\setup\idm_install.exe`

**So installieren Sie den Remote Loader als `Root`-Benutzer oder als verwaltungsberechtigter Benutzer:**

1. Melden Sie sich als `Root` oder Administrator an dem Computer an, auf dem die Identity Manager-Engine installiert werden soll.

   ---

   **HINWEIS:** Sie können den Java Remote Loader als Nicht-`Root`-Benutzer installieren.

   ---

2. Führen Sie im Verzeichnis mit den Installationsdateien einen der folgenden Schritte aus:
   - **Linux (Konsole)** – Geben Sie Folgendes ein: `/install.bin -i console`

- **Linux (Benutzeroberfläche)** – Geben Sie Folgendes ein: `/install.bin`
- **Windows** – Führen Sie `idm_install.exe` aus.

3 Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf **Weiter**.

4 Wählen Sie im Fenster „Komponenten auswählen“ die zu installierenden Remote Loader-Komponenten aus.

Weitere Informationen zu den Optionen finden Sie in Abschnitt 15.2, „Erläuterungen zum Installationsprogramm“, auf Seite 142.

5 (Optional) Wählen Sie mit den folgenden Schritten bestimmte Treiber für die einzelnen Komponenten aus:

5a Klicken Sie auf **Ausgewählte Komponenten anpassen** und dann auf **Weiter**.

5b Erweitern Sie den Eintrag **Treiber** unter der zu installierenden Komponente.

5c Wählen Sie die zu installierenden Treiber aus.

6 Klicken Sie auf **Weiter**.

7 Klicken Sie im Fenster mit dem Aktivierungshinweis auf **OK**. Weitere Informationen finden Sie in Abschnitt 53.7, „Aktivieren von Identity Manager“, auf Seite 486.

8 Geben Sie zur Authentifizierung ein Benutzerkonto und das zugehörige Passwort an, das über ausreichende Berechtigungen zum Erweitern des Schemas in eDirectory verfügt. Geben Sie den Benutzernamen im LDAP-Format an. Beispiel: `cn=Admin,o=Firma`.

9 Überprüfen Sie die Einstellungen auf der Seite zu den Aspekten vor der Installation.

10 Klicken Sie auf **Installieren**.

11 Aktivieren Sie Identity Manager. Weitere Informationen finden Sie in Abschnitt 53.7, „Aktivieren von Identity Manager“, auf Seite 486.

12 Konfigurieren Sie den Remote Loader für die Verbindung mit den Treibern und mit Identity Manager. Weitere Informationen finden Sie in Kapitel 20, „Konfigurieren des Remote Loaders und der Treiber“, auf Seite 181.

13 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.

14 (Optional) Die Standardinstallationsverzeichnisse sind in der Datei `/tmp/idmInstall.log` aufgeführt.

## 19.2 Ausführen einer automatischen Installation des Remote Loaders

Für eine automatische Installation des Remote Loaders erstellen Sie eine Eigenschaftendatei mit den für die Installation erforderlichen Parametern. In den Identity Manager-Medien befindet sich ein Beispiel für eine Eigenschaftendatei:

- **Linux:** `/products/IDM/linux/setup/silent.properties`
- **Windows:** `\products\IDM\windows\setup\silent.properties`

**So lassen Sie eine automatische Installation ausführen:**

1 Erstellen Sie eine Eigenschaftendatei im Installationsverzeichnis, oder bearbeiten Sie die Beispieldatei `silent.properties`.

2 Tragen Sie in einem Texteditor die folgenden Parameter in die Datei ein:

**CONNECTED_SYSTEM_SELECTED**

Gibt an, ob die 32-Bit-Version des Remote Loader-Dienstes und der Treiber installiert werden sollen. Sie können sowohl die 32-Bit-Version als auch die 64-Bit-Version auf demselben Server installieren.

**X64_CONNECTED_SYSTEM_SELECTED**

Gibt an, ob die 64-Bit-Version des Remote Loader-Dienstes und der Treiber installiert werden sollen. Sie können sowohl die 32-Bit-Version als auch die 64-Bit-Version auf demselben Server installieren.

**UTLITIES_SELECTED**

Gibt an, ob die Dienstprogramme und die Systemkomponenten für den Remote Loader installiert werden sollen.

**DOT_NET_REMOTELOADER_SELECTED**

Gibt an, ob der .NET Remote Loader-Dienst und die Treiber auf dem Windows-Server installiert werden sollen.

3 Für die automatische Installation geben Sie einen der folgenden Befehle im Verzeichnis der Eigenschaftsdatei ein:

- **Linux:** `install.bin -i silent -f Dateiname.properties`
- **Windows:** `install.exe -i silent -f Dateiname.properties`

4 (Optional) Die Standardinstallationsverzeichnisse sind in der Datei `/tmp/idmInstall.log` aufgeführt.

# 19.3 Installieren des Java Remote Loaders unter Linux

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 UNIX- oder Linux-Rechner mit einer öffentlich unterstützten Version von Java (JRE 5.0 oder höher).

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 `.so`- 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 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 20, „Konfigurieren des Remote Loaders und der Treiber“, auf Seite 181.

## 19.4 Installieren des Java Remote Loaders unter Windows

Der Java Remote Loader dient in Identity Manager zum Datenaustausch zwischen der aktiven Identity Manager-Engine auf einem Server und den Identity Manager-Treibern an anderen Speicherorten, an denen `rdxml` nicht aktiviert ist. Installieren Sie den Java Remote Loader (dirxml_jremote) auf einer beliebigen unterstützten Windows-Plattform mit einer JRE (1.8.0 oder höher) und Java-Sockets.

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

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

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

4 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 `C:\NetIQ\IdentityManager`.

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.

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

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

Legen Sie beispielsweise Folgendes fest:

```
CLASSPATH=E:\RL\JAVARL\lib\activation.jar;E:\RL\JAVARL\lib\commondrivershim.ja
r;E:\RL\JAVARL\lib\delimitedtextshim.jar;E:\RL\JAVARL\lib\delimitedtextutil.ja
r;E:\RL\JAVARL\lib\dirxml.jar;E:\RL\JAVARL\lib\dirxml_misc.jar;E:\RL\JAVARL\li
b\dirxml_remote.jar;E:\RL\JAVARL\lib\jco3environment.jar;E:\RL\JAVARL\lib\mail
.jar;E:\RL\JAVARL\lib\mapdb.jar;E:\RL\JAVARL\lib\nxsl.jar;E:\RL\JAVARL\lib\shi
mwrapper.jar;E:\RL\JAVARL\lib\xds.jar;E:\RL\JAVARL\lib\xp.jar
```

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

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

Die JAR-Datei `dirxml_jremote.tar.gz` enthält diese Datei. Weitere Informationen finden Sie unter Kapitel 20, „Konfigurieren des Remote Loaders und der Treiber“, auf Seite 181.

11 Starten Sie den Remote Loader mit den folgenden Befehlen:

**11a** So geben Sie ein Passwort für den Remote Loader an:

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

Beispiel:

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

**11b** So starten Sie den Remote Loader:

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

Beispiel:

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

**11c** So stoppen Sie den Remote Loader:

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

Beispiel:

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

# 20 Konfigurieren des Remote Loaders und der Treiber

Der Remote Loader kann die in den `.dll-`, `.so-` 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 Loaders 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 Abschnitt 18.2.1, „Erläuterungen zu Schnittstellenmodulen“, auf Seite 167.



## 20.1 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 selbstsigniertes 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 Loaders 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.

---

## 20.1.1 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 Abschnitt 20.1.2, „Verwalten von selbstsignierten Serverzertifikaten“, auf Seite 182.
- **Bei einem Java-Treiber** müssen Sie einen Keystore erstellen. Weitere Informationen finden Sie in Abschnitt 20.1.3, „Erstellen einer Keystore-Datei für SSL-Verbindungen“, auf Seite 184.
- Verweisen Sie für einen **.NET-Treiber** auf ein base64-verschlüsseltes Zertifikat. Weitere Informationen finden Sie in Abschnitt 20.1.2, „Verwalten von selbstsignierten Serverzertifikaten“, auf Seite 182.

---

**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.

---

## 20.1.2 Verwalten von selbstsignierten Serverzertifikaten

Um die sichere Kommunikation zwischen dem Remote Loader und der Identity Manager-Engine zu gewährleisten, können Sie ein selbstsigniertes 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.

**HINWEIS:** Wenn der Remote Loader auf einem Server mit Windows 2012 R2 64 ( Bit) ausgeführt wird, muss das Zertifikat im Base64-Format vorliegen. Wenn Sie das DER-Format verwenden, kann der Remote Loader keine Verbindung zur Identity Manager-Engine herstellen.

**3f** Klicken Sie auf **Weiter**.

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

## 20.1.3 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 Loaders 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 184
- „Erstellen eines Keystore unter Linux“, auf Seite 184
- „Erstellen eines Keystore unter Windows“, auf Seite 185

### 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_selbstsignierten_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.

**HINWEIS:** Wenn Sie auf einem UNIX-Computer den Keystore mithilfe des selbstsignierten Zertifikats erstellen, können Sie das Zertifikat in das Base64-Format oder das binäre DER-Format exportieren.

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.

### Erstellen eines Keystore unter Windows

Führen Sie unter Windows das Keytool-Dienstprogramm aus (standardmäßig im Verzeichnis `c:\novell\remoteloader\jre\bin`).

## 20.2 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 (UNIX oder Linux) oder über die Remote Loader-Konsole (Windows) 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 den folgenden Abschnitten:

- **Linux und UNIX:** Abschnitt 20.3, „Konfigurieren des Remote Loaders für Treiberinstanzen unter UNIX oder Linux“, auf Seite 195
- **Windows:** Abschnitt 20.4, „Konfigurieren des Remote Loaders für Treiberinstanzen unter Windows“, auf Seite 196.

### 20.2.1 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 193.

**-commandport *Portnummer* (-cp *Portnummer*)**

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 1000 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 selbstsignierten 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=*Portnummer***

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 *Portnummer* (-jdp *Portnummer*)**

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 UNIX- oder Linux-JVM angegeben werden, trennen Sie die einzelnen Pfade jeweils mit Kommas voneinander ab. Bei einer Windows-JVM verwenden Sie ein Semikolon.

**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.

**-module „*Name*“ (-m „*Name*“)**

(Bedingt) Gibt bei Verwendung eines nativen Treibers das Modul an, in dem sich das zu hostende Identity Manager-Anwendungsschnittstellenmodul befindet. Diese Option weist die Anwendung an, ein `Rootfile`-Zertifikat zu verwenden. Bei einem nativen Treiber können Sie beispielsweise eine der folgenden Optionen angeben:

```
-module "c:\Novell\RemoteLoader\ADDriver.dll"
-m "c:\Novell\RemoteLoader\ADDriver.dll"
```

Alternativ:

```
-module "usr/lib/dirxml/NISDriverShim.so"
-m "usr/lib/dirxml/NISDriverShim.so"
```

**HINWEIS**

- Diese Option ist nicht zulässig, wenn Sie die Option `-class` angeben.
- Wenn Sie das `Tab`-Zeichen als Begrenzungszeichen in der Option `-module` 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.

**-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.

**-service *Wert* (-serv *Wert*)**

(Nur Windows) Gibt an, ob eine Instanz als Win32-Dienst auf einem Windows-Computer installiert werden soll. Zulässige Werte sind `install` und `uninstall` sowie die anderen Parameter, die zum Hosten eines Anwendungsschnittstellenmoduls erforderlich sind. Sie müssen beispielsweise den Parameter `-module` verwenden, während der Parameter `-commandport` und die Verbindungseinstellungen bei Bedarf angegeben werden können.

Mit diesem Befehl wird die Instanz lediglich als Dienst installiert oder deinstalliert. Der Dienst wird nicht gestartet.

Sie können diesen Befehl senden, während der Remote Loader läuft. Bei rdxml und dem Java Remote Loader ist dieser Befehl allerdings nicht zulässig.

**-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 c:\temp\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 Loaders 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.

**-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.

**-window *Wert* (-w) *Wert***

(Nur Windows) Weist die Anwendung an, das Trace-Fenster für eine Treiberinstanz auf einem Windows-Computer zu öffnen oder zu schließen. Zulässige Werte sind `Ein` und `Aus`. Beispiel:

```
-window on
```

Sie können diesen Befehl senden, während der Remote Loader läuft. Beim Java Remote Loader ist dieser Befehl nicht zulässig.

**-wizard (-wiz)**

(Nur Windows) Startet den Konfigurationsassistenten für den Remote Loader auf einem Windows-Computer. Mit dem Befehl `dirxml_remote.exe` (ohne Befehlszeilenparameter) können Sie den Assistenten auch direkt ausführen.

Wenn Sie diesen Befehl ausführen und dabei eine Konfigurationsdatei angeben (Option `-config`), wird der Assistent mit den Werten aus der Konfigurationsdatei gestartet. Im Assistenten können Sie die Konfiguration ändern, ohne die Konfigurationsdatei direkt bearbeiten zu müssen. Beispiel:

```
-wizard -config config.txt
```

Beim Java Remote Loader ist dieser Befehl nicht zulässig.

## 20.2.2 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 |

# 20.3 Konfigurieren des Remote Loaders für Treiberinstanzen unter UNIX oder Linux

Der Remote Loader kann die in den `.dll`-, `.so`- oder `.jar`-Dateien enthaltenen Identity Manager-Anwendungsschnittstellenmodule hosten. Damit der Remote Loader auf einem UNIX- oder 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 185.

---

**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
     - Keystore-Passwort
     - 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 20.2, „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 185.

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`.

## 20.4 Konfigurieren des Remote Loaders für Treiberinstanzen unter Windows

Der Remote Loader kann die in den `.dll-`, `.so-` oder `.jar`-Dateien enthaltenen Identity Manager-Anwendungsschnittstellenmodule hosten. Damit der Remote Loader ausgeführt werden kann, benötigt die Anwendung eine Konfigurationsdatei (z. B. `LDAPShim.txt`). Im Remote Loader-Konsolendienstprogramm (die Konsole) können Sie alle Instanzen der Identity Manager-Treiber verwalten, die auf dem Windows-Server ausgeführt werden. Hier können Sie die Instanzen eines Remote Loaders starten, anhalten, hinzufügen, entfernen und bearbeiten. Mit dem Installationsprogramm für den Remote Loader wird auch die Konsole installiert.

Beim Aufrüsten erkennt und importiert die Konsole die vorhandenen Treiberinstanzen. Damit ein Treiber automatisch importiert werden kann, müssen Sie die zugehörige Konfigurationsdatei im Remote Loader-Verzeichnis speichern (standardmäßig `c:\novell\remoteloader`). Anschließend können Sie die Remote-Treiber über die Konsole verwalten.

Über die Befehlszeile oder in der Remote Loader-Konsole können Sie den Remote Loader so konfigurieren, dass ein Treiber unter Windows erkannt wird. Weitere Informationen zur Verwendung der Befehlszeile finden Sie in Abschnitt 20.2, „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 185.

Dieser Abschnitt enthält Anweisungen für die folgenden Aufgaben:

- Abschnitt 20.4.1, „Erstellen einer neuen Treiberinstanz im Remote Loader unter Windows“, auf Seite 197
- Abschnitt 20.4.2, „Bearbeiten einer vorhandenen Treiberinstanz im Remote Loader unter Windows“, auf Seite 199

## 20.4.1 Erstellen einer neuen Treiberinstanz im Remote Loader unter Windows

1 Öffnen Sie die Remote Loader-Konsole.

---

**HINWEIS:** Wenn Sie während der Installation eine Verknüpfung zur Konsole erstellt haben, klicken Sie auf dem Desktop auf das Symbol `Identity Manager Remote Loader-Konsole`. Ansonsten führen Sie die Datei `rlconsole.exe` aus (standardmäßig unter `C:\novell\remoteloader\nnbit`).

---

2 Fügen Sie mit **Hinzufügen** eine Instanz des Treibers zu diesem Server hinzu.

3 Geben Sie unter **Beschreibung** einen kurzen Namen für die Instanz ein.

Die Konsole nutzt diese Angaben als Standardwert für die **Konfigurationsdatei**.

4 Wählen Sie unter **Treiber** den Namen der Java-Klasse aus.

---

**HINWEIS:** Soll der Active Directory-Treiber verwendet werden, wählen Sie **ADDriver.dll**. Weitere Informationen zu den Klassennamen für die einzelnen Treiber finden Sie unter „Erläuterungen zu den Namen für den Java-Parameter -class“, auf Seite 193.

---

5 Geben Sie unter **Konfigurationsdatei** den Pfad zu der Datei an, in der der Remote Loader die Konfigurationsparameter speichert. Der Standardwert lautet `C:\novell\remoteloader\nnbit\Beschreibung-config.txt`.

6 Legen Sie die Passwörter für den Remote Loader und das Treiberobjekt fest.

7 (Optional) Stellen Sie mit den folgenden Schritten eine TLS/SSL-Verbindung zwischen dem Remote Loader und dem Server der Identity Manager-Engine her:

**7a** Wählen Sie **SSL-Verbindung verwenden**.

---

**HINWEIS:** NetIQ empfiehlt, dieselbe SSL-Version auf dem Server der Identity Manager-Engine und für den Remote Loader zu verwenden. Wenn die SSL-Version auf dem Server nicht mit der SSL-Version des Remote Loaders 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.

---

**7b** Geben Sie unter **Herkunftsverbürgungsdatei** (Datei im base64-Format) das exportierte selbstsignierte Zertifikat aus der Organisationszertifizierungsstelle des eDirectory-Baums an. Weitere Informationen hierzu finden Sie in Abschnitt 20.1, „Herstellen einer sicheren Verbindung zur Identity Manager-Engine“, auf Seite 181 und Abschnitt 20.2, „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 185.

8 (Optional) Konfigurieren Sie die Trace-Datei für den Remote Loader mit den folgenden Schritten:

---

**HINWEIS:** NetIQ empfiehlt, die Trace-Funktion ausschließlich bei der Fehlersuche zu nutzen. Bei aktivierter Trace-Funktion sinkt die Leistung des Remote Loaders. Lassen Sie die Trace-Funktion im Produktionsmodus nicht aktiviert.

---

**8a** Geben Sie unter **Trace-Stufe** einen Wert größer null an. Dieser Wert definiert die Stufe der Informationsmeldungen sowohl vom Remote Loader als auch vom Treiber, die in einem Trace-Fenster angezeigt werden sollen. Die Werte 1 bis 4 sind von der Konsole vordefiniert. Wenn Sie eigene Meldungstypen erstellen möchten, geben Sie einen Wert größer oder gleich 5 ein.

Die häufigste Einstellung ist die Trace-Stufe 3, bei der Meldungen zur allgemeinen Verarbeitung, zu XML-Dokumenten und zum Remote Loader ausgegeben werden.

**8b** Geben Sie unter **Trace-Datei** den Pfad zu einer Datei an, in der die Trace-Meldungen protokolliert werden sollen. Beispiel: `C:\novell\remoteloader\64bit\Test-Delimited-Trace.log`.

Für jede Treiberinstanz auf einem Computer müssen Sie eine eindeutige Trace-Datei festlegen. Trace-Meldungen werden nur dann in die Trace-Datei geschrieben, wenn die Trace-Stufe größer Null ist.

**8c** Geben Sie unter **Maximaler Festplattenspeicher für alle Trace-Protokolldateien (MB)** einen ungefähren Wert für den Speicherplatz an, den die Trace-Datei für diese Instanz maximal belegen darf.

**9** (Optional) Soll der Remote Loader beim Hochfahren des Computers automatisch gestartet werden, wählen Sie **Remote Loader-Dienst für diese Treiberinstanz starten**.

---

**HINWEIS:** Wenn die SSL-Verbindung aufgrund von `handshaketimeout` fehlschlägt, während der Remote Loader eine Verbindung zur Identity Manager-Engine aufbaut, müssen Sie die Standardvariable `handshaketimeout` auf 10000 festlegen und sowohl den Treiber als auch den Remote Loader neu starten.

---

**10** (Bedingt) Sollen die Parameter für die Java-Konfiguration bearbeitet werden, führen Sie die folgenden Schritte aus:

**10a** Wählen Sie **Advanced** (Erweitert) aus.

**10b** Geben Sie unter **Klassenpfad** die Pfade an, in denen die JVM nach Paket- (`.jar`) und Klassendateien (`.class`) suchen soll. Sollen mehrere Pfade angegeben werden, trennen Sie die Pfade jeweils mit Doppelpunkten (UNIX oder Linux) bzw. mit Semikolons (Windows) voneinander ab.

Dieser Parameter entspricht dem Befehl `java -classpath`.

**10c** Geben Sie unter **JVM-Optionen** die Optionen an, die beim Starten der JVM-Instanz des Treibers verwendet werden sollen.

**10d** Geben Sie die anfängliche und die maximale Heap-Größe (in MB) für die JVM-Instanz an.

**10e** Geben Sie für die Suite B-Kommunikation `enforceSuiteB=true` an. Diese Kommunikation wird nur unter dem TLS 1.2-Protokoll unterstützt.

Weitere Informationen hierzu finden Sie in Abschnitt 20.1, „Herstellen einer sicheren Verbindung zur Identity Manager-Engine“, auf Seite 181 und Abschnitt 20.2, „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 185.

**10f** Klicken Sie auf **OK**.

**11** (Optional) Geben Sie die Version des sicheren Protokolls in der Konfigurationsdatei des Remote Loaders an, um zuzulassen, dass der Remote Loader das sichere Protokoll verwendet, während er eine Verbindung zur Identity Manager-Engine aufbaut. Beispiel: `secureprotocol=TLSv1_2`

Weitere Informationen finden Sie unter Abschnitt 20.2, „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 185.

---

**HINWEIS:** Überspringen Sie diesen Schritt, wenn Sie die Version des sicheren Protokolls bereits auf dem Treiber konfiguriert haben.

---

**12** (Optional) Geben Sie `enforceSuiteB=true` in der Konfigurationsdatei des Remote Loaders an, um zuzulassen, dass die Remote Loader-Kommunikation die von Suite B angegebenen Protokolle verwendet. Diese Kommunikation wird nur unter dem TLS 1.2-Protokoll unterstützt.

Weitere Informationen finden Sie unter Abschnitt 20.2, „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 185.

**HINWEIS:** Überspringen Sie diesen Schritt, wenn Sie bereits die Suite B-Kommunikation auf dem Treiber aktiviert haben.

13 Klicken Sie auf **OK**.

### 20.4.2 Bearbeiten einer vorhandenen Treiberinstanz im Remote Loader unter Windows

1 Wählen Sie in der Remote Loader-Konsole die gewünschte Treiberinstanz in der Spalte **Beschreibung** aus.

2 Klicken Sie auf **Beenden**.

3 Geben Sie das Passwort für den Remote Loader ein, und klicken Sie auf **OK**.

4 Klicken Sie auf **Bearbeiten**.

5 Bearbeiten Sie die Konfigurationsdaten. Weitere Informationen zu den einzelnen Parametern finden Sie unter „Erstellen einer neuen Treiberinstanz im Remote Loader unter Windows“, auf Seite 197.

6 Klicken Sie zum Speichern der Änderungen auf **OK**.

## 20.5 Konfigurieren des Java Remote Loaders 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 185.

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
  - Keystore-Passwort

- localaddress
- Hostname
- kmo
- secureprotocol
- enforceSuiteB
- useMutualAuth

- -java (bedingt)
- -javadebugport
- -password
- -service
- -setpasswords
- Trace-Dateiparameter (optional):
  - -trace
  - -tracefile
  - -tracefilemax

**HINWEIS:** Weitere Informationen zu den Parametern finden Sie in Abschnitt 20.2, „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 185.

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
```

## 20.6 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 185.

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**.

## 20.7 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 selbstsignierten 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:

- Abschnitt 20.7.1, „Exportieren der Zertifikate für die Identity Manager Engine und den Remote Loader“, auf Seite 202
- Abschnitt 20.7.2, „Aktivieren eines Treibers für die beiderseitige Authentifizierung“, auf Seite 205

## 20.7.1 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 202
- „Exportieren eines Drittanbieter-Zertifikats für Remote Loader“, auf Seite 204

### 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 20-1*** *Beispiele für verschiedene Treibertypen*

| Treibertyp | Befehl | Ausgabe |
|---|---|---|
| Java-Treiber | `dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client java '/home/certs'` | Datei `clientkmo_client.ks` im Verzeichnis `/home/certs/`<br><br>Das Standardpasswort für den Keystore lautet `dirxml`. |
| Nativer Treiber | `dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client native 'C:\certs'` | Dateien `clientkmo_clientcert.pem`, `clientkmo_clientkey.pem` und `trustedcert.b64` im Verzeichnis `C:\certs` |
| .NET-Treiber | `dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client dotnet 'C:\certs'` | Dateien `clientkmo_clientcert.pfx` und `trustedcert.b64` im Verzeichnis `C:\certs` |

## 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. Der .NET-Treiber verwendet die Datei im PFX-Format. Daher müssen Sie die Datei für einen .NET-Treiber konvertieren.

### Nativer Treiber

Führen Sie die folgenden Schritte durch:

1. Rufen Sie den privaten Schlüssel im PEM-Format von der PFX-Datei ab.

   Geben Sie einen Befehl ein, beispielsweise `openssl pkcs12 -in servercert.pfx -nocerts -out serverkey.pem –nodes`

2. Rufen Sie den Zertifikatsschlüssel im PEM-Format von der PFX-Datei ab.

   Geben Sie einen Befehl ein, beispielsweise `openssl pkcs12 -in servercert.pfx -nokeys -out servercert.pem`

### 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.

## 20.7.2 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 205
- „Konfigurieren des Remote Loaders für Treiberinstanzen“, auf Seite 207

### 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 Standardportnummer 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 **Passwort festlegen:** Mit dieser Option wird ein Anwendungspasswort festgelegt oder geändert.
   - 5f **Passwort löschen:** Löscht das Passwort für die Anwendung.
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=192.99.90.17 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=192.99.90.17 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 Loaders 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.

### Konfigurieren unter UNIX oder Linux

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. Öffnen Sie in einem Texteditor die Remote Loader-Konfigurationsdatei für den Treiber.
4. 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' storepass='dirxml' key='clientkmo' keypass='dirxml'"
     ```

   - 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' keypass='dirxml'
     certform=PEM keyform=PEM"
     ```

5. Speichern und schließen Sie die Datei.
6. Starten Sie den Treiber neu.

## Konfigurieren unter Windows

1. Wählen Sie in der Remote Loader-Konsole die gewünschte Treiberinstanz in der Spalte **Beschreibung** aus.
2. Klicken Sie auf **Beenden**.
3. Geben Sie das Passwort für den Remote Loader ein, und klicken Sie auf **OK**.
4. Klicken Sie auf **Bearbeiten**.
5. Führen Sie die folgenden Schritte durch, um die Konfigurationsinformationen zur Aktivierung der beiderseitigen Authentifizierung zu bearbeiten:

   **5a** Wählen Sie **Beiderseitige Authentifizierung** aus.

   **5b** Geben Sie für einen **nativen Treiber** den Pfad zur Schlüsseldatei an, in der das Zertifikat für die Authentifizierung gespeichert ist. Die Schlüsseldatei muss im Base 64-Format vorliegen.

   **Schlüsseldatei**

   Gibt den Pfad zur Datei an, in der der Schlüssel für die Authentifizierung gespeichert ist. Die Schlüsseldatei muss im Base 64-Format vorliegen. Beispiel: Datei `clientkmo_clientkey.pem` im Verzeichnis `C:\certs\` erstellt durch `dxcmd` im Abschnitt „Exportieren eines Zertifikats von eDirectory“, auf Seite 202.

   **Schlüsselpasswort**

   Gibt das Passwort für den privaten Schlüssel für die Authentifizierung an.

   **Zertifikatsdatei**

   Gibt die Datei an, in der die Zertifikate gespeichert sind. Die Zertifikatsdatei muss im Base 64-Format vorliegen. Beispiel: Datei `clientkmo_clientkey.pem` im Verzeichnis `C:\certs\` erstellt durch `dxcmd` im Abschnitt „Exportieren eines Zertifikats von eDirectory“, auf Seite 202.

   **Herkunftsverbürgungsdatei**

   Gibt den Namen der Datei an, die das Herkunftsverbürgungszertifikat des Herausgebers des Zertifikats für das Remote-Schnittstellenmodul enthält. Die Herkunftsverbürgungsdatei muss im Base 64-Format vorliegen. Beispiel: trustedcert.b64-Dateien im Verzeichnis `C:\certs\` erstellt durch `dxcmd` in Abschnitt „Exportieren eines Zertifikats von eDirectory“, auf Seite 202.

   **5c** Geben Sie für einen **Java-Treiber** den Pfad der Keystore-Datei an, die das Zertifikat enthält. Die Keystore-Datei muss mindestens ein Schlüsselpaar aus öffentlichem und privatem Schlüssel enthalten.

   **Keystore-Datei**

   Gibt den Pfad zur Java-Keystore-Datei an, die für die Authentifizierung verwendet werden soll. Die Keystore-Datei enthält Verschlüsselungsschlüssel und Zertifikate. Die Keystore-Datei muss mindestens ein Schlüsselpaar aus öffentlichem und privatem Schlüssel enthalten. Beispiel: Datei `clientkmo_client.ks` im Verzeichnis `C:\certs\` erstellt durch `dxcmd` im Abschnitt „Exportieren eines Zertifikats von eDirectory“, auf Seite 202.

   **Schlüssel-Alias**

   Gibt den Namen des Schlüsselpaars aus öffentlichem und privatem Schlüssel in der Keystore-Datei an, mit dem symmetrische Schlüssel generiert werden sollen. Beispiel: `clientkmo`.

   **Keystore-Passwort**

   Gibt das Passwort an, mit dem die Keystore-Datei geladen wird.

**Passwort für privaten Schlüssel**

Gibt das Passwort für den privaten Schlüssel an, der im Keystore gespeichert ist. Mit diesem Schlüssel verschlüsselt Identity Manager die SSL-Kommunikation.

**5d** Geben Sie für einen **.NET-Treiber** den Pfad zur Schlüsseldatei an, in dem das Zertifikat für die Authentifizierung gespeichert ist.

**Schlüsseldatei**

Gibt den Pfad zur Datei an, in der der Schlüssel für die Authentifizierung gespeichert ist. Beispiel:`clientkmo_clientcert.pfx` im Verzeichnis `C:\certs\` erstellt durch `dxcmd` in Abschnitt „Exportieren eines Zertifikats von eDirectory“, auf Seite 202.

**Schlüsselpasswort**

Gibt das Passwort für den privaten Schlüssel für die Authentifizierung an.

**Herkunftsverbürgungsdatei**

Gibt den Namen der Datei an, die das Herkunftsverbürgungszertifikat des Herausgebers des Zertifikats für das Remote-Schnittstellenmodul enthält. Die Herkunftsverbürgungsdatei muss im Base 64-Format vorliegen. Beispiel: Datei `trustedcert.b64` im Verzeichnis `C:\certs\` erstellt durch `dxcmd` in Abschnitt „Exportieren eines Zertifikats von eDirectory“, auf Seite 202.

**5e** Klicken Sie auf **OK**.

**6** Klicken Sie auf **OK**.

# 20.8 Überprüfen der Konfiguration

Weitere Informationen zum Starten und Anhalten des Remote Loaders finden Sie in Kapitel 21, „Starten und Anhalten des Remote Loaders“, auf Seite 211.

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
   ```

5. Installieren Sie den Remote Loader als Win32-Dienst. Beispiel:

   ```
   dirxml_remote -config config.txt -service install
   ```

# 21 Starten und Anhalten des Remote Loaders

Der Remote Loader wird entweder als Dienst oder als Daemon ausgeführt und muss von Zeit zu Zeit neu gestartet werden. In diesem Kapitel wird erläutert, wie Sie den Remote Loader anhalten und starten.



## 21.1 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.



### 21.1.1 Starten von Treiberinstanzen unter UNIX oder Linux

NetIQ bietet zwei Möglichkeiten zum Starten einer Treiberinstanz für den Remote Loader auf einem UNIX- oder Linux-Computer:



#### Automatisches Starten von Treiberinstanzen unter UNIX oder Linux

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 unter UNIX oder Linux über die Befehlszeile

Auf Linux-Plattformen unterstützt die Binärkomponente `rdxml` die Befehlszeilenfunktionen für den Remote Loader. Diese Komponente befindet sich standardmäßig im Verzeichnis `/usr/bin/`.

Weitere Informationen zu den Parametern in diesem Abschnitt finden Sie unter „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 185.

1. Öffnen Sie eine Befehlszeilen-Eingabeaufforderung.
2. Geben Sie die Passwörter zum Authentifizieren der Treiberinstanz bei der Identity Manager-Engine mit einem der folgenden Befehle ein:
   - **Linux/UNIX:** `rdxml -config filename -sp Remote Loader password Driver Object` *`password`*

- **Java Remote Loader:** `dirxml_jremote -config filename -sp Remote Loader password Driver Object password`

3 Starten Sie die Treiberinstanz mit dem folgenden Befehl:

```
rdxml -config Dateiname
```

4 Melden Sie sich bei iManager an, und starten Sie den Treiber.

5 Stellen Sie sicher, dass der Remote Loader ordnungsgemäß funktioniert.

- **Linux:** Prüfen Sie mit dem Befehl `ps` oder mit einer Trace-Datei, ob die Befehls- und Verbindungsports überwacht werden.
- **UNIX:** Überwachen Sie den Remote Loader, indem Sie den Befehl „tail“ auf die Trace-Datei anwenden:

  ```
  tail -f trace filename
  ```

  Wenn in der letzten Zeile des Protokolls der nachfolgende Text angezeigt wird, läuft der Loader ordnungsgemäß, und er wartet auf die vom Identity Manager Remote-Schnittstellenmodul kommenden Verbindungen:

  ```
  TRACE: Remote Loader: Entering listener accept()
  ```

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.

## 21.1.2 Starten von Treiberinstanzen unter Windows

NetIQ bietet drei Möglichkeiten zum Starten einer Treiberinstanz für den Remote Loader auf einem Windows-Computer:


- „Automatisches Starten von Treiberinstanzen unter Windows“, auf Seite 212
- „Starten von Treiberinstanzen unter Windows über die Konsole“, auf Seite 212
- „Starten von Treiberinstanzen unter Windows über die Befehlszeile“, auf Seite 213


### Automatisches Starten von Treiberinstanzen unter Windows

Sie können eine Treiberinstanz für den Remote Loader so konfigurieren, dass sie beim Hochfahren des Windows-Computers automatisch gestartet wird.

1 Öffnen Sie die Remote Loader-Konsole.

Wenn Sie während der Installation eine Verknüpfung zur Remote Loader-Konsole erstellt haben, klicken Sie auf dem Desktop auf das Symbol `Identity Manager Remote Loader-Konsole`. Ansonsten führen Sie die Datei `rlconsole.exe` aus (standardmäßig unter `C:\novell\remoteloader\nnbit`).

2 Wählen Sie eine Treiber-Instanz aus, und klicken Sie auf **Bearbeiten**.

3 Wählen Sie **Remote Loader-Service für diese Treiber-Instanz erstellen**.

4 Speichern Sie die Änderungen, und schließen Sie die Konsole.

### Starten von Treiberinstanzen unter Windows über die Konsole

1 Öffnen Sie die Remote Loader-Konsole.

Wenn Sie während der Installation eine Verknüpfung zur Remote Loader-Konsole erstellt haben, klicken Sie auf dem Desktop auf das Symbol `Identity Manager Remote Loader-Konsole`. Ansonsten führen Sie die Datei `rlconsole.exe` aus (standardmäßig unter `C:\novell\remoteloader\nnbit`).

2 Wählen Sie eine Treiber-Instanz aus, und klicken Sie anschließend auf **Starten**.

### Starten von Treiberinstanzen unter Windows über die Befehlszeile

Die Datei `dirxml_remote.exe` unterstützt die Befehlszeilenfunktion für den Remote Loader. Die ausführbare Datei befindet sich standardmäßig im Verzeichnis `c:\novell\RemoteLoader`. Weitere Informationen zu den Parametern in diesem Abschnitt finden Sie unter „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 185.

1 Öffnen Sie eine Befehlszeilen-Eingabeaufforderung.

2 Geben Sie die Passwörter zum Authentifizieren der Treiberinstanz für den Remote Loader bei der Identity Manager-Engine mit dem folgenden Befehl ein:

```
dirxml_remote -config filename -setpasswords password password
```

Beispiel:

```
dirxml_remote -config config.txt -sp Novell4 idmpwd6
```

3 Starten Sie die Treiberinstanz mit dem folgenden Befehl:

```
dirxml_remote -config filename
```

Beispiel:

```
dirxml_remote -config config.txt
```

4 Melden Sie sich bei iManager an, und starten Sie den Treiber.

5 Stellen Sie sicher, dass der Remote Loader ordnungsgemäß funktioniert.

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.

6 (Bedingt) Falls Sie den Remote Loader nicht als Win32-Dienst installiert haben, geben Sie den folgenden Befehl ein:

```
dirxml_remote -config filename -service install
```

Beispiel:

```
dirxml_remote -config config.txt -service install
```

## 21.2 Anhalten einer Treiberinstanz im Remote Loader

Für jede Plattform gilt eine andere Methode, mit der Sie eine Treiberinstanz im Remote Loader anhalten. Weitere Informationen zu den Parametern in diesem Abschnitt finden Sie unter „Erläuterungen zu den Kommunikationsparametern für den Remote Loader“, auf Seite 185.

**HINWEIS**

- Wenn mehrere Remote Loader-Instanzen auf einem UNIX- oder 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. Beispiel: Der Remote Loader läuft als Windows-Dienst. 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:

**Linux/UNIX**

Geben Sie den Befehl `rdxml -config` *`Dateiname`* `-u` ein. Beispiel:

```
rdxml -config config.txt -u
```

**Windows**

Verwenden Sie die Remote Loader-Konsole.

Wenn Sie während der Installation eine Verknüpfung zur Remote Loader-Konsole erstellt haben, klicken Sie auf dem Desktop auf das Symbol `Identity Manager Remote Loader-Konsole`. Ansonsten führen Sie die Datei `rlconsole.exe` aus (standardmäßig unter `C:\novell\remoteloader\`*`nn`*`bit`).

**Java Remote Loader**

Geben Sie den Befehl `dirxml_jremote -config` *`Dateiname`* `-u` ein. Beispiel:

```
dirxml_jremote -config config.txt -u
```

# VII Installieren von iManager

In diesem Abschnitt finden Sie die Schritte für die Installation der erforderlichen Komponenten für iManager. Mit dem Setup-Programm können Sie die folgenden Komponenten installieren:

- iManager (Server-Version)
- iManager Workstation (Client-Version)
- Java
- Novell International Cryptographic Infrastructure (NICI)
- Tomcat

Die Installationsdateien befinden sich im Verzeichnis `products/iManager/installs`*`Serverplattform`*`/` in der `.iso`-Image-Datei des Identity Manager-Installationspakets. Standardmäßig installiert das Installationsprogramm die Komponenten an den folgenden Speicherorten:

- **Linux:** `/opt/novell`
- **Windows:** `C:\Novell`

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie in Kapitel 22, „Planen der Installation von iManager“, auf Seite 217.

# 22 Planen der Installation von iManager

In diesem Abschnitt finden Sie die Voraussetzungen, die Überlegungen und die notwendige Systemeinrichtung für die Installation von iManager. Informieren Sie sich zunächst anhand der Checkliste über den Installationsvorgang.



## 22.1 Checkliste für die Installation von iManager

NetIQ empfiehlt, vor Beginn der Installation 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 25. |
| ❑ | 2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |
| ❑ | 3. Informieren Sie sich über den Unterschied zwischen iManager und iManager Workstation. Weitere Informationen finden Sie in Abschnitt 22.2, „Erläuterungen zur Server- und Client-Version von iManager“, auf Seite 219. |
| ❑ | 4. (Bedingt) Lesen Sie die folgenden Überlegungen, und ermitteln Sie, ob die Linux-Computer den Voraussetzungen für die Installation von iManager und iManager Workstation entsprechen:<br>◆ Für iManager beachten Sie Abschnitt 22.4.2, „Überlegungen für die Installation von iManager auf einer Linux-Plattform“, auf Seite 221.<br>◆ Für iManager Workstation beachten Sie Abschnitt 22.4.4, „Überlegungen für die Installation von iManager Workstation auf Linux-Clients“, auf Seite 222. |
| ❑ | 5. (Bedingt) Lesen Sie die folgenden Überlegungen, und ermitteln Sie, ob die Windows-Computer den Voraussetzungen für die Installation von iManager und iManager Workstation entsprechen:<br>◆ Für iManager beachten Sie Abschnitt 22.4.3, „Überlegungen für die Installation von iManager auf einer Windows-Plattform“, auf Seite 222.<br>◆ Für iManager Workstation beachten Sie Abschnitt 22.4.5, „Überlegungen für die Installation von iManager Workstation auf Windows-Clients“, auf Seite 223. |

| | Checkliste |
|---|---|
| ❑ | 6. Prüfen Sie die Hardware- und Software-Voraussetzungen der Computer, auf denen iManager gehostet werden soll:<br>◆ Für iManager beachten Sie Abschnitt 22.5, „Systemanforderungen für iManager Server“, auf Seite 224.<br>◆ Für iManager Workstation beachten Sie Abschnitt 22.6, „Systemanforderungen für iManager Workstation (Client-Version)“, auf Seite 225. |
| ❑ | 7. (Bedingt) Zur geführten Installation auf Computern mit dem Betriebssystem SLES 12 SP1 (oder höher) müssen die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in Abschnitt 6.3, „Installieren von Identity Manager auf Servern mit SLES 12 SP1 (oder höher)“, auf Seite 63. |
| ❑ | 8. (Bedingt) Stellen Sie bei Computern mit RHEL 6.x- oder Rhel 7.x-Betriebssystem sicher, dass die erforderlichen Bibliotheken installiert sind. Weitere Informationen finden Sie in Abschnitt 6.4, „Installieren von Identity Manager auf einem RHEL 6.*x- oder 7.x-Server“, auf Seite 63*. |
| ❑ | 9. Greifen Sie auf die Installationsdateien für iManager zu (standardmäßig im Verzeichnis `products/iManager/installs`*`Serverplattform`*`/` in der `.iso`-Image-Datei des Identity Manager-Installationspakets).<br>Alternativ laden Sie die Installationsdateien von der NetIQ Downloads-Website herunter. Suchen Sie nach iManager-Produkten, wählen Sie die gewünschte iManager-Version aus, und laden Sie die `.tgz`- und die `tar.bz2`- bzw. die `win.zip`-Datei in ein Verzeichnis auf dem Server herunter. Beispiel: `iMan_277_linux.tgz` und `iMan_277_workstation_linux.tar.bz2` oder `iMan_277_win.zip`. |
| ❑ | 10. (Optional) Weitere Informationen zum Installieren von Plugins finden Sie in Abschnitt 22.3, „Erläuterungen zur Installation der iManager Plugins“, auf Seite 219. |
| ❑ | 11. (Optional) Weitere Informationen zu den Aktionen, die Sie nach der Installation von iManager ausführen können, finden Sie in Kapitel 24, „Aufgaben nach Abschluss der Installation für iManager“, auf Seite 239. |
| ❑ | 12. Anweisungen zum Installieren von iManager und iManager Workstation finden Sie in den folgenden Abschnitten:<br>◆ Anweisungen für Linux-Computer finden Sie in Abschnitt 23.1, „Installieren von iManager und iManager Workstation unter Linux“, auf Seite 227.<br>◆ Anweisungen für Windows-Computer finden Sie in Abschnitt 23.2, „Installieren von iManager und iManager Workstation unter Windows“, auf Seite 232.<br>◆ Anweisungen zur automatischen Installation finden Sie in Abschnitt 23.3, „Automatische Installation von iManager“, auf Seite 236. |

## 22.2 Erläuterungen zur Server- und Client-Version von iManager

Sie müssen iManager auf einem Server installieren, der auf einen eDirectory-Baum zugreifen kann. Soll iManager auf einer Arbeitsstation statt auf einem Server installiert werden, benötigen Sie **iManager Workstation**, die clientgestützte Version von iManager. Anhand der folgenden Richtlinien können Sie ermitteln, welche dieser Versionen für Ihre Umgebung am besten geeignet ist und ob die Installation beider Versionen für Ihre eDirectory-Verwaltungsrichtlinien von Vorteil wäre.

- Wenn ein einzelner Administrator eDirectory immer von derselben Client-Arbeitsstation aus verwaltet, können Sie iManager Workstation nutzen. iManager Workstation ist 100 %ig eigenständig und erfordert nur geringen Einrichtungsaufwand. Beim Laden bzw. Entladen werden die benötigten Ressourcen automatisch gestartet und gestoppt. iManager Workstation kann auf verschiedenen Linux- bzw. Windows-Client-Arbeitsstationen installiert und ausgeführt werden, ist von der serverbasierten iManager-Instanz unabhängig und kann gleichzeitig mit jeder anderen Version von iManager verwendet werden, die in Ihrem Netzwerk installiert ist.

  iManager-Plugins werden nicht automatisch zwischen verschiedenen Instanzen von iManager synchronisiert. Wenn Sie mehrere Administratoren haben und benutzerdefinierte Plugins verwenden, müssen iManager Workstation und diese Plugins auf den Client-Arbeitsstationen aller Administratoren installiert sein.
- Wenn Sie eDirectory von mehreren Client-Arbeitsstationen aus verwalten oder mehrere Administratoren haben, installieren Sie den iManager-Server so, dass der Zugriff von sämtlichen verbundenen Arbeitsstationen aus möglich ist. Zudem müssen benutzerdefinierte Plugins nur einmal pro iManager-Server installiert werden.

## 22.3 Erläuterungen zur Installation der iManager Plugins

Standardmäßig werden die Plugin-Module nicht zwischen iManager-Servern reproduziert. Sie müssen die gewünschten Plugin-Module auf jedem einzelnen iManager-Server installieren.

Bei einer Neuinstallation wählt das Setup-Programm die „typischen“ Plugins selbsttätig aus. Bei der Aufrüstung sind nur die Plugins bereits ausgewählt, die aktualisiert werden müssen. Sie können die Standardauswahl außer Kraft setzen und neue Plugins zum Herunterladen hinzufügen. Bei einer Aufrüstung empfiehlt NetIQ jedoch, die Auswahl der vorausgewählten Plugins nicht aufzuheben. Im Allgemeinen sollten Sie alle Plugins aufrüsten, die Sie mit einer früheren Version von iManager installiert hatten. Neuere Plugins sind außerdem unter Umständen nicht mit früheren Versionen von iManager kompatibel.

Die Basis-Plugins für iManager sind nur als Teil des kompletten Software-Downloads von iManager verfügbar (beispielsweise eDirectory-Verwaltungs-Plugins). Wenn keine spezifischen Aktualisierungen für diese Plugins vorliegen, können Sie diese nur mit dem gesamten iManager-Produkt herunterladen und installieren.

Das Installationsprogramm ermittelt die zum Herunterladen bereitstehenden Plugins mithilfe der XML-Deskriptordatei `iman_mod_desc.xml`. Die Standard-URL für diese Datei lautet http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. Sie können jedoch im Installationsprogramm eine andere Netzwerk-URL angeben. Dies gilt beispielsweise dann, wenn Sie iManager hinter einem Proxy oder einer Firewall installieren, so dass das Installationsprogramm nicht auf die Standard-URL zugreifen kann.

**WICHTIG:** Alle benutzerdefinierten Plugins, die in der Umgebung der neu installierten Version verwendet werden sollen, müssen mit dem aktuellen iManager-SDK neu kompiliert werden.

Weitere Anweisungen zum Herunterladen und Installieren von Plugins finden Sie in einem der folgenden Abschnitte:

- **Linux:** Abschnitt 23.1, „Installieren von iManager und iManager Workstation unter Linux“, auf Seite 227
- **Windows:** Abschnitt 23.2, „Installieren von iManager und iManager Workstation unter Windows“, auf Seite 232
- **Automatische Installation:** Abschnitt 23.3, „Automatische Installation von iManager“, auf Seite 236

Weitere Informationen zum Anpassen des Vorgangs zum Herunterladen und Installieren von Plugins finden Sie unter „Downloading and Installing Plug-in Modules“ (Herunterladen und Installieren von Plugin-Modulen) im *NetIQ iManager-Installationshandbuch*.

## 22.4 Voraussetzungen und Überlegungen für die Installation von iManager

In diesem Abschnitt wird die Installation der Server- und der Arbeitsstationsversion von iManager beschrieben.



### 22.4.1 Überlegungen für die Installation von iManager

Lesen Sie vor dem Installieren von iManager die folgenden Überlegungen:

- Identity Manager 4.6 unterstützt zwei Versionen von eDirectory. Installieren Sie daher die jeweils kompatible Version von iManager.
  - eDirectory 9.0.2 mit Hotfix 2: iManager 3.0.2 Patch 1. Weitere Informationen finden Sie im Installationshandbuch zu NetIQ iManager.
  - eDirectory 8.8.8 Patch 9 mit Hotfix 2: iManager 2.7.7 Patch 9. Weitere Informationen finden Sie im Installationshandbuch zu NetIQ iManager.
- Wenn Sie das Identitätsdepot als `Root`-Benutzer installiert hatten, müssen Sie auch iManager als `Root`-Benutzer installieren.
- Wenn Sie planen, mehr als 10 Administratoren gleichzeitig in iManager arbeiten zu lassen, installieren Sie iManager nicht auf demselben Server wie andere Identity Manager-Komponenten.

- Soll nur ein Administrator eingesetzt werden, können Sie install iManager auf demselben Server wie die Identity Manager-Engine installieren.
- Wenn iManager auf einem Server installiert werden soll, auf dem eine unterstützte Open Enterprise Server-Plattform ausgeführt wird, müssen Sie über den Patch-Kanal der OES-Version auf die aktuelle iManager-Version aufrüsten.
- Wenn das Server-Setup-Programm von iManager eine zuvor installierte Version von iManager erkennt, haben Sie die Möglichkeit, den Installationsvorgang anzuhalten oder die vorhandenen iManager-, JRE- und Tomcat-Installationen zu entfernen. iManager 2.7.7 erkennt beispielsweise die Version 2.7.x.
- Da iManager Workstation eine eigenständige Umgebung ist, können Sie mehrere Versionen auf derselben Arbeitsstation installieren, einschließlich älteren Versionen von Mobile iManager. Allerdings sollten Sie nicht versuchen, sie gleichzeitig zu verwenden. Wenn Sie unterschiedliche Versionen verwenden müssen, führen Sie zuerst eine Version aus, schließen Sie sie und führen Sie anschließend die andere Version aus.
- iManager Workstation kann nicht von einem Pfad ausgeführt werden, der Leerzeichen enthält. Beispiel: `C:\NetIQ\iManager Workstation\working`.
- Für Linux-Server benötigen Sie den `Root`-Zugriff, für Windows-Server entsprechend den Administratorzugriff.
- Zum Erstellen einer Sammlung funktionsbasierter Dienste (RBS: Role-Based Services) im eDirectory-Baum benötigen Sie administratoräquivalente Rechte.
- Soll der iManager RBS-Konfigurationsassistent ausgeführt werden, benötigen Sie administratoräquivalente Rechte.
- Soll ein eDirectory-Baum mit mehreren iManager-Versionen verwaltet werden, müssen Sie die RBS-Sammlung(en) auf die aktuelle Version von iManager aktualisieren.

## 22.4.2 Überlegungen für die Installation von iManager auf einer Linux-Plattform

Vor der Installation von iManager müssen bestimmte Pakete bereits auf dem Linux-Server installiert sein. Im Allgemeinen können Sie die `.rpm`-Dateien von einer Website herunterladen, beispielsweise von http://rpmfind.net/linux.

### Red Hat Enterprise Linux

Die nachfolgenden Pakete müssen installiert werden. Wenn Sie iManager unter einer 64-Bit-Version von RHEL installieren, müssen auch die 32-Bit-Versionen der RHEL-Bibliotheken installiert werden.

- `compat-libstdc++-33-`*`Version`*`.el6.i686.rpm` (RHEL 6 oder 7 als 32-Bit-Version)
- `compat-libstdc++-33-`*`Version`*`.el6.i686.rpm` (RHEL 6 oder 7 als 64-Bit-Version)
- `compat-libstdc++-33-`*`Version`*`.el6.x86_64.rpm` (RHEL 6 oder 7 als 64-Bit-Version)
- `libstdc++-4.4.`*`Version`*`.el6.i686.rpm` (RHEL 6 oder 7 als 64-Bit-Version)
- `libstdc++-4.4.`*`Version`*`.el6.x86_64.rpm` (RHEL 6 oder 7 als 64-Bit-Version für GUI-Installationsmodus)
- `glibc-2.12-`*`Version`*`.el6.i686` (RHEL 6 oder 7 als 64-Bit-Version)
- `libXau-`*`Version`*`.el6.i686.rpm` (RHEL 6 oder 7 als 64-Bit-Version)
- `libxcb-`*`Version`*`.el6.i686.rpm` (RHEL 6 oder 7 als 64-Bit-Version)
- `libX11-`*`Version`*`.el6.i686.rpm` (RHEL 6 oder 7 als 64-Bit-Version)

- `libXext-Version.el6.i686.rpm` (RHEL 6 oder 7 als 64-Bit-Version)
- `libXi-Version.el6.i686.rpm` (RHEL 6 oder 7 als 64-Bit-Version)
- `libXtst-Version.el6.i686.rpm` (RHEL 6 oder 7 als 64-Bit-Version)
- `libstdc++-Version.el6.i686.rpm` (RHEL 6 oder 7 als 64-Bit-Version)
- `libgcc-Version.el6.i686.rpm` (RHEL 6 oder 7 als 64-Bit-Version)
- `libXrender-0.9.5-1.el6.i686.rpm` (RHEL 6 oder 7 als 64-Bit-Version)

### SUSE Linux Enterprise Server (64 Bit)

Die nachfolgenden Pakete müssen installiert werden.

- `libstdc++33-32bit`
- (Bedingt) Zur geführten Installation von iManager auf einem Server mit SUSE Linux Enterprise Server (SLES) 12 SP1 (oder höher) müssen die Bibliotheken `libXtst6-32bit-1.2.1-4.4.1.x86_64`, `libXrender-32bit` und `libXi6-32bit` auf dem Server installiert sein.

Zur Verwendung des PKI-Plugins müssen Sie außerdem die folgenden RPMs auf dem iManager-Server installieren:

- **SLES 11, 64 Bit:** `compat-32bit` (`compat-32bit-2009.1.19-2.1`)
- **SLES 11, 32 Bit:** `compat` (`compat-2009.1.19-2.1`)

### SUSE Linux Enterprise Server (32 Bit)

Die nachfolgenden Pakete müssen installiert werden.

- `libstdc++33`
- `libstdc++43`

Zur Verwendung des PKI-Plugins müssen Sie außerdem die folgenden RPMs auf dem iManager-Server installieren:

- **SLES 11, 64 Bit:** `compat-32bit` (`compat-32bit-2009.1.19-2.1`)
- **SLES 11, 32 Bit:** `compat` (`compat-2009.1.19-2.1`)

## 22.4.3 Überlegungen für die Installation von iManager auf einer Windows-Plattform

Wenn Sie Microsoft IIS (Internet Information Services) oder Apache HTTP Server für Windows verwenden, müssen Sie iManager manuell in diese Webserver-Infrastrukturen integrieren. iManager verwendet auf Windows-Servern standardmäßig Tomcat.

## 22.4.4 Überlegungen für die Installation von iManager Workstation auf Linux-Clients

Vor der Installation von iManager Workstation müssen die folgenden Pakete bereits auf den Linux-Clients installiert sein:

- `GTK2`
- `GLIBC 2.3`

- `libstdc++33`
  - SUSE Linux Enterprise Desktop (SLED) 11, 32 Bit
  - SLED 11 SP1, 32 Bit
  - openSUSE 11.0, 32 Bit
  - openSUSE 11.1, 32 Bit
  - openSUSE 11.2, 32 Bit
  - openSUSE 11.3, 32 Bit
  - openSUSE 12.1
- `libstdc++33-32bit`
  - SLED 11, 64 Bit
  - SLED 11 SP1, 64 Bit
  - openSUSE 11.0, 64 Bit
  - openSUSE 11.1, 64 Bit
  - openSUSE 11.2, 64 Bit
  - openSUSE 11.3, 64 Bit
- `libgtk-2_0-0-32bit`
  - openSUSE 12.2 (64 Bit)
  - openSUSE 12.3 (64 Bit)
- `libXt6-32bit`
  - openSUSE 12.2 (64 Bit)
  - openSUSE 12.3 (64 Bit)
- `libgthread-2_0-0-32bit`
  - openSUSE 12.2 (64 Bit)
  - openSUSE 12.3 (64 Bit)
- `libXtst6-32bit`
  - openSUSE 12.2 (64 Bit)
  - openSUSE 12.3 (64 Bit)

### 22.4.5 Überlegungen für die Installation von iManager Workstation auf Windows-Clients

NetIQ empfiehlt, vor dem Installieren von iManager Workstation auf Windows-Clients die folgenden Überlegungen zu lesen:

- Wenn Sie Internet Explorer für die Verwendung eines Proxyservers für Ihr LAN konfigurieren, müssen Sie unter **Extras** > **Internetoptionen** > **Verbindungen** > **LAN-Einstellungen** die Option **Proxyserver für lokale Adressen umgehen** wählen.
- Wenn Sie einen Novell-Client vor Version 4.91 verwenden, muss der NMAS-Client (NetIQ Modular Authentication Service) bereits auf der Arbeitsstation installiert sein, bevor Sie iManager Workstation starten.

- Wenn Sie iManager Workstation aus einem Pfad ausführen, bei dem ein Verzeichnisname den Ausdruck `temp` oder `tmp` enthält (beispielsweise `c:\Programme\temp\imanager`), werden die iManager-Plugins nicht installiert. Führen Sie iManager Workstation stattdessen über `C:\imanager` oder über ein nicht temporäres Verzeichnis aus.
- Verwenden Sie beim ersten Ausführen von iManager Workstation auf einer Windows-Arbeitsstation ein Konto, das Mitglied der Administratorengruppe der jeweiligen Arbeitsstation ist.

## 22.5 Systemanforderungen für iManager Server

In diesem Abschnitt finden Sie die Mindestanforderungen für die Server, auf denen iManager installiert werden soll. Weitere Informationen zur Server-Version von iManager finden Sie in Abschnitt 22.2, „Erläuterungen zur Server- und Client-Version von iManager“, auf Seite 219.

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

| Kategorie | Anforderung |
|---|---|
| Prozessor | Pentium* III 600 MHz |
| Festplattenspeicher | **Linux**: 200 MB<br>**Windows**: 500 MB |
| Arbeitsspeicher | 512 MB (1024 MB empfohlen)<br>80 MB für iManager-Plugins |
| Betriebssystem | Identity Manager 4.6 unterstützt zwei Versionen von eDirectory. Installieren Sie daher die jeweils kompatible Version von iManager.<br>- iManager 3.0.2 Patch 1: Weitere Informationen finden Sie im Installationshandbuch zu NetIQ iManager.<br>- iManager 2.7.7 Patch 9: Weitere Informationen finden Sie im Installationshandbuch zu NetIQ iManager.<br>**HINWEIS:** iManager kann nicht auf einer Solaris-Plattform installiert werden. Allerdings kann iManager dennoch Anwendungen und Ressourcen verwenden, die auf einer Solaris-Plattform ausgeführt werden, beispielsweise eDirectory. |
| Betriebssystem-Hotfixes | NetIQ empfiehlt, die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden. |
| Webbrowser | Einen beliebigen Webbrowser, der für Ihre Version von iManager im Installationshandbuch zu NetIQ iManager aufgeführt ist.<br>- iManager 3.0.2 Patch 1: Weitere Informationen finden Sie im Installationshandbuch zu NetIQ iManager.<br>- iManager 2.7.7 Patch 9: Weitere Informationen finden Sie im Installationshandbuch zu NetIQ iManager. |
| Anwendungsserver | Tomcat 8.5.x oder die im iManager-Bundle enthaltene Version<br>**HINWEIS:** Auf einem Windows-Server können Sie iManager manuell in eine vorhandene IIS- oder Apache-Webserver-Infrastruktur integrieren. |

| Kategorie | Anforderung |
|---|---|
| Verzeichnisservices | NetIQ eDirectory 8.8.8 Patch 9 Hotfix 2 für iManager 2.7.7 Patch 9<br>Alternativ:<br>NetIQ eDirectory 9.0.2 Hotfix 2 für iManager 3.0.2 Patch 1 |
| Standardports | 8080, 8443 und 9009 |

## 22.6 Systemanforderungen für iManager Workstation (Client-Version)

In diesem Abschnitt finden Sie die Mindestanforderungen für die Server, auf denen iManager Workstation installiert werden soll. Weitere Informationen zur Client-Version von iManager finden Sie in Abschnitt 22.2, „Erläuterungen zur Server- und Client-Version von iManager“, auf Seite 219.

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

| Kategorie | Anforderung |
|---|---|
| Prozessor | Pentium* III 600 MHz |
| Festplattenspeicher | 200 MB |
| Arbeitsspeicher | 256 MB (521 MB empfohlen) |
| Betriebssystem | Identity Manager 4.6 unterstützt zwei Versionen von eDirectory. Installieren Sie daher die jeweils kompatible Version von iManager.<br>◆ iManager 3.0.2 Patch 1: Weitere Informationen finden Sie im Installationshandbuch zu NetIQ iManager.<br>◆ iManager 2.7.7 Patch 9: Weitere Informationen finden Sie im Installationshandbuch zu NetIQ iManager. |
| Webbrowser | Einen beliebigen Webbrowser, der für Ihre Version von iManager im Installationshandbuch zu NetIQ iManager aufgeführt ist.<br>◆ iManager 3.0.2 Patch 1: Weitere Informationen finden Sie im Installationshandbuch zu NetIQ iManager.<br>◆ iManager 2.7.7 Patch 9: Weitere Informationen finden Sie im Installationshandbuch zu NetIQ iManager. |
| Betriebssystem-Hotfixes | NetIQ empfiehlt, die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden. |
| Anwendungsserver | Tomcat 8.5.x (im Bundle mit iManager Workstation) |
| Software | Java 1.8.0_x oder höher, im Bundle mit iManager Workstation |
| Standardports | 8080, 8443 und 9009 |

# 23 Installieren von iManager Server und iManager Workstation

In diesem Kapitel wird die Installation von iManager beschrieben. Überprüfen Sie in Vorbereitung auf die Installation die Checkliste der Voraussetzungen und Systemanforderungen unter Abschnitt 22.4, „Voraussetzungen und Überlegungen für die Installation von iManager“, auf Seite 220.

Den vollständigen Installationsvorgang finden Sie unter „Planen der Installation von iManager“, auf Seite 217.



## 23.1 Installieren von iManager und iManager Workstation unter Linux

In diesem Abschnitt finden Sie die Schritte zur Installation von iManager und iManager auf Servern und Clients unter Linux. Es wird empfohlen, iManager auf einer separaten Arbeitsstation zu installieren, also nicht auf dem Identity Manager-Server. Überprüfen Sie in Vorbereitung auf die Installation die Voraussetzungen und Systemanforderungen:

- **iManager:** Abschnitt 22.4.2, „Überlegungen für die Installation von iManager auf einer Linux-Plattform“, auf Seite 221 und Abschnitt 22.5, „Systemanforderungen für iManager Server“, auf Seite 224
- **iManager Workstation:** Abschnitt 22.4.4, „Überlegungen für die Installation von iManager Workstation auf Linux-Clients“, auf Seite 222 und Abschnitt 22.6, „Systemanforderungen für iManager Workstation (Client-Version)“, auf Seite 225
- Beachten Sie auch die Versionshinweise zur betreffenden Version.

### 23.1.1 Installieren von iManager unter Linux

Im Folgenden wird beschrieben, wie Sie die Server-Version von iManager auf einem Linux-Server mithilfe eines Installationsassistenten installieren (wahlweise über die Benutzeroberfläche oder die Konsole). Anweisungen für die automatische, unbeaufsichtigte Installation finden Sie in Abschnitt 23.3, „Automatische Installation von iManager“, auf Seite 236.

Wenn das Setup-Programm für iManager Server eine zuvor installierte Version von iManager erkennt, haben Sie die Möglichkeit, den Installationsvorgang anzuhalten oder die vorhandenen iManager-, JRE- und Tomcat-Installationen zu entfernen.

Nach einer erfolgreichen Installation generiert das Setup-Programm eine Konfigurationsdatei (standardmäßig `/var/log/install.properties`) mit Werten, die auf den während des Installationsprozesses gestellten Fragen basieren. Sie können diese Datei für die Verwendung in einer automatischen Installation ändern. Weitere Informationen finden Sie in Abschnitt 23.3, „Automatische Installation von iManager“, auf Seite 236.

**So installieren Sie iManager unter Linux:**

1. Melden Sie sich als `Root` oder als `Root`-Äquivalent an dem Computer an, auf dem das Installationsprogramm ausgeführt werden soll.
2. (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die iManager-Installationsdateien befinden (standardmäßig unter `products/iManager/installs/Linux/`).

   iManager 3.0.2 Patch 1 befindet sich beispielsweise im Verzeichnis `<ISO-Extraktionsverzeichnis>/products/iManager/installs/linux` und iManager 2.7.7 Patch 9 befindet sich im Verzeichnis `<ISO-Extraktionsverzeichnis>/products/iManager277/installs/linux`.
3. (Bedingt) Wenn Sie die Installationsdateien für iManager von der NetIQ Downloads-Website heruntergeladen haben, ermitteln Sie den Namen der `.tgz`-Datei. Beispiel: `iMan_277_linux.tgz`.
4. Extrahieren Sie den iManager-Ordner mit dem folgenden Befehl:

   ```
   tar -zxvf iMan_Version_linux.tgz
   ```
5. Wechseln Sie in einer Shell zum Verzeichnis */Extraktionsverzeichnis*`/products/iManager/installs/linux`.

   Dieser Pfad ist relativ zu dem Verzeichnis, in das Sie die iManager-Dateien kopiert bzw. extrahiert haben.
6. (Bedingt) Wenn Sie die Installation über die Befehlszeile durchführen möchten (textbasierte Installation), geben Sie den folgenden Befehl ein:

   ```
   ./iManagerInstallLinux.bin
   ```
7. (Bedingt) Soll der Assistent für das Installationsprogramm gestartet werden, geben Sie den folgenden Befehl ein:

   ```
   ./iManagerInstallLinux.bin -i gui
   ```
8. Wählen Sie im Eröffnungsbildschirm eine Sprache aus, und klicken Sie auf **OK**.
9. Lesen Sie die Einführung, und klicken Sie auf **Weiter**.
10. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf **Weiter**.
11. Geben Sie für die zu installierenden Komponenten die Option **iManager, Tomcat, JVM** an.

    ---

    **HINWEIS:** Wählen Sie *ausschließlich* diese Option. Wenn Sie eine der anderen beiden Optionen wählen, funktioniert iManager nicht erwartungsgemäß.

    ---
12. Klicken Sie auf **Weiter**.
13. (Optional) Sollen IPv6-Adressen in iManager verwendet werden, klicken Sie im Fenster „IPv6 aktivieren“ auf **Ja**.

    Sobald Sie iManager installiert haben, können Sie IPv6-Adressen aktivieren. Weitere Informationen finden Sie in Abschnitt 24.2, „Konfigurieren von iManager nach der Installation für die Verwendung von IPv6-Adressen“, auf Seite 243.
14. Klicken Sie auf **Weiter**.

**15** (Optional) Wenn Sie Plugins im Rahmen der Installation herunterladen und installieren möchten, führen Sie die folgenden Schritte aus:

**15a** Geben Sie an, dass Plugins heruntergeladen und installiert werden sollen, und klicken Sie auf **Weiter**.

**15b** (Bedingt) Bei der konsolenbasierten Installation geben Sie eine Liste mit den Nummern der herunterzuladenden Plugins ein. Trennen Sie die Plugin-Nummern dabei jeweils mit Kommas voneinander ab.

**15c** (Bedingt) Wenn Sie den Assistenten verwenden, markieren Sie die Kontrollkästchen der herunterzuladenden Plugins.

(Optional) Sollen die Plugins von einem anderen Netzwerkort heruntergeladen werden, geben Sie eine andere **Netzwerk-URL** an.

Wenn Sie eine Alternativ-URL für das Herunterladen von Plugins verwenden, müssen Sie den Inhalt der URL überprüfen und sicherstellen, dass das Plugin geeignet ist. Standardmäßig lädt das Installationsprogramm die Plugins von der folgenden URL herunter: http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. Weitere Informationen finden Sie in Abschnitt 22.3, „Erläuterungen zur Installation der iManager Plugins“, auf Seite 219.

**15d** Klicken Sie auf **Weiter**.

**15e** (Bedingt) Unter Umständen wird im Setup-Programm die folgende Meldung angezeigt:

```
No new or updated plug-ins found. All plug-ins are downloaded or updated or
the iManager download server is unavailable.
```

In diesem Fall liegt mindestens eine der folgenden Bedingungen vor:

- Auf der Download-Website sind keine aktualisierten Plugins verfügbar.
- Es liegt ein Problem mit Ihrer Internetverbindung vor. Überprüfen Sie die Verbindung, und wiederholen Sie den Vorgang.
- Die Verbindung mit der Deskriptor-Datei (http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml) war nicht erfolgreich. Diese URL verweist auf eine XML-Deskriptordatei mit den verfügbaren iManager-Plugins.
- Die iManager-Installation wird hinter einem Proxy durchgeführt, der keine Verbindung zu der oben angeführten URL zulässt.

**15f** Geben Sie an, ob die Plugin-Installation von einem lokalen Laufwerk aus erfolgen soll, und klicken Sie auf **Weiter**.

**15g** (Bedingt) Wenn die Plugin-Installation von einem lokalen Verzeichnis aus erfolgen soll, geben Sie den Verzeichnispfad der entsprechenden Plugin-Dateien (`.npm`) an.

Der Standardpfad lautet `/Extraktionsstandort/iManager/installs/plugins`, Sie können hier jedoch einen gültigen Mountpunkt angeben.

**15h** Klicken Sie auf **Weiter**.

**16** Geben Sie die Ports für die Tomcat-Ausführung an.

Die Standardports lauten 8080 für HTTP, 8443 für HTTPS und 9009 für den MOD_JK-Connector-Port.

**17** Klicken Sie auf **Weiter**.

18 (Optional) Geben Sie einen autorisierten Benutzer und den Namen des entsprechenden eDirectory-Baums an, der von diesem Benutzer verwaltet werden soll.

**HINWEIS**

- NetIQ rät davon ab, diese Einstellungen leer zu lassen. Wenn Sie diese Felder frei lassen, erlaubt iManager sämtlichen Benutzern die Installation von Plugins und die Änderung von iManager-Servereinstellungen. Nach Abschluss der Installation können Sie einen autorisierten Benutzer angeben. Weitere Informationen finden Sie in Abschnitt 24.3, „Angeben eines autorisierten Benutzers für eDirectory“, auf Seite 243.
- Das Installationsprogramm überprüft nicht den Benutzerberechtigungsnachweis für eDirectory.

19 Klicken Sie auf **Weiter**.

20 Lesen Sie die Informationen auf der Seite zu den Aspekten vor der Installation, und klicken Sie dann auf **Weiter**.

21 Klicken Sie nach Abschluss der Installation auf **Fertig**.

22 Klicken Sie nach der Initialisierung von iManager auf den ersten Link auf der Einführungsseite, und melden Sie sich an. Weitere Informationen finden Sie im Abschnitt Zugreifen auf iManager im *NetIQ iManager -Verwaltungshandbuch*.

**HINWEIS:** Wenn Sie iManager Workstation in Zukunft als Nicht-Root-Benutzer ausführen möchten, führen Sie iManager beim ersten Mal nicht als `Root` aus. Weitere Informationen finden Sie in Abschnitt 23.2, „Installieren von iManager und iManager Workstation unter Windows“, auf Seite 232.

23 Ändern Sie mit dem Befehl `chmod` die Berechtigungen für die folgenden InstallAnywhere-Dateien in `644` (Lesen), damit Änderungen verhindert werden:

```
/var/opt/novell/tomcat7/webapps/nps/UninstallerData/.com.zerog.registry.xml
```

```
/var/opt/novell/tomcat7/webapps/nps/UninstallerData/Uninstall_PluginName/
.com.zerog.registry.xml
```

Ändern Sie nicht den Inhalt in diesen Dateien. Eine Änderung des Inhalts kann sich auf andere Installationen auswirken, die auf InstallAnywhere zugreifen.

## 23.1.2 Installieren von iManager Workstation auf Linux-Clients

iManager Workstation ist eine eigenständige Umgebung. Sie können mehrere Versionen auf derselben Arbeitsstation installieren (einschließlich älterer Versionen von Mobile iManager). Allerdings sollten Sie nicht versuchen, sie gleichzeitig auszuführen. Wenn Sie unterschiedliche Versionen verwenden müssen, führen Sie zuerst eine Version aus, schließen Sie sie, und führen Sie anschließend die andere Version aus.

**HINWEIS:** iManager Workstation kann nicht von einem Pfad ausgeführt werden, der Leerzeichen enthält. Beispiel: `products/NetIQ/iManager Workstation/working`.

**So installieren Sie iManager auf einem Linux-Client:**

1 (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die iManager-Installationsdateien befinden (standardmäßig unter `products/iManager/installs/Linux/`).

iManager 3.0.2 Patch 1 befindet sich beispielsweise im Verzeichnis `<ISO-Extraktionsverzeichnis>/products/iManager/installs/win` und iManager 2.7.7 Patch 9 befindet sich im Verzeichnis `<ISO-Extraktionsverzeichnis>/products/iManager277/installs/win`.

2. (Bedingt) Wenn Sie die Installationsdateien für iManager von der NetIQ Downloads-Website heruntergeladen haben, ermitteln Sie den Namen der `tar.bz2`-Datei. Beispiel: `iMan_277_workstation_linux.tar.bz2`.

3. Extrahieren Sie die `tar.bz2`-Datei mit dem folgenden Befehl:

   ```
   tar -xjvf iMan_Version_workstation_linux.tar.bz2
   ```

   Beispiel:

   ```
   tar -xjvf iMan_277_workstation_linux.tar.bz2.
   ```

   Beim Extraktionsvorgang wird ein `imanager`-Ordner in dem Ordner erstellt, in dem sich auch die `tar.bz2`-Datei befindet.

4. (Optional) Führen Sie zum Installieren oder Aufrüsten der NICI-Software (Novell International Cryptography Infrastructure) die folgenden Schritte aus:

   **4a** Melden Sie sich als `Root` oder als `Root`-Äquivalent an dem Computer an, auf dem NICI installiert oder aufgerüstet werden soll.

   **4b** Führen Sie im Verzeichnis `imanager/NICI/linux` den folgenden Befehl aus:

   ```
   rpm -Uvh nici.i586.rpm
   ```

   Mit diesem Befehl wird NICI neu installiert bzw. eine vorhandene Version von NICI aufgerüstet.

5. (Bedingt) Wenn Sie iManager Workstation in Zukunft als Nicht-Root-Benutzer ausführen möchten, führen Sie iManager beim ersten Mal nicht als `Root` aus. Begeben Sie sich zum Verzeichnis `imanager/bin` und führen Sie das iManager Workstation-Startskript aus.

   ```
   ./iManager.sh
   ```

6. Geben Sie im Anmeldungsbildschirm von iManager einen Benutzernamen, ein Passwort und einen eDirectory-Baum an.

   Weitere Informationen zum Zugreifen auf iManager finden Sie im Abschnitt Zugreifen auf iManager im *NetIQ iManager -Verwaltungshandbuch*.

7. (Bedingt) Sollen IPv6-Adressen aktiviert werden, führen Sie die folgenden Schritte aus:

   1. Öffnen Sie unter *`Benutzer_Installationsverzeichnis die Datei`* `/Tomcat/conf/catalina.properties`.
   2. Legen Sie in der Datei `catalina.properties` die folgenden Konfigurationseinträge fest:

      ```
      java.net.preferIPv4Stack=false
      ```

      ```
      java.net.preferIPv4Addresses=true
      ```

   3. Starten Sie Tomcat neu.

## 23.2 Installieren von iManager und iManager Workstation unter Windows

In diesem Abschnitt finden Sie die Schritte zur Installation von iManager und iManager auf Servern und Clients unter Windows. Überprüfen Sie in Vorbereitung auf die Installation die Voraussetzungen und Systemanforderungen:

- **iManager:** Abschnitt 22.4.2, „Überlegungen für die Installation von iManager auf einer Linux-Plattform“, auf Seite 221.
- **iManager Workstation**: Abschnitt 22.4.4, „Überlegungen für die Installation von iManager Workstation auf Linux-Clients“, auf Seite 222.
- Beachten Sie auch die Versionshinweise zur betreffenden Version.

### 23.2.1 Installieren von iManager unter Windows

Im Folgenden wird beschrieben, wie Sie die Server-Version von iManager auf einem Windows-Server mithilfe eines Installationsassistenten installieren. Anweisungen für die automatische, unbeaufsichtigte Installation finden Sie in Abschnitt 23.3, „Automatische Installation von iManager“, auf Seite 236.

Wenn das Setup-Programm für iManager Server eine zuvor installierte Version von iManager erkennt, haben Sie die Möglichkeit, den Installationsvorgang anzuhalten oder die vorhandenen iManager-, JRE- und Tomcat-Installationen zu entfernen. Wenn das Setup-Programm die zuvor installierte Version von iManager entfernt, wird die Verzeichnisstruktur im alten Verzeichnis *TOMCAT_HOME* gesichert, um zuvor erstellte, benutzerdefinierte Inhalte zu erhalten.

**So installieren Sie iManager Server unter Windows:**

1. Melden Sie sich an dem Computer, auf dem iManager installiert werden soll, als Benutzer mit Administratorrechten an.
2. (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die iManager-Installationsdateien befinden (standardmäßig unter `products/iManager/installs/Win/`).
3. (Bedingt) Wenn Sie die Installationsdateien für iManager von der NetIQ Downloads-Website heruntergeladen haben, führen Sie die folgenden Schritte aus:
   - **3a** Ermitteln Sie den Namen der `win.zip`-Datei. Beispiel: `iMan_277_win.zip`.
   - **3b** Extrahieren Sie die `win.zip`-Datei in einen Ordner auf dem lokalen Computer.
4. Führen Sie `iManagerInstall.exe` aus (standardmäßig im Ordner `\products\iManager\installs\win`).
5. (Optional) Soll die Fehlersuchausgabe des Installationsprogramms angezeigt werden, drücken Sie direkt nach dem Starten des Installationsprogramms die `Strg`-Taste, und halten Sie sie gedrückt, bis ein Konsolenfenster geöffnet wird. Weitere Informationen zum Durchführen der Fehlerbehebung finden Sie unter „Fehlersuche“ im *NetIQ iManager-Administrationshandbuch*.
6. Wählen Sie im Begrüßungsbildschirm von iManager eine Sprache aus, und klicken Sie auf **OK**.
7. Klicken Sie im Fenster **Einführung** auf **Weiter**.
8. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf **Weiter**.

9 (Bedingt) Wenn auf dem Server bereits eine Version von JVM oder Tomcat oder andere unterstützende Komponenten vorhanden sind, die als Teil von iManager installiert werden, führen Sie im Fenster **Erkennungsübersicht** die folgenden Schritte aus:

**9a** Prüfen Sie unter **Folgende Komponenten installieren**, ob die für die Komponenten aufgeführten Versionen mit den zu installierenden Versionen übereinstimmen.

**9b** (Optional) Wenn im Setup-Programm nicht die zu installierenden Versionen aufgeführt sind, wechseln Sie zu den entsprechenden Komponenten im Installationsordner.

10 Klicken Sie auf **Weiter**.

11 Geben Sie im Fenster **PORT-Eingang abrufen** die HTTP- und SSL-Portnummern an, an denen der Tomcat-Server ausgeführt werden muss, und klicken Sie auf **Weiter**.

Standardmäßig lauten die Werte des HTTP-Ports und SSL-Ports 8080 bzw. 8443. Wenn Sie an den Standardports jedoch einen anderen Dienst oder Tomcat-Server konfiguriert haben, können Sie andere Ports konfigurieren.

12 (Optional) Sollen IPv6-Adressen in iManager verwendet werden, klicken Sie im Fenster **IPv6 aktivieren** auf **Ja**.

Sobald Sie iManager installiert haben, können Sie IPv6-Adressen aktivieren. Weitere Informationen finden Sie in Abschnitt 24.2, „Konfigurieren von iManager nach der Installation für die Verwendung von IPv6-Adressen“, auf Seite 243.

13 Klicken Sie auf **Weiter**.

14 Geben Sie im Fenster **Installationsordner** den Ordner an, in dem die Installationsdateien gespeichert werden sollen, und klicken Sie auf **Weiter**.

Der standardmäßige Installationsstandort lautet `C:\Programme\Novell`.

15 (Optional) Wenn Sie Plugins im Rahmen der Installation herunterladen und installieren möchten, führen Sie die folgenden Schritte aus:

**15a** Wählen Sie im Fenster **Plugins zum Herunterladen und Installieren auswählen** die gewünschten Plugins aus.

**15b** (Optional) Sollen die Plugins von einem anderen Netzwerkort heruntergeladen werden, geben Sie eine andere **Netzwerk-URL** an.

Wenn Sie eine Alternativ-URL für das Herunterladen von Plugins verwenden, müssen Sie den Inhalt der URL überprüfen und sicherstellen, dass das Plugin geeignet ist. Standardmäßig lädt das Installationsprogramm die Plugins von der folgenden URL herunter: http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. Weitere Informationen finden Sie in Abschnitt 22.3, „Erläuterungen zur Installation der iManager Plugins“, auf Seite 219.

**15c** Klicken Sie auf **Weiter**.

**15d** (Bedingt) Unter Umständen wird im Setup-Programm die folgende Meldung angezeigt:

```
No new or updated plug-ins found. All plug-ins are downloaded or updated or
the iManager download server is unavailable.
```

Wenn Sie diesen Fehler sehen, liegt mindestens eine der folgenden Bedingungen vor:

- Auf der Download-Website sind keine aktualisierten Plugins verfügbar.
- Es liegt ein Problem mit Ihrer Internetverbindung vor. Überprüfen Sie die Verbindung, und wiederholen Sie den Vorgang.

- Die Verbindung mit der Deskriptor-Datei (http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml) war nicht erfolgreich. Diese URL verweist auf eine XML-Deskriptordatei mit den verfügbaren iManager-Plugins.
- Die iManager-Installation wird hinter einem Proxy durchgeführt, der keine Verbindung zu der oben angeführten URL zulässt.

**15e** (Optional) Sollen die Plugins aus einem lokalen Verzeichnis installiert werden, geben Sie im Fenster „Plugins zum Installieren von Datenträger auswählen“ den Pfad des Verzeichnisses an, in dem sich die entsprechenden `.npm`-Plugin-Dateien befinden.

Mit diesem Schritt können Sie zuvor heruntergeladene bzw. benutzerdefinierte Plugins installieren. Der Standardpfad lautet `/Extraktionsverzeichnis/products/iManager/plugins`. Sie können jedoch auch einen anderen gültigen Pfad angeben.

**15f** Klicken Sie auf **Weiter**.

**16** (Optional) Geben Sie im Fenster **Benutzer- und Baumname abrufen** einen autorisierten Benutzer an sowie den Namen des eDirectory-Baums, den dieser Benutzer verwalten soll.

---

**HINWEIS**

- Wenn eDirectory nicht den Standardport 524 verwendet, sondern einen anderen Port, geben Sie die IP-Adresse oder den DNS-Namen des eDirectory-Servers plus die Portnummer an. Verwenden Sie nicht `localhost`. Soll eine IPv6-Adresse angegeben werden, geben Sie beispielsweise `https://[2001:db8::6]:1080/nps/servlet/webacc?taskId=fw.Startup&forceMaster=true` ein.
- NetIQ rät davon ab, diese Einstellungen leer zu lassen. Wenn Sie diese Felder frei lassen, erlaubt iManager sämtlichen Benutzern die Installation von Plugins und die Änderung von iManager-Servereinstellungen. Nach Abschluss der Installation können Sie einen autorisierten Benutzer angeben. Weitere Informationen finden Sie in Abschnitt 24.3, „Angeben eines autorisierten Benutzers für eDirectory“, auf Seite 243.
- Das Installationsprogramm überprüft nicht den Benutzerberechtigungsnachweis für eDirectory.

---

**17** Klicken Sie auf **Weiter**.

**18** Lesen Sie die Seite „Übersicht vor der Installation“, und klicken Sie auf **Installieren**.

**19** Nach Abschluss der Installation werden im Fenster **Installation abgeschlossen** relevante Meldungen zum Erfolg des Vorgangs angezeigt.

---

**HINWEIS:** Im Fenster **Installation abgeschlossen** wird unter Umständen die folgende Fehlermeldung trotz erfolgreicher Installation angezeigt:

```
The installation of iManager version is complete, but some errors occurred
during the install.
Please see the installation log Log file path for details. Press "Done" to quit
the installer.
```

---

**20** (Bedingt) Wenn die in Schritt 19 genannte Fehlermeldung im Installationsprogramm angezeigt wird, gehen Sie wie folgt vor:

**20a** Notieren Sie den Pfad zur Protokolldatei, der in der Fehlermeldung angezeigt wird.

**20b** Klicken Sie im Fenster **Installation abgeschlossen** auf **Fertig**.

**20c** Öffnen Sie die Protokolldatei.

**20d** (Bedingt) Wenn die Protokolldatei folgende Fehlermeldung enthält, können Sie die Fehlermeldung ignorieren: Die Installation wurde erfolgreich ausgeführt und iManager funktioniert ordnungsgemäß.

```
Custom Action: com.novell.application.iManager.install.InstallDLLs
Status: ERROR
Additional Notes: ERROR - class
com.novell.application.iManager.install.InstallDLLs
NonfatalInstallException C:\WINDOWS\system32\msvcr71.dll (The process
cannot access the file because it is being used by another process)
```

**20e** (Bedingt) Wenn die Protokolldatei den in Schritt 20d aufgeführten Fehler nicht enthält, empfiehlt NetIQ, die Installation zu wiederholen.

**21** Klicken Sie auf **Fertig**.

**22** Klicken Sie nach der Initialisierung von iManager auf den ersten Link auf der Einführungsseite, und melden Sie sich an. Weitere Informationen finden Sie im Abschnitt Zugreifen auf iManager im *NetIQ iManager 2.7.7-Verwaltungshandbuch*.

## 23.2.2 Installieren von iManager Workstation unter Windows

iManager Workstation ist eine eigenständige Umgebung. Sie können mehrere Versionen auf derselben Arbeitsstation installieren (einschließlich älterer Versionen von Mobile iManager). Allerdings sollten Sie nicht versuchen, sie gleichzeitig auszuführen. Wenn Sie unterschiedliche Versionen verwenden müssen, führen Sie zuerst eine Version aus, schließen Sie sie, und führen Sie anschließend die andere Version aus.

---

**HINWEIS:** iManager Workstation kann nicht von einem Pfad ausgeführt werden, der Leerzeichen enthält. Beispiel: `C:\NetIQ\iManager Workstation\working`.

---

**So installieren Sie iManager Workstation unter Windows:**

1. (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die iManager-Installationsdateien befinden (standardmäßig unter `products/iManager/installs/win/`).
2. (Bedingt) Wenn Sie die Installationsdateien für iManager von der NetIQ Downloads-Website heruntergeladen haben, führen Sie die folgenden Schritte aus:
   - **2a** Ermitteln Sie den Namen der `win.zip`-Datei. Beispiel: `iMan_277_workstation_win.zip`.
   - **2b** Extrahieren Sie die `win.zip`-Datei in einen Ordner auf dem lokalen Computer.
3. Führen Sie im Ordner `imanager\bin` die Datei `iManager.bat` aus.
4. Geben Sie im Anmeldefenster für iManager den Berechtigungsnachweis für einen autorisierten Benutzer sowie den von diesem Benutzer verwalteten eDirectory-Baum an.

   Weitere Informationen zum Zugreifen auf iManager finden Sie im Abschnitt Zugreifen auf iManager im *NetIQ iManager -Verwaltungshandbuch*.
5. (Bedingt) Sollen IPv6-Adressen aktiviert werden, führen Sie die folgenden Schritte aus:
   1. Öffnen Sie unter *`Benutzer_Installationsverzeichnis die Datei`* `/Tomcat/conf/catalina.properties`.
   2. Legen Sie in der Datei `catalina.properties` die folgenden Konfigurationseinträge fest:

      ```
      java.net.preferIPv4Stack=false
      ```

```
java.net.preferIPv4Addresses=true
```

3. Starten Sie den Tomcat-Service neu.

# 23.3 Automatische Installation von iManager

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 `install.properties` ab. Sie können die automatische Installation wahlweise mit der Standarddatei ausführen oder die Datei bearbeiten und so den Installationsvorgang anpassen.

Überprüfen Sie in Vorbereitung auf die Installation die Voraussetzungen und Systemanforderungen:

- **iManager:** Abschnitt 22.4.2, „Überlegungen für die Installation von iManager auf einer Linux-Plattform“, auf Seite 221.
- **iManager Workstation**: Abschnitt 22.4.4, „Überlegungen für die Installation von iManager Workstation auf Linux-Clients“, auf Seite 222.
- Beachten Sie auch die Versionshinweise zur betreffenden Version.

## 23.3.1 Bearbeiten der Eigenschaftendatei zum Ausführen einer angepassten automatischen Installation

Wenn Sie mehr Kontrolle darüber haben möchten, welche Module installiert werden, können Sie den Vorgang der automatischen Installation anpassen.

1 Öffnen Sie die Datei `install.properties` (standardmäßig im Verzeichnis *`products`*`/iManager` in der `.iso`-Image-Datei für das Identity Manager-Installationspaket für die verschiedenen Betriebssystemumgebungen).

---

**HINWEIS:** Wenn Sie bereits die aktuelle Version von iManager auf einem Server installiert haben, können Sie die Datei `installer.properties` verwenden, die durch das Setup-Programm generiert wurde. Diese Datei (standardmäßig im Verzeichnis `/var/log`) enthält die Werte, die Sie während der Installation angegeben haben.

---

2 Fügen Sie der Eigenschaftendatei folgende Parameter und Werte hinzu:

**`$PLUGIN_INSTALL MODE$`**

Gibt die Eigenschaft an, mit der gesteuert wird, ob Plugins installiert werden. Fügen Sie einen der folgenden Werte hinzu:

- `DISK` (Standard) – Weist das Setup-Programm an, die Plugins von der lokalen Festplatte zu installieren.
- `NET` – Weist das Setup-Programm an, die Plugins vom Netzwerk zu installieren.
- `BOTH` – Weist das Setup-Programm an, die Plugins sowohl von der Festplatte als auch vom Netzwerk zu installieren.
- `SKIP` – Die Plugins werden nicht installiert.

**$PLUGIN_DIR$**

Gibt einen alternativen Pfad zu den Plugins an, die sich auf der lokalen Festplatte befinden. Der Standardpfad lautet *Stammverzeichnis_des_Installationsprogramms*/iManager/installs/*Plattformpfad*/plugin.

Das Installationsprogramm installiert alle Module im Plugin-Verzeichnis, nicht jedoch in den Unterverzeichnissen.

**$PLUGIN_INSTALL_URL$**

Gibt die Netzwerk-URL an, über die das Installationsprogramm die Plugins herunterladen kann, standardmäßig http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. Wenn Sie eine alternative URL angeben, müssen Sie den Inhalt der URL überprüfen und ermitteln, ob das Plugin für Ihre Zwecke geeignet ist. Weitere Informationen finden Sie in Abschnitt 22.3, „Erläuterungen zur Installation der iManager Plugins“, auf Seite 219.

**$LAUNCH_BROWSER$**

Gibt an, ob das Installationsprogramm nach Abschluss des Installationsvorgangs die Datei gettingstarted.html starten soll.

**$USER_INSTALL_DIR$**

Gibt den Pfad an, in dem iManager installiert werden soll.

**USER_INPUT_ENABLE_IPV6**

Gibt an, ob die Verwendung von IPv6-Adressen in iManager aktiviert werden soll. Standardmäßig stellt das Installationsprogramm diesen Wert auf yes ein.

3 Geben Sie für jedes Plugin-Modul, das heruntergeladen und installiert werden soll, jeweils die Modul-ID und die Version aus der Datei MANIFEST.MF im Ordner META-INF/ für .npm (Plugin-Modul) ein. Beispiel:

```
$PLUGIN_MODULE_ID_1$=eDirectoryBackupAndRestore

$PLUGIN_VERSION_1$=2.7.20050517

$PLUGIN_MODULE_ID_2$=ldap

$PLUGIN_VERSION_2$=2.7.20050517
```

**HINWEIS**

- Wenn Sie keine Module angeben, installiert das Programm die am häufigsten verwendeten Module, die in der Datei iman_mod_desc.xml auf der Download-Website als „selected“ gekennzeichnet sind.
- Wenn Sie keine Version für ein Modul definieren, installiert das Setup-Programm ein beliebiges Modul, das mit dem .npm-Namen übereinstimmt.

## 23.3.2 Ausführen der automatischen Installation von iManager

Anhand der Datei `install.properties` (standardmäßig im Verzeichnis *`products`*`/iManager` in der `.iso`-Image-Datei für das Identity Manager-Installationspaket für die verschiedenen Betriebssystemumgebungen) können Sie iManager automatisch auf einem Linux- oder Windows-Server installieren lassen. Im Verzeichnis *`products`*`/iManager` befindet sich auch die ausführbare Datei für die Installation.

1. Wechseln Sie in einem Konsolenfenster in das Verzeichnis, das die Datei `install.properties` enthält.
2. Geben Sie in der Befehlszeile einen der folgenden Befehle ein:
   - **Linux**: `./iManagerInstall`*`Plattform`*`.bin -i silent`
   - **Windows:** `iManagerInstall.exe -i silent`

# 24 Aufgaben nach Abschluss der Installation für iManager

Nach der Installation von iManager können Sie die Konfigurationseinstellungen bearbeiten, also beispielsweise die IPv6-Adressierung aktivieren oder den autorisierten Benutzer für einen eDirectory-Baum ändern. NetIQ empfiehlt außerdem, die selbstsignierten Zertifikate zu ersetzen, die im Rahmen des Installationsvorgangs erstellt wurden.



## 24.1 Ersetzen der temporären selbstsignierten Zertifikate für iManager

Eigenständige iManager-Installationen enthalten ein vorübergehendes, selbstsigniertes Zertifikat für die Verwendung durch Tomcat. Dieses Zertifikat ist ein Jahr lang gültig. NetIQ bietet dieses Zertifikat als Hilfestellung zum Einrichten des Systems, so dass Sie iManager direkt nach der Installation des Produkts installieren können. NetIQ und OpenSSL empfehlen, selbstsignierte Zertifikate ausschließlich für Testzwecke zu verwenden. Ersetzen Sie das temporäre Zertifikat stattdessen durch ein sicheres Zertifikat.

Tomcat speichert das selbstsignierte Zertifikat in einem Keystore mit dem Tomcat-Format (JKS). Im Normalfall würden Sie einen privaten Schlüssel als Ersatz für das Zertifikat importieren. Mit dem `keytool`, in dem Sie den Tomcat-Keystore bearbeiten, können Sie jedoch keine privaten Schlüssel importieren. Dieses Werkzeug verwendet lediglich einen selbst generierten Schlüssel.

In diesem Abschnitt erfahren Sie, wie Sie mit NetIQ Certificate Server in eDirectory ein Schlüsselpaar aus öffentlichem und privatem Schlüssel generieren und das temporäre Zertifikat ersetzen. Wenn Sie mit eDirectory arbeiten, können Sie mit NetIQ Certificate Server auf sichere Weise Zertifikate generieren, verfolgen, speichern und widerrufen, ganz ohne zusätzliche Investition.

---

**HINWEIS:** Die Informationen in diesem Abschnitt gelten nicht für OES Linux, bei dem sowohl Tomcat als auch Apache installiert werden. In der OES Linux-Dokumentation finden Sie Informationen dazu, wie das eigensignierte Apache-/Tomcat-Zertifikat ersetzt werden kann.

---

### 24.1.1 Ersetzen der selbstsignierten Zertifikate in iManager unter Linux

In diesem Abschnitt wird beschrieben, wie Sie ein Schlüsselpaar in eDirectory erstellen und die öffentlichen und privaten Schlüssel sowie die Root-Schlüssel der Zertifizierungsstelle (Certificate Authority, CA) auf der Linux-Plattform mithilfe einer PKCS#12-Datei exportieren. Hierzu muss u. a. die

Tomcat-Konfigurationsdatei `server.xml` so bearbeitet werden, dass die PKCS12-Direktive verwendet wird, und die Konfiguration muss auf eine tatsächlich vorhandene P12-Datei verweisen. (Es kann nicht der standardmäßige JKS-Keystore verwendet werden.)

Für diesen Prozess werden die folgenden Dateien verwendet:

- `/var/opt/novell/novlwww/.keystore` mit dem temporären Schlüsselpaar
- `/opt/novell/jdk1.7.0_25/jre/lib/security/cacerts` mit den Herkunftsverbürgungszertifikaten
- `/etc/opt/novell/tomcat8/server.xml` zum Konfigurieren der Verwendung von Zertifikaten in Tomcat

**So ersetzen Sie die selbstsignierten Zertifikate in iManager unter Linux:**

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 Tomcat-Basisverzeichnis:
   - **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 (`.pfx`) im Verzeichnis `/var/opt/novell/novlwww`.
3. Konvertieren Sie die `.pfx`-Datei mit den folgenden Schritten in eine `.pem`-Datei:
   - **3a** Geben Sie einen Befehl ein, beispielsweise `openssl pkcs12 -in newtomcert.pfx -out newtomcert.pem`.
   - **3b** Geben Sie das Passwort für das Zertifikat ein, das Sie in Schritt 2 angegeben haben.
   - **3c** Geben Sie ein Passwort für die neue `.pem`-Datei an.

     Wenn Sie möchten, können Sie dasselbe Passwort verwenden.
4. Konvertieren Sie die `.pem`-Datei mit den folgenden Schritten in eine `.p12`-Datei:
   - **4a** Geben Sie einen Befehl ein, beispielsweise `openssl pkcs12 -export -in newtomcert.pem -out newtomcert.p12 -name "New Tomcat"`.
   - **4b** Geben Sie das Passwort für das Zertifikat ein, das Sie in Schritt 3 angegeben haben.
   - **4c** Geben Sie ein Passwort für die neue `.p12`-Datei an.

     Wenn Sie möchten, können Sie dasselbe Passwort verwenden.
5. Beenden Sie Tomcat mit dem folgenden Befehl:

   ```
   /etc/init.d/novell-tomcat7 stop
   ```

6 Damit die soeben erstellte `.p12`-Zertifikatsdatei tatsächlich in Tomcat verwendet wird, fügen Sie die Variablen `keystoreType`, `keystoreFile` und `keystorePass` in die Tomcat-Konfigurationsdatei ein (standardmäßig `/etc/opt/novell/tomcat7.0.42/server.xml`). Beispiel:

```
<Connector className="org.apache.coyote.tomcat7.CoyoteConnector"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="false" disableUploadTimeout="true">
   <Factory className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
 clientAuth="false" protocol="TLS" keystoreType="PKCS12"  keystoreFile="/var/
opt/novell/novlwww/newtomcert.p12" keystorePass="password" />
</Connector>
```

---

**HINWEIS:** Wenn Sie den Keystore-Typ auf PKCS12 festlegen, müssen Sie den vollständigen Pfad der Zertifikatsdatei angeben, da Tomcat nicht mehr standardmäßig den Tomcat-Basispfad verwendet.

---

7 Damit die `.p12`-Zertifikatsdatei ordnungsgemäß arbeitet, führen Sie die folgenden Schritte aus:

**7a** Weisen Sie das Eigentum an der Datei dem entsprechenden Tomcat-Benutzer bzw. der Tomcat-Gruppe zu (standardmäßig `novlwww`). Beispiel: `chown novlwww:novlwww newtomcert.p12`.

**7b** Ändern Sie die Dateiberechtigungen wie folgt: `user=rw`, `group=rw` und `others=r`. Beispiel: `chmod 654 newtomcert.p12`.

8 Starten Sie Tomcat mit dem folgenden Befehl neu:

```
/etc/init.d/novell-tomcat7 start
```

## 24.1.2 Ersetzen der selbstsignierten Zertifikate in iManager unterWindows

In diesem Abschnitt wird beschrieben, wie Sie ein Schlüsselpaar in eDirectory erstellen und die öffentlichen und privaten Schlüssel sowie die Root-Schlüssel der Zertifizierungsstelle (Certificate Authority, CA) auf der Windows-Plattform mithilfe einer `PKCS#12`-Datei exportieren. Hierzu muss u. a. die Tomcat-Konfigurationsdatei `server.xml` so bearbeitet werden, dass die PKCS12-Direktive verwendet wird, und die Konfiguration muss auf eine tatsächlich vorhandene P12-Datei verweisen. (Es kann nicht der standardmäßige JKS-Keystore verwendet werden.)

Für diesen Prozess werden die folgenden Dateien verwendet:

- `C:\Programme\Novell\Tomcat\conf\ssl\.keystore` mit dem temporären Schlüsselpaar
- `C:\Programme\Novell\jre\lib\security\cacerts` mit den Herkunftsverbürgungszertifikaten
- `C:\Programme\Novell\Tomcat\conf\server.xml` zum Konfigurieren der Verwendung von Zertifikaten in Tomcat

**So ersetzen Sie die selbstsignierten Zertifikate in iManager unter Windows:**

1 Erstellen Sie ein neues Zertifikat mit den folgenden Schritten:

**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:

**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 (`.pfx`).

**3** Konvertieren Sie die `.pfx`-Datei mit den folgenden Schritten in eine `.pem`-Datei:

---

**HINWEIS:** OpenSSL ist nicht standardmäßig unter Windows installiert. Von der OpenSSL-Website können Sie jedoch eine Version für die Windows-Plattform herunterladen. Sie können das Zertifikat auch auf einer Linux-Plattform konvertieren, auf der OpenSSL standardmäßig installiert ist. Weitere Informationen zum Konvertieren der Datei unter Linux finden Sie in Abschnitt 24.1, „Ersetzen der temporären selbstsignierten Zertifikate für iManager“, auf Seite 239.

---

**3a** Geben Sie einen Befehl ein, beispielsweise `openssl pkcs12 -in newtomcert.pfx -out newtomcert.pem`.

**3b** Geben Sie das Passwort für das Zertifikat ein, das Sie in Schritt 2 angegeben haben.

**3c** Geben Sie ein Passwort für die neue `.pem`-Datei an.

Wenn Sie möchten, können Sie dasselbe Passwort verwenden.

**4** Konvertieren Sie die `.pem`-Datei mit den folgenden Schritten in eine `.p12`-Datei:

**4a** Geben Sie einen Befehl ein, beispielsweise `openssl pkcs12 -export -in newtomcert.pem -out newtomcert.p12 -name "New Tomcat"`.

**4b** Geben Sie das Passwort für das Zertifikat ein, das Sie in Schritt 3 angegeben haben.

**4c** Geben Sie ein Passwort für die neue `.p12`-Datei an.

Wenn Sie möchten, können Sie dasselbe Passwort verwenden.

**5** Kopieren Sie die Datei `.p12` file an den Speicherort der Tomcat-Zertifikate (standardmäßig `C:\Programme\Novell\Tomcat\conf\ssl\`).

**6** Beenden Sie den Tomcat-Dienst mit dem folgenden Befehl:

```
/etc/init.d/novell-tomcat7 stop
```

**7** Damit die soeben erstellte `.p12`-Zertifikatsdatei tatsächlich in Tomcat verwendet wird, fügen Sie die Variablen `keystoreType`, `keystoreFile` und `keystorePass` in die Tomcat-Datei `server.xml` ein. Beispiel:

```
<Connector className="org.apache.coyote.tomcat7.CoyoteConnector"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="false" disableUploadTimeout="true">
   <Factory className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
 clientAuth="false" protocol="TLS" keystoreType="PKCS12"
 keystoreFile="/conf/ssl/newtomcert.p12" keystorePass="password" />
```

Wenn Sie den Keystore-Typ auf `PKCS12` einstellen, müssen Sie den vollständigen Pfad der Zertifikatsdatei angeben, da Tomcat nicht mehr standardmäßig den Tomcat-Basispfad verwendet.

8 Starten Sie den Tomcat-Dienst.

## 24.2 Konfigurieren von iManager nach der Installation für die Verwendung von IPv6-Adressen

Nach der Installation können Sie die Verwendung von IPv6-Adressen in iManager aktivieren.

1. Öffnen Sie die Datei `catalina.properties` im Installationsverzeichnis, das sich standardmäßig in einem der folgenden Verzeichnisse befindet:

   **Linux:** Verzeichnis `/var/opt/novell/tomcat8/conf/`

   **Windows:** Ordner *`Installationsverzeichnis`*`\Tomcat\conf`

2. Legen Sie in der Eigenschaftendatei die folgenden Konfigurationseinträge fest:

   ```
   java.net.preferIPv4Stack=false
   ```

   ```
   java.net.preferIPv4Addresses=true
   ```

3. Starten Sie Tomcat neu.

## 24.3 Angeben eines autorisierten Benutzers für eDirectory

Nach der Installation von iManager können Sie den Berechtigungsnachweis für den autorisierten Benutzer sowie den zugehörigen, von diesem Benutzer verwalteten eDirectory-Baum ändern. Weitere Informationen finden Sie unter „iManager-autorisierte Benutzer und Gruppen“ im *NetIQ iManager -Administrationshandbuch*.

1 Melden Sie sich bei iManager an.

2 Klicken Sie in der Ansicht „Konfigurieren“ auf **iManager-Server** > **iManager konfigurieren** > **Sicherheit**.

3 Aktualisieren Sie den Berechtigungsnachweis für den Benutzer sowie den Namen des Baums.

# VIII Installieren von Designer für Identity Manager

In diesem Abschnitt finden Sie die Schritte für die Installation von Designer für Identity Manager. Standardmäßig installiert das Installationsprogramm die Komponenten in den folgenden Speicherorten:

- **Linux:** `/opt/netiq`
- **Windows:** `C:\NetIQ`

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie in Kapitel 25, „Planen der Installation von Designer“, auf Seite 247.

# 25 Planen der Installation von Designer

In diesem Abschnitt finden Sie die Voraussetzungen, die Überlegungen und die notwendige Systemeinrichtung für die Installation von Designer. Informieren Sie sich zunächst anhand der Checkliste über den Installationsvorgang.



## 25.1 Checkliste für die Installation von Designer

NetIQ empfiehlt, vor Beginn der Installation die nachfolgenden Schritte auszuführen:

| | **Checkliste** |
|---|---|
| ❑ | 1. Sehen Sie sich die Informationen zur Produktarchitektur an, um die Interaktion zwischen den Identity Manager-Komponenten kennenzulernen. Weitere Informationen finden Sie in Abschnitt 2.1, „Designer für Identity Manager“, auf Seite 27. |
| ❑ | 2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |
| ❑ | 3. Lesen Sie die Überlegungen zur Installation von Designer, und prüfen Sie, ob der Computer den Voraussetzungen entspricht. Weitere Informationen finden Sie in Abschnitt 25.2, „Voraussetzungen für die Installation von Designer“, auf Seite 248. |
| ❑ | 4. Stellen Sie sicher, dass der Computer, auf dem Sie Designer installieren, den angegebenen Software- und Hardware-Voraussetzungen entspricht. Weitere Informationen finden Sie in Abschnitt 25.3, „Systemanforderungen für Designer“, auf Seite 248. |
| ❑ | 5. (Bedingt) Zur geführten Installation auf Computern mit dem Betriebssystem SLES 12 SP1 (oder höher) müssen die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in Abschnitt 6.3, „Installieren von Identity Manager auf Servern mit SLES 12 SP1 (oder höher)“, auf Seite 63. |
| ❑ | 6. Befolgen Sie die Anweisungen zum Installieren von Designer in einem der folgenden Abschnitte:<br>◆ „Verwenden des Installationsbefehls unter Linux“, auf Seite 251<br>◆ „Ausführen der ausführbaren Windows-Datei“, auf Seite 251<br>◆ „Verwenden der automatischen Installation“, auf Seite 252 |
| ❑ | 7. Installieren Sie die restlichen Identity Manager-Komponenten. |
| ❑ | 8. (Optional) Starten Sie ein Projekt für die Identity Manager-Lösung gemäß den Anweisungen im *NetIQ Designer for Identity Manager Administration Guide* (Administrationshandbuch zu NetIQ Designer für Identity Manager). |

## 25.2 Voraussetzungen für die Installation von Designer

In diesem Abschnitt finden Sie die Voraussetzungen und die Systemvoraussetzungen für die Installation von Designer.

Lesen Sie vor dem Installieren oder Aufrüsten von Designer die folgenden Überlegungen:

- Soll Designer auf einem Computer mit einem openSUSE-64-Bit-Betriebssystem installiert werden, muss die Umgebung den folgenden Voraussetzungen entsprechen:
  - Vor dem Installieren von Designer müssen Sie das 32-Bit-NICI-Paket (Novell International Cryptographic Infrastructure) installieren.
  - Sie müssen alle Bibliotheken von openSUSE.org installieren, insbesondere `bug-buddy`, `gtk2` (32 Bit) und `libgthread`.
  - Vor dem Installieren von Designer müssen Sie die compat-Bibliothek `libgthread-2_0-0-32bit-2.17.2+2.17.3+20080708+r7171-3.1.x86_64.rpm` installieren.
  - Sie müssen die 32-Bit-Version der RPM-Bibliothek `gtk2` installieren, selbst wenn Designer auf einem Computer mit 64-Bit-Betriebssystem installiert werden soll.
- 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 5.6, „Erläuterungen zur Sprachunterstützung“, auf Seite 58.
- (Bedingt) Zur geführten Installation auf einem Server mit SLES 12 SP1 (oder höher) müssen die Bibliotheken `libXtst6-32bit-1.2.1-4.4.1.x86_64`, `libXrender-32bit` und `libXi6-32bit` auf dem Server installiert sein.
- Designer 2.1*x*-Arbeitsbereiche können nicht in Designer 3.0 oder höher verwendet werden, da Arbeitsbereiche aus älteren Versionen nicht mit den neueren Designer-Versionen kompatibel sind. Designer speichert Projekte und Konfigurationsinformationen in **Arbeitsbereichen**. Die Designer 4.x-Arbeitsbereiche werden beispielsweise standardmäßig in den folgenden Verzeichnissen installiert:
  - **Linux:** `$HOME/designer_workspace`
  - **Windows 10 und Windows 7:** Verzeichnis `%UserProfile%\designer_workspace` für
- Wenn Designer aufgerüstet werden soll und Sie die Workflow-Bereitstellung und die Bereitstellung mit Rollen ausführen, beachten Sie das Aufrüstungsverfahren in Abschnitt 58.5, „Migrieren des Benutzeranwendungstreibers“, auf Seite 553.

## 25.3 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 | 1024 MB |

| Kategorie | Anforderung |
| --- | --- |
| Betriebssystem (zertifiziert) | Eines der folgenden 64-Bit-Betriebssysteme:<br>**Server**<br>◆ OpenSUSE 13.2<br>◆ SUSE Linux Enterprise Server 12 SP1<br>◆ SUSE Linux Enterprise Server 11 SP4<br>◆ Windows Server 2012 R2<br>◆ Windows Server 2012<br>◆ Windows Server 2008 R2<br>◆ Windows Server 2008<br>**müssen zuerst entfernt werden**<br>◆ SUSE Linux Enterprise Desktop 11 SP4<br>◆ SUSE Linux Enterprise Desktop 12 SP1<br>◆ Windows 10<br>◆ Windows 8<br>◆ Windows 7<br>NetIQ empfiehlt, vor der Installation von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden.<br>**HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird. |
| Betriebssystem (unterstützt) | Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme<br>**HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert. |
| Virtualisierungssystem | ◆ Hyper-V Server 2012 R2<br>◆ VMWare ESX 5.0 und höher<br>◆ Windows Server 2012 R2-Virtualisierung mit Hyper-V (unterstützt)<br>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. |
| Webbrowser | Einer der folgenden Browser (ggf. höhere Version):<br>◆ Internet Explorer 11<br>◆ Chrome 51<br>◆ Firefox 46 |

# 26 Installation von Designer

Je nach Zielcomputer können Sie Identity Manager Designer wahlweise mit einer ausführbaren Datei, mit einer Binärdatei oder im Textmodus installieren. Auch die automatische Installation ist möglich. Verwenden Sie das Installationsprogramm, das sich standardmäßig in den folgenden Verzeichnissen befindet:

- **Linux-Computer:** `/products/Designer/install`
- **Windows-Computer:** `\products\Designer\install.exe`

In diesem Abschnitt finden Sie Informationen zum Installieren von Designer in einer neuen Umgebung. Weitere Informationen zum Aufrüstung von Designer finden Sie in Abschnitt 55.1, „Aufrüstung von Designer“, auf Seite 503.

Verschiedene Identity Manager-Komponenten nutzen Pakete in Designer. Beim Installieren von Designer fügt das Installationsprogramm automatisch bestimmte Pakete in das neue Projekt ein.



## 26.1 Verwenden des Installationsbefehls unter Linux

Sie können die Installation im Textmodus vornehmen oder die Binärdatei ausführen. Geben Sie einen der folgenden Befehle im Verzeichnis ein, in dem sich das Installationsprogramm befindet:

- **Binärdatei:** `./install`
- **Expertenmodus:** `./install -i console`

## 26.2 Ausführen der ausführbaren Windows-Datei

1. Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem Designer installiert werden soll.
2. Führen Sie die Datei `install.exe` aus.
3. Befolgen Sie die Anweisungen im Assistenten, bis die Installation abgeschlossen ist.

## 26.3 Verwenden der automatischen Installation

Mithilfe von Skripten können Sie Designer automatisch installieren, ohne dass der Benutzer eingreifen muss. Mit der Option `-i silent` werden standardmäßige Parameterwerte für die Installation verwendet, sofern Sie nicht die Datei `designerInstaller.properties` bearbeitet haben.

1. Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem Designer installiert werden soll.
2. Rufen Sie das Verzeichnis mit dem Installationsprogramm auf.
3. (Optional) Wenn Sie das Installationsverzeichnis und die Sprache für Designer konfigurieren möchten, führen Sie die nachfolgenden Schritte aus.

   **3a** Öffnen Sie die Datei `designerInstaller.properties` (standardmäßig im Verzeichnis *`Pfad_zu_nicht_komprimierten_Designer_Dateien`*`/products/Designer`).

   **3b** Bearbeiten Sie in der Eigenschaftendatei die Werte für die folgenden Parameter:

   **USER_INSTALL_DIR**

   Gibt den Verzeichnispfad für die Installation von Designer an. Beispiel:

   ```
   USER_INSTALL_DIR=/home/user/designer
   ```

   Wenn Sie einen Pfad angeben, der nicht mit dem Verzeichnis `designer` endet, hängt das Designer-Installationsprogramm ein Verzeichnis `designer` an.

   **SELECTED_DESIGNER_LOCALE**

   Legt eine der folgenden Sprachen fest, in denen Designer nach der Installation ausgeführt werden soll:

   - `zh_CN` – Chinesisch (vereinfacht)
   - `zh_TW` – Chinesisch (traditionell)
   - `nl` – Niederländisch
   - `en` – Englisch
   - `fr` – Französisch
   - `de` – Deutsch
   - `it` – Italienisch
   - `ja` – Japanisch
   - `pt_BR` – Portugiesisch (Brasilien)
   - `es` – Spanisch

   **3c** Speichern und schließen Sie die Eigenschaftendatei.
4. Führen Sie einen der folgenden Befehle aus:
   - **Linux:** `install -i silent -f` *`Pfad`*`\designerInstaller.properties`
   - **Windows:** `install -i silent -f` *`Pfad`*`/designerInstaller.properties`

## 26.4 Bearbeiten eines Installationspfads mit Leerzeichen

Sie können Designer in einem Verzeichnis installieren, dessen Name ein oder mehrere Leerzeichen enthält. Nach der Installation von Designer müssen Sie allerdings die Dateien `StartDesigner.sh` und `Designer.ini` bearbeiten, damit Designer ordnungsgemäß funktioniert. Ersetzen Sie die Leerzeichen jeweils manuell durch ein Escape-Zeichen („\“). Beispiel:

Änderung

```
root/designer installation
```

in

```
root/designer\ installation
```

# IX Installieren von PostgreSQL und Tomcat für Identity Manager

In diesem Abschnitt wird beschrieben, wie Sie die folgenden Anwendungsserver und Datenbankprogramme installieren, die vom Großteil der Identity Manager-Komponenten verwendet werden:

- Apache Tomcat
- PostgreSQL

Die Installationsdateien befinden sich im Verzeichnis `products/RBPM/` im Identity Manager-Installationspaket. Standardmäßig installiert das Installationsprogramm die Anwendungen in den folgenden Speicherorten:

- **Linux:** `/opt/netiq/idm/apps/`
- **Windows:** `C:\netiq\idm\apps\`

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie in Abschnitt 27.1, „Checkliste für die Installation von Tomcat und PostgreSQL“, auf Seite 257.

# 27 Planen der Installation von PostgreSQL und Tomcat

Identity Manager 4.6 unterstützt lediglich Apache Tomcat als Anwendungsserver. Wenn Ihr Unternehmen eine unterstützte Version von Tomcat anbietet, können Sie diese Version zusammen mit Identity Manager nutzen.

NetIQ hat Tomcat und PostgreSQL alternativ als Arbeitserleichterung zu einem einzigen Installationsprogramm zusammengefasst. Hierbei können Sie diese Anwendungen installieren, ohne sie einzeln herunterladen zu müssen. NetIQ stellt weder Aktualisierungen für diese Komponenten noch Informationen zu Verwaltung, Konfiguration oder Anpassung dieser Komponenten bereit, abgesehen von den kurzen Ausführungen in der NetIQ Identity Manager-Dokumentation.



## 27.1 Checkliste für die Installation von Tomcat und PostgreSQL

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 den folgenden Abschnitten:<br>◆ Abschnitt 4.5, „Verwenden des Single-Sign-On-Zugriffs in Identity Manager“, auf Seite 42<br>◆ Abschnitt 4.4, „Verwenden von Self-Service Password Management in Identity Manager“, auf Seite 40 |
| ❑ | 2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.3.4, „Empfohlene Servereinrichtung“, auf Seite 53. |
| ❑ | 3. Legen Sie fest, ob NetIQ Sentinel vor der Installation von Tomcat oder PostgreSQL installiert werden soll. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |

| | Checkliste |
|---|---|
| ❑ | 4. Lesen Sie die Überlegungen zur Installation der Anwendungen, und prüfen Sie, ob die Computer den Voraussetzungen entsprechen:<br>◆ Abschnitt 27.4, „Voraussetzungen für die Installation von Tomcat“, auf Seite 259<br>◆ Abschnitt 27.3, „Voraussetzungen für die Installation von PostgreSQL“, auf Seite 259 |
| ❑ | 5. (Bedingt) Zur geführten Installation auf Computern mit dem Betriebssystem SLES 12 SP1 (oder höher) müssen die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in Abschnitt 6.3, „Installieren von Identity Manager auf Servern mit SLES 12 SP1 (oder höher)“, auf Seite 63. |
| ❑ | 6. (Bedingt) Stellen Sie bei Computern mit RHEL 6.x- oder Rhel 7.x-Betriebssystem sicher, dass die erforderlichen Bibliotheken installiert sind. Weitere Informationen finden Sie in Abschnitt 6.4, „Installieren von Identity Manager auf einem RHEL 6.*x- oder 7.x-Server“, auf Seite 63*. |
| ❑ | 7. Installieren Sie die Anwendungen:<br>◆ Anweisungen zur geführten Installation finden Sie in Abschnitt 28.1, „Installieren von PostgreSQL und Tomcat mit dem Assistenten“, auf Seite 261.<br>◆ Anweisungen zur automatischen Installation finden Sie in Abschnitt 28.2, „Automatische Installation von Tomcat und PostgreSQL für Identity Manager“, auf Seite 263. |
| ❑ | 8. Installieren Sie die restlichen Identity Manager-Komponenten. |

## 27.2 Erläuterungen zum Installationsvorgang für PostgreSQL und Tomcat

Sie können eine oder beide Anwendungen zur Installation auswählen. Wenn bereits eine unterstützte PostgreSQL-Version auf dem Server vorliegt, kann beispielsweise die Installation dieser Anwendung entfallen. Bei den einzelnen Installationen sind die folgenden Überlegungen zu beachten:

**PostgreSQL**

Der Installationsvorgang installiert die Datenbank für die Identitätsanwendungen und erstellt den verwaltungsbefugten Benutzer `idmadmin` als Eigentümer der Datenbank. Hierbei wird jedoch nicht das Schema in der Datenbank für die Identitätsanwendungen angelegt. Die Schemainformationen werden hinzugefügt, sobald Sie die Identitätsanwendungen installieren.

Wenn bereits eine unterstützte PostgreSQL-Version auf dem Server ausgeführt wird, fordert das Installationsprogramm Sie auf, das Passwort für den standardmäßigen Benutzer `postgres` einzugeben. Das Programm erstellt dann den Benutzer `idmadmin` und weist ihm dasselbe Passwort wie für den Benutzer `postgres` zu.

Zum Abschluss startet das Installationsprogramm die Datenbankinstanz. Wenn Sie andere Identity Manager-Komponenten installieren, die die Datenbank verwenden (z. B. die Benutzeranwendung), muss die Instanz ausgeführt werden.

Sie müssen für Identitätsanwendungen nicht PostgreSQL für die Datenbank verwenden.

**Tomcat**

Der Installationsvorgang erstellt den IDM-Apps-Tomcat-Dienst. Zur Unterstützung des Tomcat-Anwendungsservers werden außerdem Apache ActiveMQ und Oracle JRE installiert. Diese unterstützen Tomcat beim Senden von E-Mail-Benachrichtigungen.

Nach Abschluss des Installationsprogramms wird Tomcat nicht automatisch gestartet. Tomcat muss angehalten werden, bevor Sie andere Identity Manager-Komponenten installieren, beispielsweise die Identitätsberichterstellung.

## 27.3 Voraussetzungen für die Installation von PostgreSQL

Lesen Sie die folgenden Überlegungen, bevor Sie die Installation von PostgreSQL planen:

- Sie können die PostgreSQL-Version aus dem Bundle mit Identity Manger in einer Umgebung installieren, in der eine frühere Version des Datenbankprogramms ausgeführt wird. Damit die neue Installation die frühere Version nicht überschreibt, legen Sie ein anderes Verzeichnis für die Dateien fest.
- Die Identitätsanwendungen stellen gewisse Anforderungen an die verwendete Datenbank, beispielsweise PostgreSQL. Weitere Informationen finden Sie in Abschnitt 33.3.5, „Voraussetzungen für die Installation der Datenbank für die Identitätsanwendungen“, auf Seite 305.
- (Bedingt) Unter Windows können Sie nicht mehrere PostgreSQL-Versionen installieren, da das Dienstkonto für Postgres nicht mehrere Instanzen gleichzeitig verarbeiten kann. Deinstallieren Sie die frühere Version, und installieren Sie dann diese Postgres-Version.

## 27.4 Voraussetzungen für die Installation von Tomcat

Lesen Sie die folgenden Überlegungen, bevor Sie die Installation von Tomcat planen:

- Sie können Tomcat und PostgreSQL wahlweise auf demselben Server oder auch auf verschiedenen Servern installieren.
- Der Installationsvorgang installiert unterstützte Versionen von Oracle JRE und Apache ActiveMQ.
- Außerdem werden die erforderlichen Dateien für die Revision von Tomcat-Ereignissen durch den Apache-Dienst Log4j installiert.
- Bei Bedarf können Sie Ihr eigenes Tomcat-Installationsprogramm anstelle des Programms im Installations-Kit von Identity Manager verwenden. Wenn Sie allerdings den Apache Log4j-Dienst zusammen mit Ihrer Tomcat-Version nutzen möchten, überprüfen Sie, ob die entsprechenden Dateien installiert sind. Weitere Informationen finden Sie in Abschnitt 29.4, „Protokollieren der Anmeldung mit dem Apache-Log4j-Dienst“, auf Seite 271. Diese Voraussetzung gilt für die Verwendung von Tomcat für OSP, die Identitätsanwendungen und die Identitätsberichterstellung.
- Damit die Zustellung von Email-Benachrichtigungen gewährleistet ist, installieren Sie MQServer.
- Die Identitätsanwendungen stellen gewisse Anforderungen an den Tomcat-Anwendungsserver, auf dem sie ausgeführt werden. Weitere Informationen finden Sie unter Abschnitt 33.3.3, „Voraussetzungen und Überlegungen für den Anwendungsserver“, auf Seite 304.

- Der Installationsvorgang legt den JRE-Speicherort in der Datei `setenv.sh` fest (standardmäßig im Verzeichnis `/opt/netiq/idm/apps/tomcat/bin/`). Wenn Sie die Identitätsanwendungen und die Identitätsberichterstellung in Tomcat installieren, wird der Eintrag `JAVA_OPTs` bzw. `CATALINA_OPTS` in der Datei `setenv.sh` aktualisiert.
- Führen Sie Tomcat nicht als `Root` aus. Der Installationsvorgang erstellt ein Benutzerkonto für den Tomcat-Dienst; das Konto `Root` ist dabei nicht zulässig.

## 27.5 Systemanforderungen für PostgreSQL

Für PostgreSQL gelten dieselben Anforderungen an die Computer wie für die Identitätsanwendungen. Weitere Informationen finden Sie in Abschnitt 33.4, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 307. Beachten Sie auch die Versionsnoten zur aktuellen Version von Identity Manager sowie die PostgreSQL-Dokumentation.

## 27.6 Systemanforderungen für Tomcat

Für Tomcat gelten dieselben Anforderungen an die Computer wie für die Identitätsanwendungen. Weitere Informationen finden Sie in Abschnitt 33.4, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 307. Beachten Sie auch die Versionsnoten zur aktuellen Version von Identity Manager sowie die Apache-Dokumentation.

# 28 Installieren von PostgreSQL und Tomcat

In diesem Abschnitt finden Sie die Schritte für die Installation von Tomcat und PostgreSQL.



## 28.1 Installieren von PostgreSQL und Tomcat mit dem Assistenten

Im Folgenden wird beschrieben, wie Sie Tomcat und PostgreSQL auf einer Linux- oder Windows-Plattform mithilfe eines geführten Verfahrens installieren (wahlweise über die Benutzeroberfläche oder an der Konsole). Anweisungen für die automatische, unbeaufsichtigte Installation finden Sie in Abschnitt 28.2, „Automatische Installation von Tomcat und PostgreSQL für Identity Manager“, auf Seite 263.

Überprüfen Sie in Vorbereitung auf die Installation die Checkliste der Voraussetzungen und Systemanforderungen in den folgenden Abschnitten:

- Abschnitt 27.4, „Voraussetzungen für die Installation von Tomcat“, auf Seite 259
- Abschnitt 27.3, „Voraussetzungen für die Installation von PostgreSQL“, auf Seite 259
- Versionshinweise zur betreffenden Version

---

**HINWEIS:** Sie müssen Passwörter für die Datenbank angeben, unabhängig davon, ob Sie PostgreSQL installieren oder eine vorhandene Version von PostgreSQL verwenden. Dieses Installationsprogramm unterstützt jedoch keine Passwörter, die ein "- oder $-Zeichen enthalten. Ändern Sie das Passwort nach Abschluss des Installationsvorgangs, wenn Sie diese Sonderzeichen verwenden möchten.

---

**So führen Sie eine geführte Installation aus:**

1. Melden Sie sich als `Root` oder Administrator an dem Computer an, auf dem die Anwendungen installiert werden sollen.
2. Stellen Sie sicher, dass der geplante Installationspfad keine Verzeichnisse mit den folgenden Namen enthält:
   - tomcat
   - postgres
   - activemq
   - jre
3. (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die OSP-Installationsdateien befinden:
   - **Linux:** `products/RBPM/postgre_tomcat_install/`
   - **Windows:** `products/RBPM/postgre_tomcat_install`

4 (Bedingt) Wenn Sie die Installationsdateien von der NetIQ Downloads-Website heruntergeladen haben, führen Sie die folgenden Schritte aus:

**4a** Navigieren Sie zur `.tgz`- oder `win.zip`-Datei für das heruntergeladene Image.

**4b** Extrahieren Sie den Inhalt der Datei in ein Verzeichnis auf dem lokalen Computer.

5 Führen Sie im Verzeichnis mit den Installationsdateien einen der folgenden Schritte aus:

- **Linux (Konsole)** – Geben Sie Folgendes ein: `/TomcatPostgreSQL.bin -i console`
- **Linux (Benutzeroberfläche)** – Geben Sie Folgendes ein: `/TomcatPostgreSQL.bin`
- **Windows** – Führen Sie die folgende Datei aus: `TomcatPostgreSQL.exe`

6 Legen Sie im Installationsprogramm die gewünschte Sprache für die Installation fest, und klicken Sie auf **OK**.

7 Lesen Sie den Einführungstext, und klicken Sie auf **Weiter**.

8 Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf **Weiter**.

9 Geben Sie an, ob Tomcat und/oder PostgreSQL installiert werden soll.

10 Legen Sie abschließend Werte für die folgenden Parameter fest:

- **Übergeordneter Tomcat-Ordner**

  *Gilt nur dann, wenn Tomcat installiert werden soll.*

  Gibt das Verzeichnis an, in dem die Tomcat-Dateien installiert werden sollen.

- **Tomcat-Details**

  *Gilt nur dann, wenn Tomcat installiert werden soll.*

  Gibt die erforderlichen Ports für Tomcat an.

  **Port zum Herunterfahren von Tomcat**

  Gibt den Port an, über den alle Webapps und Tomcat sauber heruntergefahren werden sollen. Der Standardwert ist 8005.

  **Tomcat-HTTP-Port**

  Gibt den Port an, über den der Tomcat-Server mit den Client-Computern kommunizieren soll. Der Standardwert ist 8080. Für SSL gilt der Standardwert 8443.

  **Tomcat-Umleitungsport**

  (Bedingt) Gibt den Port an, an den der Anwendungsserver Anforderungen weiterleiten soll, für die ein SSL-Transport erforderlich ist, wenn das TLS/SSL-Protokoll nicht verwendet wird. Der Standardwert ist 8443.

  **Tomcat-AJP-Port**

  (Optional) Gibt den Port an, über den der Anwendungsserver mit einem Web-Connector über das AJP-Protokoll anstatt über `http` kommunizieren soll. Der Standardwert ist 8009.

  Mit diesem Parameter geben Sie an, dass der Anwendungsserver den statischen Inhalt in der Web-Anwendung verwalten und/oder die SSL-Verarbeitung des Anwendungsservers nutzen soll.

- **Übergeordneter PostgreSQL-Ordner**

  *Gilt nur dann, wenn PostgreSQL installiert werden soll.*

  Gibt das Verzeichnis an, in dem die PostgreSQL-Dateien installiert werden sollen.

- **PostgreSQL-Details**

  *Gilt nur dann, wenn PostgreSQL installiert werden soll.*

  Gibt die Einstellungen für die PostgreSQL-Datenbank für die Identitätsanwendungen an.

**HINWEIS:** Wenn bereits eine unterstützte PostgreSQL-Version auf dem Server ausgeführt wird, fordert das Installationsprogramm Sie auf, das Passwort für den standardmäßigen Benutzer `postgres` einzugeben. Das Programm erstellt dann den Benutzer `idmadmin` und weist ihm dasselbe Passwort wie für den Benutzer `postgres` zu.

Dieses Installationsprogramm unterstützt jedoch keine Passwörter, die ein `"`- oder `$`-Zeichen enthalten.

***Datenbankname***

Gibt den Namen der Datenbank an. Der Standardwert lautet `idmuserappdb`.

***Datenbankadministrator***

(Optional) Gibt das Konto `idmadmin` an, also den Datenbankadministrator, der Datenbanktabellen, Ansichten und andere Artefakte erstellen kann.

Dieses Konto ist nicht mit dem standardmäßigen Benutzer „postgres“ identisch.

***Passwort für Admin.Benutzer***

Gibt das Passwort für den Datenbankadministrator und den standardmäßigen Benutzer `postgres` an.

Dieses Installationsprogramm unterstützt jedoch keine Passwörter, die ein `"`- oder `$`-Zeichen enthalten.

***PostgreSQL-Port***

Gibt den Port des Servers an, auf dem die Postgres-Datenbank gehostet wird. Der Standardwert ist 5432.

**11** Lesen Sie die Seite Übersicht vor der Installation.

**12** Starten Sie den Installationsvorgang.

**13** Klicken Sie nach Abschluss des Installationsvorgangs auf *Fertig*.

## 28.2 Automatische Installation von Tomcat und PostgreSQL für Identity Manager

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 `silent.properties` ab. Sie können die automatische Installation wahlweise mit der Standarddatei ausführen oder die Datei bearbeiten und so den Installationsvorgang anpassen. Anweisungen zur geführten Installation finden Sie in Abschnitt 28.1, „Installieren von PostgreSQL und Tomcat mit dem Assistenten“, auf Seite 261.

Überprüfen Sie in Vorbereitung auf die Installation die Checkliste der Voraussetzungen und Systemanforderungen in den folgenden Abschnitten:

- Abschnitt 27.4, „Voraussetzungen für die Installation von Tomcat“, auf Seite 259
- Abschnitt 27.3, „Voraussetzungen für die Installation von PostgreSQL“, auf Seite 259
- Abschnitt 28.2.1, „Schützen der Passwörter für eine automatische Installation“, auf Seite 264
- Versionshinweise zur betreffenden Version

### 28.2.1 Schützen der Passwörter für eine automatische Installation

Wenn Sie die Passwörter nicht in der Datei `silent.properties` festlegen möchten, können Sie sie in der Umgebung definieren. In diesem Fall ruft die automatische Installation die Passwörter nicht aus der Datei `silent.properties` ab, sondern aus der Umgebung. Dadurch können Sie noch mehr Sicherheit erzielen.

Für die Installation müssen Sie die folgenden Passwörter angeben:

- NETIQ_DB_PASSWORD
- NETIQ_DB_PASSWORD_CONFIRM

**Linux**

Verwenden Sie den Befehl `export`. Beispiel:

```
export NETIQ_DB_PASSWORD_CONFIRM=myPassWord
```

**Windows**

Verwenden Sie den Befehl `set`. Beispiel:

```
set NETIQ_DB_PASSWORD_CONFIRM=myPassWord
```

Das Installationsprogramm unterstützt jedoch keine Passwörter, die ein "- oder $-Zeichen enthalten. Ändern Sie das Passwort nach der Installation von PostgreSQL, falls Sie diese Sonderzeichen verwenden möchten.

### 28.2.2 Automatische Installation von Tomcat und PostgreSQL

1. Melden Sie sich an dem Computer an, auf dem die Anwendungen installiert werden sollen.
2. (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die OSP-Installationsdateien befinden:
   - **Linux:** `products/RBPM/postgre_tomcat_install`
   - **Windows:** `products/RBPM/postgre_tomcat_install`
3. (Bedingt) Wenn Sie die Installationsdateien 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 ein Verzeichnis auf dem lokalen Computer.
4. Legen Sie die Installationsparameter mit den folgenden Schritten fest:
   - **4a** Stellen Sie sicher, dass sich die `silent.properties`-Datei in demselben Verzeichnis wie die ausführbare Datei für die Installation befindet.
   - **4b** Öffnen Sie die Datei `silent.properties` in einem Texteditor.
   - **4c** Legen Sie die Parameterwerte fest. Eine Beschreibung der Parameter finden Sie in Schritt 10 auf Seite 262.

     **HINWEIS:** Soll eine vorhandene PostgreSQL-Datenbank für Ihre Benutzeranwendung auf einem Linux-Server verwendet werden, geben Sie `installed` unter `NETIQ_USE_INSTALLED_POSTGRES` an. Die Datenbankinstanz muss von einer unterstützten PostgreSQL-Version ausgeführt werden. Außerdem ist es nicht nötig, die Datenbank zu konfigurieren.
   - **4d** Speichern und schließen Sie die Datei.

5 Starten Sie den Installationsvorgang mit einem der folgenden Befehle:

- **Linux:** `TomcatPostgreSQL.bin -i silent -f silent.properties`
- **Windows:** `install -i silent -f silent.properties`

---

**HINWEIS:** Wenn sich die `silent.properties`-Datei nicht in demselben Verzeichnis befindet wie das Installationsskript, werden Sie aufgefordert, den vollständigen Pfad zu dieser Datei einzugeben. Das Skript entpackt die notwendigen Dateien in ein temporäres Verzeichnis und startet dann die automatische Installation.

---

# X Installieren der Single-Sign-on-Komponente

In diesem Abschnitt installieren Sie den OSP (One SSO Provider), um den Single-Sign-on-Zugriff auf die Identitätsanwendungen und Identitätsberichterstellung zu unterstützen.

Die Installationsdateien befinden sich im Verzeichnis `products/RBPM/osp_install` im Identity Manager-Installationspaket. Standardmäßig installiert das Installationsprogramm die Komponenten an den folgenden Speicherorten:

- **Linux:** `/opt/netiq/idm/apps/osp`
- **Windows:** `C:\netiq\idm\apps\osp`

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren.

# 29 Planen der Installation von Single Sign-on für Identity Manager

In diesem Abschnitt finden Sie Informationen zu den Voraussetzungen, Überlegungen und der Systemeinrichtung für die Installation von One SSO Provider (OSP).



## 29.1 Checkliste für die Single-Sign-on-Komponente

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 4.5, „Verwenden des Single-Sign-On-Zugriffs in Identity Manager“, auf Seite 42. |
| ❑ | 2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |
| ❑ | 3. Stellen Sie sicher, dass Tomcat installiert ist. Weitere Informationen finden Sie in Kapitel 28, „Installieren von PostgreSQL und Tomcat“, auf Seite 261. |
| ❑ | 4. (Bedingt) Sollen die Ereignisse mit dem Apache Log4j-Dienst in Tomcat festgehalten werden, stellen Sie sicher, dass die entsprechenden Dateien vorliegen. Weitere Informationen finden Sie in Abschnitt 29.4, „Protokollieren der Anmeldung mit dem Apache-Log4j-Dienst“, auf Seite 271. |
| ❑ | 5. (Bedingt) Zur geführten Installation auf Computern mit dem Betriebssystem SLES 12 SP1 (oder höher) müssen die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in Abschnitt 6.3, „Installieren von Identity Manager auf Servern mit SLES 12 SP1 (oder höher)“, auf Seite 63. |
| ❑ | 6. (Bedingt) Stellen Sie bei Computern mit RHEL 6.x- oder Rhel 7.x-Betriebssystem sicher, dass die erforderlichen Bibliotheken installiert sind. Weitere Informationen finden Sie in Abschnitt 6.4, „Installieren von Identity Manager auf einem RHEL 6.*x- oder 7.x-Server“, auf Seite 63*. |
| ❑ | 7. Installieren Sie OSP:<br>◆ Anweisungen zur geführten Installation finden Sie in Abschnitt 30.1, „Installieren von One SSO Provider mit dem Assistenten“, auf Seite 273.<br>◆ Anweisungen zur automatischen Installation finden Sie in Abschnitt 30.2, „Automatische Installation von One SSO Provider“, auf Seite 276. |

| | Checkliste |
|---|---|
| ❑ | 8. Installieren Sie SSPR (Self Service Password Reset) zur Verwaltung der Benutzerpasswörter für Identitätsanwendungen. Weitere Informationen finden Sie in Teil XI, „Installieren der Passwortverwaltungskomponente“, auf Seite 279. |
| ❑ | 9. Installieren und konfigurieren Sie die Identitätsanwendungen für den Single-Sign-on-Zugriff. Weitere Informationen finden Sie in Teil XII, „Installieren der Identitätsanwendungen“, auf Seite 295. |

## 29.2 Voraussetzungen für die Installation von One SSO Provider (OSP)

Die folgenden Identity Manager-Komponenten nehmen die Benutzerauthentifizierung über OSP vor:

- Identitätsanwendungen
- Identitätsberichterstellung

NetIQ empfiehlt, vor dem Installieren von OSP die folgenden Überlegungen zu lesen:

- Zum Ausführen von OSP können Sie bei Bedarf Ihr eigenes Tomcat-Installationsprogramm anstelle des Programms im Installations-Kit von Identity Manager verwenden. Wenn Sie allerdings den Apache Log4j-Dienst zusammen mit Ihrer Tomcat-Version nutzen möchten, überprüfen Sie, ob die entsprechenden Dateien installiert sind. Weitere Informationen finden Sie in Abschnitt 29.4, „Protokollieren der Anmeldung mit dem Apache-Log4j-Dienst“, auf Seite 271.
- Sie können OSP für die Verwendung von NetIQ Access Manager 4.0 über die SAML 2.0-Authentifizierung konfigurieren. Weitere Informationen finden Sie in Kapitel 49, „Single Sign-On per SAML-Authentifizierung mit NetIQ Access Manager“, auf Seite 451.
- OSP benötigt Herkunftsverbürgungszertifikate für die Kommunikation der Identitätsanwendungen und der Berichterstellung mit dem Authentifizierungsserver. Der Installationsvorgang erstellt automatisch ein Zertifikat für TLS/SSL in der Datei `osp.jks`. Sie können außerdem ein Herkunftsverbürgungszertifikat für eine SAML-Assertion mit eDirectory anlegen lassen.

  **HINWEIS:** Diese Zertifikate laufen zwei Jahre nach dem Erstellungsdatum ab. Sobald die Zertifikate ablaufen, müssen Sie neue Zertifikate erstellen. Weitere Informationen hierzu finden Sie in Abschnitt 40.3.1, „Beglaubigungsserver“, auf Seite 379 und Teil XV, „Konfiguration des Single-Sign-On-Zugriffs in Identity Manager“, auf Seite 443.

## 29.3 Systemanforderungen für One SSO Provider (OSP)

Für OSP ist der Apache Tomcat-Anwendungsserver erforderlich. Die Version von Tomcat muss mit der für die Identitätsanwendungen erforderlichen Version übereinstimmen.

Alle anderen Anforderungen entsprechen den Serveranforderungen für die Identitätsanwendungen. Weitere Informationen finden Sie in Abschnitt 33.3, „Voraussetzungen und Überlegungen für die Installation der Identitätsanwendungen“, auf Seite 300 sowie in den aktuellen Versionshinweisen.

# 29.4 Protokollieren der Anmeldung mit dem Apache-Log4j-Dienst

Die Ereignisse, die in Tomcat auftreten, können wahlweise mit dem Apache-Dienst Log4j oder mit dem Dienst java.util.logging protokolliert werden. Das Tomcat-Installationsprogramm im Installations-Kit von Identity Manager enthält die erforderlichen Dateien für Log4j. Wenn Sie eine eigene Tomcat-Version installieren, benötigen Sie die folgenden Dateien zum Ausführen des Apache-Protokollierungsdienstes:

- `log4j-1.2.16.jar`
- `tomcat-juli-adapters.jar`
- `tomcat-juli.jar`

Fügen Sie die Dateien mit den folgenden Schritten zu Ihrer Tomcat-Installation hinzu:

1. Laden Sie die JULI-Dateien für Tomcat 8.5.x von der Apache-Website herunter:
   - `tomcat-juli.jar`
   - `tomcat-juli-adapters.jar`
2. Laden Sie die Datei `log4j-1.2.16.jar` von der Apache-Website herunter.
3. Legen Sie die folgenden Verzeichnisse im Verzeichnis `$TOMCAT_HOME/lib` ab:
   - `log4j-1.2.16.jar`
   - `tomcat-juli-adapters.jar`
4. Legen Sie die Datei `tomcat-juli.jar` im Verzeichnis `$TOMCAT_HOME/bin` ab.
5. Legen Sie einen Wert für `-Dlog4j.configuration` in `CATALINA_OPTS` fest, oder erstellen Sie eine Datei `log4j.properties` im Verzeichnis `$TOMCAT_HOME/lib`.

# 30 Installieren von Single Sign-on für Identity Manager



## 30.1 Installieren von One SSO Provider mit dem Assistenten

Im Folgenden wird beschrieben, wie Sie OSP auf einer Linux- oder Windows-Plattform mithilfe eines Installationsassistenten installieren (wahlweise im GUI-Format oder an der Konsole). Anweisungen für die automatische, unbeaufsichtigte Installation finden Sie in Abschnitt 30.2, „Automatische Installation von One SSO Provider“, auf Seite 276. Überprüfen Sie in Vorbereitung auf die Installation die Voraussetzungen und Systemanforderungen in Abschnitt 29.1, „Checkliste für die Single-Sign-on-Komponente“, auf Seite 269.

1. Melden Sie sich als `Root` oder Administrator an dem Server an, auf dem OSP installiert werden soll.
2. Stoppen des Tomcat-Servers.
3. (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die OSP-Installationsdateien befinden (standardmäßig unter `products/rbpm/osp_install`).
4. (Bedingt) Wenn Sie die OSP-Installationsdateien heruntergeladen haben, führen Sie die folgenden Schritte aus:
   - **4a** Navigieren Sie zur `.tgz`- oder `win.zip`-Datei für das heruntergeladene Image.
   - **4b** Extrahieren Sie den Inhalt der Datei in ein Verzeichnis auf dem lokalen Computer.
5. Führen Sie im Verzeichnis mit den Installationsdateien einen der folgenden Schritte aus:
   - **Linux (Benutzeroberfläche)** – Geben Sie Folgendes ein: `/osp-install-linux.bin`
   - **Windows**: Führen Sie `osp-install.exe` aus
6. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Weiter**.
7. Legen Sie einen Pfad für die installierten Dateien fest.
8. Führen Sie die geführte Installation mit den folgenden Parametern aus:
   - **Tomcat-Details**

     Gibt das Basisverzeichnis für den Tomcat-Server an. Beispiel: `/opt/netiq/idm/apps/tomcat`. Der Installationsvorgang legt einige weitere Dateien für OSP in diesem Ordner ab.

- **Tomcat-Verbindung**

  Gibt die Einstellungen für die URL an, über die die Benutzer eine Verbindung zu OSP auf dem Tomcat-Server aufbauen. Beispiel: `https:meinserver.meinefirma.de:8543`.

  ***Protokoll***

  Gibt an, ob *http* oder *https* verwendet werden soll. Soll die Kommunikation per SSL (Secure Sockets Layer) erfolgen, wählen Sie `https`.

  ***Hostname***

  Gibt den DNS-Namen oder die IP-Adresse des Servers an, auf dem OSP installiert werden soll. Verwenden Sie nicht `localhost`.

  ***Port***

  Gibt den Port an, über den der Server mit den Client-Computern kommunizieren soll.

- **Tomcat-Java-Home**

  Gibt das Basisverzeichnis für Java auf dem Tomcat-Server an. Beispiel: `/usr/lib/jvm/default-java`. Der Installationsvorgang legt einige weitere Dateien für OSP in diesem Verzeichnis ab.

- **Authentifizierungsdetails**

  Gibt die Anforderungen für das Herstellen einer Verbindung zum Authentifizierungsserver an, auf dem sich eine Liste der Benutzer befindet, die sich bei der Anwendung anmelden können. Weitere Informationen zum Authentifizierungsserver finden Sie in Abschnitt 4.5.1, „Erläuterungen zur Authentifizierung mit One SSO Provider (OSP)“, auf Seite 42.

  ***LDAP-Host***

  Gibt den DNS-Namen oder die IP-Adresse des LDAP-Authentifizierungsservers an. Verwenden Sie nicht `localhost`.

  ***LDAP-Port***

  Gibt den Port an, über den der LDAP-Authentifizierungsserver mit Identity Manager kommunizieren soll. Geben Sie beispielsweise 389 als nicht sicheren Port oder 636 für SSL-Verbindungen an.

  ***SSL verwenden***

  Gibt an, ob die Kommunikation zwischen dem Identitätsdepot und dem Authentifizierungsserver über das SSL-Protokoll (Secure Sockets Layer) erfolgen soll.

  ***JRE-Truststore-Datei (cacerts-Datei)***

  *Gilt nur dann, wenn SSL für die LDAP-Verbindung verwendet werden soll.*

  Gibt den Pfad zum Zertifikat an. Beispiel: `C:\netiq\idm\apps\jre\lib\security\cacerts`.

  ***Passwort für JRE-Truststore***

  *Gilt nur dann, wenn SSL für die LDAP-Verbindung verwendet werden soll.*

  Gibt das Passwort für die `cacerts`-Datei an.

  ***Admin-DN***

  *Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.*

  Gibt den DN eines Administratorkontos für den LDAP-Authentifizierungsserver an. Beispiel: `cn=admin,ou=sa,o=system`.

  ***Admin-Passwort***

  *Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.*

  Gibt das Passwort des Administratorkontos für den LDAP-Authentifizierungsserver an.

***Benutzercontainer***

*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.*

Gibt den Container auf dem LDAP-Authentifizierungsserver an, in dem die Benutzerkonten gespeichert sind, die sich bei Access Review anmelden können. Beispiel: `o=data`.

***Admin-Container***

*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.*

Gibt den Container auf dem LDAP-Authentifizierungsserver an, in dem die Administratorkonten für Access Review gespeichert sind. Beispiel: `ou=sa,o=system`.

***Keystore-Passwort***

*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.*

Gibt das Passwort an, das für den neuen Keystore für den LDAP-Authentifizierungsserver erstellt werden soll.

Das Passwort muss mindestens sechs Zeichen umfassen.

- **Auditing-Details (OSP)**

Gibt die Einstellungen für die Revision von OSP-Ereignissen an, die auf dem Authentifizierungsserver auftreten.

***Auditing für OSP aktivieren***

Gibt an, ob die OSP-Ereignisse an einen Revisionsserver gesendet werden sollen.

Wenn Sie diese Einstellung wählen, geben Sie außerdem den Speicherort für den Audit-Protokoll-Cache an.

***Cache-Ordner für Audit-Protokoll***

*Gilt nur dann, wenn Sie die Revision für OSP aktivieren.*

Gibt den Speicherort des Cache-Verzeichnisses für die Revision an. Beispiel: `/var/opt/novell/naudit/jcache`.

***Vorhandenes Zertifikat angeben / Zertifikat erzeugen***

Gibt an, ob ein vorhandenes Zertifikat für den NAudit Server verwendet oder ein neues Zertifikat erstellt werden soll.

***Öffentlichen Schlüssel eingeben***

*Gilt nur dann, wenn ein vorhandenes Zertifikat verwendet werden soll.*

Gibt das benutzerdefinierte Zertifikat mit öffentlichem Schlüssel an, mit dem der NAudit-Dienst die gesendeten Revisionsmeldungen authentifizieren soll.

***RSA-Schlüssel eingeben***

*Gilt nur dann, wenn ein vorhandenes Zertifikat verwendet werden soll.*

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

**9** Fahren Sie zur Installation von SSPR mit Teil XI, „Installieren der Passwortverwaltungskomponente“, auf Seite 279 fort.

Weitere Informationen zum Konfigurieren der „Passwort vergessen“-Verwaltung finden Sie in Abschnitt 39.6, „Konfigurieren der „Passwort vergessen“-Verwaltung“, auf Seite 359.

## 30.2 Automatische Installation von One SSO Provider

Bei der automatischen (nicht interaktiven) Installation wird keine Benutzeroberfläche angezeigt, und der Benutzer muss keinerlei Fragen beantworten.

1. Melden Sie sich als `Root` oder Administrator an dem Computer an, auf dem die Komponenten installiert werden sollen.
2. Halten Sie Tomcat an.
3. (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die OSP-Installationsdateien befinden (standardmäßig unter `osp_`).
4. (Bedingt) Wenn Sie die Installationsdateien von der NetIQ Downloads-Website heruntergeladen haben, führen Sie die folgenden Schritte aus:
   - **4a** Navigieren Sie zur `.tgz`- oder `.zip`-Datei für das heruntergeladene Image.
   - **4b** Extrahieren Sie den Inhalt der Datei in einen Ordner auf dem lokalen Computer.
5. Bearbeiten Sie die Datei `osp.install.properties` für die OSP-Installation (standardmäßig in demselben Verzeichnis wie die Installationsskripte).

   Weitere Informationen zu den Einstellungen für die Installation finden Sie in Schritt 7 und Schritt 8 auf Seite 273.
6. Starten Sie die automatische Installation mit einem der folgenden Befehle:
   - **Linux**: `osp-install-linux.bin -i silent -f` *`Pfad_zur_silent.properties-Datei`*
   - **Windows**: `osp-install-win.exe -i silent -f` *`Pfad_zur_silent.properties-Datei`*
7. Installieren Sie SSPR. Weitere Informationen finden Sie unter Teil XI, „Installieren der Passwortverwaltungskomponente“, auf Seite 279.

## 30.3 Konfiguration des Single-Sign-On-Zugriffs

Der Single-Sign-On-Zugriff kann direkt nach der Installation von OSP konfiguriert werden. Vor der ersten Konfiguration müssen Sie jedoch die Identitätsanwendungen installieren. Weitere Informationen finden Sie in Teil XV, „Konfiguration des Single-Sign-On-Zugriffs in Identity Manager“, auf Seite 443.

---

**HINWEIS:** Wird One SSO Provider im Automatikmodus konfiguriert, muss der richtige Pfad zum Installations-, Java-, Tomcat- und SSL-Keystore-Ordner in der Datei `osp.configure.properties` angegeben werden. Beispiel:

**Installationsordner:**

- **Linux**: `USER_INSTALL_DIR=/opt/netiq/idm/apps/osp`
- **Windows**: `USER_INSTALL_DIR=C:\netiq\idm\apps\osp`

**Tomcat-Ordner:**

- **Linux**: `NETIQ_TOMCAT_HOME=/opt/netiq/idm/apps/tomcat`
- **Windows**: `NETIQ_TOMCAT_HOME=C:\netiq\idm\apps\tomcat`

**Java-Ordner:**

- **Linux**: `NETIQ_JAVA_HOME=/opt/netiq/idm/apps/jre`
- **Windows**: `NETIQ_JAVA_HOME=C:\netiq\idm\apps\jre`

**SSL-Keystore-Ordner:**

- **Linux**: `NETIQ_SSL_KEYSTORE_FILE=/opt/netiq/idm/apps/jre/lib/security/cacerts`
- **Windows**: `USER_INSTALL_DIR=C:\netiq\idm\apps\jre\lib\security\cacerts`

---

# XI Installieren der Passwortverwaltungskomponente

In diesem Abschnitt installieren Sie SSPR (Self Service Password Reset – Zurücksetzen von Passwörtern per Selbstbedienung), womit Sie Identity Manager so konfigurieren, dass Benutzer ihre Passwörter zurücksetzen dürfen.

SSPR wird in die Identitätsanwendungen, die Identitätsberichterstellung und OSP eingebunden und leitet die Benutzer, die ihr Passwort zurücksetzen müssen, ohne weitere Schritte an die geeigneten Webseiten weiter. Sobald die Benutzer die Schritte in Selbstbedienung abgeschlossen habe, leitet SSPR die Benutzer wieder zu der Anwendung zurück, auf die sie ursprünglich zuzugreifen versucht hatten.

---

**HINWEIS:** In Identity Manager 4.6 (oder höher) fungiert SSPR als primäres Passwortverwaltungstool.

---

In Identity Manager ist SSPR nicht erforderlich. Zum Zurücksetzen von Benutzerpasswörtern stehen auch andere Methoden zur Verfügung. Sie müssen dann jedoch möglicherweise einige Konfigurationseinstellung für Identity Manager bearbeiten. Weitere Informationen finden Sie unter Abschnitt 39.6, „Konfigurieren der „Passwort vergessen“-Verwaltung“, auf Seite 359.

Die Installationsdateien befinden sich im Verzeichnis `products/RBPM/sspr_install`. Standardmäßig installiert das Installationsprogramm die Komponenten an den folgenden Speicherorten:

- **Linux**: `/opt/netiq/idm/apps/sspr`
- **Windows**: `C:\netiq\idm\apps\sspr`

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren.

# 31 Planen der Installation der Passwortverwaltung für Identity Manager

In diesem Abschnitt finden Sie Informationen zu den Voraussetzungen, Überlegungen und der Systemeinrichtung für die Installation von SSPR (Self Service Password Reset).

- Abschnitt 31.1, „Checkliste für die Installation der Passwortverwaltungskomponenten“, auf Seite 281
- Abschnitt 31.2, „Voraussetzungen für die Installation der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung“, auf Seite 282
- Abschnitt 31.3, „Systemanforderungen für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung“, auf Seite 282
- Abschnitt 31.4, „Verwenden des Apache Log4j-Diensts für Passwortereignisse“, auf Seite 282

## 31.1 Checkliste für die Installation der Passwortverwaltungskomponenten

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 4.4, „Verwenden von Self-Service Password Management in Identity Manager“, auf Seite 40. |
| ❑ | 2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |
| ❑ | 3. Stellen Sie sicher, dass Tomcat installiert ist. Weitere Informationen finden Sie in Kapitel 28, „Installieren von PostgreSQL und Tomcat“, auf Seite 261. |
| ❑ | 4. (Bedingt) Sollen die Ereignisse mit dem Apache Log4j-Dienst in Tomcat festgehalten werden, stellen Sie sicher, dass die entsprechenden Dateien vorliegen. Weitere Informationen finden Sie in Abschnitt 29.4, „Protokollieren der Anmeldung mit dem Apache-Log4j-Dienst“, auf Seite 271. |
| ❑ | 5. (Bedingt) Zur geführten Installation auf Computern mit dem Betriebssystem SLES 12 SP1 (oder höher) müssen die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in Abschnitt 6.3, „Installieren von Identity Manager auf Servern mit SLES 12 SP1 (oder höher)“, auf Seite 63. |
| ❑ | 6. (Bedingt) Stellen Sie bei Computern mit RHEL 6.x- oder Rhel 7.x-Betriebssystem sicher, dass die erforderlichen Bibliotheken installiert sind. Weitere Informationen finden Sie in Abschnitt 6.4, „Installieren von Identity Manager auf einem RHEL 6.*x- oder 7.x-Server“, auf Seite 63*. |

| | Checkliste |
|---|---|
| ❑ | 7. Installieren von SSPR:<br>◆ Anweisungen zur geführten Installation finden Sie in Abschnitt 32.1, „Installation von SSPR (Self-Service Passwort Request) mit dem Assistenten“, auf Seite 285.<br>◆ Anweisungen zur automatischen Installation finden Sie in Abschnitt 32.2, „Automatische Installation von SSPR (Self Service Password Reset)“, auf Seite 288. |
| ❑ | 8. Installieren Sie die Identitätsanwendungen, und konfigurieren Sie sie für den Single-Sign-On-Zugriff und die Passwortverwaltung. Weitere Informationen finden Sie in Teil XII, „Installieren der Identitätsanwendungen“, auf Seite 295. |

## 31.2 Voraussetzungen für die Installation der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung

Die Installation von NetIQ Self Service Password Reset (SSPR) muss den Serveranforderungen für die Identitätsanwendungen entsprechen, wobei die folgenden Überlegungen gelten:

- SSPR benötigt das TSL/SSL-Protokoll für die Kommunikation.
- SSPR benötigt eine unterstützte Version des Tomcat-Anwendungsservers. Weitere Informationen finden Sie in Abschnitt 27.4, „Voraussetzungen für die Installation von Tomcat“, auf Seite 259 sowie in den aktuellen Versionshinweisen.
- NetIQ empfiehlt, die Voraussetzungen und Anforderungen im *NetIQ Self Service Password Reset Administration Guide* (Administrationshandbuch für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung) zu lesen.

## 31.3 Systemanforderungen für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung

Für SSPR ist der Apache Tomcat-Anwendungsserver erforderlich. Die Version von Tomcat muss mit der für die Identitätsanwendungen erforderlichen Version übereinstimmen.

Alle anderen Anforderungen entsprechen den Serveranforderungen für die Identitätsanwendungen. Weitere Informationen finden Sie in Abschnitt 33.3, „Voraussetzungen und Überlegungen für die Installation der Identitätsanwendungen“, auf Seite 300 sowie in den aktuellen Versionshinweisen.

## 31.4 Verwenden des Apache Log4j-Diensts für Passwortereignisse

Die Ereignisse, die in Tomcat auftreten, können wahlweise mit dem Apache-Dienst Log4j oder mit dem Dienst java.util.logging protokolliert werden. Das Tomcat-Installationsprogramm im Installations-Kit von Identity Manager enthält die erforderlichen Dateien für Log4j. Wenn Sie eine eigene Tomcat-Version installieren, benötigen Sie die folgenden Dateien zum Ausführen des Apache-Protokollierungsdienstes:

- `log4j-1.2.16.jar`

- `tomcat-juli-adapters.jar`
- `tomcat-juli.jar`

Fügen Sie die Dateien mit den folgenden Schritten zu Ihrer Tomcat-Installation hinzu:

1. Laden Sie die JULI-Dateien für Tomcat 8.5.x von der Apache-Website herunter:
   - `tomcat-juli.jar`
   - `tomcat-juli-adapters.jar`
2. Laden Sie die Datei `log4j-1.2.16.jar` von der Apache-Website herunter.
3. Legen Sie die folgenden Verzeichnisse im Verzeichnis `$TOMCAT_HOME/lib` ab:
   - `log4j-1.2.16.jar`
   - `tomcat-juli-adapters.jar`
4. Legen Sie die Datei `tomcat-juli.jar` im Verzeichnis `$TOMCAT_HOME/bin` ab.
5. Legen Sie einen Wert für `-Dlog4j.configuration` in `CATALINA_OPTS` fest, oder erstellen Sie eine Datei `log4j.properties` im Verzeichnis `$TOMCAT_HOME/lib`.

# 32 Installieren der Passwortverwaltung für Identity Manager

In diesem Abschnitt wird der Installationsvorgang für SSPR beschrieben. Sie können diese Programme auf dem Server installieren, auf dem die OSP-Komponente installiert ist, oder auch auf einem separaten Server.



---

**HINWEIS:** Wenn Sie sich für die bisherige Methode für vergessene Passwörter entscheiden, entfällt die Installation von SSPR. Weitere Informationen finden Sie in Abschnitt 4.4.2, „Erläuterungen zum bisherigen Anbieter für die Passwortverwaltung“, auf Seite 41.

---

## 32.1 Installation von SSPR (Self-Service Passwort Request) mit dem Assistenten

Im Folgenden wird beschrieben, wie Sie SSPR auf einer Linux- oder Windows-Plattform mithilfe eines Installationsassistenten installieren (wahlweise im GUI-Format oder an der Konsole). Anweisungen für die automatische, unbeaufsichtigte Installation finden Sie in Abschnitt 32.2, „Automatische Installation von SSPR (Self Service Password Reset)“, auf Seite 288. Überprüfen Sie in Vorbereitung auf die Installation die Voraussetzungen und Systemanforderungen in Abschnitt 31.1, „Checkliste für die Installation der Passwortverwaltungskomponenten“, auf Seite 281.

1. Melden Sie sich als `Root`-Benutzer oder Administrator bei dem Server an, auf dem SSPR installiert werden soll.
2. Stoppen des Tomcat-Servers.
3. (Bedingt) Wenn Ihnen die `ISO`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die SSPR-Installationsdateien befinden (standardmäßig im Verzeichnis `products/rbpm/sspr_install`).
4. (Bedingt) Wenn Sie die SSPR-Installationsdateien heruntergeladen haben, führen Sie die folgenden Schritte durch:
   - **4a** Navigieren Sie zur `.tgz`- oder `win.zip`-Datei für das heruntergeladene Image.
   - **4b** Extrahieren Sie den Inhalt der Datei in ein Verzeichnis auf dem lokalen Computer.
5. Führen Sie im Verzeichnis mit den Installationsdateien einen der folgenden Schritte aus:
   - **Linux (Benutzeroberfläche)** – Geben Sie Folgendes ein: `/sspr-install.bin`
   - **Windows**: Führen Sie `sspr-install.exe` aus
6. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Weiter**.

7 Legen Sie einen Pfad für die installierten Dateien fest.

8 Führen Sie die geführte Installation mit den folgenden Parametern aus:

- **Tomcat-Details**

  Gibt das Basisverzeichnis für den Tomcat-Server an. Beispiel: `/opt/netiq/idm/apps/tomcat`. Der Installationsvorgang legt einige weitere Dateien für SSPR in diesem Ordner ab.

- **Tomcat-Verbindung**

  Gibt die Einstellungen für die URL an, über die Benutzer eine Verbindung zu SSPR auf dem Tomcat-Server aufbauen. Beispiel: `https://meinserver.meinefirma.de:8080`.

  ---

  **HINWEIS:** Wenn Folgendes zutrifft, müssen Sie außerdem die Option **Mit externen Authentifizierungsserver verbinden** wählen und Werte für den externen Server angeben:

  - Sie installieren SSPR.
  - OSP wird auf einer anderen Instanz des unterstützten Anwendungsservers ausgeführt als SSPR.

  ---

  ***Protokoll***

  Gibt an, ob *http* oder *https* verwendet werden soll. Soll die Kommunikation per SSL (Secure Sockets Layer) erfolgen, wählen Sie `https`.

  ***Hostname***

  Gibt den DNS-Namen oder die IP-Adresse des Servers an, auf dem SSPR installiert werden soll. Verwenden Sie nicht `localhost`.

  ***Port***

  Gibt den Port an, über den der Server mit den Client-Computern kommunizieren soll.

  ***Mit externen Authentifizierungsserver verbinden***

  Gibt an, ob der Authentifizierungsserver (OSP) auf einer Tomcat-Instanz gehostet wird. Auf dem Authentifizierungsserver befindet sich eine Liste der Benutzer, die sich bei SSPR anmelden können.

  Wenn Sie diese Einstellung wählen, müssen Sie außerdem Werte für **Protokoll**, **Hostname** und **Port** für den Authentifizierungsserver angeben.

- **Tomcat-Java-Home**

  Gibt das Basisverzeichnis für Java auf dem Tomcat-Server an. Beispiel: `/opt/netiq/idm/jre`. Der Installationsvorgang legt einige weitere Dateien für OSP in diesem Verzeichnis ab.

- **Authentifizierungsdetails**

  Gibt die Anforderungen für das Herstellen einer Verbindung zum Authentifizierungsserver an, auf dem sich eine Liste der Benutzer befindet, die sich bei der Anwendung anmelden können. Weitere Informationen zum Authentifizierungsserver finden Sie in Abschnitt 4.5.1, „Erläuterungen zur Authentifizierung mit One SSO Provider (OSP)“, auf Seite 42.

  ***LDAP-Host***

  Gibt den DNS-Namen oder die IP-Adresse des LDAP-Authentifizierungsservers an. Verwenden Sie nicht `localhost`.

  ***LDAP-Port***

  Gibt den Port an, über den der LDAP-Authentifizierungsserver mit Identity Manager kommunizieren soll. Geben Sie beispielsweise `389` als nicht sicheren Port oder `636` für SSL-Verbindungen an.

***SSL verwenden***

Gibt an, ob die Kommunikation zwischen dem Identitätsdepot und dem Authentifizierungsserver über das SSL-Protokoll (Secure Sockets Layer) erfolgen soll.

***JRE-Truststore-Datei (cacerts-Datei)***

*Gilt nur dann, wenn SSL für die LDAP-Verbindung verwendet werden soll.*

Gibt den Pfad zum Zertifikat an. Beispiel: `C:\netiq\idm\apps\jre\lib\security\cacerts`.

***Passwort für JRE-Truststore***

*Gilt nur dann, wenn SSL für die LDAP-Verbindung verwendet werden soll.*

Gibt das Passwort für die `cacerts`-Datei an.

***Admin-DN***

*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.*

Gibt den DN eines Administratorkontos für den LDAP-Authentifizierungsserver an. Beispiel: `cn=admin,ou=sa,o=system`.

***Admin-Passwort***

*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.*

Gibt das Passwort des Administratorkontos für den LDAP-Authentifizierungsserver an.

***Benutzercontainer***

*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.*

Gibt den Container auf dem LDAP-Authentifizierungsserver an, in dem die Benutzerkonten gespeichert sind, die sich bei Access Review anmelden können. Beispiel: `o=data`.

***Admin-Container***

*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.*

Gibt den Container auf dem LDAP-Authentifizierungsserver an, in dem die Administratorkonten für Access Review gespeichert sind. Beispiel: `ou=sa,o=system`.

***Keystore-Passwort***

*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.*

Gibt das Passwort an, das für den neuen Keystore für den LDAP-Authentifizierungsserver erstellt werden soll.

Das Passwort muss mindestens sechs Zeichen umfassen.

- **SSPR-Details**

Gibt die erforderlichen Einstellungen für die Konfiguration von SSPR an.

**Konfigurationspasswort**

Gibt das Passwort an, mit dem ein Administrator die SSPR-Funktion konfigurieren soll.

Standardmäßig umfasst SSPR kein Konfigurationspasswort. Ohne Passwort kann jeder Benutzer, der sich bei SSPR anmeldet, auch die Konfigurationseinstellungen bearbeiten.

**SSPR-Umleitungs-URL**

Gibt die absolute URL an, zu der der Client weitergeleitet wird, wenn Vorgänge wie eine Änderung des Passworts oder der Challenge-Fragen in SSPR erfolgt sind. Beispielsweise Weiterleitung zum Dashboard.

Hierbei gilt das folgende Format: `Protokoll://Server:Port/Pfad`. Beispiel: `http://idm_userapp_server_ip:port_no/idmdash/#/landing`.

- **Authentifizierungsserver – Details**

  Gibt das Passwort an, mit dem der SSPR-Dienst eine Verbindung zum OSP-Client auf dem Server herstellen soll. Dies wird auch als Client-Geheimnis bezeichnet.

  Mit dem RBPM-Konfigurationsprogramm können Sie dieses Passwort nach der Installation bearbeiten.

- **Auditing-Details (SSPR)**

  Gibt die Einstellungen für die Revision von SSPR-Ereignissen an, die auf dem Authentifizierungsserver auftreten.

  ***Auditing für SSPR aktivieren***

  Gibt an, ob die SSPR-Ereignisse an einen Revisionsserver gesendet werden sollen.

  Wenn Sie diese Einstellung wählen, legen Sie außerdem die Einstellungen für den Syslog-Server fest.

  ***Syslog-Hostname***

  *Gilt nur dann, wenn Sie die Revision für SSPR aktivieren.*

  Gibt den DNS-Namen oder die IP-Adresse des Servers an, auf dem der Syslog-Server gehostet wird. Verwenden Sie nicht `localhost`.

  ***Syslog-Port***

  *Gilt nur dann, wenn Sie die Revision für SSPR aktivieren.*

  Gibt den Port des Servers an, auf dem der Syslog-Server gehostet wird.

9 Zum Konfigurieren der Identitätsanwendungen und der Identitätsberichterstellung für SSPR fahren Sie mit Teil XII, „Installieren der Identitätsanwendungen“, auf Seite 295 fort.

10 Aktualisieren Sie die SSO-Client-Parameter im Konfigurationsaktualisierungs-Dienstprogramm. Weitere Informationen hierzu finden Sie unter, Abschnitt 40.4.8, „Zurücksetzen von Passwörtern per Selbstbedienung“, auf Seite 389.

Weitere Informationen zum Konfigurieren der „Passwort vergessen“-Verwaltung finden Sie in Abschnitt 39.6, „Konfigurieren der „Passwort vergessen“-Verwaltung“, auf Seite 359.

## 32.2 Automatische Installation von SSPR (Self Service Password Reset)

Bei der automatischen (nicht interaktiven) Installation wird keine Benutzeroberfläche angezeigt, und der Benutzer muss keinerlei Fragen beantworten.

1 Melden Sie sich als `Root` oder Administrator an dem Computer an, auf dem die Komponenten installiert werden sollen.

2 Halten Sie Tomcat an.

3 (Bedingt) Wenn Ihnen die `ISO`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die SSPR-Installationsdateien befinden (standardmäßig im Verzeichnis `sspr`).

4 (Bedingt) Wenn Sie die Installationsdateien von der NetIQ Downloads-Website heruntergeladen haben, führen Sie die folgenden Schritte aus:

  **4a** Navigieren Sie zur `.tgz`- oder `.zip`-Datei für das heruntergeladene Image.

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

5 Bearbeiten Sie die Datei `silent.properties` für die SSPR-Installation (standardmäßig in demselben Verzeichnis wie die Installationsskripte).

Weitere Informationen zu den Einstellungen für die Installation finden Sie in Schritt 7 auf Seite 286 und Schritt 8 auf Seite 286.

6 Starten Sie die automatische Installation mit einem der folgenden Befehle:

- **Linux**: `sspr-install-linux.bin -i silent -f Pfad_zur_silent.properties-Datei`
- **Windows**: `sspr-install-win.exe -i silent -f Pfad_zur_silent.properties-Datei`

7 Aktualisieren Sie die SSO-Client-Parameter im Konfigurationsaktualisierungs-Dienstprogramm. Weitere Informationen hierzu finden Sie unter, Abschnitt 40.4.8, „Zurücksetzen von Passwörtern per Selbstbedienung“, auf Seite 389.

## 32.3 Aufgaben nach Abschluss der Installation

Nach der Installation von SSPR können Sie die Konfigurationseinstellungen bearbeiten, z. B. die Administratorberechtigung des LDAP-Gruppen-DN für das Standardprofil ändern oder eine andere Umleitungs-URL angeben. NetIQ empfiehlt außerdem, die im Installationsvorgang erstellten URLs zu überprüfen und bei Bedarf zu ändern.

Stellen Sie vor der Konfiguration der SSPR-Einstellungen sicher, dass SSPR ohne Fehler installiert wurde.

1 Melden Sie sich über die folgende URL als Administrator beim SSPR-Portal an:

`protocol://server:port/web-context`

Beispiel:

`https://192.168.0.1:8543/sspr`

2 Klicken Sie oben rechts auf der Seite im Dropdown-Menü auf **Konfigurations-Editor** und wählen Sie **Module > Authentifiziert > Administration**.

3 Wählen Sie **Standardeinstellungen > Standardeinstellungen für LDAP-Anbieter > NetIQ IDM-/OAuth-Integration**.

4 Wählen Sie **LDAP > LDAP-Verzeichnisse > Standard > Verbindung > LDAP-Zertifikate**, klicken Sie auf **Von Server importieren** und prüfen Sie, ob die LDAP-Zertifikate fehlerfrei importiert wurden.

Testen Sie hierzu das LDAP-Profil und stellen Sie fest, ob alle konfigurierten Server erreichbar sind.

5 Wählen Sie **Module > Authentifiziert > Administration** und prüfen Sie, ob die Administratorberechtigung dem LDAP-Gruppen-DN für das Standardprofil zugewiesen wurde.

6 Wählen Sie **Module > Einstellungen > Anwendung > Anwendung** und legen Sie die Umleitungs-URL `https://<Server:Port>/idmdash/#/landing` fest, falls noch keine URL angegeben ist.

Beispiel: `https:/192.168.0.1:8543/idmdash/#/landing`.

7 Wählen Sie **Module > Einstellungen > Benutzeroberfläche > Darstellung** und legen Sie unter **Benutzeroberflächenthema** die Option **Micro Focus** fest, falls diese Option noch nicht angegeben ist.

8 Wählen Sie **Einstellungen > Single Sign On (SSO)-Client > OAuth** und prüfen Sie, ob die Werte für die folgenden Parameter fehlerfrei angegeben sind:

**OAuth-Anmelde-URL**

Gibt die URL für die Anmeldung beim OAuth-Server an. Bei der Anmeldung wird der Benutzer über diese URL an die Authentifizierung mit OSP weitergeleitet.

Beispiel: `https://192.168.0.1:8543/osp/a/idm/auth/oauth2/grant`

**OAuth-Profildienst-URL**

Gibt die URL für den Webdienst an, über den Identity Manager die Attributdaten vom Benutzer zurückgibt.

Beispiel: `https://192.168.0.1:8543/osp/a/idm/auth/oauth2/getattributes`

**OAuth-Codeauflösungsdienst-URL**

Gibt die URL für den OAuth-Codeauflösungsdienst an. Über diese Webdienst-URL löst SSPR das Artefakt auf, das der OAuth-Identitätsserver zurückgibt.

Beispiel: `https://192.168.0.1:8543/osp/a/idm/auth/oauth2/authcoderesolve`

**OAUTH-Webdienstserver-Zertifikat**

Importiert das Zertifikat für den OAuth-Webdienstserver.

**OAuth-Client-ID**

Gibt die Client-ID des OAuth-Clients an.

**Gemeinsames OAuth-Geheimnis**

Gibt ein Passwort für das gemeinsame OAuth-Geheimnis an. Dieses Passwort wird von OSP- und SSPR-Anwendungen gemeinsam genutzt.

**OAuth-Benutzername/DN-Anmeldeattribut**

Gibt das Attribut des Benutzers an, mit dem SSPR eine Aufforderung an den OAuth-Server sendet, die Authentifizierung der Benutzer lokal vorzunehmen.

9 Zum Speichern der Konfiguration klicken Sie auf **Änderungen speichern**.

# 32.4 Fehlersuche für SSPR

SSPR meldet einen Fehler, wenn die Einstellungen nicht ordnungsgemäß definiert sind. Sie müssen die Einstellungen nach dem Konfigurieren überprüfen. In diesem Abschnitt erfahren Sie, wie Sie häufige Fehler nach der Installation und Konfiguration von SSPR beheben.

- Abschnitt 32.4.1, „Universelles Passwort ist nicht dem Container zugewiesen, in dem sich der Benutzer befindet“, auf Seite 290
- Abschnitt 32.4.2, „Benutzer haben keinen Schreibzugriff auf pwmResponseSet-Attribute“, auf Seite 291
- Abschnitt 32.4.3, „Einschränken der Konfiguration verursacht einen Fehler“, auf Seite 291

## 32.4.1 Universelles Passwort ist nicht dem Container zugewiesen, in dem sich der Benutzer befindet

So weisen Sie die Richtlinie „Universelles Passwort“ einem Benutzercontainer zu:

1 Melden Sie sich bei iManager an.

2 Wählen Sie **Rollen und Aufgaben > Passwortrichtlinien** und wählen Sie die Passwortrichtlinie aus.

3 So wählen Sie einen Benutzer mit Verwaltungsrechten aus:

**3a** Klicken Sie auf **Universelles Passwort > Konfigurationsoptionen > Abruf des universellen Passworts**.

**3b** Wählen Sie **Abrufen der Passwörter durch Administrator zulassen** oder **Abrufen der Passwörter durch Folgende zulassen** und klicken Sie auf **OK**.

Beispiel: `cn=uaadmin,ou=sa,o=data`

4 Klicken Sie auf **Richtlinienzuweisung** und weisen Sie `Container` dem Container zu, in dem sich der Benutzer befindet.

Beispiel: `o=data` oder verwaltungsbefugte Benutzer.

### 32.4.2 Benutzer haben keinen Schreibzugriff auf pwmResponseSet-Attribute

So bearbeiten Sie die Rechte für einen Benutzer:

1 Melden Sie sich bei iManager an.

2 Wählen Sie **Objekte anzeigen > Trustees für Objekt bearbeiten**.

3 Klicken Sie auf den Link **Zugewiesene Rechte**, klicken Sie auf **Eigenschaft hinzufügen** und aktivieren Sie die Option **Alle Eigenschaften in Schema anzeigen**.

4 Wählen Sie die Eigenschaft **pwmResponseSet** und klicken Sie auf **OK**.

5 Aktivieren Sie die erforderlichen Rechte für die in Schritt 4 ausgewählte Eigenschaft.

6 Klicken Sie auf **Fertig**.

### 32.4.3 Einschränken der Konfiguration verursacht einen Fehler

Zur Behebung dieses Fehlers starten Sie den Tomcat-Server mit dem folgenden Befehl neu:

```
/etc/init.d/idmapps_tomcat_init restart
```

## 32.5 Konfigurieren von OSP und SSPR für Clustering

Identity Manager unterstützt die SSPR-Konfiguration in einer Tomcat-Clusterumgebung.

### 32.5.1 Konfigurieren von SSPR zur Unterstützung von Clustering

Führen Sie die folgenden Schritte durch, um SSPR zu konfigurieren, das bereits auf einem separaten Computer vorhanden ist:

1 Die Voraussetzungen und Systemanforderungen finden Sie in Abschnitt 31.1, „Checkliste für die Installation der Passwortverwaltungskomponenten“, auf Seite 281.

2 Befolgen Sie die Anweisungen in Abschnitt 32.1, „Installation von SSPR (Self-Service Passwort Request) mit dem Assistenten“, auf Seite 285 und berücksichtigen Sie die folgenden Schritte während des Installationsvorgangs.

a. Wählen Sie auf der Seite „Anwendungsserver-Verbindung“ die Option **Connect to external authentication server** (Mit externem Authentifizierungsserver verbinden) und geben Sie den DNS-Namen des Servers an, auf dem das Lastausgleichprogramm installiert ist.

b. Geben Sie auf der Seite „Authentifizierungsdetails“ die IP-Adresse und den Port des Identity Manager-Engine-Servers an. Das Passwort für die Zertifikate der Zertifizierungsstelle lautet „changeit“.

c. Aktualisieren Sie nach der SSPR-Installation die SSL-Einstellungen. Weitere Informationen finden Sie unter Abschnitt 52.3, „Aktualisieren der SSL-Einstellungen für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung“, auf Seite 469.

3 Starten Sie zur Aktualisierung der SSPR-Informationen im ersten Knoten des Clusters das Konfigurationsprogramm unter `/opt/netiq/idm/apps/UserApplication/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.

## 32.5.2 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 39.6, „Konfigurieren der „Passwort vergessen“-Verwaltung“, auf Seite 359.

2 Weitere Informationen zum Link „Passwort ändern“ finden Sie in Abschnitt 39.6.4, „Aktualisieren der SSPR-Links im Dashboard für eine dezentrale Umgebung oder eine Cluster-Umgebung“, auf Seite 364.

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/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.

---

5 (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
```

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. Weitere Informationen hierzu finden Sie unter, Schritt 10 auf Seite 349.

11 Aktivieren Sie den Berechtigungsindex für das Clustering. Weitere Informationen hierzu finden Sie unter, Abschnitt 36.2, „Aktivieren des Berechtigungsindex für das Clustering“, auf Seite 320.

12 Aktivieren Sie den Tomcat-Cluster. Weitere Informationen hierzu finden Sie unter, Schritt 9 auf Seite 321.

13 Starten Sie Tomcat in allen Knoten neu.

14 Konfigurieren Sie den Benutzeranwendungstreiber für das Clustering. Weitere Informationen hierzu finden Sie unter, Abschnitt 38.2, „Konfigurieren des Benutzeranwendungstreibers für das Clustering“, auf Seite 352.

# XII Installieren der Identitätsanwendungen

In diesem Abschnitt finden Sie die Schritte für die Installation der erforderlichen Komponenten und des Rahmenwerks für die Identitätsanwendungen:

- Katalogadministrator
- Dashboard für Identitätsanwendungen
- Rollen- und Ressourcenservice-Treiber
- Benutzeranwendung
- Benutzeranwendungstreiber

Standardmäßig installiert das Installationsprogramm diese Komponenten in den folgenden Speicherorten:

- **Linux:** `/opt/netiq/idm`
- **Windows:** `C:\netiq\idm\apps`

Die Identitätsanwendungen müssen während und nach der Installation auf andere Identity Manager-Komponenten zugreifen. NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie in Kapitel 33, „Planen der Installation der Identitätsanwendungen“, auf Seite 297.

# 33 Planen der Installation der Identitätsanwendungen

Die Installation der Identitätsanwendungen enthält die folgenden Komponenten:

- Katalogadministrator
- Startseite und Bereitstellungs-Dashboard

  **HINWEIS:** Identity Manager 4.6 enthält zwar die Funktion „Startseite und Bereitstellungs-Dashboard", doch diese Funktion ist inzwischen veraltet. Wenn sich Benutzer bei den Identitätsanwendungen anmelden, werden sie auf das Identitätsanwendungen-Dashboard umgeleitet statt auf die Startseite.

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

Die Installation umfasst nicht die beiden erforderlichen Treiber für die Identitätsanwendungen (Benutzeranwendungstreiber und Ressourcenservice-Treiber). Diese Treiber werden zusammen mit der Identity Manager-Engine installiert. Weitere Informationen finden Sie in Kapitel 16, „Vorbereiten der Installation der Engine, der Treiber und der Plugins“, auf Seite 147.

**HINWEIS:** Technisch gesehen zählt die Identitätsberichterstellung zu den Identitätsanwendungen, da in dieser Komponente ebenfalls SSPR und OSP verwendet wird und Sie die Einstellungen mit dem RBPM-Konfigurationsprogramm bearbeiten. Für die Identitätsberichterstellung steht allerdings ein eigenes Installationsprogramm bereit, sie kann auf einem anderen Server installiert werden, und sie nutzt eine andere Datenbank. Weitere Informationen finden Sie in Abschnitt 41.4, „Systemanforderungen für die Identitätsberichterstellung“, auf Seite 397.

# 33.1 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 37. |
| ❑ | 2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.3.4, „Empfohlene Servereinrichtung“, auf Seite 53. |
| ❑ | 3. Legen Sie fest, ob ein Sentinel vor der Installation der Identitätsanwendungen installiert werden soll. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |
| ❑ | 4. Das Identitätsdepot muss das SecretStore-Modul enthalten. Weitere Informationen finden Sie in Abschnitt 12.1.2, „Hinzufügen von SecretStore zum Identitätsdepotschema“, auf Seite 123. |
| ❑ | 5. Stellen Sie sicher, dass die Identity Manager-Engine installiert ist. Weitere Informationen zum Installieren der Engine finden Sie in Kapitel 16, „Vorbereiten der Installation der Engine, der Treiber und der Plugins“, auf Seite 147. |
| ❑ | 6. 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 33.3, „Voraussetzungen und Überlegungen für die Installation der Identitätsanwendungen“, auf Seite 300. |
| ❑ | 7. (Bedingt) Zur geführten Installation auf Computern mit dem Betriebssystem SLES 12 SP1 (oder höher) müssen die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in Abschnitt 6.3, „Installieren von Identity Manager auf Servern mit SLES 12 SP1 (oder höher)“, auf Seite 63. |
| ❑ | 8. (Bedingt) Stellen Sie bei Computern mit RHEL 6.x- oder Rhel 7.x-Betriebssystem sicher, dass die erforderlichen Bibliotheken installiert sind. Weitere Informationen finden Sie in Abschnitt 6.4, „Installieren von Identity Manager auf einem RHEL 6.*x- oder 7.x-Server“, auf Seite 63*. |
| ❑ | 9. 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 33.4, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 307. |
| ❑ | 10. Stellen Sie sicher, dass eDirectory an den standardmäßigen LDAP-Ports 389 und 636 ausgeführt wird, damit Sie keine Fehlermeldung über ein ungültiges Schema erhalten. Sie können das eDirectory-Schema nach der Installation manuell erweitern. Weitere Informationen finden Sie in Abschnitt 34.1, „Hinzufügen des Benutzeranwendungsschemas als Protokollanwendung zum Audit Server“, auf Seite 311. |
| ❑ | 11. Erstellen Sie ein Benutzeranwendungsadministrator-Konto im eDirectory-Identitätsdepot. Weitere Informationen finden Sie in Abschnitt 34.2, „Erstellen eines Benutzeranwendungsadministrator-Kontos“, auf Seite 312. |

| | Checkliste |
|---|---|
| ❑ | 12. Installieren und konfigurieren Sie eine Datenbank für die Identitätsanwendungen auf dem lokalen Computer oder auf einem verbundenen Server.<br>◆ Weitere Informationen zur Datenbank finden Sie in Abschnitt 33.3.5, „Voraussetzungen für die Installation der Datenbank für die Identitätsanwendungen“, auf Seite 305.<br>◆ Anweisungen zum Installieren der Datenbank finden Sie in Kapitel 35, „Konfigurieren der Datenbank für die Identitätsanwendungen“, auf Seite 315. |
| ❑ | 13. Bereiten Sie einen Anwendungsserver auf dem lokalen Computer oder in einem Cluster vor.<br>◆ Erläuterungen zu den Anforderungen finden Sie in Abschnitt 33.3.3, „Voraussetzungen und Überlegungen für den Anwendungsserver“, auf Seite 304.<br>◆ Anweisungen zum Vorbereiten des Clusters finden Sie in Kapitel 36, „Vorbereiten der Umgebung auf die Identitätsanwendungen“, auf Seite 319.<br>◆ Anweisungen zum Installieren eines Anwendungsservers finden Sie in Abschnitt 36.3, „Vorbereiten des Anwendungsservers auf die Identitätsanwendungen“, auf Seite 320. |
| ❑ | 14. (Bedingt) Sollen die Ereignisse mit dem Apache Log4j-Dienst in Tomcat festgehalten werden, stellen Sie sicher, dass die entsprechenden Dateien vorliegen. Weitere Informationen finden Sie in Abschnitt 29.4, „Protokollieren der Anmeldung mit dem Apache-Log4j-Dienst“, auf Seite 271. |
| ❑ | 15. Ermitteln Sie anhand des Inhalts des Installations-Kits für die Identitätsanwendungen, welche Dateien für Ihre Umgebung erforderlich sind. Weitere Informationen finden Sie in Abschnitt 33.2, „Erläuterungen zu den Installationsdateien für die Identitätsanwendungen“, auf Seite 300. |
| ❑ | 16. Erstellen Sie den Benutzeranwendungstreiber sowie den Rollen- und den Ressourcenservice-Treiber, und stellen Sie diese Treiber bereit. Weitere Informationen finden Sie in Kapitel 38, „Erstellen und Bereitstellen der Treiber für die Identitätsanwendungen“, auf Seite 351. |
| ❑ | 17. Installieren Sie die Identitätsanwendungen. Weitere Informationen finden Sie in Kapitel 37, „Installieren der Identitätsanwendungen“, auf Seite 325. |
| ❑ | 18. Führen Sie die abschließenden Aufgaben im Installationsvorgang gemäß den Anweisungen in Kapitel 39, „Abschließen der Installation der Identitätsanwendungen“, auf Seite 355 aus. |
| ❑ | 19. Stellen Sie sicher, dass die Identitätsanwendungen und die Single-Sign-On-Einstellungen fehlerfrei konfiguriert sind. Weitere Informationen finden Sie in Kapitel 51, „Überprüfen des Single-Sign-On-Zugriffs auf die Identitätsanwendungen“, auf Seite 465. |
| ❑ | 20. (Optional) Weitere Informationen zum Aufnehmen der Arbeit mit den Identitätsanwendungen finden Sie im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*. |

## 33.2 Erläuterungen zu den Installationsdateien für die Identitätsanwendungen

Die Installationsdateien für die Identitätsanwendungen befinden sich im Verzeichnis `/products/RBPM/user_app_install` im Installationspaket.

| Datei | Beschreibung |
|---|---|
| `configupdate.properties` | Wenn Sie die automatische Installation planen, konfigurieren Sie mit dieser Datei das rollenbasierte Bereitstellungsmodul. Weitere Informationen finden Sie in Abschnitt 37.3, „Automatische Installation der Identitätsanwendungen“, auf Seite 333. |
| `IdmUserApp.exe` oder `IdmUserApp.bin` | Das Installationsprogramm für die Identitätsanwendungen. Für jede Plattform steht ein eigenes Installationsprogramm bereit. |
| `user_app.configure.properties` | Wenn Sie die automatische Installation planen, konfigurieren Sie mit dieser Datei die Identitätsanwendungen. Weitere Informationen finden Sie in Abschnitt 37.3, „Automatische Installation der Identitätsanwendungen“, auf Seite 333. |
| `user_app.install.properties` | Wenn Sie die automatische Installation planen, installieren Sie mit dieser Datei die Identitätsanwendungen. Weitere Informationen finden Sie in Abschnitt 37.3, „Automatische Installation der Identitätsanwendungen“, auf Seite 333. |

Das Installationsprogramm führt die folgenden Schritte aus:

- Festlegung einer vorhandenen Version eines zu verwendenden Anwendungsservers.
- Festlegung einer vorhandenen Version einer zu verwendenden Datenbank. In der Datenbank werden Identitätsanwendungsdaten und Konfigurationsinformationen gespeichert.
- Konfigurieren der JDK-Zertifikatsdatei, sodass die Benutzeranwendung (die auf Tomcat ausgeführt wird) sicher mit dem Identitätsdepot und dem Benutzeranwendungstreiber kommunizieren kann.
- Konfigurieren und Bereitstellen der Java-WAR-Datei (Web Application Archive) für die Benutzeranwendung auf Tomcat
- Bereitstellen einer Möglichkeit zum Protokollieren über Sentinel- oder OpenXDAS-Audit-Clients.
- Bereitstellen einer Möglichkeit zum Importieren eines vorhandenen Master-Schlüssels zur Wiederherstellung einer bestimmten Installation der Identitätsanwendungen und zur Unterstützung von Clustern.

## 33.3 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*.


- Abschnitt 33.3.1, „Überlegungen zur Installation der Identitätsanwendungen“, auf Seite 301
- Abschnitt 33.3.2, „Überlegungen zur Konfiguration und Nutzung der Identitätsanwendungen“, auf Seite 303

- Abschnitt 33.3.3, „Voraussetzungen und Überlegungen für den Anwendungsserver“, auf Seite 304
- Abschnitt 33.3.4, „Voraussetzungen für die Installation der Identitätsanwendungen in einer Cluster-Umgebung“, auf Seite 305
- Abschnitt 33.3.5, „Voraussetzungen für die Installation der Datenbank für die Identitätsanwendungen“, auf Seite 305

## 33.3.1 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:
  - Designer
  - Identitätsdepot
  - Identity Manager-Engine
  - Remote Loader
  - One SSO Provider (OSP)

  Weitere Informationen zu den erforderlichen Versionen und Patches für diese Komponenten finden Sie in den aktuellen Versionshinweisen.
- Das Identitätsdepot muss das SecretStore-Modul enthalten und das Modul muss konfiguriert sein. Weitere Informationen finden Sie unter Abschnitt 12.1.2, „Hinzufügen von SecretStore zum Identitätsdepotschema“, auf Seite 123.
- Das Identitätsdepot muss die erstellte und bereitgestellte Benutzeranwendung und die Rollen und Ressourcen-Service-Treiber enthalten. Weitere Informationen finden Sie unter Kapitel 38, „Erstellen und Bereitstellen der Treiber für die Identitätsanwendungen“, auf Seite 351.
- Installieren Sie die folgenden Bestandteile des Rahmenwerks, bevor Sie die Identitätsanwendungen installieren:
  - Ein Anwendungsserver auf dem lokalen Computer. Weitere Informationen finden Sie in Abschnitt 33.3.3, „Voraussetzungen und Überlegungen für den Anwendungsserver“, auf Seite 304.
  - Eine Datenbank auf dem lokalen Computer oder auf einem verbundenen Server. Weitere Informationen finden Sie in Abschnitt 33.3.5, „Voraussetzungen für die Installation der Datenbank für die Identitätsanwendungen“, auf Seite 305.
- (Bedingt) Wenn Sie die Identitätsanwendungen auf Plattformen mit SUSE Linux Enterprise Server (SLES) installieren, verwenden Sie nicht das mit SLES mitgelieferte IBM-JDK. Diese Version ist mit einigen Aspekten der Installation für die Benutzeranwendung nicht kompatibel. Laden Sie stattdessen das Oracle-JDK herunter.
- (Bedingt) Zur geführten Installation auf einem Server mit SLES 12 SP1 (oder höher) müssen die Bibliotheken `libXtst6-32bit-1.2.1-4.4.1.x86_64`, `libXrender-32bit` und `libXi6-32bit` auf dem Server installiert sein.
- (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*.

- Erstellen Sie den Benutzeranwendungstreiber, bevor Sie den Rollen- und Ressourcenservice-Treiber erstellen. Der Rollen- und Ressourcenservice-Treiber referenziert den Rollendepotcontainer (`RoleConfig.AppConfig`) im Benutzeranwendungstreiber.
- Der Rollen- und Ressourcenservice-Treiber kann nicht zusammen mit dem Remote Loader genutzt werden, da der Treiber jClient verwendet.
- Setzen Sie die Umgebungsvariable `JAVA_HOME` so, dass sie auf das JDK verweist, das mit den Identitätsanwendungen verwendet werden soll. Sie können `JAVA_HOME` außer Kraft setzen; geben Sie hierzu den Pfad manuell während der Installation ein.
- Der Installationsvorgang legt die Programmdateien standardmäßig im Verzeichnis `C:\NetIQ\IDM` oder `/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.
  - In Linux-Umgebungen können Nicht-`Root`-Benutzer in das Verzeichnis schreiben.
- Jede Benutzeranwendungsinstanz kann nur jeweils einen einzigen Benutzercontainer 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.
- (Bedingt) Wenn Sie planen, mit der externen Passwortverwaltung zu arbeiten, muss Ihre Umgebung den folgenden Voraussetzungen entsprechen:
  - Aktivieren Sie das SSL-Protokoll (Secure Sockets Layer) für Tomcat, auf dem die Identitätsanwendungen und die Datei `IDMPwdMgt.war` bereitgestellt werden sollen.
  - Stellen Sie sicher, dass der SSL-Port in Ihrer Firewall offen ist.

  Weitere Informationen zum Aktivieren von SSL für Tomcat finden Sie in Abschnitt 52.4, „Aktualisieren der SSL-Einstellungen für den Anwendungsserver“, auf Seite 469.

  Weitere Informationen zur Datei `IDMPwdMgt.war` finden Sie in Abschnitt 39.6, „Konfigurieren der „Passwort vergessen“-Verwaltung“, auf Seite 359.
- Wenden Sie zur Unterstützung der LDAP-Suche mit Virtual List View(VLV)- und Server Side Sort(SSS)-Steuerelementen Hotfix 2 unter eDirectory 9.0.2 oder eDirectory 8.8.8 Patch 9 an. Weitere Informationen finden Sie unter Kapitel 11, „Anwenden von HotFix 2 auf das Identitätsdepot“, auf Seite 115.

  Wenn Sie eDirectory mit dem integrierten Installationsprogramm installiert haben, ist dieser Hotfix nicht erforderlich. Das integrierte Installationsprogramm installiert eine aktualisierte Version von eDirectory, auf die dieser Hotfix bereits angewendet wurde.
- (Optional) Sollen Autorisierungen von verwalteten Systemen abgerufen werden, installieren Sie mindestens einen Identity Manager-Treiber.
  - Sie müssen Treiber verwenden, die von Identity Manager 3.6.1, 4.0 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. Weitere Informationen finden Sie in Abschnitt 22.3, „Erläuterungen zur Installation der iManager Plugins“, auf Seite 219.

## 33.3.2 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 Abschnitt 40.2.9, „Sonstige“, auf Seite 377.
  - Aktivieren Sie Cookies in allen Browsern. Die Anwendungen sind nicht funktionsfähig, wenn Cookies deaktiviert sind.
- Sobald Sie SSO in Ihrer Identity Manager-Umgebung aktivieren, können die Benutzer nicht mehr als Gast oder als anonymer Benutzer auf die Identitätsanwendungen zugreifen. Stattdessen werden die Benutzer aufgefordert, sich an der Benutzeroberfläche anzumelden. Weitere Informationen finden Sie in Teil XV, „Konfiguration des Single-Sign-On-Zugriffs in Identity Manager“, auf Seite 443.
- Konfigurieren Sie das Identitätsdepot so, dass bei der ersten Anmeldung eines Benutzers die NMAS-Anmeldung verwendet wird. So ist sichergestellt, dass die Universalpasswort-Funktion in Identity Manager erzwungen wird.
  - **Linux:** Fügen Sie die folgenden Befehle an das Ende des Skripts `/opt/novell/eDirectory/sbin/pre_ndsd_start` an:

    ```
    NDSD_TRY_NMASLOGIN_FIRST=true
    export NDSD_TRY_NMASLOGIN_FIRST
    ```

  - **Windows:** Fügen Sie `NDSD_TRY_NMASLOGIN_FIRST` mit dem Zeichenkettenwert `true` an den Registrierungsschlüssel HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Environment an.
- (Bedingt) Um Berichte ausführen zu können, müssen die Komponenten für die Identitätsberichterstellung in Ihrer Umgebung installiert sein. Weitere Informationen finden Sie im *Verwaltungshandbuch für die NetIQ-Identitätsberichterstellung*.
- 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. Weitere Informationen finden Sie in
- (Optional) Sie können die Identitätsanwendungen für die Verwendung von NetIQ Access Manager über die SAML -Authentifizierung konfigurieren. Weitere Informationen finden Sie unter Kapitel 49, „Single Sign-On per SAML-Authentifizierung mit NetIQ Access Manager“, auf Seite 451.

### 33.3.3 Voraussetzungen und Überlegungen für den Anwendungsserver

Für die Identitätsanwendungen muss Tomcat installiert sein, wobei die folgenden Überlegungen zu beachten sind:

- Auf Tomcat muss das Java Development Kit (JDK) oder die Java Runtime Environment (JRE) ausgeführt werden. Weitere Informationen zu den unterstützten Versionen finden Sie in Abschnitt 33.4, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 307.
- Stellen Sie die Umgebungsvariable `JAVA_HOME` so ein, dass sie auf das JDK verweist, das mit der Benutzeranwendung verwendet werden soll. Sie können `JAVA_HOME` außer Kraft setzen; geben Sie hierzu den Pfad manuell während der Installation ein.
- (Bedingt) Bei Bedarf können Sie Ihr eigenes Tomcat-Installationsprogramm anstelle des Programms im Installations-Kit von Identity Manager verwenden. Wenn Sie allerdings den Apache Log4j-Dienst zusammen mit Ihrer Tomcat-Version nutzen möchten, überprüfen Sie, ob die entsprechenden Dateien installiert sind. Weitere Informationen finden Sie in Abschnitt 29.4, „Protokollieren der Anmeldung mit dem Apache-Log4j-Dienst“, auf Seite 271.
- (Bedingt) Sollen digital signierte Dokumente beibehalten werden, müssen Sie die Identitätsanwendungen auf einem Tomcat-Anwendungsserver installieren und Novell Identity Audit verwenden. Dokumente mit Digitalsignatur werden nicht mit Workflow-Daten in der Benutzeranwendungsdatenbank gespeichert, sondern in der Protokollierungsdatenbank. Außerdem muss die Protokollierung aktiviert sein, damit diese Dokumente aufbewahrt werden. Weitere Informationen finden Sie unter Einrichten der Protokollierung in den Identitätsanwendungen im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.
- (Bedingt) In Umgebungen, in denen umfangreiche Benutzerdaten protokolliert werden oder der Verzeichnisserver zahlreiche Objekte enthält, sollten Sie mehrere Anwendungsserver für eine Bereitstellung der Identitätsanwendungen nutzen. Weitere Informationen zum Konfigurieren mit Blick auf die optimale Leistung finden Sie unter Anpassen der Leistung der Anwendungen im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.
- (Bedingt) Wenn Sie einen Tomcat-Anwendungsserver verwenden, starten Sie den Server erst dann, wenn die Installation abgeschlossen ist.
- (Bedingt) Wenn Sie planen, mit der externen Passwortverwaltung zu arbeiten, aktivieren Sie das SSL-Protokoll (Secure Sockets Layer) wie folgt:
  - Aktivieren Sie SSL für Tomcat, auf dem die Identitätsanwendungen und die Datei `IDMPwdMgt.war` bereitgestellt werden sollen.
  - Stellen Sie sicher, dass der SSL-Port in Ihrer Firewall offen ist.

  Weitere Informationen zur `Datei IDMPwdMgt.war` finden Sie unter Konfigurieren der „Passwort vergessen“-Verwaltung und im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.
- Die Einträge `JAVA_HOME` und `JRE_HOME` auf einem Tomcat-Server werden im Installationsvorgang nicht verändert. Standardmäßig legt das Schnellinstallationsprogramm für Tomcat die Datei `setenv.sh` im Verzeichnis `/opt/netiq/idm/apps/tomcat/bin/` ab. Die Installation konfiguriert außerdem den JRE-Speicherort in der Datei.

### 33.3.4 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 Portnummer 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.

Weitere Informationen zum Konfigurieren der Identitätsanwendungen einer Cluster-Umgebung finden Sie auch in Kapitel 36, „Vorbereiten der Umgebung auf die Identitätsanwendungen“, auf Seite 319.

### 33.3.5 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 Abschnitt 35.3.1, „Konfigurieren des Zeichensatzes“, auf Seite 317 oder Abschnitt 35.1, „Konfigurieren einer Oracle-Datenbank“, auf Seite 315.
- 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.

# 33.4 Systemanforderungen für die Identitätsanforderungen

In diesem Abschnitt finden Sie die Mindestanforderungen für die Server, auf denen die Identitätsanwendungen installiert werden sollen. Diese Anforderungen gelten auch für die Installation von PostgreSQL, Tomcat, OSP und SSPR.

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

| Kategorie | Anforderung |
|---|---|
| Prozessor | 1 GHz |
| Festplattenspeicher | 1 GB<br><br>**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:<br><br>◆ Open Enterprise Server 2015 SP1<br>◆ Open Enterprise Server 11 SP2<br>◆ Red Hat Enterprise Linux 7.3<br>◆ Red Hat Enterprise Linux 7.2<br>◆ Red Hat Enterprise Linux 7.1<br>◆ Red Hat Enterprise Linux 7.0<br>◆ Red Hat Enterprise Linux 6.8<br>◆ SUSE Linux Enterprise Server 12 SP1<br>◆ SUSE Linux Enterprise Server 11 SP4<br>◆ Windows Server 2012 R2<br>◆ Windows Server 2012<br><br>Eines der folgenden 32-Bit-Betriebssysteme:<br><br>◆ Open Enterprise Server 11 SP2<br><br>NetIQ empfiehlt, vor der Installation von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden.<br><br>**HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird. |
| Betriebssystem (unterstützt) | Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme<br><br>**HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert. |

| Kategorie | Anforderung |
|---|---|
| Virtualisierungssystem | ◆ Hyper-V Server 2012 R2<br>◆ VMWare ESX 5.5 und höher<br>◆ Windows Server 2012 R2-Virtualisierung mit Hyper-V (unterstützt)<br>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 | ◆ Microsoft SQL Server 2014 mit JDBC 3.0 3.0.1119.0<br>◆ Oracle 12c mit JDBC 1 2.1.0.1.0<br>◆ PostgreSQL 9.4.10 mit JDBC 4.2 (nur SLES 11 SP4)<br>◆ PostgreSQL 9.6.1 mit JDBC 4.2 (andere unterstützte Plattformen)<br>**HINWEIS:** Tragen Sie keine PostgreSQL-Versionen (z. B. 8.x oder 9.3.x) 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.x |
| Java | Java Development Kit (JDK)<br>Alternativ:<br>Java-Laufzeitumgebung (JRE) Version 1.8.0_112 (oder höher) von Sun (Oracle) |
| Anschluss | 8180 |
| Webbrowser | Einer der folgenden Browser (ggf. höhere Version):<br>◆ Apple Safari 9<br>◆ Google Chrome 51<br>◆ Microsoft Edge<br>◆ Microsoft Internet Explorer 11<br>**HINWEIS:** Die Option „Kompatibilitätsansicht“ wird in Internet Explorer nicht unterstützt.<br>◆ Mozilla Firefox 46<br>**HINWEIS:** Es müssen Cookies im Browser aktiviert sein. Wenn Cookies deaktiviert sind, ist das Produkt nicht funktionsfähig. |
| Revision | Einer der folgenden Revisionsdienste:<br>◆ OpenXDAS 0.8.345<br>◆ (Bedingt) Für Server mit SLES SP4 und Open XDAS:<br>◆ openxdas-0.8.351-1.1.i586.rpm<br>◆ openxdas-0.8.351-1.1.x86_64.rpm<br>◆ Platform Agent 2011.1r5 |
| Domänenservices für Windows | OES 2 SP11 |

| Kategorie | Anforderung |
| --- | --- |
| Verzeichnisservices | NetIQ eDirectory 8.8.8 Patch 9 Hotfix 2<br><br>Alternativ:<br><br>NetIQ eDirectory 9.0.2 Hotfix 2<br><br>**HINWEIS:** NetIQ hat einige Beschränkungen für die Installation von eDirectory 9.0.2 als Identitätsdepot festgelegt. Weitere Informationen finden Sie unter Abschnitt 8.8, „Arbeiten mit eDirectory 9.0.2 oder höher“, auf Seite 96. |

# 34 Vorbereiten des Identitätsdepots für die Identitätsanwendungen

In diesem Abschnitt erfahren Sie, wie Sie die Installation der Identitätsanwendungen vorbereiten. Die Anwendungen werden auf dem rollenbasierten Bereitstellungsmodul (RBPM) als Rahmenwerk ausgeführt. Beim Installieren der Identity Manager-Engine werden die RPMs `netiq-DXMLuad-4.5.0-0.noarch` und `netiq-DXMLrrsd-4.5.0-0.noarc` automatisch mitinstalliert. Mit diesen RPMs werden der Benutzeranwendungstreiber sowie der Rollen- und der Ressourcenservice-Treiber installiert, und das eDirectory-Schema wird auf die Interaktion mit RBPM erweitert.

Die Installationsdateien befinden sich im Verzeichnis `products/RBPM/user_app_install` in der `.iso`-Image-Datei des Identity Manager-Installationspakets.



## 34.1 Hinzufügen des Benutzeranwendungsschemas als Protokollanwendung zum Audit Server

Wenn die Benutzeranwendung auf dem Audit Server als Protokollanwendung genutzt werden soll, müssen Sie die Datei `dirxml.lsc` auf den Server kopieren. Dieser Abschnitt gilt nur für Novell Identity Audit.

1. Ermitteln Sie den Speicherort der Datei `dirxml.lsc`.

   Diese Datei befindet sich nach der Installation im Installationsverzeichnis der Identity Manager-Benutzeranwendung, beispielsweise `/opt/netiq/idm/apps/UserApplication`.
2. Greifen Sie über einen Webbrowser auf einen iManager zu, auf dem das Novell Identity Audit-Plugin installiert ist, und melden Sie sich als Administrator an.
3. Navigieren Sie zu **Rollen und Aufgaben > Revision und Protokollierung**, und wählen Sie **Protokollserver-Optionen**.
4. Navigieren Sie zum Container „Protokolldienste“ im Baum, wählen Sie den entsprechenden Audit Secure Logging-Server aus, und klicken Sie auf **OK**.
5. Wählen Sie auf der Registerkarte **Protokollanwendungen** den entsprechenden Containernamen aus, und klicken Sie auf den Link **Neue Protokollanwendung**.
6. Führen Sie im Dialogfeld „Neue Protokollanwendung“ die folgenden Schritte aus:
   - **6a** Geben Sie unter „Name der Protokollanwendung“ einen Namen ein, der in Ihrer Umgebung aussagekräftig ist.
   - **6b** Navigieren Sie unter „LSC-Datei importieren“ zur Datei `dirxml.lsc`.
   - **6c** Klicken Sie auf **OK**.
7. Klicken Sie zum Abschließen der Audit Server-Konfiguration auf **OK**.

8 Stellen Sie sicher, dass der Status der Protokollanwendung aktiviert ist (**ON**). (Der Kreis unter dem Status sollte grün sein.)

9 Starten Sie den Audit Server, damit die neuen Protokollanwendungseinstellungen wirksam werden.

## 34.2 Erstellen eines Benutzeranwendungsadministrator-Kontos

Sie müssen manuell ein Administratorkonto für die Benutzeranwendung im eDirectory-Identitätsdepot erstellen, damit das rollenbasierte Bereitstellungsmodul ordnungsgemäß installiert wird. Das Benutzeranwendungsadministrator-Konto muss ein Trustee des Containers der obersten Ebene sein und über Supervisor-Rechte für diesen Container verfügen.

Beim Erstellen des Benutzeranwendungsadministrator-Kontos müssen Sie diesem neuen Benutzerkonto eine Passwortrichtlinie zuweisen. Weitere Informationen finden Sie unter „Creating Password Policies“ im *Administrationshandbuch zur Passwortverwaltung*.

Das integrierte Installationsprogramm für Identity Manager erstellt ein standardmäßiges Benutzeranwendungsadministrator-Konto als `cn=uaadmin.ou=sa.o=data`. Dieser Kontoname wird durch Designer in die Felder eingetragen. Beim Standalone-Installationsprogramm können Sie denselben Kontonamen erstellen oder einen anderen Kontonamen verwenden.

Führen Sie die folgenden Befehle in einer LDAP Data Interchange Format(LDIF)-Datei aus, um die Berechtigungen für das Administratorkonto der Benutzeranwendung zu erstellen:

```
dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 1#subtree#[Root]#[Entry Rights]
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#description
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#directReports
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#mail
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#manager
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#photo
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#srvprvQueryList
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#srvprvUserPrefs
```

```
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#telephoneNumber
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#title

dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 17#subtree#%%RBPM_USER_APP_ADMIN_DN%%#[Entry Rights]
ACL: 35#subtree#%%RBPM_USER_APP_ADMIN_DN%%#[All Attributes Rights]
```

# 35 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 Abschnitt 33.4, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 307. Weitere Informationen zu den Überlegungen für die Benutzeranwendungsdatenbank finden Sie in Abschnitt 33.3.5, „Voraussetzungen für die Installation der Datenbank für die Identitätsanwendungen“, auf Seite 305.

---

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

---



## 35.1 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 Abschnitt 33.4, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 307.

### 35.1.1 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

### 35.1.2 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
```

---

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

---

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

### 35.1.3 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.

## 35.2 Konfigurieren einer PostgreSQL-Datenbank

Als Arbeitserleichterung bietet NetIQ ein Installationsprogramm für PostgreSQL, das die Rahmenwerkdienste und Anwendungen in Identity Manager uneingeschränkt unterstützt. Das Installationsprogramm führt Sie durch den Konfigurationsvorgang. Weitere Informationen finden Sie in Kapitel 28, „Installieren von PostgreSQL und Tomcat“, auf Seite 261.

## 35.3 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 Abschnitt 33.4, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 307.

### 35.3.1 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.

### 35.3.2 Konfigurieren des Admin-Benutzerkontos

Erstellen Sie nach dem Installieren von Microsoft SQL Server 2014 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 `sqljdbc4.jar` wird empfohlen.

---

# 36 Vorbereiten der Umgebung auf die Identitätsanwendungen

Wenn Sie die Identitätsanwendungen in einem Cluster ausführen, erzielen Sie eine höhere Verfügbarkeit. Darüber hinaus unterstützen die Anwendungen die HTTP-Sitzungsreproduktion und das Sitzungs-Failover. Wenn also 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.

In diesem Abschnitt finden Sie Anweisungen zum Vorbereiten Ihrer Umgebung (auch Cluster-Umgebungen) für die Verwendung der Identitätsanwendungen. Sie müssen die Schritte in diesem Kapitel zusammen mit den Anweisungen in einem der folgenden Abschnitte ausführen:

- Abschnitt 37.2, „Geführte Installation der Identitätsanwendungen“, auf Seite 326
- Abschnitt 37.3, „Automatische Installation der Identitätsanwendungen“, auf Seite 333

Weitere Informationen zu den Anforderungen für eine Cluster-Umgebung finden Sie in Abschnitt 33.3.4, „Voraussetzungen für die Installation der Identitätsanwendungen in einer Cluster-Umgebung“, auf Seite 305 und Abschnitt 33.4, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 307.

- Abschnitt 36.1, „Festlegen eines Speicherorts für den Berechtigungsindex“, auf Seite 319
- Abschnitt 36.2, „Aktivieren des Berechtigungsindex für das Clustering“, auf Seite 320
- Abschnitt 36.3, „Vorbereiten des Anwendungsservers auf die Identitätsanwendungen“, auf Seite 320
- Abschnitt 36.4, „Vorbereiten eines Clusters für die Identitätsanwendungen“, auf Seite 322

## 36.1 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/permindex
```

4. Speichern und schließen Sie die Datei.
5. Löschen Sie den vorhandenen Ordner `permindex` im temporären Verzeichnis.
6. Starten Sie Tomcat.

## 36.2 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**.

## 36.3 Vorbereiten des Anwendungsservers auf die Identitätsanwendungen

Bereiten Sie Tomcat, auf dem die Identitätsanwendungen ausgeführt werden sollen, entsprechend vor. Als Arbeitserleichterung ist Apache Tomcat im Installations-Kit enthalten. Weitere Informationen zum Verwenden der Anwendungen einer Cluster-Umgebung finden Sie auch in Abschnitt 36.4, „Vorbereiten eines Clusters für die Identitätsanwendungen“, auf Seite 322.

### 36.3.1 Vorbereiten einer Tomcat-Umgebung

In diesem Abschnitt wird beschrieben, wie Sie eine Umgebung vorbereiten, in der die Identitätsanwendungen in Tomcat ausgeführt werden sollen. Die `.iso`-Datei für die Installation von Identity Manager enthält ein Programm, mit dem Sie Tomcat (und optional PostgreSQL) installieren können. Weitere Informationen finden Sie in Kapitel 28, „Installieren von PostgreSQL und Tomcat“, auf Seite 261.

Bei Bedarf können Sie Ihr eigenes Tomcat-Installationsprogramm anstelle des Schnellinstallationsprogramms im Installationspaket verwenden. Wenn Sie jedoch ein anderes Installationsprogramm verwenden, fallen zusätzliche Schritte an, damit Tomcat fehlerfrei mit den Identitätsanwendungen zusammenarbeitet.

Überprüfen Sie vor Beginn der Installation, ob die Version der zu installierenden Komponenten jeweils durch die Version der Identitätsanwendungen unterstützt wird. Weitere Informationen finden Sie in Abschnitt 33.3, „Voraussetzungen und Überlegungen für die Installation der Identitätsanwendungen“, auf Seite 300.

1. Installieren Sie Apache Tomcat als Dienst auf dem Server.

   Weitere Informationen finden Sie unter Tomcat Setup (http://tomcat.apache.org/tomcat-7.0-doc/setup.html).

2. Installieren Sie die nachfolgenden Komponenten auf demselben Server wie Tomcat.
   - **Java-Laufzeitumgebung (JRE):** Weitere Informationen finden Sie im Java Platform Installation Guide (Installationshandbuch zur Java-Plattform) .
   - **Apache ActiveMQ:** Weitere Informationen finden Sie unter ActiveMQ.
   - **PostgreSQL:** Weitere Informationen finden Sie unter PostgreSQL Manuals (PostgreSQL-Handbücher).
3. Kopieren Sie die Datei `activemq-all-5.14.jar` in den Ordner *`TOMCAT_INSTALLED_HOME`*`/lib` für ActiveMQ.
4. Kopieren Sie die nachfolgenden Dateien in den Ordner *`TOMCAT_INSTALLED_HOME`*`/lib` für die Protokollierung.
   - `log4j.jar`
   - `log4j.properties`
   - `tomcat-juli-adapters.jar`
5. Legen Sie die folgenden Eigenschaften in der Datei `setenv.bat` (Windows) oder `setenv.sh` (Linux) fest.

   ```
   JAVA_HOME
   JRE_HOME
   PATH (set Java path)
   JAVA_OPTS="-Xms1024m -Xmx1024m -XX:MaxPermSize=512m"
   ```

6. Erstellen Sie einen Benutzer mit dem Namen `novlua` und eine Gruppe mit dem Namen `novlua`.

   Damit können Sie Tomcat als Nicht-`Root`-Benutzer ausführen. Weitere Informationen finden Sie in *A Guide To Apache Tomcat Linux Installation and Set-Up* (Installations- und Setup-Handbuch für Apache Tomcat unter Linux).
7. Legen Sie den Benutzer „novlua“ und die Gruppe „novlua“ als Eigentümer der Tomcat-Dateien fest.
8. Kopieren Sie die Datei `postgresql-9.4.1212jdbc42.jar` in den Ordner*/ TOMCAT_INSTALLED_HOME/*`lib`.
9. (Bedingt) Öffnen Sie in einer Clusterumgebung die Datei `server.xml`, die sich im Verzeichnis `/ TOMCAT_INSTALLED_HOME/conf/` im ersten Knoten des Clusters befindet, und kommentieren Sie die folgende Zeile aus:

   ```
   <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
   ```

   Wiederholen Sie dies für alle Knoten im Cluster.

   Zur erweiterten Tomcat-Clusterkonfiguration beachten Sie die Schritte in der Dokumentation zu Apache Tomcat.

Nach der Installation von Tomcat und der Identitätsanwendungen lässt sich die Leistung von Tomcat noch weiter erhöhen. Weitere Informationen finden Sie unter Abschnitt 37.4, „Schritte nach der Installation“, auf Seite 345.

## 36.4 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.



### 36.4.1 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 33.3, „Voraussetzungen und Überlegungen für die Installation der Identitätsanwendungen“, auf Seite 300.

### 36.4.2 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.

## 36.4.3 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 Erstellen des Master-Schlüssels finden Sie unter **Security – Master Key** (Sicherheit – Master-Schlüssel) im Schritt 6 auf Seite 326. 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.

# 37 Installieren der Identitätsanwendungen

In diesem Kapitel finden Sie Anweisungen zum Installieren und Konfigurieren eines Anwendungsservers für die Benutzeranwendung und das RBPM. Sie benötigen die richtige Version der Java-Umgebung für den Anwendungsserver.

Weitere Informationen zu den Anforderungen für Tomcat und Java finden Sie in Abschnitt 33.4, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 307.



## 37.1 Checkliste für die Installation der Identitätsanwendungen

Die nachfolgende Checkliste führt Sie durch die Installation der Identitätsanwendungen.

| | **Checkliste** |
|---|---|
| ❑ | 1. (Bedingt) Lesen Sie die Überlegungen zur Installation der Identitätsanwendungen in Tomcat in einer Cluster-Umgebung. Weitere Informationen finden Sie in Abschnitt 36.4.1, „Erläuterungen zu Clustergruppen in Tomcat-Umgebungen“, auf Seite 322. |
| ❑ | 2. Installieren Sie eine unterstützte Version des Anwendungsservers sowie des JDK (Java Development Kit) oder der JRE (Java Runtime Environment). Weitere Informationen finden Sie in Abschnitt 33.4, „Systemanforderungen für die Identitätsanforderungen“, auf Seite 307. |
| ❑ | 3. Prüfen Sie die Einstellungen in Tomcat. Weitere Informationen finden Sie in Abschnitt 36.3, „Vorbereiten des Anwendungsservers auf die Identitätsanwendungen“, auf Seite 320. |
| ❑ | 4. Konfigurieren Sie eine Datenquellendatei und einen JDBC-Anbieter für die Datenbank. |
| ❑ | 5. Installieren Sie die Identitätsanwendungen. Beachten Sie einen der folgenden Abschnitte:<br>◆ Abschnitt 37.2, „Geführte Installation der Identitätsanwendungen“, auf Seite 326<br>◆ Abschnitt 37.3, „Automatische Installation der Identitätsanwendungen“, auf Seite 333<br>**HINWEIS:** Eine automatische Installation ist nur auf Linux-Computern möglich. |
| ❑ | 6. Konfigurieren Sie Tomcat für die Identitätsanwendungen. Beachten Sie einen der folgenden Abschnitte:<br>◆ Abschnitt 37.4, „Schritte nach der Installation“, auf Seite 345 |

| | Checkliste |
|---|---|
| ❑ | 7. Stellen Sie die Identitätsanwendungen bereit, und starten Sie sie. Weitere Informationen finden Sie in „Starten der Identitätsanwendungen“, auf Seite 348. |

## 37.2 Geführte Installation der Identitätsanwendungen

Im Folgenden wird beschrieben, wie Sie die Identitätsanwendungen mithilfe eines Installationsassistenten installieren (wahlweise über die Benutzeroberfläche oder an der Konsole). Anweisungen für die automatische, unbeaufsichtigte Installation finden Sie in Abschnitt 37.3, „Automatische Installation der Identitätsanwendungen“, auf Seite 333.

Bereiten Sie die Installation gemäß den Anweisungen in Abschnitt 37.1, „Checkliste für die Installation der Identitätsanwendungen“, auf Seite 325 vor. Beachten Sie auch die Versionshinweise zur betreffenden Version.

**HINWEIS**

- Die Werte, die Sie beim Bearbeiten des Assistenten in die einzelnen Fenster eingeben, werden nicht im Installationsprogramm gespeichert. Wenn Sie mit **Zurück** zu einem früheren Fenster zurückwechseln, müssen Sie die Konfigurationswerte erneut eingeben.
- Das Installationsprogramm erstellt das Benutzerkonto *novlua* und stellt die Berechtigungen in Tomcat auf diesen Benutzer ein. Das Skript `idmapps_tomcat_init` führt beispielsweise Tomcat mit diesem Benutzerkonto aus.

**So führen Sie die geführte Installation aus:**

1. Melden Sie sich als `Root` oder als verwaltungsbefugter Benutzer an dem Computer an, auf dem die Identitätsanwendungen installiert werden sollen.
2. Halten Sie Tomcat an.
3. (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die iManager-Installationsdateien befinden (standardmäßig unter `products/RBPM/user_app_install`).
4. (Bedingt) Wenn Sie die Installationsdateien heruntergeladen haben, führen Sie die folgenden Schritte aus:
   - **4a** Navigieren Sie zur `.tgz`- oder `win.zip`-Datei für das heruntergeladene Image.
   - **4b** Extrahieren Sie den Inhalt der Datei in ein Verzeichnis auf dem lokalen Computer.
5. Führen Sie im Verzeichnis mit den Installationsdateien einen der folgenden Schritte aus:
   - **Linux (Konsole)** – Geben Sie Folgendes ein: `/IdmUserApp.bin -i console`
   - **Linux (Benutzeroberfläche)** – Geben Sie Folgendes ein: `/IdmUserApp.bin`
   - **Windows:** Führen Sie `IdmUserApp.exe` aus.
6. Führen Sie die geführte Installation mit den folgenden Parametern aus:
   - **Anwendungsserverplattform**

     Gibt Tomcat für die Ausführung der Identitätsanwendungen an. Tomcat muss bereits installiert sein.
   - **Installationsordner**

     Gibt den Pfad zu einem Verzeichnis an, in dem das Installationsprogramm die Anwendungsdateien erstellen soll.

- **Datenbankplattform**

  Gibt die Plattform der Benutzeranwendungsdatenbank an. Die Datenbank-Software muss bereits installiert sein. Während der Installation müssen Sie jedoch nicht das Datenbankschema erstellen.

  Als Arbeitserleichterung wird von NetIQ PostgreSQL zur Verfügung gestellt.

- **Datenbank-Host und Port**

  Gibt die Einstellungen für den Server an, auf dem die Benutzeranwendungsdatenbank gehostet wird.

---

**HINWEIS:** In einem Cluster müssen für jedes Clustermitglied dieselben Datenbankeinstellungen angegeben werden.

---

***Host***

Gibt den Namen oder die IP-Adresse des Servers an.

***Port***

Gibt den Port an, über den der Server mit der Benutzeranwendung kommunizieren soll.

- **Datenbankbenutzername und Passwort**

  Gibt die Einstellungen für die Ausführung der Benutzeranwendungsdatenbank an.

---

**HINWEIS**

- Wenn Sie PostgreSQL im Rahmen der Installation dieser Version von Identity Manager mitinstalliert haben, wurden die Datenbank und der Datenbankadministrator bereits angelegt. Die installierte Datenbank ist standardmäßig `idmuserappdb`, der Datenbankbenutzer ist `idmadmin`. Geben Sie dieselben Werte an, die Sie bei der PostgreSQL-Installation verwendet haben.
- In einer Cluster-Umgebung müssen für jedes Clustermitglied derselbe Datenbankname, derselbe Benutzername und dasselbe Passwort angegeben werden.

---

***Datenbankname oder SID***

Gibt den Namen der Datenbank entsprechend der Datenbankplattform an. Der Name der Datenbank lautet standardmäßig `idmuserappdb`.

- Bei einer PostgreSQL- oder SQL Server-Datenbank geben Sie den Namen für die Datenbank ein.
- Bei einer Oracle-Datenbank geben Sie die Sicherheits-ID (SID) an, die Sie mit der Datenbankinstanz erstellt haben.

***Datenbankbenutzername***

Gibt den Namen eines Kontos an, über das die Benutzeranwendung auf die Daten in den Datenbanken zugreifen und diese Daten bearbeiten kann.

***Datenbankpasswort***

Gibt das Passwort für den angegebenen Benutzernamen an.

***Datenbanktreiber-JAR-Datei***

Gibt die JAR-Datei für die Datenbankplattform an.

Der Hersteller der Datenbank stellt die Treiber-JAR-Datei bereit, die als Thin-Client-JAR-Datei für den Datenbankserver fungiert. Für PostgreSQL geben Sie beispielsweise `postgresql-9.4-1212.jdbc42.jar` an (standardmäßig im Ordner `opt\netiq\idm\apps\Postgres`).

NetIQ unterstützt keine Treiber-JAR-Dateien von Drittanbietern.

- **Datenbankadministrator**

  *Optional*

  Gibt den Namen und das Passwort für den Datenbankadministrator an.

  In diesem Feld wird automatisch das Benutzerkonto und das Passwort aufgeführt, das Sie als Benutzername und Passwort für die Datenbank angegeben haben. Soll dieses Konto verwendet werden, nehmen Sie keine Änderungen vor.

  ***Datenbankadministrator***

  (Optional) Gibt das Konto eines Datenbankadministrators an, der Datenbanktabellen, Ansichten und andere Artefakte erstellen kann.

  ***Passwort***

  (Optional) Gibt das Passwort für den Datenbankadministrator an.

- **Datenbanktabellen erstellen**

  Gibt an, ob die neue oder vorhandene Datenbank während oder erst nach der Installation konfiguriert werden soll.

  ***Tabellen jetzt erstellen***

  Das Installationsprogramm erstellt die Datenbanktabellen im Rahmen des Installationsvorgangs.

  ***Tabellen beim Start der Anwendung erstellen***

  Das Installationsprogramm hinterlässt eine Anweisung, dass die Tabellen beim ersten Starten der Benutzeranwendung erstellt werden sollen.

  ***SQL in eine Datei schreiben***

  Erzeugt ein SQL-Skript, mit dem der Datenbankadministrator die Datenbanken ausführen kann. Wenn Sie diese Option wählen, müssen Sie außerdem einen Namen für die **Schemadatei** angeben. Diese Einstellung befindet sich in der Konfiguration der **SQL-Ausgabedatei**.

  Wählen Sie diese Option, wenn Sie nicht über ausreichende Berechtigungen zum Erstellen oder Bearbeiten einer Datenbank in Ihrer Umgebung verfügen. Weitere Informationen zum Erzeugen der Tabellen mit der Datei finden Sie in Abschnitt 39.2, „Manuelles Erstellen der Datenbank“, auf Seite 355.

- **Neue Datenbank oder vorhandene Datenbank**

  Gibt an, ob Sie eine bestehende, leere Datenbank verwenden oder neue Tabellen in der bestehenden Datenbank erstellen möchten. Beachten Sie die folgenden Überlegungen:

  - Neue Datenbank

    Klicken Sie auf **Neue Datenbank, wenn die verwendete Datenbank neu ist.**Vergewissern Sie sich, dass eine Datenbank vorhanden ist, bevor Sie diese Option auswählen.

  - Vorhandene Datenbank

Wählen Sie **Vorhandene Datenbank** aus, wenn die Datenbank vorhanden ist und Benutzeranwendungstabellen aus einer früheren Installation enthält.

Wenn die vorhandene Datenbank auf einer Oracle-Plattform ausgeführt wird, müssen Sie zunächst Oracle vorbereiten und dann das Schema aktualisieren. Weitere Informationen finden Sie in Abschnitt 58.8.1, „Vorbereiten einer Oracle-Datenbank für die SQL-Datei“, auf Seite 557.

Nach Auswahl des Datenbanktyps müssen Sie angeben, wann die Datenbanktabellen erstellt werden sollen. Der Bildschirm „Datenbanktabellen erstellen“ enthält die Option zum Erstellen von Tabellen während der Installation oder beim Starten der Anwendung. Ale Alternative dazu können Sie während der Installation eine Schemadatei erstellen, anhand der der Datenbankadministrator später die Tabellen erstellen kann.

Wenn Sie eine Schemadatei generieren möchten, wählen Sie die Schaltfläche „SQL in eine Datei schreiben“ und geben Sie im Feld „Schema-Ausgabedatei“ einen Namen für die Datei an.

- **Datenbankverbindung testen**

  Gibt an, ob das Installationsprogramm zum direkten Erstellen von Tabellen bzw. zum Erstellen der `.sql`-Datei eine Verbindung zur Datenbank herstellen soll.

  Sobald Sie auf **Weiter** klicken oder die **Eingabetaste** drücken, versucht das Installationsprogramm, die Verbindung aufzubauen.

---

**HINWEIS:** Falls ein Fehler bei der Datenbankverbindung auftritt, können Sie die Installation dennoch fortsetzen. Nach der Installation müssen Sie jedoch manuell die Tabellen erstellen und die Verbindung zur Datenbank herstellen. Weitere Informationen finden Sie unter Abschnitt 39.2.2, „Manuelles Erstellen der SQL-Datei zum Generieren des Datenbankschemas“, auf Seite 356.

---

- **Java-Installation**

  Gibt den Pfad zur JRE-Datei an, mit der das Installationsprogramm gestartet wird. Beispiel: `/root/opt/java/jre7`.

- ***Anwendungsserver*-Konfiguration**

  Gibt den Pfad zu den Installationsdateien für Tomcat an. Beispiel: `/opt/apache-tomcat-7.0.52`. Der Installationsvorgang legt einige weitere Dateien in diesem Ordner ab.

- **IDM-Konfiguration**

  Gibt die Einstellungen für den Kontext der Identitätsanwendungen an, der in URLs und für die Workflow-Engine verwendet wird.

  ***Anwendungskontext***

  Gibt einen Namen an, der die Tomcat-Konfiguration, die WAR-Datei der Anwendung und den Namen im URL-Kontext umfasst.

  Das Installationsskript erstellt eine Serverkonfiguration und weist ihr den Namen zu, den Sie beim Installieren von Tomcat angegeben haben. Beispiel: `IDMProv`.

  **WICHTIG:** NetIQ empfiehlt, den angegebenen **Anwendungskontext** zu notieren. Diesen Anwendungsnamen müssen Sie in der URL angeben, wenn Sie die Identitätsanwendungen über einen Browser starten.

- **Audit-Protokollierungstyp auswählen**

  Gibt an, ob die Protokollereignisse an einen Revisionsserver gesendet werden sollen. Wählen Sie **Ja** oder **Nein**.

- **Audit-Protokollierung**

*Gilt nur dann, wenn Sie unter „Audit-Protokollierungstyp auswählen“ die Option „Ja“ angegeben haben.*

Gibt den Typ der zu aktivierenden Protokollierung an.

Weitere Informationen zum Einrichten der Protokollierung finden Sie im *User Application Administration Guide* (Benutzeranwendung: Administrationshandbuch).

***Novell Identity Audit oder NetIQ Sentinel***

Ermöglicht die Protokollierung für die Benutzeranwendung über einen Novell- oder NetIQ-Client.

---

**HINWEIS:** Wenn Sie diese Option wählen, müssen Sie außerdem den Hostnamen oder die IP-Adresse des Client-Servers sowie den Pfad zum Protokoll-Cache angeben. Diese Einstellungen befinden sich im Konfigurationsabschnitt **Novell Identity Audit oder NetIQ Sentinel**.

---

***OpenXDAS***

Gibt an, ob die Benutzeranwendung Ereignisse an den OpenXDAS-Server senden kann.

- **Sicherheit - Master-Schlüssel**

  Gibt an, ob ein vorhandener Master-Schlüssel importiert werden soll. Die Benutzeranwendung greift mithilfe des Master-Schlüssels auf verschlüsselte Daten zu. Wählen Sie **Ja** oder **Nein**.

  Der Master-Schlüssel sollte beispielsweise in den folgenden Situationen importiert werden:

  - Sie haben die erste Instanz der Identitätsanwendungen in einem Cluster installiert. Alle Instanzen der Benutzeranwendung in einem Cluster müssen denselben Master-Schlüssel verwenden. Weitere Informationen finden Sie in Abschnitt 36.4.3, „Verwenden eines einzigen Master-Schlüssels für alle Benutzeranwendungen im Cluster“, auf Seite 323.
  - Sie verlagern Ihre Installation aus einem Staging-System in ein Produktionssystem und möchten auch weiterhin auf die Datenbank des Staging-Systems zugreifen.
  - Sie stellen die Benutzeranwendung wieder her und möchten auf die verschlüsselten Daten zugreifen, die mit der bisherigen Version der Benutzeranwendung gespeichert wurden.

  ***Ja***

  Gibt an, dass ein vorhandener Master-Schlüssel importiert werden soll.

  ***Nein***

  Gibt an, dass das Installationsprogramm den Schlüssel erstellen soll.

  Bei der Installation wird der verschlüsselte Master-Schlüssel standardmäßig im Installationsverzeichnis in die Datei `master-key.txt` geschrieben.

- **Master-Schlüssel importieren**

  *Gilt nur dann, wenn Sie unter „Sicherheit – Master-Schlüssel“ die Option „Ja“ angegeben haben.*

  Wählen Sie den zu verwendenden Master-Schlüssel aus. Sie können den Master-Schlüssel aus der Datei `master-key.txt` kopieren.

- **Anwendungsserver-Verbindung**

Gibt die Einstellungen für die URL an, über die die Benutzer eine Verbindung zu den Identitätsanwendungen auf Tomcat herstellen. Beispiel: `https:meinserver.meinefirma.de:8080`.

---

**HINWEIS:** Wenn OSP auf einer anderen Instanz des Tomcat-Anwendungsservers ausgeführt wird, müssen Sie außerdem die Option **Mit externem Authentifizierungsserver verbinden** wählen und die entsprechenden Werte für den OSP-Server angeben.

---

***Protokoll***

Gibt an, ob *http* oder *https* verwendet werden soll. Soll die Kommunikation per SSL (Secure Sockets Layer) erfolgen, wählen Sie `https`.

***Hostname***

Gibt den DNS-Namen oder die IP-Adresse des Servers an, auf dem OSP gehostet wird. Verwenden Sie nicht `localhost`.

***Port***

Gibt den Port an, über den der Server mit den Client-Computern kommunizieren soll.

***Mit externen Authentifizierungsserver verbinden***

Gibt an, ob der Authentifizierungsserver (OSP) auf einer Tomcat-Instanz gehostet wird. Auf dem Authentifizierungsserver befindet sich eine Liste der Benutzer, die sich bei SSPR anmelden können.

Wenn Sie diese Einstellung wählen, müssen Sie außerdem Werte für **Protokoll**, **Hostname** und **Port** für den Authentifizierungsserver angeben.

- **Authentifizierungsserver – Details**

  Gibt das Passwort an, mit dem die Identitätsanwendungen eine Verbindung zum Authentifizierungsserver herstellen soll. Dies wird auch als Client-Geheimnis bezeichnet. Dieses Passwort wird während der Installation erstellt.

**7** Konfigurieren Sie die Einstellungen für die Identitätsanwendungen im Fenster „Konfigurationsaktualisierung“.

**7a** Suchen Sie die **Identitätsdepot-DNs**.

**7b** Klicken Sie auf **OK**.

---

**HINWEIS**

- Vergewissern Sie sich, dass die Treiber für die Benutzeranwendung und den Rollen- und Ressourcen-Service bereits erstellt und im Identitätsdepot bereitgestellt sind. Weitere Informationen finden Sie unter Abschnitt 33.3.1, „Überlegungen zur Installation der Identitätsanwendungen“, auf Seite 301.
- Wenn Sie auf **Abbrechen** klicken, werden Sie vom Installationsprogramm zum Fenster „Anwendungsserver-Verbindung“ zurückgeführt.
- Nach erfolgter Installation der Benutzeranwendung können Sie den Großteil der Einstellungen in der Datei `configureupdate.sh` bzw. `configureupdate.bat` bearbeiten. Weitere Informationen zum Festlegen der Werte für die Einstellungen finden Sie in Kapitel 40, „Konfigurieren der Einstellungen für die Identitätsanwendungen“, auf Seite 367.

---

8 (Bedingt) Wenn Sie die Identitätsanwendungen bei einer Installation über die Benutzeroberfläche sofort konfigurieren möchten, führen Sie im Fenster „IDM konfigurieren“ die folgenden Schritte aus:

**8a** Klicken Sie auf **Ja** und dann auf **Weiter**.

**8b** Klicken Sie im Fenster „Rollenbasiertes Bereitstellungsmodul – Konfiguration“ auf **Erweiterte Optionen anzeigen**.

**8c** Bearbeiten Sie die Einstellungen nach Bedarf.

---

**HINWEIS**

- Weitere Informationen zum Angeben der Werte finden Sie in Kapitel 40, „Konfigurieren der Einstellungen für die Identitätsanwendungen“, auf Seite 367.
- In Produktionsumgebungen wird die Zuweisung der Administratoren durch die Lizenzierung beschränkt. NetIQ sammelt Überwachungsdaten in der Audit-Datenbank, um sicherzustellen, dass die Lizenzierung in der Produktionsumgebung eingehalten wird. Darüber hinaus empfiehlt NetIQ, die Sicherheitsadministratorberechtigung nur einem Benutzer zu erteilen.

---

**8d** Klicken Sie auf **OK**.

9 (Bedingt) Wenn Sie die Identitätsanwendungen bei einer Installation an der Konsole sofort konfigurieren möchten, führen Sie die folgenden Schritte aus:

**9a** Starten Sie das Dienstprogramm für die Aktualisierung der Konfiguration über die Befehlszeile:

- **Linux:** `configupdate.sh`
- **Windows:** `configupdate.bat`

---

**HINWEIS:** Die Registerkarte „SSO-Client“ des Konfigurationsaktualisierungsprogramms zeigt `localhost:defaultport`, wenn die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung (SSPR) und die Identitätsberichterstellung nicht auf demselben Identitätsbenutzeranwendungsserver installiert sind. Sie müssen die **Client-ID**, das **Passwort** und die **Umleitungs-URL** des SSPR- und Berichterstellungsservers auf dem Benutzeranwendungsserver manuell aktualisieren.

---

**9b** (Optional) Soll das NMAS-Zertifikat erstellt werden, navigieren Sie zu **SSO-Clients > RBPM**, und wählen Sie unter **RBPM-zu-eDirectory-SAML-Konfiguration** die Option **Automatisch**.

**9c** Geben Sie Werte für andere Einstellungen gemäß den Anweisungen in Kapitel 40, „Konfigurieren der Einstellungen für die Identitätsanwendungen“, auf Seite 367 an.

10 Klicken Sie auf **Weiter**.

11 Klicken Sie im Fenster „Übersicht vor der Installation“ auf **Installieren**.

12 (Optional) Lesen Sie die Installationsprotokolldateien. Die Ergebnisse der einfachen Installation finden Sie in der Datei `user_application_install_log.log` im Verzeichnis `/opt/netiq/idm/apps/UserApplication/logs/`.

Weitere Informationen zur Konfiguration der Identitätsanwendungen finden Sie in der Datei `NetIQ-Custom-Install.log` im Verzeichnis `/opt/netiq/idm/apps/UserApplication/`.

13 (Optional) Wenn Sie eine externe WAR-Datei für die Passwortverwaltung verwenden, kopieren Sie sie manuell in das Installationsverzeichnis und in das Bereitstellungsverzeichnis des Remote-Anwendungsservers, auf dem die externe Passwort-WAR ausgeführt wird.

14 Führen Sie die Aufgaben nach der Installation gemäß Kapitel 39, „Abschließen der Installation der Identitätsanwendungen“, auf Seite 355 aus.

## 37.3 Automatische Installation der Identitätsanwendungen

In diesem Abschnitt wird beschrieben, wie Sie die Identitätsanwendungen automatisch installieren lassen. Eine automatische Installation erfordert keine Benutzeraktion und kann Zeit einsparen, besonders wenn die Installation auf mehreren Servern erfolgt. Eine automatische Installation ist nur auf unterstützten Linux-Computern möglich.

Bereiten Sie die Installation gemäß den Anweisungen in Abschnitt 37.1, „Checkliste für die Installation der Identitätsanwendungen“, auf Seite 325 vor. Beachten Sie auch die Versionshinweise zur betreffenden Version.

Dieser Vorgang umfasst folgende Schritte:



### 37.3.1 Festlegen von Passwörtern in der Umgebung für eine automatische Installation

Statt die Konfigurationspasswörter in der Datei `.properties` anzugeben, können Sie die Passwörter auch in der Umgebung festlegen. In diesem Fall ruft die automatische Installation die Passwörter nicht aus der Datei `silent.properties` ab, sondern aus der Umgebung. Dadurch können Sie noch mehr Sicherheit erzielen.

Für die Installation müssen Sie die folgenden Passwörter angeben:

- NOVL_DB_USER_PASSWORD
- NOVL_CONFIG_DBADMIN_PASSWORD
- NOVL_CONFIG_LDAPADMINPASS
- NOVL_CONFIG_KEYSTOREPASSWORD

**Linux**

Verwenden Sie den Befehl `export`. Beispiel:

```
export NOVL_DB_USER_PASSWORD=myPassWord
```

**Windows**

Verwenden Sie den Befehl `set`. Beispiel:

```
set NOVL_DB_USER_PASSWORD=myPassWord
```

### 37.3.2 Bearbeiten der .properties-Datei

Vor Beginn der automatischen Installation oder Konfiguration müssen Sie die Parameterwerte in der `.properties`-Datei bearbeiten. Die Tabelle in diesem Abschnitt zeigt eine Liste der Parameter. Die Parameter sind für die einfache Installation sowie für die Konfiguration des RBPM und der

Identitätsanwendungen vorgesehen. Weitere Informationen zum Angeben der Parameterwerte finden Sie in Abschnitt 37.2, „Geführte Installation der Identitätsanwendungen“, auf Seite 326 und Kapitel 40, „Konfigurieren der Einstellungen für die Identitätsanwendungen“, auf Seite 367.

1. Melden Sie sich als `Root` an dem Computer an, auf dem die Identitätsanwendungen installiert werden sollen.
2. Stellen Sie sicher, dass die Datei `silent.properties` auf dem lokalen Computer gespeichert ist.

   Standardmäßig befindet sich diese Datei im Verzeichnis `products/rbpm/user_app_install` in der `.iso`-Image-Datei des Identity Manager-Installationspakets.
3. Öffnen Sie die Datei `user_app.install.properties`.
4. Bearbeiten Sie die folgenden Parameter in der `.properties`-Datei:

| Name des Parameters in der Datei „silent.properties“ | Entsprechender Parametername in der Datei mit den Konfigurationsparametern für die Identitätsanwendungen |
|---|---|
| NOVL_CONFIG_LDAPHOST= | eDirectory-Verbindungseinstellungen: LDAP-Host.<br><br>Gibt den Hostnamen oder die IP-Adresse des LDAP-Servers an. |
| NOVL_CONFIG_LDAPADMIN= | eDirectory-Verbindungseinstellungen: LDAP-Administrator.<br><br>Gibt den Berechtigungsnachweis für den LDAP-Administrator an. Dieser Benutzer muss bereits vorhanden sein. Die Benutzeranwendung verwendet dieses Konto für eine administrative Verbindung zum Identitätsdepot. Dieser Wert ist mit dem Master-Schlüssel verschlüsselt. |
| NOVL_CONFIG_LDAPADMINPASS= | eDirectory-Verbindungseinstellungen: LDAP-Administratorpasswort.<br><br>Gibt das LDAP-Administratorpasswort an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt. |
| NOVL_CONFIG_ROOTCONTAINERNAME= | eDirectory-DNs: Stammcontainer-DN.<br><br>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. |
| NOVL_CONFIG_PROVISIONROOT= | eDirectory-DNs: Bereitstellungstreiber-DN.<br><br>Gibt den eindeutigen Namen für den Benutzeranwendungstreiber an. Wenn Ihr Treiber beispielsweise „UserApplicationDriver“ und der Treibersatz „myDriverSet“ ist und sich der Treibersatz in einem Kontext „o=myCompany“ befindet, geben Sie folgenden Wert ein:<br><br>`cn=UserApplicationDriver,cn=myDriverSet,o=myCompany` |

| Name des Parameters in der Datei „silent.properties“ | Entsprechender Parametername in der Datei mit den Konfigurationsparametern für die Identitätsanwendungen |
|---|---|
| NOVL_CONFIG_LOCKSMITH= | eDirectory-DNs: Benutzeranwendung - Administrator.<br><br>Ein vorhandener Benutzer im Identitätsdepot mit den Rechten zum Ausführen von administrativen Tätigkeiten für den in der Benutzeranwendung angegebenen Benutzercontainer. Dieser Benutzer hat die Möglichkeit, über den Karteireiter **Administration** der Benutzeranwendung das Portal zu verwalten.<br><br>Wenn der Benutzeranwendungsadministrator Aufgaben zur Workflow-Administration bearbeitet, die in iManager, NetIQ Designer für Identity Manager oder der Benutzeranwendung (Registerkarte **Anforderungen und Genehmigungen**) aufgeführt sind, gewähren Sie dem entsprechenden Administrator ausreichende Trustee-Rechte auf die Objektinstanzen im Benutzeranwendungstreiber. Weitere Informationen finden Sie in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen).<br><br>Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten **Administration > Sicherheit** in der Benutzeranwendung geändert werden. |
| NOVL_CONFIG_PROVLOCKSMITH= | eDirectory-DNs: Bereitstellungsanwendung - Administrator.<br><br>Dieser Benutzer ist in der Bereitstellungsversion von Identity Manager verfügbar. Der Administrator für die Bereitstellungsanwendung kann die Funktionen des Bereitstellungs-Workflows über die Registerkarte **Bereitstellung** (in der Registerkarte **Administration**) verwalten. Auf diese Funktionen können die Benutzer über den Karteireiter **Anforderungen und Genehmigungen** der Benutzeranwendung zugreifen. Dieser Benutzer muss im Identitätsdepot vorhanden sein, bevor ihm die Rolle des Administrators für die Bereitstellungsanwendung zugewiesen werden kann.<br><br>Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten **Administration > Sicherheit** in der Benutzeranwendung geändert werden. |

| Name des Parameters in der Datei „silent.properties“ | Entsprechender Parametername in der Datei mit den Konfigurationsparametern für die Identitätsanwendungen |
|---|---|
| NOVL_CONFIG_ROLECONTAINERDN= | Diese Rolle ist in RBPM verfügbar. Mit dieser Rolle können Mitglieder alle Rollen erstellen, entfernen oder modifizieren und Benutzern, Gruppen oder Containern Rollen zuweisen oder entziehen. Außerdem können die Rollenmitglieder damit einen Bericht für einen beliebigen Benutzer ausführen. Standardmäßig wird diese Rolle dem Benutzeranwendungsadministrator zugewiesen.<br><br>Sie können diese Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite **Rollen > Rollenzuweisungen** in der Benutzeranwendung ändern. |
| NOVL_CONFIG_COMPLIANCECONTAINERDN | Der Konformitätsmoduladministrator ist eine Systemrolle, die es Mitgliedern ermöglicht, alle Funktionen der Registerkarte **Konformität** durchzuführen. Dieser Benutzer muss im Identitätsdepot vorhanden sein, damit ihm die Rolle des Konformitätsmoduladministrators zugewiesen werden kann. |
| NOVL_CONFIG_USERCONTAINERDN= | Benutzeridentität für Metaverzeichnis: Benutzercontainer-DN.<br><br>Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Benutzercontainers an. Diese Angabe definiert den Suchbereich für Benutzer und Gruppen. Benutzer in diesem Container (und unterhalb) dürfen sich bei der Benutzeranwendung anmelden.<br><br>**WICHTIG:** Stellen Sie sicher, dass der bei der Installation des Benutzeranwendungstreibers angegebene Benutzeranwendungsadministrator in diesem Container vorhanden ist, wenn dieser Benutzer Workflows ausführen können soll. |
| NOVL_CONFIG_GROUPCONTAINERDN= | Benutzergruppen für Metaverzeichnis: Gruppencontainer-DN.<br><br>Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Gruppencontainers an. Wird von Entitätsdefinitionen innerhalb der Verzeichnisabstraktionsschicht verwendet. |
| NOVL_CONFIG_KEYSTOREPATH= | eDirectory-Zertifikate: Keystore-Pfad. Erforderlich.<br><br>Geben Sie den vollständigen Pfad zur Keystore-Datei (`cacerts`) der JRE für Tomcat an. Während der Installation der Benutzeranwendung wird die Keystore-Datei geändert. Unter Linux benötigt der Benutzer eine entsprechende Berechtigung zum Schreiben in diese Datei. |

| Name des Parameters in der Datei „silent.properties“ | Entsprechender Parametername in der Datei mit den Konfigurationsparametern für die Identitätsanwendungen |
|---|---|
| NOVL_CONFIG_KEYSTOREPASSWORD= | eDirectory-Zertifikate: Keystore-Passwort.<br><br>Geben Sie das `cacerts`-Passwort an. Die Vorgabe ist `changeit`. |
| NOVL_CONFIG_SECUREADMINCONNECTION= | eDirectory-Verbindungseinstellungen: Sichere Admin-Verbindung.<br><br>*Erforderlich*<br><br>Muss die gesamte Kommunikation über das Admin-Konto über eine SSL-Verbindung erfolgen, geben Sie `true` an. (Diese Option kann die Leistung beeinträchtigen.) Mit dieser Einstellung wird es möglich, andere Vorgänge, für die kein SSL erforderlich ist, tatsächlich ohne SSL durchzuführen.<br><br>Wenn die Kommunikation über das Admin-Konto nicht über eine SSL-Verbindung erfolgen muss, geben Sie `false` an. |
| NOVL_CONFIG_SECUREUSERCONNECTION= | eDirectory-Verbindungseinstellungen: Sichere Benutzerverbindung.<br><br>*Erforderlich*<br><br>Muss die gesamte Kommunikation über das Konto des angemeldeten Benutzers über eine SSL-Verbindung erfolgen, geben Sie `true` an. (Diese Option kann die Leistung stark beeinträchtigen.) Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können.<br><br>Wenn die Kommunikation über das Benutzerkonto nicht über eine SSL-Verbindung erfolgen muss, geben Sie `false` an. |
| NOVL_CONFIG_SESSIONTIMEOUT= | Sonstige: Sitzungszeitüberschreitung.<br><br>*Erforderlich*<br><br>Geben Sie ein Zeitüberschreitungsintervall für die Anwendungssitzung an. |
| NOVL_CONFIG_LDAPPLAINPORT= | eDirectory-Verbindungseinstellungen: Nicht sicherer LDAP-Port.<br><br>*Erforderlich*<br><br>Geben Sie den nicht sicheren Port des LDAP-Servers an. Zum Beispiel 389. |
| NOVL_CONFIG_LDAPSECUREPORT= | eDirectory-Verbindungseinstellungen: Sicherer LDAP-Port.<br><br>*Erforderlich*<br><br>Geben Sie den sicheren Port des LDAP-Servers an, z. B. Port 636. |

| Name des Parameters in der Datei „silent.properties“ | Entsprechender Parametername in der Datei mit den Konfigurationsparametern für die Identitätsanwendungen |
|---|---|
| NOVL_CONFIG_ANONYMOUS= | eDirectory-Verbindungseinstellungen: Öffentliches anonymes Konto verwenden.<br><br>*Erforderlich*<br><br>Wenn nicht angemeldete Benutzer die Möglichkeit erhalten sollen, auf das öffentliche anonyme LDAP-Konto zuzugreifen, geben Sie `true` an.<br><br>Soll stattdessen NOVL_CONFIG_GUEST aktiviert werden, geben Sie `false` an. |
| NOVL_CONFIG_GUEST= | eDirectory-Verbindungseinstellungen: LDAP-Gast.<br><br>Ermöglicht nicht angemeldeten Benutzern den Zugriff auf zulässige Portlets. Darüber hinaus müssen Sie das Gast-Benutzer-Konto deaktivieren. Das Gast-Benutzer-Konto muss bereits im Identitätsdepot vorhanden sein. Zum Deaktivieren des Kontos wählen Sie die Option **Öffentliches anonymes Konto verwenden**. |
| NOVL_CONFIG_GUESTPASS= | eDirectory-Verbindungseinstellungen: LDAP-Gastpasswort. |
| NOVL_CONFIG_EMAILNOTIFYHOST= | Email: Benachrichtigungsschablonen-Host-Token.<br><br>Gibt an, dass Tomcat die Identity Manager-Benutzeranwendung hostet. Beispiel:<br><br>`myapplication serverServer`<br><br>Dieser Wert ersetzt das $HOST$-Token in Email-Schablonen. Die erstellte URL ist eine Verknüpfung zu Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen. |
| NOVL_CONFIG_EMAILNOTIFYPORT= | Email: Benachrichtigungsschablonen-Port-Token.<br><br>Ersetzt das $PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungsaufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden. |
| NOVL_CONFIG_EMAILNOTIFYSECUREPORT= | Email: Token für den sicheren Port der Benachrichtigungsschablone.<br><br>Ersetzt das $SECURE_PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden. |
| NOVL_CONFIG_NOTFSMTPEMAILFROM= | Benachrichtigungs-SMTP-Email-Von.<br><br>*Erforderlich*<br><br>Geben Sie Emails an, die von einem Benutzer in der Bereitstellungs-Email stammen. |

| Name des Parameters in der Datei „silent.properties“ | Entsprechender Parametername in der Datei mit den Konfigurationsparametern für die Identitätsanwendungen |
|---|---|
| NOVL_CONFIG_NOTFSMTPEMAILHOST= | Email: Benachrichtigungs-SMTP-Email-Host.<br><br>*Erforderlich*<br><br>Geben Sie den SMTP-Email-Host für die Bereitstellungs-Email an. Dies kann eine IP-Adresse oder ein DNS-Name sein. Verwenden Sie nicht `localhost`. |
| NOVL_CONFIG_USEEXTPWDWAR= | Passwortverwaltung: Externe WAR-Datei für Passwort verwenden.<br><br>Wenn eine externe WAR-Datei für die Passwortverwaltung verwendet werden soll, geben Sie `true` an, und legen Sie Werte für **NOVL_CONFIG_EXTPWDWARPTH** und **NOVL_CONFIG_EXTPWDWARRTNPATH** fest.<br><br>Soll die interne Standardfunktion `./jsps/pwdmgt/ForgotPassword.jsp` (ohne http[s] am Anfang) für die Passwortverwaltung verwendet werden, wählen Sie `false`. Hierdurch wird der Benutzer nicht zu einer externen WAR-Datei, sondern zur in der Benutzeranwendung integrierten Funktionalität „Passwort vergessen“ umgeleitet. |
| NOVL_CONFIG_EXTPWDWARPATH= | Passwortverwaltung: 'Passwort vergessen'-Link.<br><br>Geben Sie die URL für die Seite „Passwort vergessen“ `ForgotPassword.jsp` in einer externen oder internen WAR-Datei für die Passwortverwaltung an. Alternativ können Sie auch die vorgegebene WAR-Datei für die Passwortverwaltung übernehmen. Weitere Informationen finden Sie in Abschnitt 39.6, „Konfigurieren der „Passwort vergessen“-Verwaltung“, auf Seite 359. |
| NOVL_CONFIG_EXTPWDWARRTNPATH= | Passwortverwaltung: Link zurück zu 'Passwort vergessen'.<br><br>Geben Sie den **Link zurück zu 'Passwort vergessen'** an, den der Benutzer nach Durchführung eines „Passwort vergessen“-Vorgangs anklicken kann. |
| NOVL_CONFIG_FORGOTWEBSERVICEURL= | Passwortverwaltung: Webservice-URL zu „Passwort vergessen“.<br><br>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:<br><br>`https://idmhost:sslport/idm/pwdmgt/service` |

| Name des Parameters in der Datei „silent.properties“ | Entsprechender Parametername in der Datei mit den Konfigurationsparametern für die Identitätsanwendungen |
|---|---|
| NOVL_CONFIG_USEROBJECTATTRIBUTE= | Benutzeridentität für Metaverzeichnis: Benutzerobjektklasse.<br><br>*Erforderlich*<br><br>Die LDAP-Benutzerobjektklasse (in der Regel inetOrgPerson). |
| NOVL_CONFIG_LOGINATTRIBUTE= | Benutzeridentität für Metaverzeichnis: Anmeldeattribut.<br><br>*Erforderlich*<br><br>Das LDAP-Attribut für den Anmeldenamen des Benutzers. Beispiel: `CN`. |
| NOVL_CONFIG_NAMINGATTRIBUTE= | Benutzeridentität für Metaverzeichnis: Benennungsattribut.<br><br>*Erforderlich*<br><br>Das als ID verwendete LDAP-Attribut beim Nachschlagen von Benutzern oder Gruppen. Dieses Attribut ist nicht identisch mit dem Anmeldeattribut, das nur für die Anmeldung, nicht aber bei der Suche nach Benutzern oder Gruppen verwendet wird. |
| NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE= | Benutzeridentität für Metaverzeichnis: Benutzermitgliedschaftsattribut. Optional.<br><br>*Erforderlich*<br><br>Das LDAP-Attribut, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten. |
| NOVL_CONFIG_GROUPOBJECTATTRIBUTE= | Benutzergruppen für Metaverzeichnis: Gruppenobjektklasse.<br><br>*Erforderlich*<br><br>Die Objektklasse für die LDAP-Gruppen (in der Regel groupofNames). |
| NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE= | Benutzergruppen für Metaverzeichnis: Gruppenmitgliedschaftsattribut.<br><br>*Erforderlich*<br><br>Geben Sie das Attribut an, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten. |
| NOVL_CONFIG_USEDYNAMICGROUPS= | Benutzergruppen für Metaverzeichnis: Dynamische Gruppen verwenden.<br><br>*Erforderlich*<br><br>Sollen dynamische Gruppen verwendet werden, geben Sie `true` an. |

| Name des Parameters in der Datei „silent.properties“ | Entsprechender Parametername in der Datei mit den Konfigurationsparametern für die Identitätsanwendungen |
|---|---|
| NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS= | Benutzergruppen für Metaverzeichnis: Klasse für dynamisches Gruppenobjekt.<br><br>*Erforderlich*<br><br>Geben Sie die Objektklasse für die dynamische Gruppe an (in der Regel dynamicGroup). |
| NOVL_CONFIG_TRUSTEDSTOREPATH= | Speicher für Herkunftsverbürgungsschlüssel: Pfad für Herkunftsverbürgungsspeicher.<br><br>Der Speicher für Herkunftsverbürgungsschlüssel enthält alle verbürgten Zertifikate der Signierer. Wurde kein Pfad angegeben, ruft die Benutzeranwendung den Pfad von der Systemeigenschaft `javax.net.ssl.trustStore` ab. Wenn der Pfad nicht vorhanden ist, verwendet die Benutzeranwendung stattdessen `jre/lib/security/cacerts`. |
| NOVL_CONFIG_TRUSTEDSTOREPASSWORD= | Speicher für Herkunftsverbürgungsschlüssel: Passwort für Herkunftsverbürgungsspeicher. |
| NOVL_CONFIG_ICSLOGOUTENABLED= | Access Manager- und iChain-Einstellungen: Gleichzeitige Abmeldung aktiviert.<br><br>Wenn die gleichzeitige Abmeldung von der Benutzeranwendung und entweder dem NetIQ Access Manager oder iChain möglich sein soll, geben Sie `true` an. Bei der Abmeldung prüft die Benutzeranwendung, ob ein iChain- oder NetIQ Access Manager-Cookie vorhanden ist; falls ja, wird der Benutzer zur ICS-Abmeldungsseite umgeleitet.<br><br>Soll die gleichzeitige Abmeldung deaktiviert werden, geben Sie `false` an. |
| NOVL_CONFIG_ICSLOGOUTPAGE= | Access Manager- und iChain-Einstellungen: Seite 'Gleichzeitige Abmeldung'.<br><br>Geben Sie die URL zur iChain- oder NetIQ-Access Manager-Abmeldungsseite an. (Die URL ist dabei ein von iChain oder vom NetIQ Access Manager erwarteter Hostname). Wenn die ICS-Protokollierung aktiviert ist und sich ein Benutzer von der Benutzeranwendung abmeldet, wird der Benutzer auf diese Seite umgeleitet. |
| NOVL_CONFIG_EMAILNOTIFYPROTOCOL= | Email: Benachrichtigungsschablonen-Protokoll-Token.<br><br>Bezieht sich auf ein nicht sicheres Protokoll, HTTP. Ersetzt das $PROTOCOL$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden. |
| NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL= | Email: Token für den sicheren Port der Benachrichtigungsschablone. |

| Name des Parameters in der Datei „silent.properties“ | Entsprechender Parametername in der Datei mit den Konfigurationsparametern für die Identitätsanwendungen |
|---|---|
| NOVL_CONFIG_OCSPURI= | Sonstige: OCSP-URI.<br><br>Wenn für die Client-Installation das OSCP (On-Line Certificate Status Protocol) verwendet wird, geben Sie einen URI (Uniform Resource Identifier) an. Beispiel für das Format: `http://hstport/ocspLocal`. Die OCSP-URI aktualisiert den Status der verbürgten Zertifikate online. |
| NOVL_CONFIG_AUTHCONFIGPATH= | Sonstige: Konfigurationspfad für Autorisierung.<br><br>Der vollständig qualifizierte Name der Konfigurationsdatei für die Autorisierung. |
| NOVL_CONFIG_CREATEDIRECTORYINDEX | Sonstiges: eDirectory-Index erstellen<br><br>Wenn das automatische Installationsprogramm Indizes für die Attribute „manager“, „ismanager“ und „srvprvUUID“ auf dem eDirectory-Server erstellen soll, der für **NOVL_CONFIG_SERVERDN** angegeben wurde, geben Sie „true“ an. Wenn dieser Parameter auf `true` gesetzt ist, können Sie **NOVL_CONFIG_REMOVEEDIRECTORYINDEX** nicht auf `true` setzen.<br><br>Zur Erzielung einer optimalen Leistung sollte die Erstellung des Index abgeschlossen sein. Die Indizes sollten sich im Online-Modus befinden, bevor Sie die Benutzeranwendung verfügbar machen. |
| NOVL_CONFIG_REMOVEDIRECTORYINDEX | Sonstiges: eDirectory-Index entfernen<br><br>Wenn das automatische Installationsprogramm Indizes vom Server entfernen soll, der für **NOVL_CONFIG_SERVERDN** angegeben wurde, geben Sie `true` an. Wenn dieser Parameter auf `true` gesetzt ist, können Sie **NOVL_CONFIG_CREATEEDIRECTORYINDEX** nicht auf `true` setzen. |
| NOVL_CONFIG_SERVERDN | Sonstiges: Server-DN<br><br>Geben Sie den eDirectory-Server an, auf dem Indizes erstellt oder entfernt werden sollen. |
| NOVL_CREATE_DB | Gibt an, wie die Datenbank erstellt werden soll. Gültige Werte:<br><br>◆ *now* – Erstellt die Datenbank sofort.<br>◆ *file* – Schreibt die SQL-Ausgabe in eine Datei.<br>◆ *startup* – Erstellt die Datenbank, wenn die Anwendung gestartet wird. |
| NOVL_DATABASE_NEW | Gibt an, ob diese Datenbank neu oder bereits vorhanden ist. Bei einer neuen Datenbank geben Sie `true` an. |

| Name des Parameters in der Datei „silent.properties“ | Entsprechender Parametername in der Datei mit den Konfigurationsparametern für die Identitätsanwendungen |
|---|---|
| NOVL_RBPM_SEC_ADMINDN | Sicherheitsadministrator<br><br>Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Sicherheitsdomäne.<br><br>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. |
| NOVL_RBPM_RESOURCE_ADMINDN | Ressourcenadministrator<br><br>Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Ressourcendomäne. Der Ressourcenadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Ressourcendomäne durchführen. |
| NOVL_RBPM_CONFIG_ADMINDN | Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Konfigurationsdomäne. 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. |
| RUN_LDAPCONFIG= | Gibt an, ob Sie die LDAP-Einstellungen jetzt oder später konfigurieren möchten. Gültige Werte:<br><br>◆ *Now* – Führt die LDAP-Konfiguration sofort aus; für die WAR werden dabei die angegebenen LDAP-Konfigurationseinstellungen eingetragen.<br><br>◆ *Later* – Installiert die Benutzeranwendungsdateien, ohne die LDAP-Einstellungen zu konfigurieren. |

## 37.3.3 Importieren von eDirectory-Zertifikaten in Identitätsanwendungen

Zum Aufbauen einer Trust-Verbindung zwischen den Identitätsanwendungen und dem eDirectory-Server importieren Sie die eDirectory-Zertifikate in die Identitätsanwendungen.

1. Exportieren Sie das eDirectory-Zertifikat aus iManager:
   - **1a** Melden Sie sich als Administrator bei iManager an.
   - **1b** Navigieren Sie zu **Rollen und Aufgaben > Zugriff auf NetIQ-Zertifikate > Serverzertifikate**.
   - **1c** Aktivieren Sie das Kontrollkästchen **SSL CertificateDNS** und klicken Sie auf **Exportieren**.
   - **1d** Wählen Sie in der Dropdown-Liste **Zertifikate** den Eintrag **SSL CertificateDNS** aus, deaktivieren Sie das Kontrollkästchen **Privaten Schlüssel exportieren** und wählen Sie das Exportformat **DER**.
   - **1e** Klicken Sie auf **Weiter**.
   - **1f** Klicken Sie auf **Exportiertes Zertifikat speichern**. Das exportierte Zertifikat wird auf dem lokalen System gespeichert.
2. Importieren Sie das eDirectory-Zertifikat in die Identitätsanwendungen:
   - **2a** Melden Sie sich beim Server, auf dem die Identitätsanwendungen installiert werden sollen, als Administrator an.
   - **2b** Kopieren Sie das eDirectory-Zertifikat, das Sie aus iManager exportiert haben, und führen Sie den Befehl `keytool` aus:

     ```
     keytool -import -trustcacerts -file Cerificate_Path -alias ALIAS_NAME -
     keystore cacerts
     ```

     Geben Sie unter `Certificate_Path` den Speicherort des eDirectory-Zertifikats auf dem Computer an.

     Geben Sie unter `ALIAS_NAME` einen beliebigen Aliasnamen für das Zertifikat an. Beispiel:

     ```
     /opt/netiq/idm/jre/bin/keytool -import -trustcacerts -file /opt /
     Certificate_Import_Path/EdirCertificate -alias EDIR_CERT -keystore /opt /
     netiq/idm/jre/lib/security/cacerts
     ```

## 37.3.4 Automatische Installation der Identitätsanwendungen

1. Melden Sie sich als Root-Benutzer an dem Computer an, auf dem die Identitätsanwendungen installiert werden sollen.
2. Öffnen Sie eine Terminalsitzung.
3. Geben Sie die Werte für die Installation an. Weitere Informationen hierzu finden Sie in Abschnitt 37.3.2, „Bearbeiten der .properties-Datei“, auf Seite 333 und Abschnitt 28.2.1, „Schützen der Passwörter für eine automatische Installation“, auf Seite 264.
4. Starten Sie das Installationsprogramm für Ihre Plattform mit dem folgenden Befehl:
   - **Linux:** `./IdmUserApp.bin -i silent -f /Ihr_Verzeichnispfad/silent.properties`
   - **Windows:** `./IdmUserApp.exe -i silent -f /Ihr_Verzeichnispfad/silent.properties`

**HINWEIS:** Wenn sich die Datei `silent.properties` nicht in demselben Verzeichnis befindet wie das Installationsskript, werden Sie aufgefordert, den vollständigen Pfad zu dieser Datei einzugeben. Das Skript entpackt die notwendigen Dateien in ein temporäres Verzeichnis und startet dann die automatische Installation.

## 37.4 Schritte nach der Installation

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

- Abschnitt 37.4.1, „Konfigurieren des Benutzeranwendungstreibers für das Clustering“, auf Seite 345
- Abschnitt 37.4.2, „Übergeben der preferIPv4Stack-Eigenschaft an die JVM“, auf Seite 345
- Abschnitt 37.4.3, „Prüfen des Serverzustands“, auf Seite 346
- Abschnitt 37.4.4, „Überwachen der Zustandsstatistiken“, auf Seite 346
- Abschnitt 37.4.5, „Erstellen von Verbundindizes“, auf Seite 347

Wenn Sie das Schnellinstallationsprogramm für Tomcat verwendet haben, übernimmt das Identity Manager-Installationsprogramm die Konfiguration für Tomcat. Falls Sie Tomcat selbst installiert haben, beachten Sie Folgendes:

- Sie können den Tomcat-Dienst anpassen und so eine höhere Leistung erzielen. Weitere Informationen finden Sie unter *So You Want High Performance* (Tipps zur Leistungssteigerung).
- Unter Umständen sollten Sie die Protokollierung von Ereignissen ermöglichen. Weitere Informationen finden Sie in Abschnitt 29.4, „Protokollieren der Anmeldung mit dem Apache-Log4j-Dienst“, auf Seite 271.

### 37.4.1 Konfigurieren des Benutzeranwendungstreibers für das Clustering

Weitere Informationen hierzu finden Sie unter, Abschnitt 38.2, „Konfigurieren des Benutzeranwendungstreibers für das Clustering“, auf Seite 352.

### 37.4.2 Übergeben der preferIPv4Stack-Eigenschaft an die JVM

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

Ohne diese Option tritt möglicherweise der folgende Fehler auf:

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

Unter Umständen wird der folgende Fehler angezeigt:

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

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

## 37.4.3 Prüfen des Serverzustands

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

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

## 37.4.4 Überwachen der Zustandsstatistiken

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

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

  Beispiel:

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

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

  Beispiel:

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

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

  Beispiel:

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

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

  Beispiel:

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

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

  Beispiel:

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

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

  Beispiel:

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

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

### 37.4.5 Erstellen von Verbundindizes

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

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

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

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

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

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

## 37.5 Deaktivieren der Einstellung „HTML-Framing verhindern“ zum Integrieren von Identity Manager in SSPR

In diesem Abschnitt wird die erforderliche Konfiguration beschrieben, mit der Identity Manager in eine vorhandene SSPR 3.2-Umgebung integriert wird, die nicht über Identity Manager 4.5 bereitgestellt wird. Anhand der konfigurierbaren Option **HTML-Framing verhindern** in SSPR können die Benutzer SSPR in einem Inline-Rahmen für jede Anwendung anzeigen lassen, die den iframe-HTML-Quellcode umfasst. Wenn Sie diese Option aktivieren, wird SSPR nicht im angegebenen iFrame für die Anwendung berücksichtigt. Deaktivieren Sie diese Option für Identity Manager mit den folgenden Schritten:

1. Gehen Sie zu der Adresse „http://*<IP/DNS-Name>:<Port>/sspr“.* Mit diesem Link gelangen Sie zum SSPR-Portal.
2. Melden Sie sich als SSPR-Administrator an.
3. Klicken Sie oben auf der Seite auf **Konfigurationseditor**, und geben Sie das OSP-Konfigurationspasswort an.

4 Klicken Sie auf **Einstellungen > Sicherheit** > **Erweiterte Einstellungen immer anzeigen**, und führen Sie die folgenden Schritte aus:

**4a** Navigieren Sie zu **HTML-Framing verhindern**, und deaktivieren Sie die Option **Aktiviert**. Speichern Sie die Einstellung mit **Speichern**.

**4b** Klicken Sie im Bestätigungsfenster auf **OK**.

# 37.6 Starten der Identitätsanwendungen

In diesem Abschnitt wird beschrieben, wie Sie die Identitätsanwendungen starten und sich erstmals bei einem Anwendungsserver anmelden. In einer Cluster-Umgebung starten Sie das Verfahren auf dem primären Knoten. Die Identitätsanwendungen sollten bereits installiert sein und zur Bereitstellung verfügbar sein. Weitere Informationen zu den Aufgaben nach der Installation finden Sie in Kapitel 39, „Abschließen der Installation der Identitätsanwendungen“, auf Seite 355.



## 37.6.1 Starten der Benutzeranwendung auf einem Tomcat-Server

In diesem Abschnitt benötigen Sie ein Startskript für den Tomcat-Anwendungsserver.

- **Linux**: `/etc/init.d/idmapps_tomcat_init start`
- **Windows**: `services.msc`

  Starten Sie den Tomcat-Dienst über `services.msc`. Mit dieser Datei können Sie den Tomcat-Dienst außerdem anhalten und neu starten.

Wenn nach diesen Schritten im Browser nicht die Seite der Benutzeranwendung angezeigt wird, prüfen Sie, ob Fehlermeldungen an der Terminalkonsole vorliegen, und beachten Sie Kapitel 60, „Fehlersuche“, auf Seite 571.

**So starten Sie die Identitätsanwendungen:**

1 Starten Sie die Datenbank für die Identitätsanwendungen. Weitere Informationen finden Sie in der Dokumentation zur Datenbank.

2 Fügen Sie das Flag `Djava.awt.headless=true` an das Startskript für Tomcat an, sodass Berichte in der Benutzeranwendung ausgeführt werden. Beispiel:

```
JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -
Dsun.jnu.encoding=UTF-8 -server -Xms1024m -Xmx1024m -XX:MaxPermSize=512m
```

**HINWEIS:** Bei einem X11 Windows-System kann dieser Schritt entfallen.

3 Starten Sie Tomcat, auf dem die Identitätsanwendungen installiert sind.

**HINWEIS:** In einem Cluster starten Sie nur den primären Knoten.

4 Legen Sie in der Befehlszeile das Installationsverzeichnis als Arbeitsverzeichnis fest.

5 Führen Sie das Startskript aus.

6 Aktivieren Sie die Kommunikation mit dem Benutzeranwendungstreiber mit den folgenden Schritten:

**6a** Melden Sie sich bei iManager an.

**6b** Klicken Sie im linken Bereich unter **Funktionen und Aufgaben > Identity Manager** auf **Identity Manager-Überblick**.

**6c** Geben Sie im Inhaltsrahmen den Treibersatz ein, der den Benutzeranwendungstreiber enthält, und klicken Sie auf **Suchen**.

**6d** Klicken Sie in der Grafik mit dem Treibersatz und den zugehörigen Treibern auf das rotweiße Symbol für den Benutzeranwendungstreiber.

**6e** Klicken Sie auf **Treiber starten**.

Beim Start versucht der Treiber mit der Benutzeranwendung einen „Handshake“ durchzuführen. Wenn der Anwendungsserver nicht läuft oder die WAR-Datei nicht erfolgreich bereitgestellt wurde, gibt der Treiber einen Fehler zurück. Ansonsten wird das Yin-Yang-Symbol als Treiberstatus angezeigt; dies bedeutet, dass der Treiber gestartet wurde.

**7** Starten Sie den Rollen- und Ressourcenservice-Treiber. Wiederholen Sie hierzu das Verfahren in Schritt 6.

**8** Starten Sie die Benutzeranwendung, und melden Sie sich an. Geben Sie hierzu die folgende URL in den Webbrowser ein:

`http://hostname:port/ApplicationName`

**Hostname**

Gibt den Namen des Anwendungsservers an (Tomcat). Beispiel: `meinserver.domain.de`

**port**

Gibt die Portnummer des Anwendungsservers an. Beispiel: `8180`.

**ApplicationName**

Gibt den Namen an, den Sie beim Installieren für die Anwendung in den Konfigurationsdaten für den Anwendungsserver angegeben haben. Beispiel: `IDMProv`.

**9** Klicken Sie oben rechts auf der Portalseite der Benutzeranwendung auf **Anmelden**.

**10** (Bedingt) Soll die Benutzeranwendung in einer Clustergruppe aktiviert werden, führen Sie die folgenden Schritte aus:

**10a** Klicken Sie auf **Administration**.

**10b** Klicken Sie im Anwendungskonfigurationsportal auf **Caching**.

**10c** Wählen Sie im Fenster „Cache-Management“ unter **Cluster aktiviert** die Option **Wahr**.

**10d** Klicken Sie auf **Speichern**.

**10e** Starten Sie den Server neu.

**10f** (Bedingt) Sollen lokale Einstellungen verwendet werden, wiederholen Sie dieses Verfahren für jeden Server im Cluster.

# 38 Erstellen und Bereitstellen der Treiber für die Identitätsanwendungen

Beim Installieren des RBPM werden die Dateien zum Erstellen der Treiber für die Identitätsanwendungen hinzugefügt. Mit der Treiberkonfigurationsunterstützung können Sie Folgendes ausführen:

- Verknüpfen eines Benutzeranwendungstreibers mit einem Rollen- und Ressourcenservice-Treiber
- Verknüpfen einer Benutzeranwendung mit einem Benutzeranwendungstreiber

Bevor Sie die Treiber konfigurieren, stellen Sie sicher, dass alle erforderlichen Pakete im Paketkatalog in Designer vorliegen. Wenn Sie ein neues Identity Manager-Projekt erstellen, werden Sie automatisch dazu aufgefordert, mehrere Pakete in das neue Projekt zu importieren.



## 38.1 Erstellen des Benutzeranwendungstreibers

Der Benutzeranwendungstreiber ist nicht nur eine Runtime-Komponente, sondern enthält auch Verzeichnisobjekte (auch die Runtime-Artefakte der Benutzeranwendung). Hiermit werden anwendungsspezifische Umgebungskonfigurationsdaten gespeichert. Der Treiber sendet außerdem eine Meldung an die Verzeichnisabstraktionsschicht, wenn wichtige Datenwerte im Identitätsdepot geändert werden. Als Reaktion auf diese Benachrichtigung wird der Cache in der Verzeichnisabstraktionsschicht aktualisiert.

1. Öffnen Sie Ihr Projekt in Designer.
2. Wählen Sie in der Ansicht **Modellierer > Bereitstellung** in der Palette den Eintrag **Benutzeranwendung**.
3. Ziehen Sie das Symbol für **Benutzeranwendung** auf die Ansicht **Modellierer.**
4. Wählen Sie im Treiberkonfigurationsassistenten die Option **Benutzeranwendungs-Basis**, und klicken Sie auf **Weiter**.
5. Eine Meldung wird angezeigt, dass mehrere zusätzliche Pakete installiert werden. Bestätigen Sie die Meldung mit **OK**.
6. (Optional) Geben Sie den Namen des Treibers an.

   Klicken Sie auf **Weiter**.
7. Geben Sie im Fenster der Verbindungsparameter die ID und das Passwort für den Benutzeranwendungsadministrator an.
8. Geben Sie den Host und den Port für den Benutzeranwendungsserver an.
9. Geben Sie den Anwendungskontext für den Benutzeranwendungsserver an.

10 (Optional) Wenn der Bereitstellungsadministrator in der Lage sein soll, Workflows im Namen einer anderen Person zu starten, für die der Bereitstellungsadministrator als Vertretung festgelegt ist, wählen Sie unter **Überschreiben des Initiators zulassen** die Option **Ja**.

11 Klicken Sie im Fenster **Installationsaufgabe bestätigen** auf **Fertig stellen**.

## 38.2 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**.

## 38.3 Erstellen des Rollen- und Ressourcenservice-Treibers

Die Benutzeranwendung verwendet den Rollen- und Ressourcenservice-Treiber zur Verwaltung der Backend-Verarbeitung von Ressourcen. Beispielsweise verwaltet er alle Ressourcenanforderungen, startet Workflows für Ressourcenanforderungen und initiiert den Bereitstellungsprozess für Ressourcenanforderungen.

1 Öffnen Sie Ihr Projekt in Designer.

2 Wählen Sie in der Ansicht **Modellierer > Bereitstellung** in der Palette den Eintrag **Rollenservice**.

3 Ziehen Sie das Symbol für **Rollenservice** auf die Ansicht **Modellierer.**

4 Wählen Sie im Treiberkonfigurationsassistenten die Option **Rollen- und Ressourcenservice-Basis**, und klicken Sie auf **Weiter**.

5 (Bedingt) Wenn dies der erste Treiber ist, den Sie in Designer installieren, klicken Sie auf **OK**, sodass das Paket **Gemeinsame Einstellungen – Advanced Edition** installiert wird.

   **5a** Geben Sie die URL für den Benutzeranwendungsserver an.

   **5b** Geben Sie den eDirectory-DN für den Benutzeranwendungsadministrator an.

5c Geben Sie den LDAP-DN für das Benutzeranwendungsbereitstellungs-Dienstkonto an. Hierzu können Sie wahlweise Ihr Benutzeranwendungsadministrator-Konto verwenden oder ein anderes Konto angeben.

Wenn dieses Dienstkonto eine Rollen- oder Ressourcen-Bereitstellungsanforderung auslöst, werden alle Genehmigungen und Bereitstellungs-Workflows, die dieser Rolle oder Ressource zugewiesen sind, umgangen.

6 (Optional) Geben Sie den Namen des Treibers an.

7 Klicken Sie auf **Weiter**.

8 Geben Sie im Fenster für die Verbindung zwischen Benutzeranwendung und Workflow den DN der Benutzergruppen-Basis-Containers und den soeben erstellten Benutzeranwendungstreiber an.

Da der Treiber noch nicht bereitgestellt wurde, wird der soeben konfigurierte Benutzeranwendungstreiber beim Durchsuchen nicht angezeigt. Sie müssen daher den DN für den Treiber eingeben.

9 Geben Sie die URL für die Benutzeranwendung an.

10 Geben Sie den LDAP-DN für das Benutzeranwendungsadministrator-Konto an.

Das Benutzeranwendungsadministrator-Konto authentifiziert sich bei der Benutzeranwendung, sodass der Genehmigungs-Workflow gestartet werden kann. Weitere Informationen finden Sie in Abschnitt 34.2, „Erstellen eines Benutzeranwendungsadministrator-Kontos“, auf Seite 312.

11 Geben Sie das Passwort für das Benutzeranwendungsadministrator-Konto an.

12 Klicken Sie auf **Weiter**.

13 Klicken Sie im Fenster zum Bestätigen der Installationsaufgaben auf **Fertig stellen**.

## 38.4 Bereitstellen der Treiber für die Benutzeranwendung

Der Benutzeranwendungstreiber sowie der Rollen- und der Ressourcenservice-Treiber können erst nach dem Bereitstellen verwendet werden.

---

**HINWEIS:** Wenn Sie eine eDirectory-Umgebung reproduzieren, müssen Sie sicherstellen, dass die Reproduktionen das NCP-Server-Objekt für Identity Manager enthalten. Identity Manager ist auf die lokalen Reproduktionen eines Servers beschränkt. Aus diesem Grund startet der Rollen- und Ressourcenservice-Treiber möglicherweise nicht ordnungsgemäß, wenn ein Sekundärserver das Serverobjekt nicht enthält.

---

**So stellen Sie die Treiber bereit:**

1 Öffnen Sie Ihr Projekt in Designer.

2 Wählen Sie in der Ansicht **Modellierer** oder **Gliederung** den Treibersatz aus.

3 Klicken Sie auf **Live > Bereitstellen**.

# 39 Abschließen der Installation der Identitätsanwendungen

In diesem Abschnitt finden Sie Anweisungen für Aufgaben, die nach der Installation der Identitätsanwendungen und ihres Rahmenwerks ggf. anfallen:



## 39.1 Prüfen des Serverzustands in einer geclusterten Umgebung

Weitere Informationen hierzu finden Sie unter, Abschnitt 37.4.3, „Prüfen des Serverzustands“, auf Seite 346

## 39.2 Manuelles Erstellen der Datenbank

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

### 39.2.1 Generieren des Datenbankschemas mit der SQL-Datei

In diesem Abschnitt wird vorausgesetzt, dass das Installationsprogramm eine SQL-Datei erstellt hat, mit der Sie das Datenbankschema erstellen können. Falls Ihnen keine SQL-Datei vorliegt, beachten Sie die Anweisungen in Abschnitt 39.2.2, „Manuelles Erstellen der SQL-Datei zum Generieren des Datenbankschemas“, auf Seite 356.

---

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

---

1. Halten Sie den Anwendungsserver an.
2. Melden Sie sich beim Datenbankserver an.

3 Löschen Sie die Datenbank, die von den Identitätsanwendungen genutzt wird.

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

5 Navigieren Sie zum SQL-Skript, das im Rahmen des Installationsvorgangs erstellt wurde (standardmäßig im Verzeichnis */Installationspfad/*`userapp/sql`).

6 (Bedingt) Bei einer Oracle-Datenbank fügen Sie einen umgekehrten Schrägstrich (/) nach der Definition der Funktion `CONCAT_BLOB` ein. Beispiel:

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

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

8 Starten Sie Tomcat neu.

## 39.2.2 Manuelles Erstellen der SQL-Datei zum Generieren des Datenbankschemas

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

1 Halten Sie Tomcat an.

2 Melden Sie sich bei dem Server an, auf dem die Datenbank der Identitätsanwendungen gehostet wird.

3 Löschen Sie die vorhandene Datenbank.

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

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

```
/opt/netiq/idm/apps/UserApplication
```

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

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

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

8 Fügen Sie die kopierte Befehlszeichenkette in ein Terminal ein.

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

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

10 Führen Sie folgenden Befehl aus.

11 (Bedingt) Wenn keine Daten in die Datenbank geschrieben werden, sondern stattdessen eine SQL-Datei erzeugt wird, übermitteln Sie die Datei an Ihren Datenbankadministrator, und bitten Sie ihn, die Datei in den Datenbankserver zu importieren. Weitere Informationen finden Sie in Abschnitt 39.2.1, „Generieren des Datenbankschemas mit der SQL-Datei“, auf Seite 355.

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

## 39.3 Aufzeichnen des Master-Schlüssels

NetIQ empfiehlt, den verschlüsselten Master-Schlüssel direkt nach der Installation zu kopieren und an einem sicheren Ort zu speichern. Erfolgt die Installation auf dem ersten Mitglied eines Clusters, müssen Sie diesen verschlüsselten Master-Schlüssel verwenden, wenn Sie die Identitätsanwendungen auf anderen Cluster-Mitgliedern installieren.

Wenn Sie die Identitätsanwendungen an der Konsole installiert haben, hat das Installationsprogramm die Datei `master-key.txt` nicht automatisch erstellt. Sie müssen daher den Master-Schlüssel manuell aus der Datei `ism-configuration.properties` kopieren.

1 Öffnen Sie die Datei `ism-configuration.properties` im Installationsverzeichnis.

2 Kopieren Sie den verschlüsselten Master-Schlüssel an einen sicheren Speicherort, auf den Sie bei einem Systemfehler zugreifen können.

**WARNUNG:** Bewahren Sie immer eine Kopie des verschlüsselten Master-Schlüssels auf. Der verschlüsselte Master-Schlüssel wird benötigt, um Zugriff auf verschlüsselte Daten zu erlangen, falls der Master-Schlüssel verloren geht. Dies ist beispielsweise bei Gerätefehlern der Fall.

## 39.4 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*.

### 39.4.1 Aufgaben vor der Installation für Nicht-Root-Benutzer

Führen Sie vor der Installation der Identity Manager-Benutzeranwendung als Nicht-Root-Benutzer die folgenden Schritte aus:

1. Importieren Sie das eDirectory-Zertifikat in die `JRE cacerts`-Datei der Benutzeranwendung.
2. Prüfen Sie, ob das Objekt **Standard-Benachrichtigungssammlung** bereitgestellt ist.
3. Tragen Sie die SAML-Methode mit dem folgenden Befehl in den eDirectory-Server ein:

   ```
   nmasinst -addmethod <admin dn> <tree-name> <configuration file present in /
   <eDirectory installed location>/nmas/NmasMethods/Novell/SAML> -h <hostname:NCP
   port> -w <pawsswd>
   ```

   Zum Beispiel unter Linux:

   ```
   nmasinst -addmethod admin.sa.system TREE /home/user1/eDirectory/nmas/
   NmasMethods/Novell/SAML/config.txt -h 10.10.10.248:524 -w novell
   ```

   Zum Beispiel unter Windows:

   ```
   nmasinst.exe -addmethod admin.sa.system tree
   C:\Users\Administrator\Desktop\SAML\config.txt -h 10.10.10.248:524
   ```

4. Erweitern Sie das erforderliche Schema:

   ```
   ndssch -h <hostname:port> -t <treename> <admin dn> authsaml.sch
   ndssch -h <hostname:port> -t <treename> <admin dn> edirectory-schema.sch
   ndssch -h <hostname:port> -t <treename> <admin dn> osp.sch
   ```

   Beispiel:

   ```
   ndssch -h 10.10.10.248 -t TREE admin.sa.system authsaml.sch
   ```

5. Starten Sie eDirectory neu.

## 39.5 Neukonfigurieren der WAR-Datei für die Identitätsanwendungen

Mit dem RBPM-Konfigurationsprogramm können Sie die WAR-Datei für die Identitätsanwendungen aktualisieren.

1. Führen Sie die Datei `configupdate.sh` bzw. `configupdate.bat` für das Dienstprogramm im Installationsverzeichnis aus.

   Weitere Informationen zu den Parametern des Dienstprogramms finden Sie in Kapitel 40, „Konfigurieren der Einstellungen für die Identitätsanwendungen“, auf Seite 367.
2. Stellen Sie die neue WAR-Datei auf Ihrem Anwendungsserver bereit.

   Bei einem Tomcat-Einzelserver werden die Änderungen auf die bereitgestellte WAR-Datei angewendet.

# 39.6 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.



## 39.6.1 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:



### 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 40.1, „Ausführen des Konfigurationsprogramms der Identitätsanwendungen“, auf Seite 367.
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.

## 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. Weitere Informationen zum Konfigurationspasswort finden Sie in Kapitel 32, „Installieren der Passwortverwaltung für Identity Manager“, auf Seite 285.

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 360.

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.

## 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 auf`groupMembership=cn=Admins,ou=Groups,o=example` eingestellt.

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

   Damit wird verhindert, dass die Benutzer die Konfiguration in SSPR verändern; dies kann nur der SSPR-Admin-Benutzer erledigen, der die uneingeschränkten Rechte zum Bearbeiten der Einstellungen besitzt.

   **5b** Überprüfen Sie, ob die LDAP-Abfrage tatsächlich Ergebnisse zurückgibt. Klicken Sie hierzu auf **Übereinstimmungen anzeigen**.

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

   **5c** Klicken Sie auf **Speichern**.

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

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

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

7 Melden Sie sich bei SSPR ab.

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

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

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

## 39.6.2 Verwenden des bisherigen Anbieters für die „Passwort vergessen“-Verwaltung

Statt SSPR können Sie in Identity Manager auch den bisherigen Anbieter für die „Passwort vergessen“-Verwaltungsfunktion heranziehen. Wenn Sie sich für den bisherigen Anbieter entscheiden, entfällt die Installation von SSPR. In diesem Fall müssen Sie jedoch die Zugriffsrechte der Benutzer auf die freigegebenen Seiten für die Passwortverwaltung neu zuweisen. In diesem Abschnitt finden Sie die zugehörigen Schritte:

- „Konfigurieren des bisherigen Anbieters für die „Passwort vergessen“-Verwaltung“, auf Seite 362
- „Neuzuweisen der Berechtigungen für die Passwortverwaltungsseiten“, auf Seite 362

Weitere Informationen zum bisherigen Anbieter finden Sie in Abschnitt 4.4.2, „Erläuterungen zum bisherigen Anbieter für die Passwortverwaltung“, auf Seite 41. Weitere Informationen zu freigegebenen Seiten und Berechtigungen finden Sie unter „Seitenverwaltung“ im *NetIQ Identity Manager – Administratorhandbuch zu den Identitätsanwendungen*.

## Konfigurieren des bisherigen Anbieters für die „Passwort vergessen“-Verwaltung

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 40.1, „Ausführen des Konfigurationsprogramms der Identitätsanwendungen“, auf Seite 367.
3. Navigieren Sie im Dienstprogramm zu **Authentifizierung > Passwortverwaltung**.
4. Wählen Sie unter **Passwortverwaltungsanbieter** die Option **Benutzeranwendung (alt)**.
5. Wählen Sie unter **Passwort vergessen** die Option **Intern**
6. Navigieren Sie zu **SSO Clients > Zurücksetzen von Passwörtern per Selbstbedienung**.
7. Für die **USP für die OSP-Umleitung** sollte die Einstellung leer sein.
8. Speichern Sie die Änderungen, und schließen Sie das Dienstprogramm.

## Neuzuweisen der Berechtigungen für die Passwortverwaltungsseiten

Die Einstellungen für die Identitätsanwendungen werden während der Installation standardmäßig auf SSPR festgelegt. Sie müssen den Benutzern, Gruppen oder Containern, die auf die freigegebenen Seiten für die Passwort-Verwaltung zugreifen sollen, die entsprechenden Berechtigungen zuweisen oder neu zuweisen. Wenn Sie Benutzern die Berechtigung `Anzeigen` für eine Containerseite oder eine freigegebene Seite zuweisen, können sie auf diese Seite zugreifen, und die Seite wird in einer Liste der verfügbaren Seiten aufgeführt.

1. Stellen Sie sicher, dass Identity Manager den bisherigen Anbieter verwendet. Weitere Informationen finden Sie in „Konfigurieren des bisherigen Anbieters für die „Passwort vergessen“-Verwaltung“, auf Seite 362.
2. Melden Sie sich bei der Benutzeranwendung als Anwendungsadministrator an. Melden Sie sich beispielsweise als `uaadmin` an.
3. Navigieren Sie zu **Administration > Seitenadministration**.
4. Navigieren Sie in der Kontrollleiste **Freigegebene Seiten** zu **Passwortverwaltung**.
5. Wählen Sie die Seite aus, für die die Berechtigungen definiert werden sollen. Beispiel: „Passwort ändern“ oder „Herausforderung/Antwort für Passwort“.
6. Klicken Sie im rechten Bereich auf **Berechtigungen zuweisen**.
7. Wählen Sie unter **Anzeigen** die Benutzer, Gruppen oder Container aus, die der Seite zugewiesen werden sollen.
8. (Optional) Damit nur ein Anwendungsadministrator auf die angegebene Seite zugreifen kann, wählen Sie **Anzeigeberechtigung ist nur für Admin eingestellt**.
9. Klicken Sie auf **Speichern**.
10. Wiederholen Sie Schritt 5 bis Schritt 9 für jede zu konfigurierende Seite.
11. Wählen Sie das **Start**-Symbol, um zum Dashboard zurückzukehren.
12. Navigieren Sie zu **Anwendungen** und wählen Sie anschließend ⚙ aus.
13. Ersetzen Sie auf der Seite **Anwendungen verwalten** den Link zum SSPR durch den Link für UserApp PwdMgt.

Weitere Informationen finden Sie in Abschnitt 39.6.4, „Aktualisieren der SSPR-Links im Dashboard für eine dezentrale Umgebung oder eine Cluster-Umgebung“, auf Seite 364 und in der *Hilfe zu den Identitätsanwendungen*.

14 Melden Sie sich ab und starten Sie Tomcat neu.

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

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

- „Angeben einer externen WAR-Datei für die „Passwort vergessen“-Verwaltung“, auf Seite 363
- „Testen der externen „Passwort vergessen“-Konfiguration“, auf Seite 364
- „Konfigurieren der SSL-Kommunikation zwischen Anwendungsservern“, auf Seite 364

### 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 40.1, „Ausführen des Konfigurationsprogramms der Identitätsanwendungen“, auf Seite 367.

   **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 364.

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

### Testen der externen „Passwort vergessen“-Konfiguration

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

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

### Konfigurieren der SSL-Kommunikation zwischen Anwendungsservern

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

## 39.6.4 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.

# 40 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, mit der das Konfigurationsprogramm gestartet wird, befindet sich in der Regel in einem Installationsunterverzeichnis der Identitätsanwendungen:

- **Linux:** Skript `configupdate.sh`
- **Windows:** Datei `configupdate.bat`

---

**HINWEIS:** 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.



## 40.1 Ausführen des Konfigurationsprogramms der Identitätsanwendungen

1. Öffnen Sie unter Linux die Datei `configupdate.sh` (standardmäßig im Installationsverzeichnis der Benutzeranwendung: `/opt/netiq/idm/apps/UserApplication`) in einem Texteditor.
2. 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.

   ---

3. Speichern und schließen Sie die Datei `configupdate.sh`.

4 Starten Sie das Konfigurationsprogramm an der Eingabeaufforderung mit einem der folgenden Befehle:

- **Linux:** `./configupdate.sh`
- **Windows:** `configupdate.bat`

**HINWEIS:** Unter Umständen dauert das Starten des Dienstpogramms mehrere Minuten.

# 40.2 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:



## 40.2.1 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.

Weitere Informationen zur Verwendung von LDAP finden Sie in Abschnitt 8.5, „Kommunizieren mit dem Identitätsdepot über LDAP“, auf Seite 91.

**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. Weitere Informationen zur Verwendung von LDAP finden Sie in Abschnitt 8.5, „Kommunizieren mit dem Identitätsdepot über LDAP“, auf Seite 91.

**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.

---

## 40.2.2 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.

**Benutzercontainer-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 Benutzercontainers 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` bzw. `configupdate.bat` ändern.
- Der Benutzeranwendungsadministrator, den Sie beim Einrichten des Benutzeranwendungstreibers angegeben haben, muss sich in diesem Container befinden. Ansonsten kann das angegebene Konto keine Workflows ausführen.

**Gruppencontainer-DN**

*Erforderlich*

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

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

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

**Benutzeranwendungstreiber**

*Erforderlich*

Gibt den eindeutigen Namen für den Benutzeranwendungstreiber an.

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

**Benutzeranwendungsadministrator**

*Erforderlich*

Gibt an, dass ein vorhandenes Benutzerkonto im Identitätsdepot berechtigt ist, administrative Tätigkeiten für den in der Benutzeranwendung angegebenen Benutzercontainer 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` bzw. `configupdate.bat` ändern.
- Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten **Administration > Sicherheit** in der Benutzeranwendung geändert werden.
- Dieses Benutzerkonto ist berechtigt, das Portal über die Registerkarte **Administration** in der Benutzeranwendung zu verwalten.
- Wenn der Benutzeranwendungsadministrator Aufgaben zur Workflow-Administration bearbeitet, die in 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.

## 40.2.3 Identitätsdepot-Benutzeridentität

In diesem Abschnitt werden die Einstellungen für die Kommunikation der Identitätsanwendungen mit einem Benutzercontainer 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.

**Benutzercontainer-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 Benutzercontainers 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` bzw. `configupdate.bat` ändern.
- Der Benutzeranwendungsadministrator, den Sie beim Einrichten des Benutzeranwendungstreibers angegeben haben, muss sich in diesem Container befinden. Ansonsten kann das angegebene Konto keine Workflows ausführen.

**Benutzersuchbereich**

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

**Benutzerobjektklasse**

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

**Anmeldeattribut**

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

**Benennungsattribut**

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

**Benutzermitgliedschaftsattribut**

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

## 40.2.4 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` bzw. `configupdate.bat` ändern.

**Gruppencontainerbereich**

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

**Gruppenobjektklasse**

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

**Gruppenmitgliedschaftsattribut**

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

**Dynamische Gruppen verwenden**

Gibt an, ob dynamische Gruppen verwendet werden sollen.

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

**Klasse für dynamisches Gruppenobjekt**

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

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

## 40.2.5 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`.

## 40.2.6 Email-Serverkonfiguration

In diesem Abschnitt werden die Werte definiert, die E-Mail-Benachrichtigungen aktivieren; sie stehen für E-Mail-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 E-Mail“ 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 Portnummer von Tomcat an, auf dem die Identitätsanwendungen gehostet werden.

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

**Benachrichtigungsschablonenprotokoll**

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

Dieser Wert ersetzt das $PROTOCOL$-Token in E-Mail-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-E-Mails an. Beispiel: `https`.

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

**Benachrichtigungs-SMTP-Email von**

Gibt das E-Mail-Konto an, von dem aus die Identitätsanwendungen die E-Mail-Benachrichtigungen senden.

**SMTP-Servername**

Gibt die IP-Adresse oder den DNS-Namen des SMTP-E-Mail-Hosts an, den die Identitätsanwendungen für Bereitstellungs-E-Mails 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 E-Mail-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 E-Mail-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 E-Mail-Nachrichten bei der Übertragung zwischen Mailservern gesichert werden soll.

**Speicherort des E-Mail-Benachrichtigungsbilds**

Gibt den Pfad zum Image an, das in E-Mail-Benachrichtigungen gesendet werden soll. Beispiel: `http://localhost:8080/IDMProv/images`.

**E-Mail signieren**

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

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

**Keystore-Pfad**

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

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

Beispiel: `/opt/netiq/idm/apps/jre/lib/security/cacerts`.

**Keystore-Passwort**

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

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

**Alias des Signaturschlüssels**

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

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

**Signaturschlüsselpasswort**

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

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

## 40.2.7 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.

## 40.2.8 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 NetIQ 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 NetIQ 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.

## 40.2.9 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 insbesondere in einer Cluster-Umgebung eine eingeschränkte Leistung der Identitätsanwendungen zur Folge haben.
- Nach der Installation der Identitätsanwendungen können Sie diese Indizes manuell mit iManager erstellen. Weitere Informationen finden Sie in Abschnitt 39.4, „Konfigurieren des Identitätsdepots für die Identitätsanwendungen“, auf Seite 357.
- 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.

## 40.2.10 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.

## 40.3 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:



### 40.3.1 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 10.10.10.48.

**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-Keystore**

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

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**

*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.

## 40.3.2 Authentifizierungskonfiguration

In diesem Abschnitt werden die Einstellungen für den Authentifizierungsserver definiert.

**Endpunkt der OAuth-Serverauthentifizierung**

*Erforderlich*

Gibt die URL an, über die der OSP oder der Authentifizierungsserver ein Token für die Authentifizierung abrufen kann.

**Endpunkt des OAuth-Servertokens**

*Erforderlich*

Gibt die URL an, über die der OSP ein erhaltenes Token bestätigen kann.

**Endpunkt des OAuth-Servertokens**

*Erforderlich*

Gibt die URL an, über die der OSP die Sitzung mit dem Authentifizierungsserver beendet.

**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`.

**OAuth-Keystore-Datei**

*Erforderlich*

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**

*Erforderlich*

Gibt das Passwort an, mit dem die OAuth-Keystore-Datei geladen wird.

**Schlüsselalias für Schlüssel für OAuth**

*Erforderlich*

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**

*Erforderlich*

Gibt das Passwort für den privaten Schlüssel an, der vom Authentifizierungsserver verwendet wird.

**URL zur benutzerdefinierten CSS-Datei für Anmeldebildschirm**

Gibt die URL eines CSS-Stylesheets an, mit dem die Darstellung der Anmeldeseite für die Identitätsanwendungen angepasst werden soll.

**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.

**Gültigkeitsdauer für Zugriffstoken**

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

**Gültigkeitsdauer für Aktualisierungstoken**

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.

## 40.3.3 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.

Weitere Informationen zum OSP finden Sie in Abschnitt 4.5, „Verwenden des Single-Sign-On-Zugriffs in Identity Manager“, auf Seite 42 und Teil XI, „Installieren der Passwortverwaltungskomponente“, auf Seite 279.

**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:** 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.

## 40.3.4 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.

- **SSPR:** Verwendet die integrierte SSPR-Methode.

  Als Arbeitserleichterung ist SSPR im Installations-Kit enthalten. Weitere Informationen zu SSPR finden Sie in Abschnitt 4.4, „Verwenden von Self-Service Password Management in Identity Manager“, auf Seite 40 und Teil XI, „Installieren der Passwortverwaltungskomponente“, auf Seite 279.

- **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
```

### 40.3.5 Novell Audit-Digitalsignatur-Zertifikat und Schlüssel

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

**Zertifikat für NetIQ 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 NetIQ 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.

## 40.4 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:

- Abschnitt 40.4.1, „Portalseite“, auf Seite 384
- Abschnitt 40.4.2, „Dashboard“, auf Seite 384
- Abschnitt 40.4.3, „IDM-Dashboard“, auf Seite 386
- Abschnitt 40.4.4, „RBPM“, auf Seite 387
- Abschnitt 40.4.5, „Berichte“, auf Seite 387
- Abschnitt 40.4.6, „DCS-Treiber“, auf Seite 388
- Abschnitt 40.4.7, „Katalogadministrator“, auf Seite 388
- Abschnitt 40.4.8, „Zurücksetzen von Passwörtern per Selbstbedienung“, auf Seite 389

Weitere Informationen zum Konfigurieren des Single-Sign-On-Zugriffs finden Sie in Teil XV, „Konfiguration des Single-Sign-On-Zugriffs in Identity Manager“, auf Seite 443.

## 40.4.1 Portalseite

In diesem Abschnitt werden die Werte für die URL definiert, über die die Benutzer auf die Portalseite für die Identitätsanwendungen zugreifen. In der Regel leitet diese URL die Benutzer direkt zur Identity Manager-Startseite weiter.

---

**HINWEIS:** Ab Identity Manager 4.6 wird das Identity Manager-Dashboard durch das Basis- und Bereitstellungs-Dashboard von Identity Manager ersetzt. Solange diese noch nicht veraltet sind, werden sie weiterhin mit den Identitätsanwendungen installiert.

---

**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 `ualanding`.

**OAuth-Client-Geheimnis**

*Erforderlich*

Gibt das Passwort für den Single-Sign-On-Client für die Identity Manager-Startseite an.

**URL-Link zur Dash-Seite**

*Erforderlich*

Gibt die relative URL an, mit der Sie auf die Identity Manager-Startseite zugreifen. Der Standardwert lautet `/dash`.

**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: `http://10.10.10.48:8180/dash/com.netiq.test`.

## 40.4.2 Dashboard

In diesem Abschnitt werden die Werte für die URL definiert, über die die Benutzer auf die Portalseite für die Identitätsanwendungen zugreifen. Normalerweise werden Benutzer durch diese URL zum Bereitstellungs-Dashboard geleitet.

---

**HINWEIS:** Ab Identity Manager 4.6 wird das Identity Manager-Dashboard durch das Basis- und Bereitstellungs-Dashboard von Identity Manager ersetzt. Solange diese noch nicht veraltet sind, werden sie weiterhin mit den Identitätsanwendungen installiert.

---

**OAuth-Client-ID**

*Erforderlich*

Gibt den Namen an, mit dem sich der Single-Sign-On-Client für das Identity Manager-Bereitstellungs-Dashboard beim Authentifizierungsserver anmelden soll. Der Standardwert lautet `uadash`.

**OAuth-Client-Geheimnis**

*Erforderlich*

Gibt das Passwort für den Single-Sign-On-Client für das Identity Manager-Bereitstellungs-Dashboard an.

**OAuth-Umleitungs-URL**

*Erforderlich*

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

Hierbei gilt das folgende Format: `Protokoll://Server:Port/Pfad`. Beispiel: `http://10.10.10.48:8180/dash/com.netiq.test`.

**eMail-Adresse des Benutzers**

*Erforderlich*

Gibt den Wert an, mit dem das rollenbasierte Bereitstellungsmodul das Attribut für die E-Mail-Adresse eines Benutzers in den REST-API-Ergebnissen zu den Benutzerinformationen identifiziert.

Dieser Wert muss mit den in Designer konfigurierten Entitäten übereinstimmen. Der Standardwert lautet `Email`.

**Benutzer – Telefon**

*Erforderlich*

Gibt den Wert an, mit dem das rollenbasierte Bereitstellungsmodul das Attribut für die Telefonnummer eines Benutzers in den REST-API-Ergebnissen zu den Benutzerinformationen identifiziert.

Dieser Wert muss mit den in Designer konfigurierten Entitäten übereinstimmen. Der Standardwert lautet `TelephoneNumber`.

**Benutzer – Mobiltelefon**

*Erforderlich*

Gibt den Wert an, mit dem das rollenbasierte Bereitstellungsmodul das Attribut für die Mobiltelefonnummer eines Benutzers in den REST-API-Ergebnissen zu den Benutzerinformationen identifiziert.

Dieser Wert muss mit den in Designer konfigurierten Entitäten übereinstimmen. Der Standardwert lautet `MobileNumber`.

**Benutzer – Vorname**

*Erforderlich*

Gibt den Wert an, mit dem das rollenbasierte Bereitstellungsmodul das Attribut für den Vornamen eines Benutzers in den REST-API-Ergebnissen zu den Benutzerinformationen identifiziert.

Dieser Wert muss mit den in Designer konfigurierten Entitäten übereinstimmen. Der Standardwert lautet `FirstName`.

**Benutzer – Standort**

*Erforderlich*

Gibt den Wert an, mit dem das rollenbasierte Bereitstellungsmodul das Attribut für den Standort eines Benutzers in den REST-API-Ergebnissen zu den Benutzerinformationen identifiziert.

Dieser Wert muss mit den in Designer konfigurierten Entitäten übereinstimmen. Der Standardwert lautet `Location`.

**Benutzer – Abteilung**

*Erforderlich*

Gibt den Wert an, mit dem das rollenbasierte Bereitstellungsmodul das Attribut für die Abteilung eines Benutzers in den REST-API-Ergebnissen zu den Benutzerinformationen identifiziert.

Dieser Wert muss mit den in Designer konfigurierten Entitäten übereinstimmen. Der Standardwert lautet `Department`.

**Benutzer – Nachname**

*Erforderlich*

Gibt den Wert an, mit dem das rollenbasierte Bereitstellungsmodul das Attribut für den Nachnamen eines Benutzers in den REST-API-Ergebnissen zu den Benutzerinformationen identifiziert.

Dieser Wert muss mit den in Designer konfigurierten Entitäten übereinstimmen. Der Standardwert lautet `LastName`.

**Benutzer – Titel**

*Erforderlich*

Gibt den Wert an, mit dem das rollenbasierte Bereitstellungsmodul das Attribut für den Titel eines Benutzers in den REST-API-Ergebnissen zu den Benutzerinformationen identifiziert.

Dieser Wert muss mit den in Designer konfigurierten Entitäten übereinstimmen. Der Standardwert lautet `Title`.

## 40.4.3 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.

**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: `http://10.10.10.48:8180/idmdash/oauth.html`.

## 40.4.4 RBPM

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

**OAuth-Client-ID**

*Erforderlich*

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

**OAuth-Client-Geheimnis**

*Erforderlich*

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

**URL-Link zur Portalseite**

*Erforderlich*

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

**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: `http://10.10.10.48:8180/IDMProv/oauth`.

## 40.4.5 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.

**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 `/dashboard`.

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`.

**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: `http://10.10.10.48:8180/IDMRPT/oauth`.

## 40.4.6 DCS-Treiber

In diesem Abschnitt werden die Werte für die Verwaltung des Treibers für den Datenerfassungsdienst (DCS-Treiber) definiert. Weitere Informationen zum Treiber finden Sie in Kapitel 44, „Verwalten der Treiber für die Berichterstellung“, auf Seite 409.

**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.

## 40.4.7 Katalogadministrator

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

**OAuth-Client-ID**

*Erforderlich*

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

**OAuth-Client-Geheimnis**

*Erforderlich*

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

**URL-Link zur Portalseite**

*Erforderlich*

Gibt die relative URL an, mit der Sie vom Katalogadministrator aus auf das Dashboard zugreifen. Der Standardwert lautet `/dashboard`.

**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: `http://10.10.10.48:8180/rra/com.netiq.test`.

### 40.4.8 Zurücksetzen von Passwörtern per Selbstbedienung

In diesem Abschnitt werden die Werte für die Kommunikation der Identitätsanwendungen mit SSPR definiert.

**OAuth-Client-ID**

*Erforderlich*

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

**OAuth-Client-Geheimnis**

*Erforderlich*

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

**OAuth-Umleitungs-URL**

*Erforderlich*

Gibt die absolute URL an, zu der der Client weitergeleitet wird, wenn Vorgänge wie eine Änderung des Passworts oder der Challenge-Fragen in SSPR erfolgt sind. Beispielsweise Weiterleitung zum Dashboard.

Hierbei gilt das folgende Format: `Protokoll://Server:Port/Pfad`. Beispiel: `http://10.10.10.48:8180/sspr/public/oauth`.

## 40.5 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:

- Abschnitt 40.5.1, „E-Mail-Lieferkonfiguration“, auf Seite 389
- Abschnitt 40.5.2, „Berichtbeibehaltungswerte“, auf Seite 390
- Abschnitt 40.5.3, „Gebietsschema bearbeiten“, auf Seite 390
- Abschnitt 40.5.4, „Rollenkonfiguration“, auf Seite 390

### 40.5.1 E-Mail-Lieferkonfiguration

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

**SMTP-Server-Host**

Gibt den DNS-Namen oder die IP-Adresse des E-Mail-Servers an, über den die Identitätsberichterstellung die Benachrichtigungen senden soll. Verwenden Sie nicht `localhost`.

**Port des SMTP-Servers**

Gibt die Portnummer für den SMTP-Server an.

**SMTP mit SSL**

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

**Authentifizierung für Server erforderlich**

Gibt an, ob für die Kommunikation mit dem E-Mail-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 E-Mail-Adresse**

Gibt die E-Mail-Adresse an, die die Identitätsberichterstellung als Absender für E-Mail-Benachrichtigungen verwenden soll.

## 40.5.2 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. Geben Sie beispielsweise für einen Zeitraum von sechs Monaten den Wert `6` ein, und wählen Sie die Option **Monat**.

**Speicherort der Berichte**

Gibt einen Pfad an, in dem die Berichtsdefinitionen gespeichert werden sollen. Beispiel: `/opt/netiq/IdentityReporting`.

## 40.5.3 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*.

## 40.5.4 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**

# XIII Installieren der Identitätsberichterstellung

In diesem Abschnitt finden Sie die Schritte für die Installation der erforderlichen Komponenten zum Ausführen von Berichten. Der Installationsvorgang umfasst alle erforderlichen Komponenten für die Anwendung:

- NetIQ-Identitätsberichterstellung
- Identity Manager-Treiber „Verwaltetes System – Gateway“ (MSGW-Treiber)
- Identity Manager-Treiber für den Datenerfassungsdienst (DCS-Treiber)

Die Installationsdateien befinden sich im Verzeichnis `products/Reporting` in der `.iso`-Image-Datei des Identity Manager-Installationspakets. Standardmäßig installiert das Installationsprogramm die Komponenten in den folgenden Speicherorten:

- **Linux:** `/opt/netiq/idm/apps/IDMReporting`
- **Windows**: `C:\NetIQ\idm\apps\IDMReporting`

Als Arbeitserleichterung enthält das Installations-Kit von Identity Manager bereits Sentinel Log Management für IGA (Sentinel) zur Verwendung als integrierter Revisionsdienst. Weitere Informationen finden Sie unter „Installieren und Verwalten von Sentinel for Log Management für Identity Governance and Administration“, auf Seite 129.

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie in Kapitel 41, „Planen der Installation der Identitätsberichterstellung“, auf Seite 393.

# 41 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.



## 41.1 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 33. |
| ❑ | 2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |
| ❑ | 3. Lesen Sie die Überlegungen zur Installation der Identitätsberichterstellung. Weitere Informationen finden Sie in Abschnitt 41.3, „Voraussetzungen für die Installation der Komponenten für die Identitätsberichterstellung“, auf Seite 395. |
| ❑ | 4. Prüfen Sie die Hardware- und Software-Voraussetzungen der Computer, auf denen die Identitätsberichterstellung gehostet werden soll. Weitere Informationen finden Sie in Abschnitt 41.4, „Systemanforderungen für die Identitätsberichterstellung“, auf Seite 397. |
| ❑ | 5. (Bedingt) Zur geführten Installation auf Computern mit dem Betriebssystem SLES 12 SP1 (oder höher) müssen die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in Abschnitt 6.3, „Installieren von Identity Manager auf Servern mit SLES 12 SP1 (oder höher)“, auf Seite 63. |
| ❑ | 6. (Bedingt) Stellen Sie bei Computern mit RHEL 6.x- oder Rhel 7.x-Betriebssystem sicher, dass die erforderlichen Bibliotheken installiert sind. Weitere Informationen finden Sie in Abschnitt 6.4, „Installieren von Identity Manager auf einem RHEL 6.*x- oder 7.x-Server“, auf Seite 63*. |
| ❑ | 7. Stellen Sie sicher, dass die Identitätsanwendungen installiert sind. Weitere Informationen finden Sie in Kapitel 33, „Planen der Installation der Identitätsanwendungen“, auf Seite 297. |
| ❑ | 8. Installieren Sie Sentinel. Weitere Informationen finden Sie in Abschnitt 14, „Installieren von Sentinel“, auf Seite 135 |

| | Checkliste |
|---|---|
| ❑ | 9. Stellen Sie sicher, dass auf dem Server, auf dem die Identitätsberichterstellung installiert werden soll, ein Anwendungsserver vorliegt (z. B. Tomcat). Weitere Informationen finden Sie in Kapitel 28, „Installieren von PostgreSQL und Tomcat“, auf Seite 261. |
| ❑ | 10. (Bedingt) Sollen die Ereignisse mit dem Apache Log4j-Dienst in Tomcat festgehalten werden, stellen Sie sicher, dass die entsprechenden Dateien vorliegen. Weitere Informationen finden Sie in Abschnitt 29.4, „Protokollieren der Anmeldung mit dem Apache-Log4j-Dienst“, auf Seite 271. |
| ❑ | 11. Installieren Sie die Identitätsberichterstellung:<br>◆ Anweisungen zur geführten Installation finden Sie in Abschnitt 42.1, „Geführte Installation der Identitätsberichterstellung“, auf Seite 399.<br>◆ Anweisungen zur automatischen Installation der Berichterstellung finden Sie in Abschnitt 42.2, „Automatische Installation der Identitätsberichterstellung“, auf Seite 404. |
| ❑ | 12. Richten Sie die Identitätsberichterstellung vollständig ein. Weitere Informationen finden Sie in Kapitel 43, „Konfigurieren der Identitätsberichterstellung“, auf Seite 407. |
| ❑ | 13. Konfigurieren Sie den Treiber „Verwaltetes System – Gateway“ (MSGW-Treiber) und den Treiber für den Datenerfassungsdienst (DCS-Treiber). Weitere Informationen finden Sie in Abschnitt 44.1, „Konfigurieren von Treibern für die Identitätsberichterstellung“, auf Seite 409. |
| ❑ | 14. Stellen Sie die Treiber bereit, und starten Sie sie. Weitere Informationen finden Sie in Abschnitt 44.2, „Bereitstellen und Starten von Treibern für die Identitätsberichterstellung“, auf Seite 415. |
| ❑ | 15. Konfigurieren Sie die Umgebung für die Treiber. Weitere Informationen finden Sie in Abschnitt 44.3, „Konfigurieren der Laufzeitumgebung“, auf Seite 420. |
| ❑ | 16. Konfigurieren Sie Identity Manager und eDirectory für das Senden von Daten an die Treiber. Weitere Informationen finden Sie in Abschnitt 44.4, „Festlegen von Revisions-Flags für den Treiber“, auf Seite 429. |

## 41.2 Erläuterungen zum Installationsvorgang für die Komponenten der Identitätsberichterstellung

Sie können Sentinel, die Identitätsberichterstellung und die Berichterstellungstreiber auf demselben Server installieren. Angesichts der Auslastung empfiehlt NetIQ jedoch, Sentinel und die Berichterstellung auf separaten Servern zu installieren. Weitere Informationen finden Sie unter Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51.

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:

- Auswahl einer Anwendungsserverplattform
- Bereitstellen der Client-WAR-Datei mit den Benutzeroberflächenkomponenten für die Berichterstellung auf Tomcat
- Bereitstellen der Kern-WAR-Datei mit den erforderlichen Kern-REST-Diensten für die Berichterstellung

- Bereitstellen der API-WAR-Datei mit der Dokumentation zu den erforderlichen REST-Diensten für die Berichterstellung
- Konfigurieren der Authentifizierungsdienste für die Identitätsberichterstellung
- Konfigurieren des E-Mail-Zustellungssystems für die Identitätsberichterstellung
- Konfigurieren der Kernberichterstellungsdienste für die Identitätsberichterstellung
- Erstellen der Benutzerkonten für die Identitätsberichterstellung (**idmrptsrv** und **idmrptuser**)
- Erstellen der Benutzerkonten für die Interaktion mit Sentinel (**appuser** und **rptuser**)

## 41.3 Voraussetzungen für die Installation der Komponenten für die Identitätsberichterstellung

NetIQ empfiehlt, die nachfolgenden Voraussetzungen und Überlegungen zu lesen, bevor Sie den Installationsvorgang beginnen.

- Abschnitt 41.3.1, „Voraussetzungen für die Identitätsberichterstellung“, auf Seite 395

### 41.3.1 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)
  - Sentinel ist auf einem separaten Linux-Computer installiert.
  - Treiber für den Datenerfassungsdienst
  - Treiber für den Dienst „Verwaltetes System – Gateway“

  Weitere Informationen zu den erforderlichen Versionen und Patches für diese Komponenten finden Sie in den aktuellen Versionshinweisen. Weitere Informationen zum Installieren der Treiber finden Sie in Kapitel 44, „Verwalten der Treiber für die Berichterstellung“, auf Seite 409.
- Das Identitätsdepot muss das SecretStore-Modul enthalten und das Modul muss konfiguriert sein. Weitere Informationen finden Sie unter Abschnitt 12.1.2, „Hinzufügen von SecretStore zum Identitätsdepotschema“, auf Seite 123.
- Installieren Sie die Identitätsberichterstellung nicht auf einem Server in einer Cluster-Umgebung.
- (Bedingt) Sollen Berichte über eine Oracle 12c-Datenbank ausgeführt werden, müssen Sie die entsprechende JDBC-Datei installieren. Weitere Informationen finden Sie unter Abschnitt 43.1, „Ausführen von Berichten über eine Oracle-Datenbank“, auf Seite 407.
- (Bedingt) Bei Bedarf können Sie Ihr eigenes Tomcat-Installationsprogramm anstelle des Programms im Installations-Kit von Identity Manager verwenden. Wenn Sie allerdings den Apache Log4j-Dienst zusammen mit Ihrer Tomcat-Version nutzen möchten, überprüfen Sie, ob die entsprechenden Dateien installiert sind. Weitere Informationen finden Sie in Abschnitt 29.4, „Protokollieren der Anmeldung mit dem Apache-Log4j-Dienst“, auf Seite 271.
- 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.

  Standardmäßig legt das Schnellinstallationsprogramm für Tomcat die Datei `setenv.sh` im Verzeichnis `/opt/netiq/idm/apps/tomcat/bin/` ab. Das Installationsprogramm konfiguriert außerdem den JRE-Speicherort in der Datei.

- (Optional) Sie können die Identitätsberichterstellung für die Verwendung von NetIQ Access Manager 4.0 über die SAML 2.0-Authentifizierung konfigurieren. Weitere Informationen finden Sie unter Kapitel 49, „Single Sign-On per SAML-Authentifizierung mit NetIQ Access Manager“, auf Seite 451.

## 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:<br>◆ Authenticate<br>◆ Passwort ändern<br>◆ Passwort entsperren<br>◆ Passwort wiederherstellen<br>◆ Unbefugter Zugriffsversuch<br>◆ Sperre gegen unbefugten Zugriff<br>◆ Benutzer mit Sperre gegen unbefugten Zugriff<br>**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:<br>◆ Passwort ändern<br>◆ Passwort bestätigen<br>◆ Anmelden<br>◆ Abmelden |

| Ereignisname | Revisions-Flag |
|---|---|
| Alle anderen Berichterstellungsereignisse | Wählen Sie in der **NetIQ Identity Manager-Benutzeranwendung** die Option **Administration** > **Protokollierung** > **Auditdienst aktivieren** |

## 41.4 Systemanforderungen für die Identitätsberichterstellung

In diesem Abschnitt finden Sie die Mindestanforderungen für die Server, auf denen die Identitätsberichterstellungskomponenten installiert werden sollen. Weitere Informationen dazu, ob die Komponenten auf demselben Server installiert werden sollten, finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51.

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

| Kategorie | Anforderung |
|---|---|
| Prozessor | Pentium* III 600-MHz-Prozessor |
| Festplattenspeicher | 1 GB<br><br>**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:<br><br>◆ Open Enterprise Server 2015 SP1<br>◆ Open Enterprise Server 11 SP2<br>◆ Red Hat Enterprise Linux 7.2<br>◆ Red Hat Enterprise Linux 7.1<br>◆ Red Hat Enterprise Linux 7.0<br>◆ SUSE Linux Enterprise Server 12 SP1<br>◆ SUSE Linux Enterprise Server 11 SP4<br>◆ Windows Server 2012 R2<br><br>NetIQ empfiehlt, vor der Installation von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden.<br><br>**HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird. |
| Betriebssystem (unterstützt) | Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme<br><br>**HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert. |

| Kategorie | Anforderung |
|---|---|
| Virtualisierungssystem | ◆ Hyper-V Server 2012 R2<br>◆ VMWare ESX 5.5 und höher<br>◆ Windows Server 2012 R2-Virtualisierung mit Hyper-V (unterstützt)<br>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 | Die Berichterstellungsdatenbank kann auf der folgenden Plattform ausgeführt werden (ggf. höhere Version):<br>◆ PostgreSQL 9.6.x<br>Sie können Berichte über die folgenden Datenbanken (ggf. höhere Version) ausführen:<br>◆ Oracle 12c<br>◆ PostgreSQL 9.6.x |
| Anwendungsserver | Apache Tomcat 8.5.x |
| Java | Java Development Kit (JDK)<br>Alternativ:<br>Java-Laufzeitumgebung (JRE) Version 1.8.0_112 (oder höher) von Sun (Oracle) |
| Webbrowser | Einer der folgenden Browser (ggf. höhere Version):<br>**Desktop**<br>◆ Apple Safari 7.0.1<br>◆ Apple Safari 5.1.7 für Windows<br>◆ Google Chrome 51<br>◆ Microsoft Internet Explorer 11<br>◆ Mozilla Firefox 47<br>**iPad**<br>◆ Apple Safari 7<br>◆ Google Chrome 51<br>**HINWEIS:** Es müssen Cookies im Browser aktiviert sein. Wenn Cookies deaktiviert sind, ist das Produkt nicht funktionsfähig. |
| Revision | Sentinel Log Management für IGA |

# 42 Installieren der Identitätsberichterstellung

In diesem Kapitel wird die Installation der Identitätsberichterstellung beschrieben.



## 42.1 Geführte Installation der Identitätsberichterstellung

Im Folgenden wird beschrieben, wie Sie die Identitätsberichterstellung mithilfe eines Installationsassistenten installieren (wahlweise über die Benutzeroberfläche oder an der Konsole). Anweisungen für die automatische, unbeaufsichtigte Installation finden Sie in Abschnitt 42.2, „Automatische Installation der Identitätsberichterstellung“, auf Seite 404.

Überprüfen Sie in Vorbereitung auf die Installation die Voraussetzungen und Systemanforderungen in Abschnitt 41.4, „Systemanforderungen für die Identitätsberichterstellung“, auf Seite 397. Beachten Sie auch die Versionshinweise zur betreffenden Version.

1. Melden Sie sich an dem Computer an, auf dem die Identitätsberichterstellung installiert werden soll.
2. Halten Sie Tomcat an.
3. (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die Installationsdateien für die Identitätsberichterstellung befinden (standardmäßig unter `products/Reporting/`).
4. (Bedingt) Wenn Sie die Installationsdateien für die Identitätsberichterstellung von der NetIQ Downloads-Website heruntergeladen haben, führen Sie die folgenden Schritte aus:
   - **4a** Navigieren Sie zur `.tgz`-Datei für das heruntergeladene Image.
   - **4b** Extrahieren Sie den Inhalt der Datei in einen Ordner auf dem lokalen Computer.
5. Führen Sie im Verzeichnis mit den Installationsdateien einen der folgenden Schritte aus:
   - **Linux (Konsole)** – Geben Sie Folgendes ein: `/rpt-install.bin -i console`
   - **Linux (Benutzeroberfläche)** – Geben Sie Folgendes ein: `/rpt-install.bin`
   - **Windows** – Führen Sie die folgende Datei aus: `rpt-install.exe`
6. Legen Sie im Installationsprogramm die gewünschte Sprache für die Installation fest, und klicken Sie auf **OK**.
7. Lesen Sie den Einführungstext, und klicken Sie auf **Weiter**.
8. Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
9. Führen Sie die geführte Installation mit den folgenden Parametern aus:
   - **Installationsordner**

Gibt den Pfad zu einem Verzeichnis an, in dem das Installationsprogramm die Anwendungsdateien erstellt, z. B. Installationsprotokolldateien, Hilfsskripte und Konfigurationsskripte.

- **Berichterstellungseinrichtung**

  Gbit die Umgebung, in der die Identitätsberichterstellung erfolgen soll, und die zugehörigen Einstellungen an. Für **Identity Manager** geben Sie die folgenden Werte an:

  ***Identitätsdepot-Server***

  Gibt den Hostnamen des eDirectory-Servers an.

  ***Sicherer LDAP-Port***

  Gibt den Port an, über den eine LDAP-Verbindung zum eDirectory-Server per SSL hergestellt werden soll. Der Standardport ist 636.

- **Anwendungsserver-Details**

  Gibt Tomcat an, auf dem die Identitätsberichterstellung ausgeführt werden soll. Der Anwendungsserver muss bereits installiert sein.

  ***Sekundär***

  Gibt an, ob sich die aktuelle Installation auf einem sekundären Clusterknoten befindet.

  ***Tomcat-Stammordner***

  Gibt den Pfad zur Tomcat-Instanz an. Beispiel: `/opt/netiq/idm/apps/tomcat`.

  ***Java JRE-Basisordner***

  Gibt den Speicherort des Java JRE-Basisordners an.

  Der Pfad enthält eine Datei mit dem Konfigurationsaktualisierungsprogramm; er wird zum Starten dieses Dienstprogramms nach der Installation der Identitätsberichterstellung verwendet.

- **Anwendungsadresse**

  Gibt die Einstellungen für den Server an, auf dem die Datenbank gehostet wird.

  ***Protokoll***

  Gibt an, ob *http* oder *https* verwendet werden soll. Soll die Kommunikation per SSL erfolgen, wählen Sie `https`.

  ***Hostname***

  Gibt den DNS-Namen oder die IP-Adresse von Tomcat an. Verwenden Sie nicht `localhost`.

  ***Port***

  Gibt den Port an, über den Tomcat mit Identity Manager kommunizieren soll.

  ***Mit externen Authentifizierungsserver verbinden***

  Gibt an, ob der Authentifizierungsserver (OSP) auf einer Tomcat-Instanz gehostet wird. Auf dem Authentifizierungsserver befindet sich eine Liste der Benutzer, die sich bei der Identitätsberichterstellung anmelden können.

  Wenn Sie diese Einstellung wählen, müssen Sie außerdem Werte für **Protokoll**, **Hostname** und **Port** für den Authentifizierungsserver angeben.

- **Authentifizierungsserver-Details**

  Gibt das Passwort für den Identitätsberichterstellungsdienst an.

  Mit diesem Passwort stellt Identity Manager die Verbindung zum OSP-Client auf dem Authentifizierungsserver her.

- **Datenbankdetails**

Gibt die Einstellungen für die Berichterstellungsdatenbank an, z. B. ob im Installationsvorgang gleich die Datenbank angelegt oder eine SQL-Datei zur späteren Erstellung der Datenbank erzeugt werden soll.

***Datenbankname***

Geben Sie den Datenbanknamen gemäß Ihren Anforderungen an:

- **Neue Berichterstellungsinstallation**

  Geben Sie den Namen Ihrer Berichterstellungsdatenbank an. Beispiel: `idmrptdb` oder `SIEM`.

- **Migration von EAS**

  Geben Sie den Namen der EAS-Datenbank an, z. B. `SIEM`.

***Datenbank-Host***

Geben Sie den Datenbankhost gemäß Ihren Anforderungen an:

- **Neue Berichterstellungsinstallation**

  Geben Sie den DNS-Namen oder die IP-Adresse des Servers an, auf dem die Datenbank erstellt werden soll.

- **Migration von EAS**

  Geben Sie den DNS-Namen oder die IP-Adresse des Servers an, auf dem die `SIEM`-Datenbank gehostet wird.

***Datenbanktyp***

Wählen Sie die zu verwendende Datenbank aus.

Geben Sie außerdem die folgenden Details an, wenn Sie **Oracle** auswählen:

- **JAR-Datei des JDBC-Treibers**

  Gibt den Pfad zur JAR-Datei für den JDBC-Oracle-JDBC-Treiber an. Beispiel: `opt\oracl\ojdbc7.jar`.

  Weitere Informationen finden Sie in Abschnitt 43.1, „Ausführen von Berichten über eine Oracle-Datenbank“, auf Seite 407.

- **JDBC-Treiberklassenname**

  Gibt die Klasse des JDBC-Treibers an.

- **JDBC-Treibertyp**

  Gibt den Typ des JDBC-Treibers an.

***Passwort freigeben***

Hiermit können Sie ein einzelnes Passwort für alle Berichterstellungsbenutzer angeben, wenn diese sich mit der Datenbank verbinden.

***Geben Sie ein Kennwort an.***

Hiermit können Sie ein eindeutiges Passwort für jeden Berichterstellungsbenutzer der Datenbank angeben.

***Datenbank-Port***

Gibt den Port für die Verbindung mit der Datenbank an. Der Standardport hat die Nummer 5432.

***Datenbank jetzt oder beim Start konfigurieren***

Gibt an, dass Ihnen die Anmeldeeinstellungen für die Datenbank vorliegen, sodass das Installationsprogramm die Datenbank sofort oder beim Starten der Berichterstellung anlegen kann. Sie müssen außerdem die folgenden Werte angeben:

- **DBA-Benutzer-ID**

*Gilt nur, wenn Sie die Option* **Datenbank jetzt oder beim Starten konfigurieren** *wählen.*

Gibt den Namen des Verwaltungskontos für den SIEM-Datenbankserver an. Beispiel: *postgres*

- **DBA-Passwort**

  *Gilt nur, wenn Sie die Option* **Datenbank jetzt oder beim Starten konfigurieren** *wählen.*

  Gibt das Passwort des Administratorkontos für die Datenbank an.

***Generate SQL for later* (SQL für später generieren)**

Weist das Installationsprogramm an, eine SQL-Datei zu erzeugen, mit der der Datenbankadministrator die Datenbank nach Abschluss des Installationsvorgangs erstellt.

***Datenbankverbindung testen***

Gibt an, ob das Installationsprogramm die für die Datenbank angegebenen Werte testen soll.

Sobald Sie auf **Weiter** klicken oder die **Eingabetaste** drücken, versucht das Installationsprogramm, die Verbindung aufzubauen.

---

**HINWEIS:** Falls ein Fehler bei der Datenbankverbindung auftritt, können Sie die Installation dennoch fortsetzen. Nach der Installation müssen Sie jedoch manuell die Tabellen erstellen und die Verbindung zur Datenbank herstellen. Weitere Informationen finden Sie unter Abschnitt 42.3, „Manuelles Erstellen des Datenbankschemas“, auf Seite 405.

---

- **Standardsprache**

  Gibt die Sprache für Suchvorgänge in der Identitätsberichterstellung an.

- **Identitätsdepot-Berechtigungsnachweis**

  Gibt die Einstellungen an, mit denen die Identitätsberichterstellung eine Verbindung zum Identitätsdepot herstellt.

  ***Identitätsdepot-Administrator***

  Gibt den eindeutigen Namen des LDAP-Administrators an. Beispielsweise `cn=admin`. Dieser Benutzer muss bereits im Identitätsdepot vorhanden sein.

  ***Identitätsdepot-Administratorpasswort***

  Gibt das Passwort für den Identitätsdepot-Administrator an.

  **Keystore-Pfad**

  Gibt den vollständigen Pfad zur Keystore-Datei (`cacerts`) der JRE an, mit der Tomcat ausgeführt wird.

  ***Keystore-Passwort***

  Gibt das Passwort für die Keystore-Datei an.

  ***Container-DN der Berichtsadministratorrolle***

  Geben Sie den DN des Containers an, in dem die Berichtsystemadministratorrolle gespeichert ist.

  ***DN des Berichtsadministratorbenutzers***

  Gibt ein vorhandenes Benutzerkonto im Identitätsdepot an, das berechtigt ist, administrative Tätigkeiten für die Identitätsberichterstellung auszuführen.

- **E-Mail-Zustellung**

Gibt die Einstellungen für den SMTP-Server an, der die Berichtsbenachrichtigungen sendet. Mit dem RBPM-Konfigurationsprogramm können Sie diese Einstellungen nach der Installation bearbeiten.

***Standardmäßige E-Mail-Adresse***

Gibt die E-Mail-Adresse an, die die Identitätsberichterstellung als Absender für E-Mail-Benachrichtigungen verwenden soll.

***SMTP-Server***

Gibt die IP-Adresse oder den DNS-Namen des SMTP-E-Mail-Hosts an, den die Identitätsberichterstellung für Bereitstellungs-E-Mails verwendet. Verwenden Sie nicht `localhost`.

***SMTP-Server-Port***

Gibt die Portnummer für den SMTP-Server an. Der Standardport ist 465.

***SSL für SMTP verwenden***

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

***Authentifizierung für Server erforderlich***

Gibt an, ob die Kommunikation mit dem SMTP-Server authentifiziert werden soll. Sie müssen außerdem die folgenden Werte angeben:

- ***SMTP-Benutzername***

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

- ***SMTP-Passwort***

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

- **Berichtsdetails**

Gibt die Einstellungen für Berichtdefinitionen und abgeschlossene Berichte an.

***Abgeschlossene Berichte speichern für***

Gibt den Zeitraum an, über den die abgeschlossenen Berichte in der Identitätsberichterstellung beibehalten werden sollen, bevor sie gelöscht werden.

Geben Sie beispielsweise für einen Zeitraum von sechs Monaten den Wert 6 ein, und wählen Sie die Option **Monat**.

***Speicherort für Berichtsdefinitionen***

Gibt einen Pfad an, in dem die Berichtsdefinitionen gespeichert werden sollen.

Beispiel: `/opt/netiq/IdentityReporting`.

- **Novell Identity Audit**

Gibt die Einstellungen für das Senden von Protokollereignissen an einen Revisionsserver an.

NetIQ stellt Sentinel Log Management für IGA als Arbeitserleichterung bereit.

***Revision für Identitätsberichterstellung aktivieren***

Gibt an, ob die Protokollereignisse an einen Audit-Server gesendet werden sollen.

***Audit Server***

*Gilt nur dann, wenn Sie die Option* **Revision für Identitätsberichterstellung aktivieren** *wählen.*

Geben Sie den Hostnamen des Revisionsservers an; es handelt sich dabei um die IP, unter der Sentinel gehostet wird.

***Cache-Ordner für Audit-Protokoll***

*Gilt nur dann, wenn Sie die Option* **Revision für Identitätsberichterstellung aktivieren** *wählen.*

Geben Sie den Speicherort des Cache-Verzeichnisses für die Revision an. Beispiel: `/opt/novell/Identity Reporting`.

---

**HINWEIS:** Die Protokollierungsereignis-Datei muss gültige Pfade für das Cache-Verzeichnis und die Datei `nauditpa.jar` enthalten. Falls diese Einstellungen nicht ordnungsgemäß konfiguriert sind, wird die Identitätsberichterstellung nicht gestartet.

---

***Vorhandenes Zertifikat angeben/Zertifikat erzeugen***

*Gilt nur dann, wenn Sie die Option „Revision für Identitätsberichterstellung aktivieren“ wählen.*

Gibt an, ob ein vorhandenes Zertifikat für den NAudit Server verwendet oder ein neues Zertifikat erstellt werden soll.

***Öffentlichen Schlüssel eingeben***

*Gilt nur dann, wenn ein vorhandenes Zertifikat verwendet werden soll.*

Geben Sie das benutzerdefinierte Zertifikat mit öffentlichem Schlüssel an, mit dem der NAudit-Dienst die gesendeten Revisionsmeldungen authentifiziert.

***RSA-Schlüssel eingeben***

*Gilt nur dann, wenn ein vorhandenes Zertifikat verwendet werden soll.*

Geben Sie den Pfad zur benutzerdefinierten Datei mit dem privaten Schlüssel an, mit dem der NAudit-Dienst die gesendeten Revisionsmeldungen authentifiziert.

10 Klicken Sie im Fenster „Übersicht vor der Installation“ auf **Installieren**.

## 42.2 Automatische Installation der Identitätsberichterstellung

Bei der automatischen (nicht interaktiven) Installation wird keine Benutzeroberfläche angezeigt, und der Benutzer muss keinerlei Fragen beantworten. Stattdessen ruft das System die Daten aus einer standardmäßigen `.properties`-Datei ab. Sie können die automatische Installation wahlweise mit der Standarddatei ausführen oder die Datei bearbeiten und so den Installationsvorgang anpassen. Anweisungen zur geführten Installation finden Sie in „Geführte Installation der Identitätsberichterstellung“, auf Seite 399.

Überprüfen Sie in Vorbereitung auf die Installation die Voraussetzungen und Systemanforderungen in Abschnitt 41.4, „Systemanforderungen für die Identitätsberichterstellung“, auf Seite 397. Beachten Sie auch die Versionshinweise zur betreffenden Version.

1 (Bedingt) Mit dem Befehl `export` oder `set` müssen die Administratorpasswörter für die automatische Installation nicht in der `.properties`-Datei angegeben werden. Beispiel:

- **Linux:** `export NOVL_ADMIN_PWD=`*`MeinPasswort`*
- **Windows:** `set NOVL_ADMIN_PWD=`*`MeinPasswort`*

Die automatische Installation ruft die Passwörter nicht aus der `.properties`-Datei ab, sondern aus der Umgebung.

Geben Sie die folgenden Passwörter ein:

**NOVL_DB_RPT_USER_PASSWORD**

Gibt das Passwort des Administrators für die SIEM-Datenbank an.

**NOVL_IDM_SRV_PWD**

Gibt das Passwort des Eigentümers des Datenbankschemas und der Objekte für die Berichterstellung an.

**NOVL_IDM_USER_PWD**

Gibt das Passwort für den Benutzer „idmrptuser“ an, der über den schreibgeschützten Zugriff auf Berichterstellungsdaten verfügt.

**NOVL_ADMIN_PWD**

(Bedingt) Gibt das Passwort eines LDAP-Administrators an, sodass Suchvorgänge in Untercontainern während der Laufzeit ausgeführt werden können.

**NOVL_SMTP_PASSWORD**

(Bedingt) Gibt das Passwort für den standardmäßigen STMP-E-Mail-Benutzer an, sodass die E-Mail-Kommunikation authentifiziert wird.

2 Legen Sie die Installationsparameter mit den folgenden Schritten fest:

**2a** Stellen Sie sicher, dass sich die `.properties`-Datei in demselben Verzeichnis wie die ausführbare Datei für die Installation befindet.

Als Arbeitserleichterung stellt NetIQ zwei `.properties`-Dateien bereit (standardmäßig im Verzeichnis `products/Reporting` im `.iso`-Image):

- `rpt_installonly.properties`, wenn die Standard-Installationseinstellungen verwendet werden sollen
- `rpt_configonly.properties`, wenn die Standard-Installationseinstellungen verwendet werden sollen

**2b** Öffnen Sie die `.properties`-Datei in einem Texteditor.

**2c** Legen Sie die Parameterwerte fest. Eine Beschreibung der Parameter finden Sie in Schritt 9 auf Seite 399.

---

**HINWEIS:** Die `.properties`-Datei für die Installation der Standard Edition enthält lediglich die erforderlichen Parameter für diese Version.

---

**2d** Speichern und schließen Sie die Datei.

3 Starten Sie den Installationsvorgang mit einem der folgenden Befehle:

- **Linux:** `./rpt-install.bin -i silent -f` *`Pfad_zur_Eigenschaftsdatei`*
- **Windows:** `./rpt-install.exe -i silent -f` *`Pfad_zur_Eigenschaftsdatei`*

---

**HINWEIS:** Wenn sich die `.properties`-Datei nicht in demselben Verzeichnis befindet wie das Installationsskript, werden Sie aufgefordert, den vollständigen Pfad zu dieser Datei einzugeben. Das Skript entpackt die notwendigen Dateien in ein temporäres Verzeichnis und startet dann die automatische Installation.

---

## 42.3 Manuelles Erstellen des Datenbankschemas

Sie können die Datenbanktabellen nach der Installation neu erstellen, ohne die Installation wiederholen zu müssen. In diesem Abschnitt wird beschrieben, wie Sie das Datenbankschema erstellen.

1 Halten Sie Tomcat an.

Beispiel:

```
/etc/init.d/idmapps_tomcat_init stop
```

2. (Bedingt) Löschen Sie die vorhandene Datenbank
3. (Bedingt) Erstellen Sie eine neue Datenbank mit demselben Namen wie die Datenbank, die Sie in Schritt 2 gelöscht haben.
4. (Bedingt) Löschen Sie die Datenbank-Checksummen
   - **4a** Melden Sie sich bei Ihrer Datenbank als `idm_rpt_cfg` an.
   - **4b** Führen Sie den folgenden Befehl für PostgresSQL aus:

     ```
       DO
     $do$
      BEGIN
       IF EXISTS
        (select table_name from information_schema.tables where table_schema =
     'public' and table_name = 'databasechangelog')
       THEN
        update databasechangelog set md5sum = null;
       END IF;
     END $do$
     ```

     Alternativ:

     Führen Sie den folgenden Befehl für Oracle aus:

     ```
       BEGIN
      FOR i IN
       (select null from ALL_TABLES where OWNER = user and TABLE_NAME =
     'DATABASECHANGELOG')
      LOOP
       EXECUTE IMMEDIATE 'update DATABASECHANGELOG set MD5SUM = NULL';
      END LOOP;
     END;
     ```

   - **4c** Melden Sie sich bei Ihrer Datenbank als `idm_rpt_data` an.
   - **4d** Führen Sie die in Schritt 4b ausgestellten Befehle als `idm_rpt_data`-Benutzer aus.
5. Definieren Sie die JAVA_HOME-Variable. Beispiel:

   ```
   export JAVA_HOME=/opt/netiq/idm/apps/jre
   ```

6. Initialisieren Sie die Datenbank mit dem installierten Skript neu:

   ```
   /opt/netiq/idm/apps/IdentityReporting/bin/db-init.sh -cfg_password *** -
   data_password ***
   ```

   ```
   /opt/netiq/idm/apps/IdentityReporting/bin/db-init.sh -cfg_password *** -
   data_password *** -sql >
   /opt/netiq/idm/apps/IdentityReporting/sql/output.sql
   ```

7. Starten Sie Tomcat. Beispiel:

   ```
   /etc/init.d/idmapps_tomcat_init start
   ```

# 43 Konfigurieren der Identitätsberichterstellung

Auch nach der Installation der Identitätsberichterstellung können Sie noch zahlreiche Installationseigenschaften bearbeiten. Hierzu steht Ihnen jeweils ein spezielles Dienstprogramm für die Aktualisierung der Konfiguration für Ihre Plattform zur Verfügung. Unter Linux führen Sie die Datei `configupdate.sh` aus, unter Windows die Datei `configupdate.bat`.

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.



## 43.1 Ausführen von Berichten über eine Oracle-Datenbank

Mit der Identitätsberichterstellung können Berichte über Remote-Oracle-Datenbanken ausgeführt werden. Hierzu müssen Sie allerdings eine Oracle-JDBC-Datei zur Bibliothek Ihres Anwendungsservers hinzufügen.

1. Laden Sie die Datei `ojdbc7.jar` von der Oracle-Website herunter.
2. Kopieren Sie die Datei an den jeweiligen Speicherort für Ihren Anwendungsserver:
   - **Tomcat:** Verzeichnis `common/lib` im Verzeichnis *`tomcat_install`*.

Weitere Informationen zu den unterstützten Oracle-Datenbanken finden Sie in Abschnitt 41.4, „Systemanforderungen für die Identitätsberichterstellung“, auf Seite 397.

## 43.2 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.

In Tomcat wird die WAR-Datei `rptdoc` automatisch während der Installation der Identitätsberichterstellung bereitgestellt.

Löschen Sie in einer Staging- oder Produktionsumgebung die WAR-Dateien `rptdoc` und die zugehörigen Ordner manuell aus der Tomcat-Umgebung.

# 44 Verwalten der Treiber für die Berichterstellung

Für die Identitätsberichterstellung sind die folgenden Treiber erforderlich:

- Identity Manager-Treiber „Verwaltetes System – Gateway“ (MSGW-Treiber)
- Identity Manager-Treiber für den Datenerfassungsdienst (DCS-Treiber)

Mit den Paketverwaltungswerkzeugen in Designer können Sie die Treiber installieren und konfigurieren. Dieser Vorgang umfasst folgende Schritte:



## 44.1 Konfigurieren von Treibern für die Identitätsberichterstellung

In diesem Abschnitt wird beschrieben, wie Sie den Treiber „Verwaltetes System – Gateway“ (MSGW-Treiber) und den Treiber für den Datenerfassungsdienst (DCS-Treiber) für die Identitätsberichterstellung installieren und konfigurieren.

---

**HINWEIS:**

In·diesem·Abschnitt·wird·vorausgesetzt,·dass·Sie·bereits·den·Benutzeranwendungstreiber·sowie·den·Rollen- und Ressourcenservice-Treiber für RBPM installiert und konfiguriert haben. Weitere Informationen finden Sie in Kapitel 38, „Erstellen und Bereitstellen der Treiber für die Identitätsanwendungen“, auf Seite 351.

---

### 44.1.1 Installieren der Treiberpakete für die Identitätsberichterstellung

Bevor Sie die Treiber konfigurieren, stellen Sie sicher, dass alle erforderlichen Pakete für die Treiber im Paketkatalog vorliegen. Wenn Sie ein neues Identity Manager-Projekt in Designer erstellen, werden Sie automatisch dazu aufgefordert, mehrere Pakete in das neue Projekt zu importieren. Es ist nicht nötig, die Pakete direkt während der Installation zu importieren; Sie müssen die Pakete allerdings nachträglich installieren, damit die Identitätsberichterstellung ordnungsgemäß funktioniert.

1. Öffnen Sie Ihr Projekt in Designer.
2. Wählen Sie **Paketkatalog > Paket importieren**.
3. Klicken Sie im Dialogfeld „Paket auswählen“ auf **Alles auswählen** und dann auf **OK**.

   Designer fügt mehrere neue Paketordner unter dem **Paketkatalog** hinzu. Diese Paketordner entsprechen den Objekten in der Palette auf der rechten Seite der Ansicht Modellierer in Designer.
4. Klicken Sie auf **Speichern**.

### 44.1.2 Konfigurieren des Treibers „Verwaltetes System – Gateway“ (MSGW-Treiber)

1. Öffnen Sie Ihr Projekt in Designer.
2. Wählen Sie in der Palette der Ansicht **Modellierer** die Option **Dienst > Verwaltetes System – Gateway**.
3. Ziehen Sie das Symbol für **Verwaltetes System – Gateway** auf die Ansicht **Modellierer**.
4. Wählen Sie im Treiberkonfigurationsassistenten die Option **'Verwaltetes System – Gateway' – Basis**, und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster „Obligatorische Funktionen auswählen“ die gewünschten Funktionen aus, und klicken Sie auf **Weiter**.
6. (Bedingt) Wenn Sie nach dem zusätzlichen Paket **Erweiterte Java-Klasse** gefragt werden, wählen Sie das Paket aus, und klicken Sie auf **OK**.
7. (Optional) Geben Sie den Namen für den Treiber an.
8. Klicken Sie auf **Weiter**.
9. Geben Sie unter „Verbindungsparameter“ die Werte an, über die die Identitätsberichterstellung Daten vom Treiber anfordert.

   Bei Angabe mehrerer IP-Adressen werden alle Schnittstellen jeweils über dieselbe Portnummer überwacht. Wenn Sie beispielsweise die Adresse `164.99.88.30,127.0.0.1` und den Port `9000` angeben, verwendet der Treiber die folgenden Einstellungen:

   ```
   164.99.88.30:9000
   127.0.0.1:9000
   ```
10. (Optional) Aktivieren Sie das Endpunkt-Tracing. Wählen Sie hierzu **Wahr**, und geben Sie einen Speicherort für die Trace-Datei an.
11. Klicken Sie auf **Weiter**.
12. (Optional) Verbinden Sie den Treiber mit den folgenden Schritten mit einem Remote Loader:

    **12a** Wählen Sie im Remote Loader-Fenster die Option **Ja**.

    **12b** Legen Sie die Einstellungen für den zu verwendenden Remote Loader fest.

13 Klicken Sie auf **Weiter**.

14 Überprüfen Sie die Angaben im Fenster zum Bestätigen der Installationsaufgaben, und klicken Sie auf **Fertig stellen**.

15 (Optional) Konfigurieren Sie weitere Einstellungen für den Treiber mit den folgenden Schritten in der Modellierer-Ansicht:

**15a** Klicken Sie mit der rechten Maustaste auf die Linie, die den MSGW-Treiber mit dem Treibersatz verbindet, und klicken Sie auf **Eigenschaften**.

**15b** Wählen Sie im Dialogfeld „Eigenschaften“ die Option **Treiberkonfiguration > Startoption**.

**15c** Wählen Sie die Startoption **Manuell**, und klicken Sie auf **Anwenden**.

**15d** Wählen Sie die Registerkarte **Treiberparameter**.

**15e** (Optional) Bearbeiten Sie auf der Registerkarte **Treiberoptionen** die Einstellungen für den Treiber, die Verbindungen und das Endpunkt-Tracing.

Unter Umständen müssen Sie die Einstellungen zunächst einblenden; wählen Sie hierzu unter **Verbindungsparameter** und **Treiberparameter** die Option **Anzeigen**.

**15f** (Optional) Soll der Treiber regelmäßig Statusmeldungen über den Herausgeberkanal senden, klicken Sie auf die Registerkarte **Herausgeber-Optionen**, und geben Sie für **Herausgeber-Heartbeat-Intervall** einen Zeitraum (in Minuten) an.

Wenn im angegebenen Zeitraum kein Datenverkehr über den Herausgeberkanal erfolgt, sendet der Treiber einen neuen Heartbeat.

**15g** Klicken Sie auf **Anwenden**.

16 (Optional) Legen Sie Globalkonfigurationswerte für den Server mit den folgenden Schritten fest:

**16a** Erweitern Sie im Navigationsbereich den Eintrag **Globalkonfigurationswerte**.

**16b** Legen Sie beispielsweise die folgenden Globalkonfigurationswerte fest:

**Verwaltete Systeme über Treibersätze hinweg abfragen**

Definiert den Wirkungsbereich des MSGW-Treibers. Mit **Wahr** gibt der Treiber Informationen zu den verwalteten Systemen über die Treibersätze hinweg zurück. Ansonsten ist der Bereich auf den lokalen Treibersatz beschränkt.

**Endpunktanforderungsdaten zu Abfragen hinzufügen**

Gibt an, ob Endpunktanforderungsdaten in die vom Treiber gesendeten Abfragen aufgenommen werden sollen. Diese Angaben werden als `Vorgangsdaten`-Konten hinzugefügt.

**Name des Knotens für Endpunktanforderungsdaten**

Gibt einen Knotennamen an, der zu den `Vorgangsdaten` in den Abfragen hinzugefügt werden soll. Die Knotenattribute enthalten die Details zur Anforderung.

**16c** Klicken Sie auf **Anwenden**.

17 (Optional) Prüfen Sie die installierten Pakete. Klicken Sie hierzu im Navigationsbereich auf **Pakete**.

Die Einstellungen unter **Aktion** müssen nur dann geändert werden, wenn Sie ein bestimmtes Paket deinstallieren möchten.

18 Klicken Sie auf **OK**.

19 Aktivieren Sie den Abonnentenkanal, sodass die Identitätsberichterstellung ordnungsgemäß funktioniert.

## 44.1.3 Konfigurieren des Treibers für den Datenerfassungsdienst (DCS-Treiber)

1. Öffnen Sie Ihr Projekt in Designer.
2. Wählen Sie in der Palette der Ansicht **Modellierer** die Option **Dienst > Datenerfassungsdienst**.
3. Ziehen Sie das Symbol für **Datenerfassungsdienst** auf die Ansicht **Modellierer**.
4. Wählen Sie im Treiberkonfigurationsassistenten die Option **Datenerfassungsdienst-Basis**, und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster „Obligatorische Funktionen auswählen“ die gewünschten Funktionen aus, und klicken Sie auf **Weiter**.
6. Wählen Sie die gewünschten optionalen Funktionen aus, und klicken Sie auf **Weiter**.
7. (Bedingt) Wenn Sie nach dem zusätzlichen Paket **LDAP-Bibliothek** gefragt werden, führen Sie die folgenden Schritte aus:
   - **7a** Wählen Sie das Paket aus, und klicken Sie auf **OK**.
   - **7b** (Optional) Konfigurieren Sie ein globales Verbindungsprofil für alle Treiber. Wählen Sie hierzu auf der Seite „LDAB-Bibliothek installieren“ die Option **Ja**.
8. Klicken Sie auf **Weiter**.
9. (Optional) Geben Sie den Namen für den Treiber an.
10. Klicken Sie auf **Weiter**.
11. Geben Sie unter „Verbindungsparameter“ die Werte an, über die die Identitätsberichterstellung Daten vom Treiber anfordert.

    Geben Sie beispielsweise den Benutzer und das Passwort des Berichterstellungsadministrators zur Authentifizierung an.

    Bei Angabe mehrerer IP-Adressen werden alle Schnittstellen jeweils über dieselbe Portnummer überwacht. Wenn Sie beispielsweise die Adresse `164.99.88.30,127.0.0.1` und den Port `9000` angeben, verwendet der Treiber die folgenden Einstellungen:

    ```
    164.99.88.30:9000
    127.0.0.1:9000
    ```

12. Klicken Sie auf **Weiter**.
13. Legen Sie unter **Identitätsdepotregistrierung** die Einstellungen für das Identitätsdepot fest.

    Sie müssen eine IP-Adresse angeben. Die Adresse localhost ist für die Registrierung des Identitätsdepots nicht zulässig.
14. (Optional) Registrieren Sie den MSGW-Treiber mit den folgenden Schritten:
    - **14a** Klicken Sie unter **'Verwaltetes System – Gateway' – Registrierung** auf **Ja**.
    - **14b** Geben Sie den DN des Treibers sowie den Benutzernamen und das Passwort für den LDAP-Administrator an.

      **HINWEIS:** Da der Treiber noch nicht bereitgestellt wurde, wird der soeben konfigurierte MSGW-Treiber beim Durchsuchen nicht angezeigt. Sie müssen daher den DN für den Treiber eingeben.
15. Klicken Sie auf **Weiter**.
16. (Optional) Verbinden Sie den Treiber mit den folgenden Schritten mit einem Remote Loader:
    - **16a** Wählen Sie im Remote Loader-Fenster die Option **Ja**.
    - **16b** Legen Sie die Einstellungen für den zu verwendenden Remote Loader fest.

**17** Klicken Sie auf **Weiter**.

**18** Legen Sie unter **Scoping-Konfiguration** die Rolle für den DSC-Treiber fest.

**19** Überprüfen Sie die Angaben im Fenster zum Bestätigen der Installationsaufgaben, und klicken Sie auf **Fertig stellen**.

**20** (Optional) Konfigurieren Sie weitere Einstellungen für den Treiber mit den folgenden Schritten in der Modellierer-Ansicht:

**20a** Klicken Sie mit der rechten Maustaste auf die Linie, die den DCS-Treiber mit dem Treibersatz verbindet, und klicken Sie auf **Eigenschaften**.

**20b** Wählen Sie im Dialogfeld „Eigenschaften“ die Option **Treiberkonfiguration > Startoption**.

**20c** Wählen Sie die Startoption **Manuell**, und klicken Sie auf **Anwenden**.

**20d** Wählen Sie die Registerkarte **Treiberparameter**.

NetIQ empfiehlt Ihnen, in Umgebungen, in denen der Treiber sehr viele Ereignisse empfängt, die Anzahl der Stapel pro Datei auf maximal 5 festzulegen. Wenn Sie diesen Parameter auf einen Wert größer 5 festlegen, werden die Ereignisse vom Treiber nicht effizient verarbeitet.

**20e** (Optional) Bearbeiten Sie auf der Registerkarte **Treiberoptionen** die Einstellungen für den Treiber, die Verbindungen und die Registrierung.

In einer Testumgebung sollten Sie niedrige Werte verwenden, damit die Ereignisse fehlerfrei verarbeitet werden können. In einer Produktionsumgebung sollten Sie dagegen höhere Werte angeben, sodass das System Ereignisse nicht unnötig verarbeitet.

**IP-Adresse**

Gibt die IP-Adresse des Servers an, auf dem die Identitätsberichterstellung gehostet wird.

**Anschluss**

Gibt die Portnummer für REST-Verbindungen der Identitätsberichterstellung an.

**Protokoll**

Gibt das Protokoll für den Zugriff auf die Identitätsberichterstellung an. Bei HTTPS müssen Sie außerdem angeben, ob das Zertifikat des Servers als verbürgt betrachtet werden soll.

**Name**

Gibt den Namen an, mit dem das Identitätsdepot in der Identitätsberichterstellung bezeichnet werden soll.

**Beschreibung**

Gibt eine kurze Beschreibung des Identitätsdepots an.

**Adresse**

Gibt die IP-Adresse des Identitätsdepots an.

```
164.99.130.127
```

---

**HINWEIS:** Sie müssen eine IP-Adresse angeben. Die Adresse „localhost“ ist für die Registrierung des Identitätsdepots nicht zulässig.

---

**'Verwaltetes System – Gateway' registrieren**

Gibt an, ob der MSGW-Treiber registriert werden soll.

**DN des Treibers 'Verwaltetes System – Gateway' (LDAP)**

Gibt den DN des MSGW-Treibers mit Schrägstrichen an.

**Konfigurationsmodus des Treibers 'Verwaltetes System – Gateway'**

Gibt an, ob der Treiber lokal oder remote konfiguriert ist.

**Benutzer-DN (LDAP)**

Gibt den LDAP-DN des Benutzers an, mit dem sich der Treiber beim MSGW-Treiber authentifizieren soll. Dieser DN muss bereits im Identitätsdepot vorhanden sein.

**Passwort**

Gibt das Passwort für den Benutzer an.

**Zeitabstand zwischen Ereigniseinreichungen**

Maximal zulässiger Zeitraum (in Minuten), über den ein Ereignis in der Persistenzschicht verbleiben darf, bis es an den DCS (und an die Datenbank für die Identitätsberichterstellung) weitergeleitet wird.

**20f** (Bedingt) Sollen Daten aus den Identitätsanwendungen erfasst werden, legen Sie die entsprechenden Werte zur **Unterstützung für SSO-Dienst** fest. Weitere Informationen finden Sie in Abschnitt 44.1.4, „Konfigurieren der Identitätsberichterstellung für das Erfassen von Daten aus den Identitätsanwendungen“, auf Seite 414.

**20g** Klicken Sie auf **Anwenden**.

**21** Konfigurieren Sie die DNs mit den folgenden Schritten:

**21a** Wählen Sie im Navigationsmenü den Befehl **Engine-Steuerungswerte**.

**21b** Wählen Sie unter **Ausführliche Form für DN-Syntax-Attributwerte** die Option **Wahr**.

**21c** Klicken Sie auf **Anwenden**.

**22** (Optional) Legen Sie Globalkonfigurationswerte für den Server mit den folgenden Schritten fest:

**22a** Erweitern Sie im Navigationsbereich den Eintrag **Globalkonfigurationswerte**.

**22b** Wählen Sie unter **Optionen für Überschreiben anzeigen** die Option **Anzeigen**.

**22c** Ändern Sie die Einstellungen so, dass die Globalkonfigurationsoptionen außer Kraft gesetzt werden.

**22d** Klicken Sie auf **Anwenden**.

**23** Klicken Sie auf **OK**.

## 44.1.4 Konfigurieren der Identitätsberichterstellung für das Erfassen von Daten aus den Identitätsanwendungen

Damit die Identitätsberichterstellung Daten aus den Identitätsanwendungen erfassen kann, müssen Sie den DCS-Treiber für die Unterstützung des Single Sign-On konfigurieren.

**1** Öffnen Sie Ihr Projekt in Designer.

**2** Klicken Sie in der Ansicht **Gliederung** mit der rechten Maustaste auf den DCS-Treiber, und klicken Sie auf **Eigenschaften**.

**3** Klicken Sie auf **Treiberkonfiguration > Treiberparameter**.

**4** Klicken Sie auf **Verbindungsparameter anzeigen > Anzeigen**.

**5** Klicken Sie auf **Unterstützung für SSO-Dienst > Ja**.

**6** Legen Sie die Parameter für die Single-Sign-On-Funktion fest:

**Adresse des SSO-Dienstes**

*Erforderlich*

Gibt die relative URL des Authentifizierungsservers an, der Token an den OSP ausgibt. Beispiel: `10.10.10.48`.

Dieser Wert muss mit dem Wert übereinstimmen, den Sie im RBPM-Konfigurationsprogramm für **Hostkennung für OSP-Server** angegeben haben. Weitere Informationen finden Sie in Abschnitt 40.3.1, „Beglaubigungsserver“, auf Seite 379.

**Port des SSO-Dienstes**

*Erforderlich*

Gibt den Port für den Authentifizierungsserver an. Der Standardwert ist 8180.

Dieser Wert muss mit dem Wert übereinstimmen, den Sie im RBPM-Konfigurationsprogramm für **TCP-Port für OSP-Server** angegeben haben. Weitere Informationen finden Sie in Abschnitt 40.3.1, „Beglaubigungsserver“, auf Seite 379.

**ID des SSO-Dienst-Clients**

*Erforderlich*

Gibt den Namen an, mit dem sich der DCS-Treiber für die Identitätsberichterstellung beim Authentifizierungsserver anmelden soll. Der Standardwert lautet `dcsdrv`.

Dieser Wert muss mit dem Wert übereinstimmen, den Sie im RBPM-Konfigurationsprogramm für **OSP-Client-ID** angegeben haben. Weitere Informationen finden Sie in Abschnitt 40.4.5, „Berichte“, auf Seite 387.

**Client-Geheimnis des SSO-Dienstes**

*Erforderlich*

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

Dieser Wert muss mit dem Wert übereinstimmen, den Sie im RBPM-Konfigurationsprogramm für **OSP-Client-Geheimnis** angegeben haben. Weitere Informationen finden Sie in Abschnitt 40.4.5, „Berichte“, auf Seite 387.

**Protokoll**

Gibt an, ob der Dienst-Client über das (unsichere) `http`-Protokoll oder das (sichere) `https`-Protokoll mit dem Authentifizierungsserver kommuniziert.

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

8 (Bedingt) Wenn Sie diese Einstellungen nach dem Bereitstellen des Treibers ändern, müssen Sie den Treiber erneut bereitstellen und neu starten. Weitere Informationen finden Sie in Abschnitt 44.2, „Bereitstellen und Starten von Treibern für die Identitätsberichterstellung“, auf Seite 415.

9 Wiederholen Sie diesen Vorgang für alle DCS-Treiber in Ihrer Umgebung.

## 44.2 Bereitstellen und Starten von Treibern für die Identitätsberichterstellung

Für die Identitätsberichterstellung sind die folgenden Treiber erforderlich:

- Identity Manager-Treiber „Verwaltetes System – Gateway“ (MSGW-Treiber)
- Identity Manager-Treiber für den Datenerfassungsdienst (DCS-Treiber)

Dieser Vorgang umfasst folgende Schritte:

- Abschnitt 44.2.1, „Bereitstellen der Treiber“, auf Seite 416
- Abschnitt 44.2.2, „Überprüfen der Funktionsfähigkeit der verwalteten Systeme“, auf Seite 416
- Abschnitt 44.2.3, „Starten der Treiber für die Identitätsberichterstellung“, auf Seite 419

Weitere Informationen zum Installieren und Konfigurieren dieser Treiber finden Sie in Abschnitt 44.1, „Konfigurieren von Treibern für die Identitätsberichterstellung“, auf Seite 409.

## 44.2.1 Bereitstellen der Treiber

Sie müssen die beiden Treiber für die Identitätsberichterstellung bereitstellen.

1. Öffnen Sie Ihr Projekt in Designer.
2. Klicken Sie in der Ansicht **Modellierer** oder **Gliederung** mit der rechten Maustaste auf den bereitzustellenden Treibersatz.
3. Wählen Sie **Live** > **Bereitstellen**.
4. Geben Sie den Identitätsdepot-Berechtigungsnachweis für den ausgewählten Treiber an.

## 44.2.2 Überprüfen der Funktionsfähigkeit der verwalteten Systeme

Bevor Sie den Treiber „Verwaltetes System – Gateway“ (MSGW-Treiber) und den Treiber für den Datenerfassungsdienst (DCS-Treiber) starten, überprüfen Sie, ob die zugrunde liegenden verwalteten Systeme ordnungsgemäß konfiguriert sind. Dieser Vorgang trägt dazu bei, Probleme in der Umgebung zu isolieren, die nicht mit der Konfiguration der Berichterstellungstreiber zusammenhängen.

Bei der Fehlersuche Ihrer Active Directory-Umgebung sollten Sie beispielsweise die Active Directory-Berechtigung testen; hierzu weisen Sie eine Ressource in der Benutzeranwendung zu.

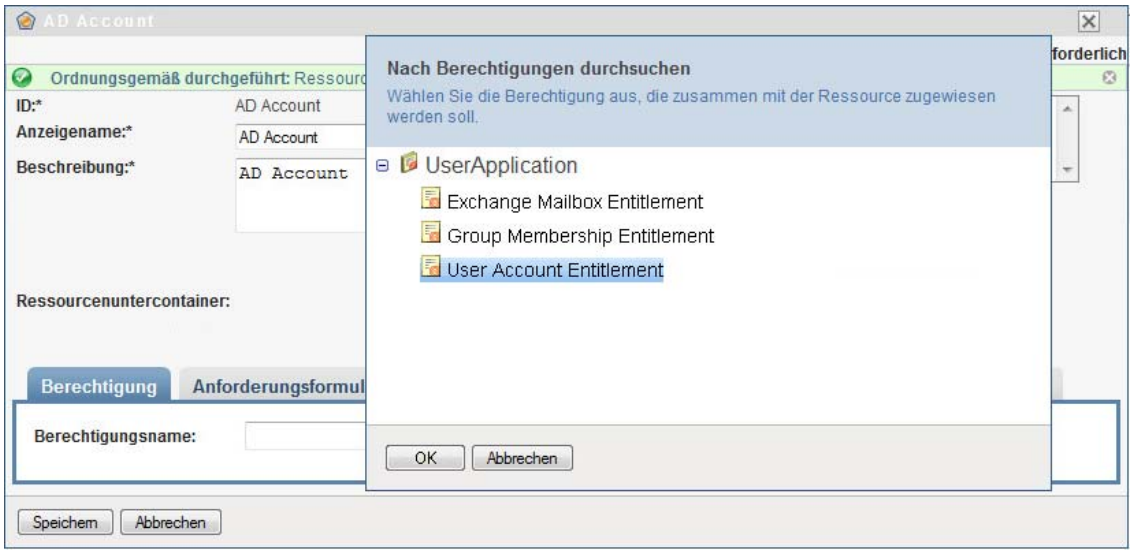
---

**HINWEIS:** Weitere Informationen zum Active Directory-Treiber finden Sie im *NetIQ Identity Manager Driver for Active Directory Implementation Guide* (Implementierungshandbuch zum NetIQ Identity Manager-Treiber für Active Directory).

---

Im Folgenden finden Sie einen Vorschlag für ein Verfahren, mit dem Sie die ordnungsgemäße Konfiguration von Active Directory ermitteln:

1. Stellen Sie sicher, dass sowohl die Benutzeranwendung als auch die Identitätsberichterstellung auf demselben Server ausgeführt werden.
2. Stellen Sie in iManager sicher, dass der Benutzeranwendungstreiber und der Rollen- und Ressourcenservice-Treiber ausgeführt werden, und stellen Sie sicher, dass der Treiber für das verwaltete System ausgeführt wird.
3. Überprüfen Sie, ob die Benutzeranwendung Daten aus Active Directory abrufen kann. Melden Sie sich hierzu als Benutzeranwendungsadministrator bei der Benutzeranwendung an.
4. Erstellen Sie im Ressourcenkatalog eine neue Ressource für Active Directory-Konten:
5. Binden Sie die Ressource an eine Berechtigung im Active Directory-Treiber, z. B. **Benutzerkontenberechtigung**.

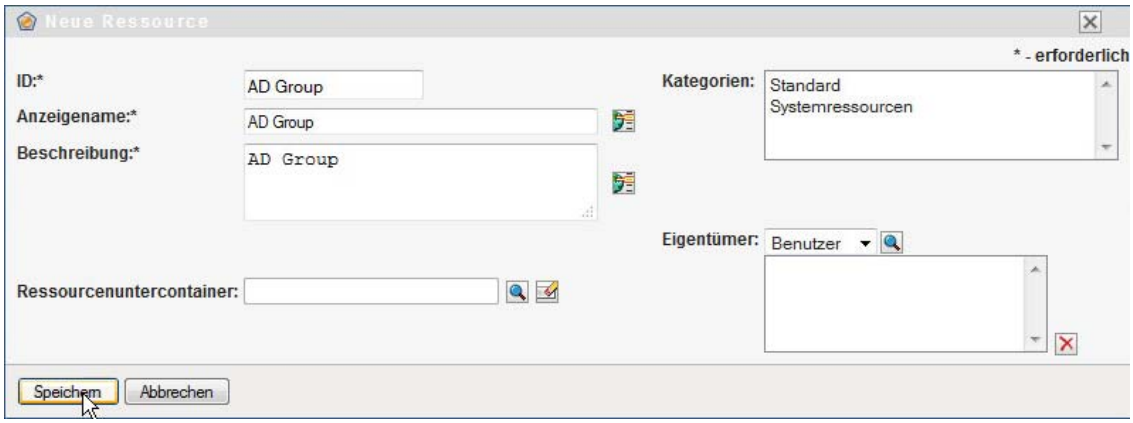



Die Benutzeranwendung kann die Berechtigung aus dem Treiber abrufen.

6 Diese spezielle Ressource gehört zu Konten; konfigurieren Sie die Ressource daher so, dass ein Kontowert zugewiesen wird.

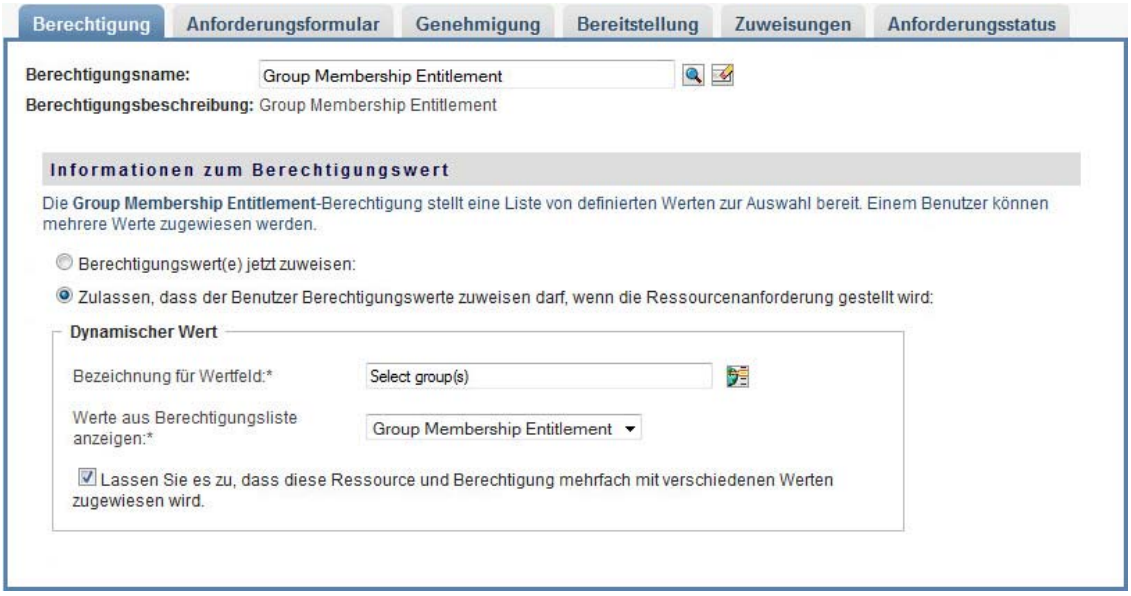

7 Wählen Sie den Kontowert aus, und klicken Sie auf **Hinzufügen**.

8 Erstellen Sie eine weitere Ressource, mit der Gruppen zugewiesen werden.




9 Binden Sie die Ressource an eine geeignete Berechtigung für Gruppen. Ordnen Sie diese spezielle Ressource zur **Gruppenmitgliedschaftsberechtigung** zu.

10 Konfigurieren Sie diese Ressource so, dass dem Benutzer der Berechtigungswert zum Zeitpunkt der Anforderung zugewiesen wird und der Benutzer mehrere Werte für eine einzelne Zuweisungsanforderung auswählen kann.




11 Überprüfen Sie, ob die Berechtigungen fehlerfrei erstellt wurden.


Damit ist ersichtlich, dass die zugrunde liegende Architektur des verwalteten Systems (in diesem Fall Active Directory) ordnungsgemäß funktioniert. Dies kann bei einer späteren Fehlersuche für eventuell auftretende Probleme hilfreich sein.

## 44.2.3 Starten der Treiber für die Identitätsberichterstellung

In diesem Abschnitt finden Sie Anweisungen zum Starten des Treibers „Verwaltetes System – Gateway“ (MSGW-Treiber) und des Treibers für den Datenerfassungsdienst (DCS-Treiber).

1. Öffnen Sie iManager.
2. Klicken Sie mit der rechten Maustaste auf den MSGW-Treiber, und klicken Sie auf **Treiber starten**.
3. Klicken Sie mit der rechten Maustaste auf den DCS-Treiber, und klicken Sie auf **Treiber starten**.
4. Überprüfen Sie nach dem Starten, ob zusätzliche Informationen in der Serverkonsole angezeigt werden. Beispiel:

   ```
   21:22:56,399 INFO  [LogEvent] [DCS_Driver_Registration_Add] DCS Driver DN
   TREE\novell\TestDrivers\Data Collection Service Driver; DCS-Report Driver
   d44571a5708446bad65832481bb401d
   ```

5. Melden Sie sich als Berichterstellungsadministrator bei der Berichterstellung an.
6. Klicken Sie links im Navigationsbereich auf **Überblick**.
7. Überprüfen Sie, ob die im Abschnitt **Konfiguration** vermerkt ist, dass ein Identitätsdepot konfiguriert wurde.
8. Klicken Sie im Navigationsbereich auf **Identitätsdepots**.
9. Überprüfen Sie, ob auf der Seite „Identitätsdepot“ Details zum DCS- und zum MSGW-Treiber angezeigt werden. Der Status des MSGW-Treibers muss besagen, dass der Treiber initialisiert wurde.

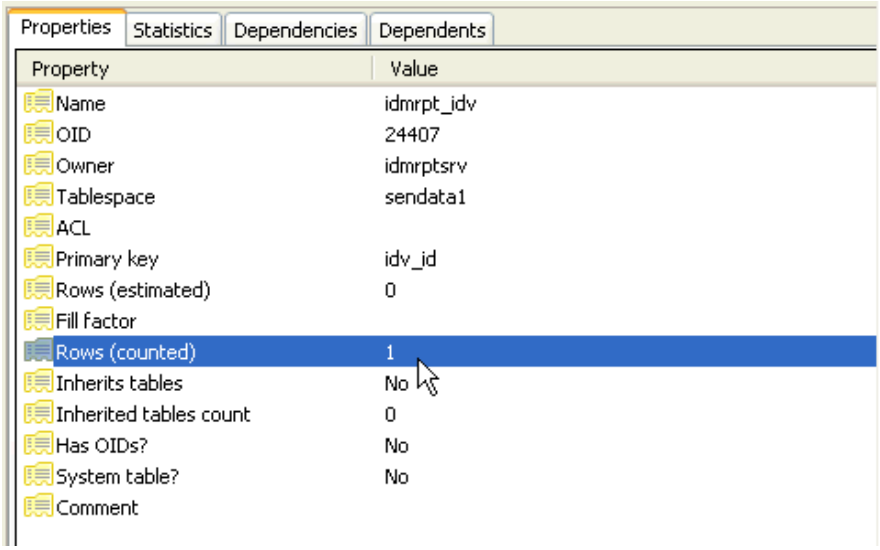
   Zu diesem Zeitpunkt können Sie den gesamten Inhalt des Identity Information Warehouse einsehen und sich über die umfangreichen Daten zum Identitätsdepot sowie über die verwalteten Systeme in Ihrem Unternehmen informieren.
10. Zum Anzeigen der Daten im Identity Information Warehouse öffnen Sie die SIEM-Datenbank in einem Datenbankverwaltungswerkzeug wie PGAdmin für PostgreSQL. Die SIEM-Datenbank sollte die folgenden Schemas umfassen:

    **idm_rpt_cfg**

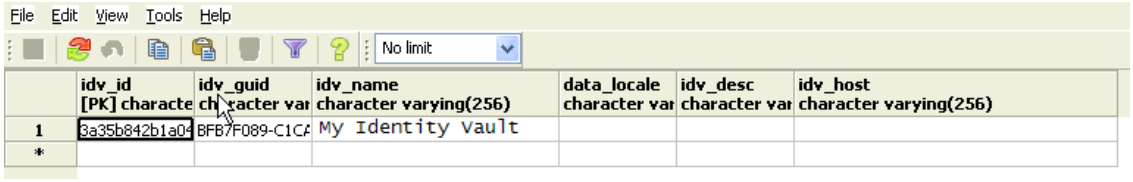
    Enthält Konfigurationsdaten für die Berichterstellung, z. B. Berichtdefinitionen und Zeitpläne. Dieses Schema wird durch das Installationsprogramm für die Identitätsberichterstellung zur Datenbank hinzugefügt.

    **idm_rpt_data**

    Enthält Daten, die durch den MSGW-Treiber und den DCS-Treiber erfasst wurden. Dieses Schema wird durch das Installationsprogramm für die Identitätsberichterstellung zur Datenbank hinzugefügt.
11. Zum Anzeigen der Daten, die durch die Treiber erfasst wurden, erweitern Sie den Eintrag **idm_rpt_data > Tabellen > idmrpt_idv**.
12. Überprüfen Sie, ob eine einzelne Zeile für den neuen DCS-Treiber in diese Tabelle eingefügt wurde:




13 Überprüfen Sie, ob die Daten in dieser Tabelle den Namen des Identitätsdepots enthalten:




Wenn die neue Zeile in dieser Tabelle sichtbar ist, wurde der Treiber ordnungsgemäß registriert.

## 44.3 Konfigurieren der Laufzeitumgebung

Dieser Abschnitt enthält einige zusätzliche Konfigurationsschritte, 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:

- Abschnitt 44.3.1, „Konfigurieren des DCS-Treibers für das Erfassen von Daten aus den Identitätsanwendungen“, auf Seite 421
- Abschnitt 44.3.2, „Migrieren des DCS-Treibers“, auf Seite 422
- Abschnitt 44.3.3, „Zusätzliche Unterstützung für benutzerdefinierte Attribute und Objekte“, auf Seite 423
- Abschnitt 44.3.4, „Zusätzliche Unterstützung für mehrere Treibersätze“, auf Seite 426
- Abschnitt 44.3.5, „Konfigurieren der Treiber für die Ausführung im Remote-Modus mit SSL“, auf Seite 427

Weitere Informationen zu Problemen mit mindestens einem oder mehreren Treibern, die Sie nicht ohne weiteres selbst beheben können, finden Sie unter Fehlersuche für die Treiber im *Administratorhandbuch für die NetIQ-Identitätsberichterstellung*.

## 44.3.1 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) Wenn Ihr Projekt noch keinen Treiber für den Datenerfassungsdienst umfasst, importieren Sie den Treiber in Ihr Projekt. Weitere Informationen finden Sie in Kapitel 38, „Erstellen und Bereitstellen der Treiber für die Identitätsanwendungen“, auf Seite 351.
4. (Bedingt) Falls Sie den DCS-Treiber noch nicht auf die unterstützte Patch-Version aufgerüstet haben, führen Sie die folgenden Schritte aus:
   - **4a** Laden Sie die aktuelle Patch-Datei für den DCS-Treiber herunter.
   - **4b** Extrahieren Sie die Patch-Datei in ein Verzeichnis auf Ihrem Server.
   - **4c** 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
     ```

   - **4d** Starten Sie eDirectory neu.
   - **4e** 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 41.3, „Voraussetzungen für die Installation der Komponenten für die Identitätsberichterstellung“, auf Seite 395.
   - **4f** Stellen Sie den DCS-Treiber in Designer erneut bereit, und starten Sie ihn neu.
5. Klicken Sie in der Ansicht **Gliederung** mit der rechten Maustaste auf den DCS-Treiber, und wählen Sie **Eigenschaften**.
6. Klicken Sie auf **Treiberkonfiguration**.
7. Klicken Sie auf die Registerkarte **Treiberparameter**.
8. Klicken Sie auf **Verbindungsparameter anzeigen**, und wählen Sie **Anzeigen**.
9. Klicken Sie auf **Unterstützung für SSO-Dienst**, und wählen Sie **Ja**.
10. Geben Sie die IP-Adresse und den Port des Berichterstellungsmoduls ein.
11. Geben Sie das Passwort für den SSO-Dienst-Client ein. Das Standardpasswort lautet `driver`.
12. Klicken Sie auf **Anwenden** und dann auf **OK**.
13. Klicken Sie in der Ansicht **Modellierer** mit der rechten Maustaste auf den DCS-Treiber, und wählen Sie **Treiber > Bereitstellen**.
14. Klicken Sie auf **Bereitstellen**.

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

16 Klicken Sie auf **OK**.

## 44.3.2 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**.

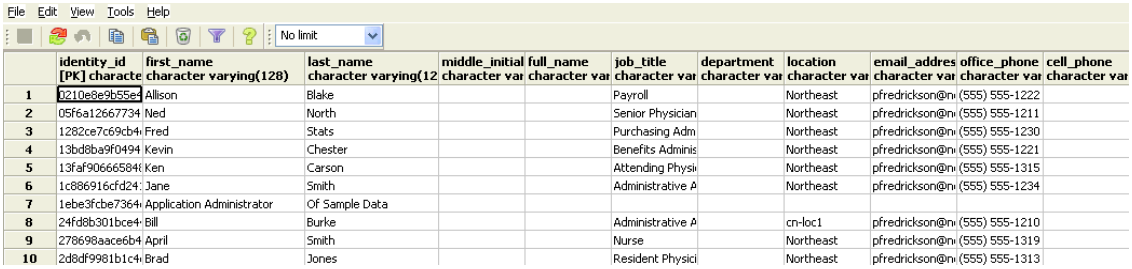
---

**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.

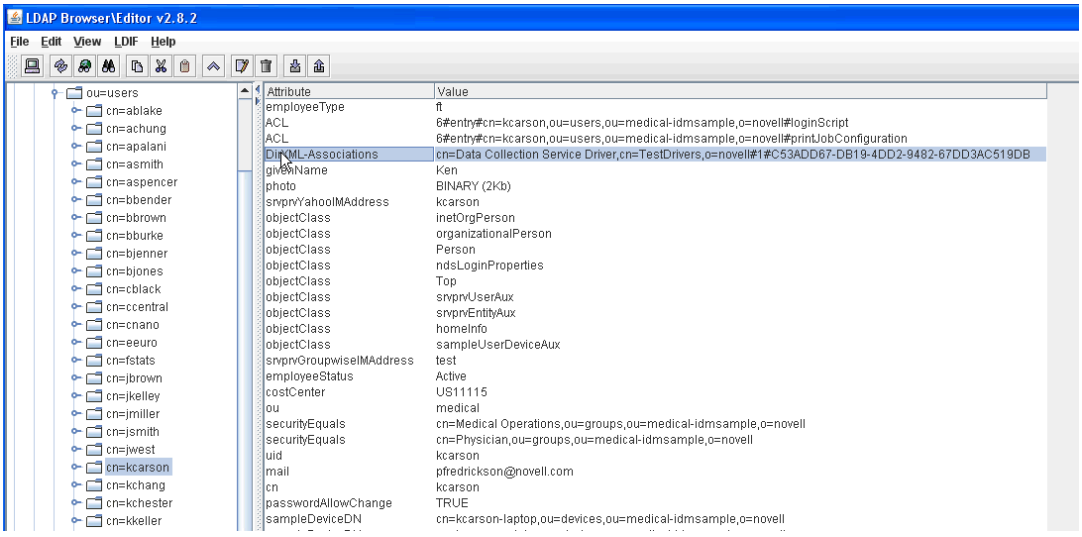
5 Die Tabellen **idmrpt_identity** und **idmrpt_acct** enthalten Informationen zu den Identitäten und Konten im Identitätsdepot. Überprüfen Sie, ob die folgenden Arten von Informationen in diesen Tabellen vorliegen:



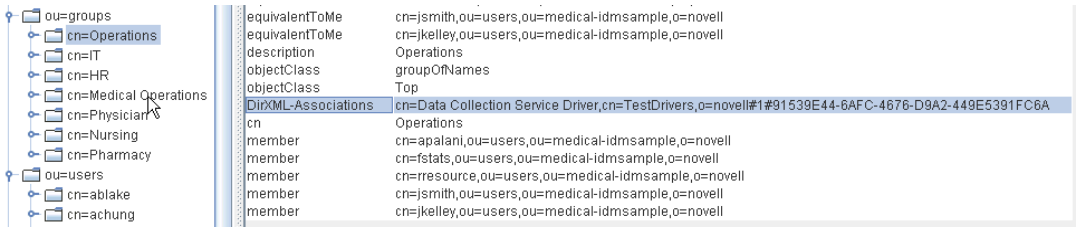

| | identity_id [PK] characte | first_name character varying(128) | last_name character varying(12 | middle_initial character var | full_name character var | job_title character var | department character var | location character var | email_addres character var | office_phone character var | cell_phone 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_group boolean | idmrpt_valid_from timestamp without tin | idmrpt_deleted boolean | idmrpt_syn_state smallint |
|---|---|---|---|---|---|---|---|
| Pharmacy | Pharmacy | FALSE | | FALSE | 2010-07-07 21:28:11 | FALSE | 1 |
| IT | Information Tec | FALSE | | FALSE | 2010-07-07 21:28:11 | FALSE | 1 |
| HR | Human Resourc | FALSE | | FALSE | 2010-07-07 21:28:11 | FALSE | 1 |
| Physician | Physician | FALSE | | FALSE | 2010-07-07 21:28:11 | FALSE | 1 |
| Operations | Operations | FALSE | | FALSE | 2010-07-07 21:28:11 | FALSE | 1 |
| Medical Operatic | Medical Operatic | FALSE | | FALSE | 2010-07-07 21:28:11 | FALSE | 1 |
| Nursing | Nursing | FALSE | | FALSE | 2010-07-07 21:28:11 | FALSE | 1 |
| | | | | | | | |

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

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.

### 44.3.3 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 424
- „Angeben eines Namens und einer Beschreibung in der Datenbank“, auf Seite 424
- „Hinzufügen von erweiterten Attributen zu bekannten Objekttypen“, auf Seite 425


## 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.

## 44.3.4 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. Anweisungen zum Konfigurieren des DCS-Treibers auf diesem Server finden Sie in Abschnitt 44.1.3, „Konfigurieren des Treibers für den Datenerfassungsdienst (DCS-Treiber)“, auf Seite 412.
- **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.

## 44.3.5 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 427 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 428 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 427 ein.

**5e** Speichern Sie den Treiber, und starten Sie ihn neu.

## 44.4 Festlegen von Revisions-Flags für den Treiber

In diesem Abschnitt werden die empfohlenen Revisionseinstellungen für den Treiber „Verwaltetes System – Gateway“ (MSGW-Treiber) und den Treiber für den Datenerfassungsdienst (DCS-Treiber) beschrieben.

- Abschnitt 44.4.1, „Festlegen von Revisions-Flags in Identity Manager“, auf Seite 429
- Abschnitt 44.4.2, „Festlegen von Revisions-Flags in eDirectory“, auf Seite 430

### 44.4.1 Festlegen von Revisions-Flags in Identity Manager

NetIQ empfiehlt, Revisions-Flags für die Treiber in Identity Manager festzulegen. Diese Flags gelten für Novell Auditing (nicht für XDAS).

Wählen Sie in iManager die Option **Treibersatzeigenschaften > Protokollierumfang > Bestimmte Ereignisse protokollieren**.

| Kategorie | Empfohlene Flags |
|---|---|
| Metadirectory-Engine-Ereignisse | ◆ Metadirectory-Engine-Warnmeldungen |
| Statusereignisse | ◆ Erfolg<br>**HINWEIS:** Für den Bericht **Korrelierte Ressourcenzuweisungsereignisse pro Benutzer** ist das Erfolgs-Flag erforderlich. Wenn dieser Bericht (oder eine benutzerdefinierte Version dieses Berichts) ausgeführt werden soll, müssen Sie das Erfolgs-Flag aktivieren.<br>◆ Fehler<br>◆ Fatal (Schwerwiegend) |
| Vorgangsereignisse | ◆ Bearbeiten<br>◆ Add Association<br>◆ Check Password<br>◆ Wert hinzufügen<br>◆ Hinzufügen<br>◆ Umbenennen<br>◆ Verknüpfung entfernen<br>◆ Check Object Password<br>◆ Clear Attribute<br>◆ Remove Value<br>◆ Get Named Password<br>◆ Entfernen<br>◆ Verschieben<br>◆ Passwort ändern<br>◆ Wert hinzufügen (bei Änderung)<br>◆ Reset Attributes |

| Kategorie | Empfohlene Flags |
|---|---|
| Transformationsereignisse | ◆ Password Reset<br>◆ User Agent Request<br>◆ Password Sync |
| Berechtigungsbereitstellungsereignisse | ◆ SSO-Berechtigungen festlegen<br>◆ SSO-Berechtigungen löschen<br>◆ SSO-Passwortfrage und -antwort festlegen |

## 44.4.2 Festlegen von Revisions-Flags in eDirectory

NetIQ empfiehlt, Revisions-Flags für die Treiber in eDirectory festzulegen. Diese Flags gelten für Novell Auditing (nicht für XDAS).

Wählen Sie in iManager die Option **eDirectory-Revision > Revisionskonfiguration > Novell Auditing**.

| Kategorie | Empfohlene Flags |
|---|---|
| Global | ◆ Keine reproduzierten Ereignisse senden |
| Meta | ◆ *(Alle Flags auswählen)* |
| Objekte | ◆ Eigenschaft hinzufügen<br>◆ Anmeldung zulassen<br>◆ Passwort ändern<br>◆ 'Sicherheit gleicht' ändern<br>◆ Erstellen<br>◆ Löschen<br>◆ Eigenschaft löschen<br>◆ Anmelden<br>◆ Abmelden<br>◆ RDN bearbeiten<br>◆ Verschieben (Ursprung)<br>◆ Verschieben (Ziel)<br>◆ Entfernen<br>◆ Umbenennen<br>◆ Wiederherstellung<br>◆ Suchen<br>◆ Passwort bestätigen |
| Attribute | ◆ *(Alle Flags auswählen)* |

| Kategorie | Empfohlene Flags |
|---|---|
| Agent | ◆ DS neu geladen<br>◆ Lokaler Agent geöffnet<br>◆ Lokaler Agent geschlossen<br>◆ NLM geladen |
| Sonstige | ◆ CA-Schlüssel erstellen<br>◆ Neu zertifizierter öffentlicher Schlüssel |
| LDAP | ◆ LDAP – Binden<br>◆ LDAP – Binden (Antwort)<br>◆ LDAP – Bearbeiten<br>◆ LDAP – Bearbeiten (Antwort)<br>◆ LDAP – Passwort bearbeiten<br>◆ LDAP – Bindung aufheben<br>◆ LDAP – Löschen<br>◆ LDAP – Löschen (Antwort)<br>◆ LDAP – DN bearbeiten<br>◆ LDAP – DN bearbeiten (Antwort)<br>◆ LDAP-Suche<br>◆ LDAP-Suche (Antwort)<br>◆ LDAP – Hinzufügen<br>◆ LDAP – Hinzufügen (Antwort) |

# XIV Installieren von Analyzer für Identity Manager

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.

Die Installationsdateien befinden sich im Verzeichnis `products/Analyzer` in der `.iso`-Image-Datei des Identity Manager-Installationspakets. Standardmäßig installiert das Installationsprogramm die Komponenten in den folgenden Speicherorten:

- **Linux:** `home/admin/analyzer`
- **Windows:** `C:\NetIQ\Analyzer`

NetIQ empfiehlt, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie in Abschnitt 45.1, „Checkliste für die Installation von Analyzer“, auf Seite 435.

# 45 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.



## 45.1 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 25. |
| ❑ | 2. Legen Sie fest, welche Server für die Identity Manager-Komponenten verwendet werden sollen. Weitere Informationen finden Sie in Abschnitt 5.3, „Empfehlungen für Installationsszenarien und Servereinrichtung“, auf Seite 51. |
| ❑ | 3. (Bedingt) Zur geführten Installation auf Computern mit dem Betriebssystem SLES 12 SP1 (oder höher) müssen die entsprechenden Bibliotheken installiert sein. Weitere Informationen finden Sie in Abschnitt 6.3, „Installieren von Identity Manager auf Servern mit SLES 12 SP1 (oder höher)“, auf Seite 63. |
| ❑ | 4. Stellen Sie sicher, dass Ihre Umgebung den Überlegungen und Voraussetzungen für das Hosten von Analyzer entspricht. Weitere Informationen finden Sie in den folgenden Abschnitten:<br>◆ Abschnitt 45.2, „Voraussetzungen für die Installation von Analyzer“, auf Seite 436<br>◆ Abschnitt 45.3, „Systemanforderungen für die Installation von Analyzer“, auf Seite 436 |
| ❑ | 5. Befolgen Sie die Anweisungen zum Installieren von Analyzer in einem der folgenden Abschnitte:<br>◆ Anweisungen zur Verwendung des Installationsassistenten finden Sie in Abschnitt 46.1, „Installieren von Analyzer mit dem Assistenten“, auf Seite 439<br>◆ Anweisungen zur automatischen Installation finden Sie in Abschnitt 46.2, „Automatische Installation von Analyzer“, auf Seite 440. |
| ❑ | 6. (Optional) Sollen Audit-Ereignisse automatisch von Analyzer empfangen und angezeigt werden, installieren Sie den XDAS-Client. Weitere Informationen finden Sie in Abschnitt 46.4, „Installieren eines Audit-Clients für Analyzer“, auf Seite 441. |
| ❑ | 7. Aktivieren Sie Analyzer gemäß den Anweisungen in „Aktivieren von Analyzer“, auf Seite 488. |
| ❑ | 8. (Optional) Rüsten Sie Analyzer gemäß den Anweisungen in Abschnitt 55.7, „Aufrüsten von Analyzer“, auf Seite 532 auf. |

## 45.2 Voraussetzungen für die Installation von Analyzer

Installieren Sie vor der Installation von Analyzer ein geeignetes Paket, in dem sich die Bibliothek `/usr/lib/libpng12.so.0` befindet.

## 45.3 Systemanforderungen für die Installation von 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 | Mindestens 512 MB (empfohlen 4 GB) |
| Bildauflösung | 1024 × 768 (empfohlen 1280 × 1025) |
| Betriebssystem (zertifiziert) | Eines der folgenden 64-Bit-Betriebssysteme:<br>◆ openSUSE 13.2<br>◆ SUSE Linux Enterprise Server 12 SP1<br>◆ SUSE Linux Enterprise Server 11 SP4<br>◆ Windows Server 2012 R2<br>◆ Windows Server 2012<br>◆ Windows Server 2008<br>Eines der folgenden 32-Bit-Betriebssysteme:<br>◆ openSUSE 13.2<br>NetIQ empfiehlt, vor der Installation von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden.<br>**HINWEIS:** *Zertifiziert* bedeutet, dass das Betriebssystem vollständig getestet wurde und unterstützt wird. |
| Betriebssystem (unterstützt) | Aktuelle Version der Service Packs für die zertifizierten Betriebssysteme<br>**HINWEIS:** *Unterstützt* bedeutet, dass das Betriebssystem noch nicht getestet wurde; es ist jedoch davon auszugehen, dass es funktioniert. |
| Virtualisierungssystem | ◆ Hyper-V Server 2012 R2<br>◆ VMWare ESX 5.0 und höher<br>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 | ◆ compat-2008.5.6-6.1.i586.rpm (32-Bit-System)<br>Alternativ:<br>compat-32bit-2008.5.6-6.1.x86_64.rpm (64-Bit-System)<br>◆ Gettext-Dienstprogramm (nur für Linux-Computer) |

# 46 Installation von Analyzer

In diesem Abschnitt finden Sie die Schritte für die Installation von Analyzer und die Konfiguration Ihrer Umgebung für Analyzer.



## 46.1 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 46.2, „Automatische Installation von Analyzer“, auf Seite 440.

Überprüfen Sie in Vorbereitung auf die Installation die Voraussetzungen und Systemanforderungen in Abschnitt 45.1, „Checkliste für die Installation von Analyzer“, auf Seite 435.

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 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 im Verzeichnis `products/Analyzer/` aus:
   - **4a** **Linux:** `./install.bin`
   - **4b** **Windows:** `install.exe`
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 auf einem Linux-Computer die in Abschnitt 46.3, „Hinzufügen von XULrunner zur Analyzer.ini auf Linux-Plattformen“, auf Seite 440 aufgeführten Schritte 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 488.

## 46.2 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 46.3, „Hinzufügen von XULrunner zur Analyzer.ini auf Linux-Plattformen“, auf Seite 440 aufgeführten Schritte aus.

7 Aktivieren Sie Analyzer gemäß den Anweisungen in „Aktivieren von Analyzer“, auf Seite 488.

## 46.3 Hinzufügen von XULrunner zur Analyzer.ini auf Linux-Plattformen

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:
   - **Linux:** `home/admin/analyzer`
   - **Windows:** `C:\NetIQ\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.

## 46.4 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 je einen XDAS-Client für Linux und für Windows. 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:
   - **Linux:** Installieren Sie den erforderlichen Client (32 Bit oder 64 Bit) mit dem Befehl `rpm`.
   - **Windows:** Starten Sie die `.msi`-Datei. Der Windows-Client steht nur in einer 32-Bit-Version zur Verfügung.
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.

# XV 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. Weitere Informationen zum OSP finden Sie in Abschnitt 4.5, „Verwenden des Single-Sign-On-Zugriffs in Identity Manager“, auf Seite 42.

# 47 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. Informieren Sie sich, wie Identity Manager den Single-Sign-On-Zugriff über OSP vornimmt. Weitere Informationen finden Sie in Abschnitt 4.5, „Verwenden des Single-Sign-On-Zugriffs in Identity Manager“, auf Seite 42. |
| ❑ | 2. Installieren Sie OSP. Weitere Informationen finden Sie in Teil XI, „Installieren der Passwortverwaltungskomponente“, auf Seite 279. |
| ❑ | 3. Installieren Sie die Identitätsanwendungen. Weitere Informationen finden Sie in Teil XII, „Installieren der Identitätsanwendungen“, auf Seite 295. |
| ❑ | 4. (Optional) Installieren Sie die Identitätsberichterstellung. Weitere Informationen finden Sie in Teil XIII, „Installieren der Identitätsberichterstellung“, auf Seite 391. |
| ❑ | 5. Konfigurieren Sie die Identitätsanwendungen für den Single-Sign-On-Zugriff per OSP. Weitere Informationen finden Sie in Kapitel 48, „Single-Sign-On-Zugriff in Identity Manager mit One SSO Provider (OSP)“, auf Seite 447. |
| ❑ | 6. Installieren Sie das gewünschte Authentifizierungssystem für Identity Manager. Beispiel: Access Manager oder Kerberos. |
| ❑ | 7. (Bedingt) Konfigurieren Sie Access Manager und OSP. Weitere Informationen finden Sie in Kapitel 49, „Single Sign-On per SAML-Authentifizierung mit NetIQ Access Manager“, auf Seite 451. |
| ❑ | 8. Überprüfen Sie die Single-Sign-On-Einstellungen. Weitere Informationen finden Sie in Kapitel 51, „Überprüfen des Single-Sign-On-Zugriffs auf die Identitätsanwendungen“, auf Seite 465. |

# 48 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.

## 48.1 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 Abschnitt 39.4, „Konfigurieren des Identitätsdepots für die Identitätsanwendungen“, auf Seite 357 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.

## 48.2 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 40.1, „Ausführen des Konfigurationsprogramms der Identitätsanwendungen“, auf Seite 367.
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. Weitere Informationen finden Sie unter Kapitel 32, „Installieren der Passwortverwaltung für Identity Manager“, auf Seite 285.
- 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. Weitere Informationen finden Sie in Kapitel 32, „Installieren der Passwortverwaltung für Identity Manager“, auf Seite 285.

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. Weitere Informationen finden Sie unter Kapitel 32, „Installieren der Passwortverwaltung für Identity Manager“, auf Seite 285.
- 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 Portnummern für die folgenden Identity Manager-Komponenten:

- Katalogadministrator
- Identity Manager-Dashboard
- Identitätsberichterstellung
- Benutzeranwendung

**4** Speichern Sie die Änderungen mit **OK**, und schließen Sie das Konfigurationsprogramm.

**5** Starten Sie Tomcat.

## 48.3 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. Der standardmäßige Pfad zur Keystore-Datei für SSPR lautet:

- **Linux/UNIX:** `/[Java_Home]/lib/security/cacerts`
- **Windows:** `C:\[Java_Home]\lib\security\cacerts`

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).

# 49 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).

## 49.1 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.

## 49.2 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.



### 49.2.1 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 49.2.2, „Installieren des Access Manager-Zertifikats im Identity Manager-Truststore“, auf Seite 453.

## 49.2.2 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/idm/apps/jre/bin/keytool -keystore /opt/netiq/idm/apps/jre/lib/security/cacerts -storepass <Passwort> -importcert -trustcacerts -alias <NAM-Zert> -file custom_location/<exportierte_Datei>`
4. Installieren Sie das OSP-Zertifikat im Access Manager-Truststore.

   Weitere Informationen finden Sie in Abschnitt 49.2.3, „Installieren des SSL-Serverzertifikats im Access Manager-Truststore“, auf Seite 453.

## 49.2.3 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 49.4.2, „Erstellen eines Attributsatzes für SAML“, auf Seite 455.

## 49.3 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 40.1, „Ausführen des Konfigurationsprogramms der Identitätsanwendungen“, auf Seite 367.
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.

## 49.4 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:

- Abschnitt 49.4.1, „Kopieren der Metadaten für Identity Manager“, auf Seite 454
- Abschnitt 49.4.2, „Erstellen eines Attributsatzes für SAML“, auf Seite 455
- Abschnitt 49.4.3, „Hinzufügen von Identity Manager als verbürgter Dienstanbieter“, auf Seite 455

### 49.4.1 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 455 zugreifen können.

## 49.4.2 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**.

## 49.4.3 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 454 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 455 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**.

## 49.5 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/nam/idp/webapps/nidp/jsp`.

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**.

# 50 Single Sign-On mit Kerberos

Sie können Kerberos als Authentifizierungsmethode mit Single Sign-On (SSO) für die Identitätsanwendungen verwenden. Hiermit erhalten die Benutzer außerdem die Möglichkeit, sich über die integrierte Windows-Authentifizierung bei den Anwendungen anzumelden. In diesem Abschnitt finden Sie Anweisungen, wie Sie Active Directory für den Aufbau von Verbindungen mit den Identitätsanwendungen über Kerberos konfigurieren:



## 50.1 Konfigurieren des Kerberos-Benutzerkontos in Active Directory

Konfigurieren Sie Active Directory für die Kerberos-Authentifizierung mit den Active Directory-Verwaltungstools. Sie müssen ein neues Active Directory-Benutzerkonto für die Identitätsanwendungen und die Identitätsberichterstellung erstellen. Der Namen des Benutzerkontos muss den DNS-Namen des Servers enthalten, auf dem die Identitätsanwendungen und die Identitätsberichterstellung gehostet werden.

---

**HINWEIS:** Geben Sie Domänen oder Bereiche in Großbuchstaben an. Beispiel: `@MEINEFIRMA.COM`.

---

1 Erstellen Sie als Administrator in Active Directory mit der Microsoft Management Console (MMC) ein neues Benutzerkonto mit dem DNS-Namen des Servers, der die Identitätsanwendungen hostet.

   Wenn der DNS-Name des Identitätsanwendungsservers beispielsweise `rbpm.meinefirma.de` lautet, erstellen Sie den Benutzer anhand der folgenden Informationen:

   **Vorname:** rbpm

   **Benutzeranmeldename:** HTTP/rbpm.meinefirma.de

   **Prä-Windows-Anmeldename:** rbpm

   **Passwort einstellen:** Geben Sie das entsprechende Passwort an. Beispiel: `Passw0rt`.

   **Kennwort läuft nie ab:** Wählen Sie diese Option.

   **Benutzer muss Kennwort bei der nächsten Anmeldung ändern:** Belassen Sie diese Option deaktiviert.

2 Weisen Sie den neuen Benutzer dem Dienstprinzipalnamen (SPN) zu.

   **2a** Öffnen Sie auf dem Active Directory-Server eine cmd-Shell.

   **2b** Geben Sie Folgendes in die Befehlszeile ein:

   ```
   setspn -A HTTP/DNS_Identity_Applications_server@WINDOWS-DOMAIN userID
   ```

   Beispiel:

```
setspn -A HTTP/rbpm.mycompany.com@MYCOMPANY.COM rbpm
```

**2c** Überprüfen Sie „setspn“. Geben Sie hierzu `setspn -L` *`Benutzer-ID`* ein.

**3** So generieren Sie die `keytab`-Datei mit dem `ktpass`-Dienstprogramm:

**3a** Geben Sie Folgendes in die Befehlszeile ein:

```
ktpass /out filename.keytab /princ servicePrincipalName /mapuser
userPrincipalName /mapop set /pass password /crypto ALL /ptype
KRB5_NT_PRINCIPAL
```

Beispiel:

```
ktpass /out rbpm.keytab /princ HTTP/rbpm.mycompany.com@MYCOMPANY.COM /mapuser
rbpm  /mapop set /pass Passw0rd /crypto All /ptype KRB5_NT_PRINCIPAL
```

---

**WICHTIG:** Geben Sie Domänen oder Bereiche in Großbuchstaben an. Beispiel: `@MEINEFIRMA.COM`.

---

**3b** Kopieren Sie die Datei `rbpm.keytab` zum Identitätsanwendungsserver.

**4** Erstellen Sie als Administrator in Active Directory über die MMC ein Endbenutzerkonto als Vorbereitung für SSO.

Der Name des Endbenutzerkontos muss mit einem Attributwert eines eDirectory-Benutzers übereinstimmen, damit das Single Sign-On unterstützt werden kann. Erstellen Sie den Benutzer mit einem Namen wie `cnano`, notieren Sie das Passwort, und deaktivieren Sie die Option **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**.

**5** (Optional) Wiederholen Sie diese Schritte für die Identitätsberichterstellung, wenn Sie die Berichterstellungskomponente auf einem separaten Server installiert haben.

**6** Konfigurieren Sie den Server für die Identitätsanwendungen, um die Kerberos-Konfiguration zu akzeptieren. Weitere Informationen finden Sie unter Abschnitt 50.2, „Konfigurieren des Identitätsanwendungsservers“, auf Seite 460.

## 50.2 Konfigurieren des Identitätsanwendungsservers

Sie müssen den Identitätsanwendungsserver für die Verwendung der Kerberos-Keytab-Datei und des Benutzerkontos konfigurieren, das Sie in Active Directory erstellt haben. Führen Sie zunächst die Anweisungen in Abschnitt 50.1, „Konfigurieren des Kerberos-Benutzerkontos in Active Directory“, auf Seite 459 aus, bevor Sie den Vorgang fortsetzen.

---

**HINWEIS:** Geben Sie Domänen oder Bereiche in Großbuchstaben an. Beispiel: `@MEINEFIRMA.COM`.

---

**1** Führen Sie die folgenden Schritte durch, um die Betriebssystemeinstellungen für die Kerberos-Konfiguration zu definieren:

**1a** Öffnen Sie die `KRB5`-Datei in einem Texteditor auf dem Server, der die Identitätsanwendungen hostet.

**Linux:** `/etc/krb5.conf`

**Windows:** `C:\Windows\krb5.ini`

**UNIX:** `/etc/krb5/krb5.conf`

**1b** Fügen Sie der `KRB5`-Datei die folgenden Informationen hinzu:

```
[libdefaults]
    default_realm = WINDOWS-DOMAIN
    kdc_timesync = 0
    forwardable = true
    proxiable = false
[realms]
    WINDOWS-DOMAIN = {
         kdc = FQDN Active Directory Server
         admin_server = FQDN Active  Directory Server
    }
[domain_realm]
    .your.domain = WINDOWS-DOMAIN
    your.domain = WINDOWS-DOMAIN
```

Beispiel:

```
[libdefaults]
    default_realm = MYCOMPANY.COM
    kdc_timesync = 0
    forwardable = true
    proxiable = false
[realms]
    MYCOMPANY.COM = {
         kdc = myadserver.mycompany.com
         admin_server = myadserver.mycompany.com
    }
[domain_realm]
    .mycompany.com = MYCOMPANY.COM
    mycompany.com = MYCOMPANY.COM
```

**1c** Speichern Sie die Änderungen, und schließen Sie die `krb5`-Datei.

**2** (Bedingt) Führen Sie die folgenden Schritte durch, um die Kerberos-Konfigurationsinformationen für Tomcat zu definieren:

**2a** Erstellen Sie auf dem Tomcat-Anwendungsserver eine Beispieldatei `Kerberos_login.config` mit dem folgenden Inhalt:

---

**HINWEIS:** Der novlua-Benutzer benötigt Berechtigungen zur Erstellung der Datei `Kerberos_login.config`.

---

```
com.sun.security.jgss.krb5.accept {
    com.sun.security.auth.module.Krb5LoginModule required
    debug="true"
    refreshKrb5Config="true"
    useTicketCache="true"
    ticketCache="/opt/netiq/idm/apps/tomcat/kerberos/spnegoTicket.cache"
    doNotPrompt="true"
    principal="HTTP/DNS_Identity_Applications_server@WINDOWS-DOMAIN"
    useKeyTab="true"
        keyTab="/absolute_path/filename.keytab"
    storeKey="true";
    };
```

Beispiel auf einem Windows-Server:

```
keyTab="c:\\NetIQ\\IdentityManager\\apps\\tomcat\kerberos\\rbpm.keytab"
```

**2b** Geben Sie in der Datei Werte für `principal` und `keyTab` an. Beispiel:

```
principal="HTTP/rbpm.mycompany.com@MYCOMPANY.COM"
keyTab="/home/usr/rbpm.keytab"
```

- Der Wert für `principal` muss identisch sein mit dem Wert, den Sie für Kerberos angegeben haben. Weitere Informationen finden Sie unter Schritt 3 auf Seite 460.
- Geben Sie den absoluten Pfad der `keytab`-Datei auf Ihrem Identitätsanwendungsserver an. Die Datei muss sich nicht im Standardverzeichnis für die Identitätsanwendungen befinden.

**2c** Verweisen Sie mit der folgenden Zeile auf die Datei `Kerberos_login.config` in der JVM-Datei `java.security`:

```
login.config.url.1=file:/opt/netiq/idm/apps/tomcat/kerberos/
Kerberos_login.config
```

Der angegebene Pfad ist der standardmäßige Installationsspeicherort für einen Linux-Server.

Beispiel einer `java.security`-Datei auf einem Windows-Server:

```
login.config.url.1=file:c:/NetIQ/IdentityManager/apps/tomcat/kerberos/
Kerberos_login.config
```

**3** Führen Sie die folgenden Schritte durch, um die Authentifizierungsmethode im RBPM-Konfigurationsprogramm anzugeben:

**3a** Öffnen Sie das `configupdate`-Dienstprogramm.

**3b** Klicken Sie auf die Registerkarte **Authentifizierung**.

**3c** Blättern Sie nach unten zum Abschnitt **Authentifizierungsmethode**.

**3d** Wählen Sie im Feld **Methode** die Option **Kerberos**.

**3e** Wählen Sie im Feld **Zuordnungsattributname** die Option `cn`.

---

**HINWEIS:** Weitere Informationen zum RBPM-Konfigurationsprogramm finden Sie in Kapitel 40, „Konfigurieren der Einstellungen für die Identitätsanwendungen“, auf Seite 367.

---

**4** (Optional) Wiederholen Sie diese Schritte für die Identitätsberichterstellung, wenn Sie die Berichterstellungskomponente auf einem separaten Server installiert haben.

**5** Konfigurieren Sie die Browser, über die Endbenutzer auf die Identitätsanwendungen zugreifen. Weitere Informationen finden Sie unter Abschnitt 50.3, „Konfigurieren der Endbenutzer-Browser für die Verwendung der integrierten Windows-Authentifizierung“, auf Seite 462.

## 50.3 Konfigurieren der Endbenutzer-Browser für die Verwendung der integrierten Windows-Authentifizierung

Die Browser, über die Ihre Endbenutzer auf die Identitätsanwendungen und Identitätsberichterstellung zugreifen, müssen auch für die integrierte Windows-Authentifizierung konfiguriert sein. In diesem Abschnitt finden Sie Anweisungen zur Konfiguration eines Endbenutzer-Computers zur Unterstützung des Single-Sign-on-Zugriffs mit der integrierten Windows-Authentifizierung.

**HINWEIS:** Sie müssen diesen Vorgang für jeden Endbenutzer-Computer wiederholen, auf dem Sie den Single-Sign-on-Zugriff auf die Identitätsanwendungen und Identitätsberichterstellung bereitstellen.

1. Melden Sie sich auf dem Computer an, auf dem Benutzer Single-Sign-on-Zugriff benötigen.
2. Öffnen Sie die Systemsteuerung mit den Internetoptionen.
3. Klicken Sie auf **Sicherheit**.
4. Klicken Sie auf **Vertrauenswürdige Sites** und dann auf **Sites**.
5. Fügen Sie den DNS-Namen des Identitätsanwendungsservers hinzu.

   Beispiel: `rbpm.meinefirma.de`
6. Klicken Sie auf **Hinzufügen** und dann auf **Schließen**.
7. Klicken Sie auf **Stufe anpassen...**.
8. Wählen Sie unter **Benutzerauthentifizierung** die Option **Automatic logon with current user name and password** (Automatische Anmeldung mit aktuellem Benutzernamen und Passwort).
9. Klicken Sie auf **OK**.
10. Klicken Sie in den Internetoptionen auf **Erweitert**.
11. Wählen Sie unter „Sicherheit“ die Option **Enable Integrated Windows Authentication** (Integrierte Windows-Authentifizierung aktivieren) aus.
12. Wiederholen Sie diesen Vorgang für jeden Endbenutzer-Computer, auf dem Sie den Single-Sign-on-Zugriff auf die Identitätsanwendungen und Identitätsberichterstellung bereitstellen.

# 51 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:

- Katalogadministrator: `/rra`
- 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 40, „Konfigurieren der Einstellungen für die Identitätsanwendungen“, auf Seite 367.

**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.

# 52 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.

**HINWEIS:** Für die Kommunikation zwischen SSPR und OSP müssen Sie das SSL-Protokoll verwenden.

Zum Generieren eines Zertifikats benötigen Sie eine Zertifizierungsstelle, einen Keystore sowie eine Zertifizierungsantragsdatei (`.csr`) im Keystore. Das Verfahren ist abhängig davon, ob Sie ein selbstsigniertes Zertifikat oder ein Zertifikat von einer gültigen Zertifizierungsstelle benötigen.

## 52.1 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. Stellen Sie sicher, dass ein Keystore zur Verfügung steht, in dem die Authentifizierungszertifikate gespeichert werden können. Weitere Informationen finden Sie in Abschnitt 52.5, „Erstellen eines Keystore und eines Zertifizierungsantrags“, auf Seite 470. |
| ❑ | 2. (Bedingt) In einer Testumgebung verwenden Sie selbstsignierte Zertifikate. Weitere Informationen finden Sie in Abschnitt 52.6, „Aktivieren von SSL mit einem selbstsignierten Zertifikat“, auf Seite 471. |
| ❑ | 3. (Bedingt) In einer Produktionsumgebung importieren Sie ein signiertes Zertifikat. Weitere Informationen finden Sie in Abschnitt 52.7, „Aktivieren von SSL mit einem signierten Zertifikat“, auf Seite 472. |
| ❑ | 4. Stellen Sie sicher, dass der Authentifizierungsserver, die Identitätsanwendungen und die Identitätsberichterstellung für die Unterstützung der SSL-Kommunikation konfiguriert sind. Weitere Informationen finden Sie in Abschnitt 52.2, „Aktualisieren der SSL-Einstellungen im Konfigurationsprogramm“, auf Seite 468. |
| ❑ | 5. Generieren Sie Client-Zertifikate, und kopieren Sie sie auf die Client-Arbeitsstationen. Weitere Informationen finden Sie in Abschnitt 52.8, „Überprüfen der Client-Arbeitsstationen auf Zertifikate“, auf Seite 474. |
| ❑ | 6. Prüfen Sie, ob eine sichere Kommunikation zwischen Sentinel und den Identity Manager-Komponenten konfiguriert ist. Weitere Informationen finden Sie unter Abschnitt 52.9, „Aktivieren von SSL zwischen Sentinel und Identity Manager-Komponenten“, auf Seite 474. |

## 52.2 Aktualisieren der SSL-Einstellungen im Konfigurationsprogramm

Beim Installieren der Identitätsanwendungen und der Identitätsberichterstellung sollten Sie die Kommunikationsmethode *https* angeben. Beispiel: *„Protokoll“, auf Seite 331*. Nach der Installation können Sie dann mit dem RBPM-Konfigurationsprogramm festlegen, dass die Anwendungen über SSL kommunizieren sollen. Weitere Informationen zu diesen Parametern finden Sie in Kapitel 40, „Konfigurieren der Einstellungen für die Identitätsanwendungen“, auf Seite 367.

1. Halten Sie Tomcat an. Beispiel: `/etc/init.d/idmapps_tomcat_init stop`.
2. Navigieren Sie zum RBPM-Konfigurationsprogramm (standardmäßig im Installationsverzeichnis der Identitätsanwendungen). Beispiel: `/opt/netiq/idm/apps/UserApplication`.
3. Starten Sie das Konfigurationsprogramm an der Eingabeaufforderung mit einem der folgenden Befehle:
   - **Linux:** `./configupdate.sh`
   - **Windows:** `configupdate.bat`

   **HINWEIS:** Unter Umständen dauert das Starten des Dienstpogramms mehrere Minuten.
4. Klicken Sie auf **Authentifizierung**, und bearbeiten Sie die folgenden Einstellungen:

   **TCP-Port für OAuth-Server**

   Gibt den Port für den Authentifizierungsserver an.

   **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.
5. Klicken Sie auf **SSO-Clients**.

6 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`.

7 Speichern Sie die Änderungen im Konfigurationsprogramm.

## 52.3 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.

## 52.4 Aktualisieren der SSL-Einstellungen für den Anwendungsserver

Der Anwendungsserver, der die Identitätsanwendungen und die Identitätsberichterstellung hostet, muss so konfiguriert werden, dass er die SSL-Konfiguration unterstützt. In diesem Abschnitt finden Sie Anweisungen für die Aktualisierung eines Tomcat-Anwendungsservers, bei dem es sich um den Standardanwendungsserver handelt.

1 Halten Sie Tomcat an.

   Beispiel: `/ect/init.d/idmapps_tomcat_init stop`.

2 Navigieren Sie zum `conf`-Verzeichnis für Tomcat, das sich standardmäßig unter `opt/netiq/idm/apps/tomcat/conf` befindet.

3 Im `/conf`-Verzeichnis muss sich eine Keystore-Datei befinden. Beispiel: `idmapps.keystore`.

   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 52.5, „Erstellen eines Keystore und eines Zertifizierungsantrags“, auf Seite 470.

4 Öffnen Sie in einem Texteditor die Datei `server.xml` im `conf`-Verzeichnis.

5 Fügen Sie in der `server.xml`-Datei folgenden Inhalt hinzu:

```
<Connector port="port_number" protocol="HTTP/1.1" maxThreads="150"
SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLS" keystoreFile="path_to_file/filename.keystore"
keystorePass="password"
```

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"
```

NetIQ empfiehlt Ihnen, in „keystorePass“ ein verschlüsseltes Passwort anzugeben anstatt eines Klartext-Passworts. Weitere Informationen zur Verwendung von Klartext-Passwörtern und verschlüsselten Passwörtern in der SSL-Kommunikation finden Sie unter Sichern von Tomcat.

6 Starten Sie Tomcat.

Beispiel: `/ect/init.d/idmapps_tomcat_init start`.

## 52.5 Erstellen eines Keystore und eines Zertifizierungsantrags

Ein Keystore ist eine Java-Datei, die Verschlüsselungsschlüssel und (optional) Sicherheitszertifikate enthält. Der Keystore wird mit dem Java-Dienstprogramm in der JRE erstellt. Sie erstellen die `JKS`-Datei, generieren ein Zertifikat und importieren dann das Zertifikat im 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.

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 Geben Sie zum Erstellen des Keystores den folgenden Befehl ein:

```
cd /opt/netiq/idm/apps/tomcat/conf
export PATH=/opt/netiq/idm/jre/bin:$PATH
```

3 Geben Sie zum Erstellen des Keystores den folgenden Befehl ein:

```
keytool -genkey -alias keystore_name -keyalg RSA -keystore
keystore_name.keystore -validity 3650
```

Beispiel:

```
keytool -genkey -alias IDMkey -keyalg RSA -keystore IDMkey.keystore -validity
3650
```

4 Wenn Sie dazu aufgefordert werden, geben Sie die Parameterwerte gemäß den folgenden Überlegungen an:

- Wenn Sie nach Ihrem Vor- und Nachnamen gefragt werden, geben Sie den vollständig qualifizierten Namen des Servers ein. 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 Generieren Sie den Zertifizierungsantrag mit den folgenden Schritten:

**6a** Erstellen Sie im Verzeichnis „conf“ eine einfache Textdatei mit dem Namen *`Ihr_Antrag`*`.csr`. Beispiel: `IDMZertAntrag.csr`.

**6b** Geben Sie in der Befehlszeile den folgenden Befehl ein:

```
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.

7 (Bedingt) Reichen Sie zur Erstellung eines signierten Zertifikats die `CRS`-Datei bei einer gültigen Zertifizierungsstelle ein.

8 Kopieren Sie die Keystore-Datei in das Verzeichnis `tomcat/conf` für jede Anwendungsserverinstanz, in der Sie die Identitätsberichterstellung und SSPR bereitgestellt haben.

## 52.6 Aktivieren von SSL mit einem selbstsignierten Zertifikat

Verwenden Sie in Ihrer Testumgebung nach Möglichkeit ein eigensigniertes Zertifikat, da dieses einfacher zu beschaffen ist als ein signiertes Zertifikat von einer gültigen Zertifizierungsstelle.


- Abschnitt 52.6.1, „Exportieren der Zertifizierungsstelle“, auf Seite 471
- Abschnitt 52.6.2, „Generieren eines selbstsignierten Zertifikats“, auf Seite 472


### 52.6.1 Exportieren der Zertifizierungsstelle

Mit iManager können Sie die Zertifizierungsstelle (CA) aus Ihrem eDirectory-Server exportieren und so ein selbstsigniertes 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 > Selbstsigniertes Zertifikat**.

6 Wählen Sie das gewünschte selbstsignierte Zertifikat aus.

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 Verschieben Sie die gespeicherte `cert.der`-Datei in ein Verzeichnis, in dem das exportierte Zertifikat gespeichert werden soll.

### 52.6.2 Generieren eines selbstsignierten Zertifikats

Zum Erstellen eines selbstsignierten Zertifikats benötigen Sie einen Keystore und eine Zertifizierungsantragsdatei.

1 Erstellen Sie einen Keystore und eine Zertifizierungsantragsdatei.

Weitere Informationen finden Sie in Abschnitt 52.5, „Erstellen eines Keystore und eines Zertifizierungsantrags“, auf Seite 470.

2 Melden Sie sich bei iManager an.

3 Navigieren Sie zu **Certificate Server > Zertifikat ausstellen**.

4 Navigieren Sie zur `.csr`-Datei, die Sie in Schritt 6 auf Seite 471 erstellt haben.

5 Klicken Sie zweimal auf **Weiter**.

6 Wählen Sie unter „Zertifikattyp“ die Option **Nicht angegeben**.

7 Klicken Sie zweimal auf **Weiter**.

8 Aktualisieren Sie die SSL-Einstellungen im Konfigurationsprogramm. Weitere Informationen finden Sie in Abschnitt 52.2, „Aktualisieren der SSL-Einstellungen im Konfigurationsprogramm“, auf Seite 468.

9 Starten Sie Tomcat neu.

## 52.7 Aktivieren von SSL mit einem 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. NetIQ empfiehlt Ihnen, die Dokumentation für den Anwendungsserver zu beachten, damit das Zertifikat fehlerfrei importiert wird.

Bei diesem Verfahren wird vorausgesetzt, dass Ihnen ein signiertes Zertifikat einer gültigen Zertifizierungsstelle vorliegt. Weitere Informationen finden Sie in Abschnitt 52.5, „Erstellen eines Keystore und eines Zertifizierungsantrags“, auf Seite 470.

**So verwenden Sie ein signiertes Zertifikat und SSL:**

1 Legen Sie eine Kopie des Zertifikats im Konfigurationsverzeichnis auf dem Anwendungsserver ab. Beispiel: `opt/netiq/idm/apps/tomcat/conf`.

---

**HINWEIS**

- Wenn Sie die Identitätsanwendungen, die Identitätsberichterstellung, OSP und SSPR auf verschiedenen Instanzen des Anwendungsservers bereitstellen, muss jede Instanz eine Kopie des Zertifikats erhalten.
- Speichern Sie außerdem eine Sicherungskopie dieses Zertifikats in einem sicheren Speicherort.

---

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.

**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.cer
```

Beispiel:

```
keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file
IDMTESTREE.cer
```

---

**HINWEIS:** Sie müssen das Alias **Root** eingeben.

---

Wenn das Zertifikat ordnungsgemäß importiert wurde, wird die Meldung **Zertifikat wurde zum Keystore hinzugefügt** angezeigt.

**3c** Überprüfen Sie, ob das signierte Zertifikat fehlerfrei ist. Führen Sie hierzu den nachfolgenden Befehl im Verzeichnis `conf` aus.

```
keytool -list -v -alias root -keystore your.keystore
```

Beispiel:

```
keytool -list -v -alias root -keystore IDMkey.keystore
```

Der Server zeigt eine Liste der selbstsignierten und der signierten Zertifikate an.

4 Halten Sie Tomcat an.

5 (Bedingt) Aktivieren Sie SSL für Tomcat mit den folgenden Schritten:

**5a** Öffnen Sie die Datei `server.xml` (standardmäßig im Verzeichnis `netiq/idm/apps/tomcat/conf`) in einem Texteditor.

**5b** Kommentieren Sie den folgenden Abschnitt in der Datei aus bzw. fügen Sie den folgenden Abschnitt hinzu:

```
<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" />
```

Hierbei gilt:

**keystoreFile**

Gibt den Pfad zur `userapp.keystore`-Datei an, die sich standardmäßig im Verzeichnis `/netiq/idm/apps/tomcat/conf/userapp.keystore` befindet.

**keystorePass**

Gibt das Passwort für die `userapp.keystore`-Datei an.

Überprüfen Sie, ob die richtigen Werte für `keystoreFile` und `keystorePass` angegeben wurden. NetIQ empfiehlt Ihnen, in „keystorePass“ ein verschlüsseltes Passwort anzugeben anstatt eines Klartext-Passworts. Weitere Informationen zur Verwendung von Klartext-Passwörtern und verschlüsselten Passwörtern in der SSL-Kommunikation finden Sie unter Sichern von Tomcat.

Weitere Informationen zum Aktivieren von SSL für Tomcat finden Sie unter SSL Configuration HOW-TO (Anweisungen zur SSL-Konfiguration).

6 Aktualisieren Sie die SSL-Einstellungen für die Identitätsanwendungen, die Berichterstellung und SSPR. Weitere Informationen finden Sie unter Abschnitt 52.2, „Aktualisieren der SSL-Einstellungen im Konfigurationsprogramm“, auf Seite 468.

7 Starten Sie Tomcat neu.

## 52.8 Überprüfen der Client-Arbeitsstationen auf Zertifikate

Auf den Arbeitsstationen aller Benutzer, die auf die Identitätsanwendungen zugreifen, muss ein passendes Client-Zertifikat zu den Zertifikaten vorliegen, die Sie für Tomcat generiert haben. Beim Zugriff auf Identity Manager stellt SSL mithilfe der Client-Zertifikate die Identität eines Benutzers dar. Die Zertifikate dienen zur Authentifizierung des Clients beim Server.

## 52.9 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 selbstsigniertes Serverzertifikat erstellen und exportieren. Verwenden Sie ein signiertes Zertifikat, das von einer gültigen Zertifizierungsstelle ausgestellt wurde.

- Abschnitt 52.9.1, „Aktivieren von SSL zwischen Sentinel und Identity Manager-Engine/Remote Loader“, auf Seite 475
- Abschnitt 52.9.2, „Aktivieren von SSL zwischen Sentinel und Benutzeranwendung“, auf Seite 476

## 52.9.1 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 Exportieren Sie das in Schritt 1 erstellte CA-Zertifikat des eDirectory-Servers in das Base64-Format:

   **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 Importieren Sie das Zertifikat in den Truststore des Revisions-Connectors:

   **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** Kopieren Sie den privaten Schlüssel und die Zertifikate, die Sie in Schritt 3 und Schritt 4 erstellt haben, in die folgenden Speicherorte je nach Ihren Komponenten:

| Komponente | Linux-Pfad | Windows-Pfad |
|---|---|---|
| Identity Manager-Engine | `/var/opt/novell/eDirectory/data/dib` | `C:\NetIQ\IdentityManager\NDS\DIBFiles` |
| Remote Loader | `/var/opt/novell/dirxml/rdxml` | Remote Loader-Installationsverzeichnis:<br>`C:\NetIQ\IdentityManager\RemoteLoader`<br>ODER<br>`C:\NetIQ\IdentityManager\RemoteLoader\64bit`<br>ODER<br>`C:\NetIQ\IdentityManager\RemoteLoader\32bit` |
| .NET Remote Loader | | `C:\NetIQ\IdentityManager\RemoteLoader.NET` |
| Fan-out-Agent | `/opt/novell/dirxml/fanoutagent` | `C:\NetIQ\IdentityManager\FanoutAgent` |

**9** Starten Sie die Identity Manager-Dienste neu.

## 52.9.2 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 E-Mail-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 Benutzeranwendungen an.

**6** Fügen Sie den privaten Schlüssel und das Zertifikat in `configupdate.sh` ein.

**6a** Öffnen Sie `configupdate.sh`.

**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 in `configupdate.sh`.

**7** Starten Sie die Benutzeranwendungen neu.

**8** Exportieren Sie das in Schritt 1 erstellte CA-Zertifikat des eDirectory-Servers in das Base64-Format:

**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** Importieren Sie das Zertifikat in den Truststore des Revisions-Connectors:

**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.

# 53 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:



## 53.1 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.

## 53.2 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.

## 53.2.1 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*.

## 53.2.2 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 53.2.3, „Erstellen des Passwortrichtlinienobjekts im Identitätsdepot“, auf Seite 480 und Abschnitt 53.2.4, „Erstellen einer benutzerdefinierten Passwortrichtlinie“, auf Seite 481.

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.

## 53.2.3 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-Passwortrichtlinienobjekts im Identitätsdepot die Attribute aus der Datei; gehen Sie dazu folgendermaßen vor:

**Linux:**

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`.

**Windows:**

Führen Sie `ldapmodify.exe` im Verzeichnis `install/utilities` des Identity Manager-Installations-Kits aus.

## 53.2.4 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 53.2.3, „Erstellen des Passwortrichtlinienobjekts im Identitätsdepot“, auf Seite 480.

### 53.2.5 Erstellen des Standard-Benachrichtigungssammlungs-Objekts im Identitätsdepot

Die Standard-Benachrichtigungssammlung ist ein Identitätsdepotobjekt, das einen Satz von Schablonen für E-Mail-Benachrichtigungen enthält, sowie ein Server, der zum Senden von aus Schablonen erstellten E-Mails 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.

## 53.3 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.

## 53.4 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.

## 53.5 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.

## 53.6 Konfigurieren von Sentinel Log Management für IGA

Sie können die Verbindung zwischen Sentinel Log Management für IGA (Sentinel) und den Ereignisquellen, die Daten an Sentinel liefern (z. B. Identitätsberichterstellung und OSP), überwachen und verwalten. Die Ereignisquellenverwaltung (Live-Ansicht) in Sentinel hilft Ihnen dabei.


- Abschnitt 53.6.1, „Prüfen auf Sentinel-Ereignisse“, auf Seite 484
- Abschnitt 53.6.2, „Konfigurieren der Collector-Instanzen in Sentinel“, auf Seite 484
- Abschnitt 53.6.3, „Konfigurieren der Ereignisdatenbeibehaltung“, auf Seite 484
- Abschnitt 53.6.4, „Konfigurieren der Speicherplatznutzung für Sentinel“, auf Seite 484
- Abschnitt 53.6.5, „Konfigurieren der Richtlinie für die Rohdatenbeibehaltung in Sentinel“, auf Seite 485
- Abschnitt 53.6.6, „Konfigurieren der Sentinel-Link-Verbindung“, auf Seite 485

## 53.6.1 Prüfen auf Sentinel-Ereignisse

1. Melden Sie sich als Administrator bei der Sentinel-Hauptoberfläche an.

   `https://<IP-Adresse/DNS-Sentinel-Server:8443>/sentinel/views/main.html`

2. Klicken Sie auf der Symbolleiste **Anwendungen** > **Kontrollzentrum starten** an.

   Alternativ:

   Klicken Sie auf der Symbolleiste **Sammlung** > **Erweitert** > **Kontrollzentrum starten** an.

3. Melden Sie sich beim Sentinel-Kontrollzentrum an.
4. Klicken Sie in der Symbolleiste auf **Ereignisquellenverwaltung** > **Live-Ansicht**.

## 53.6.2 Konfigurieren der Collector-Instanzen in Sentinel

Konfigurieren Sie in der Ereignisquellenverwaltungsansicht manuell die folgenden Collectoren:

**NetIQ iManager und NetIQ One SSO Provider (OSP)**

Beachten Sie Schritt 7 in der **Kurzanleitung zur Collector-Konfiguration** auf der Website der Sentinel-Plugins. Die Abläufe beim Konfigurieren beider Collectoren sind identisch.

**NetIQ-Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung**

Beachten Sie den Abschnitt **Manuelle Ereignisquellenkonfiguration** auf der Website der Sentinel-Plugins.

## 53.6.3 Konfigurieren der Ereignisdatenbeibehaltung

Die Ereignisdatenbeibehaltung bestimmt den Zeitraum, über den Sentinel verschiedene Arten von Ereignisdaten im System beibehält, bis sie gelöscht werden.

1. Melden Sie sich als Administrator bei der Sentinel-Weboberfläche an.
2. Klicken Sie auf **Speicher** > **Ereignisse**.
3. Wählen Sie unter **Datenbeibehaltung** die Option **Standard-Datenbeibehaltung** und klicken Sie auf **Bearbeiten**.
4. Geben Sie Folgendes für die Ereignisdatenbeibehaltung an:

   **Richtlinienname:** Gibt den Namen für die Datenbeibehaltung an.

   **Mindestens aufbewahren:** Geben Sie den Zeitraum an, über den die Ereignisse im Sentinel-System gespeichert bleiben sollen. Der Standardwert ist 7 Tage.

   Der Wert muss eine positive Ganzzahl kleiner oder gleich dem Wert im Feld „Höchstens aufbewahren“ sein.

   **Höchstens aufbewahren:** Geben Sie den Zeitraum an, über den die Ereignisse im Sentinel-System gespeichert bleiben sollen. Der Standardwert ist 21 Tage.

   Der Wert muss eine positive Ganzzahl größer oder gleich dem Wert im Feld **Mindestens aufbewahren** sein.

5. Klicken Sie auf **Speichern**.

## 53.6.4 Konfigurieren der Speicherplatznutzung für Sentinel

1. Melden Sie sich als Administrator bei der Sentinel-Hauptoberfläche an.
2. Klicken Sie auf **Speicher** > **Ereignisse**.

3 Geben Sie unter **Speicherplatznutzung** die folgenden Werte in das Feld **Primäre Speichernutzung** ein:

- **Datenlöschung aus primärem Speicher starten, wenn zu __ % gefüllt:** Geben Sie den Grenzwert an, ab dem das Löschen der Ereignisdaten gestartet werden soll.
- **Anhalten, wenn zu __ % gefüllt:** Geben Sie den Grenzwert an, unter dem das Bereinigen des Speicherplatzes angehalten werden soll. Der freigegebene Speicherplatz sollte für die Ereignisdaten eines vollen Tages ausreichen.

## 53.6.5 Konfigurieren der Richtlinie für die Rohdatenbeibehaltung in Sentinel

Die Richtlinie für die Rohdatenbeibehaltung bestimmt den Zeitraum, über den Sentinel die Rohdaten im System beibehält, bevor sie gelöscht werden. Standardmäßig ist diese Option deaktiviert. Wenn Sie die Richtlinie aktivieren, legen Sie einen geeigneten Wert für die Rohdatenbeibehaltung gemäß Ihren Anforderungen fest. Bei einem höheren Wert für die Rohdatenbeibehaltung wird mehr Speicherplatz belegt.

Sie können die Werte für **Höchstens aufbewahren** und **Mindestens aufbewahren** bearbeiten, die den maximalen und minimalen Zeitraum (in Tagen) bestimmen, über den die Rohdatendatei im System gespeichert bleiben soll. Alle Dateien, die die Aufbewahrungsdauer übersteigen, werden dauerhaft aus dem Datenspeicher entfernt.

1 Melden Sie sich als Administrator bei der Sentinel-Hauptoberfläche an.

2 Klicken Sie auf **Speicher** > **Ereignisse**.

3 Wählen Sie unter **Datenbeibehaltung** die Option **Rohdatenbeibehaltung** und klicken Sie auf **Bearbeiten**.

4 **Mindestens aufbewahren:** Geben Sie den Zeitraum an, über den die Rohdaten im Sentinel-System gespeichert bleiben sollen.

   Der Wert muss eine positive Ganzzahl kleiner oder gleich dem Wert im Feld **Höchstens aufbewahren** sein.

   **Höchstens aufbewahren:** Geben Sie den Zeitraum an, über den die Rohdaten im Sentinel-System gespeichert bleiben sollen.

   Der Wert muss eine positive Ganzzahl größer oder gleich dem Wert im Feld **Mindestens aufbewahren** sein.

## 53.6.6 Konfigurieren der Sentinel-Link-Verbindung

Sie können Ereignisse von NetIQ Sentinel an Sentinel Log Management für IGA weiterleiten. In einer Sentinel-Link-Lösung wird das Sentinel-System, das die Ereignisse weiterleitet, als Absender bezeichnet und das Sentinel-System, bei dem die Ereignisse eingehen, entsprechend als Empfänger. Sie können mehrere Sentinel-Systeme gleichzeitig mit einem einzigen Empfängersystem verknüpfen. Zum Konfigurieren eines Sentinel-Links müssen Sie mindestens zwei Systeme konfigurieren: den Absender-Computer und dem Empfänger-Computer. Weitere Informationen zum Konfigurieren von Sentinel Link finden Sie im Überblick zu Sentinel Link.

# 53.7 Aktivieren von Identity Manager

Einige Identity Manager-Komponenten werden automatisch aktiviert, sobald Sie sich erstmalig anmelden. Andere Komponenten müssen dagegen explizit aktiviert werden.



## 53.7.1 Installation einer Produktaktivierungsberechtigung

NetIQ empfiehlt, die Produktaktivierungsberechtigung mit iManager zu installieren.

---

**HINWEIS:** Aktivieren Sie für jeden zu verwendenden Treiber den Treibersatz, in dem sich ein Treiber befindet. Sie können mit dem Berechtigungsnachweis jeden Baum aktivieren.

---

1. Nach dem Erwerb einer Lizenz erhalten Sie von NetIQ eine E-Mail 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**.

## 53.7.2 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.

## 53.7.3 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 53.7.1, „Installation einer Produktaktivierungsberechtigung“, auf Seite 486 aus. Weitere Informationen zu den Treibern finden Sie auf der Website der Identity Manager-Treiberdokumentation.

## 53.7.4 Aktivieren bestimmter Identity Manager-Komponenten

In diesem Abschnitt wird beschrieben, wie Sie bestimmte Komponenten für Identity Manager aktivieren.


- „Aktivieren von Designer und des Katalogadministrators“, auf Seite 488
- „Aktivieren von Analyzer“, auf Seite 488
- „Aktivieren von Sentinel Log Management für IGA“, auf Seite 488


### Aktivieren von Designer und des Katalogadministrators

Wenn Sie die Identity Manager-Engine oder die Identity Manager-Treiber aktivieren, werden auch Designer und der Katalogadministrator aktiviert.

### 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. (Bedingt) Rufen Sie mit den folgenden Schritten eine Analyzer-Lizenz ab:
   - **2a** Klicken Sie im Fenster **Analyzer-Aktivierung** auf **Ich brauche eine Lizenz**.
   - **2b** Navigieren Sie zur Analyzer-Lizenz, die Sie vom NetIQ-Kundenservice-Portal erhalten haben, und wählen Sie sie aus.
   - **2c** Kopieren Sie den Aktivierungscode, und schließen Sie das Kundenservice-Portal.
3. Klicken Sie im Fenster **Analyzer-Aktivierung** auf `Neue Lizenz hinzufügen`.
4. Geben Sie im Fenster **Lizenz** den Aktivierungscode ein, den Sie aus dem NetIQ-Kundenservice-Portal heruntergeladen haben, 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.

### 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 489
- „Hinzufügen eines Lizenzschlüssels über die Befehlszeile“, auf Seite 489

## 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**.

# XVI Aufrüsten von Identity Manager

In diesem Abschnitt finden Sie Informationen zum Aufrüsten der Identity Manager-Komponenten. Anweisungen zum Migrieren der vorhandenen Daten auf einen neuen Server finden Sie in Teil XVII, „Migrieren der Identity Manager-Daten in eine neue Installation“, auf Seite 545. Weitere Informationen zum Unterschied zwischen Aufrüstung und Migration finden Sie in Abschnitt 54.2, „Erläuterungen zur Aufrüstung und zur Migration“, auf Seite 495.

# 54 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.



## 54.1 Checkliste für die Aufrüstung von Identity Manager

NetIQ empfiehlt, die Schritte in der nachfolgenden Checkliste für die Aufrüstung auszuführen.

| | **Checkliste** |
|---|---|
| ❑ | 1. Informieren Sie sich über die Unterschiede zwischen Aufrüstung und Migration. Weitere Informationen finden Sie in Abschnitt 54.2, „Erläuterungen zur Aufrüstung und zur Migration“, auf Seite 495. |
| ❑ | 2. Rüsten Sie auf Identity Manager 4.5 auf. Von Versionen vor 4.5 können Sie nicht auf Version 4.6 aufrüsten oder migrieren. Weitere Informationen finden Sie im Einrichtungshandbuch zu NetIQ Identity Manager 4.5. |
| ❑ | 3. Stellen Sie sicher, dass das aktuelle 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 23. |
| ❑ | 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 6, „Überlegungen und Voraussetzungen für die Installation“, auf Seite 61 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 54.5, „Sichern der aktuellen Konfiguration“, auf Seite 500. |
| ❑ | 7. Rüsten Sie Designer auf die aktuelle Version auf. Weitere Informationen finden Sie in Abschnitt 55.1, „Aufrüstung von Designer“, auf Seite 503. |

| | Checkliste |
|---|---|
| ❑ | 8. Installieren Sie iManager auf die aktuelle Version für Identity Manager, oder rüsten Sie iManager auf diese Version auf. Beachten Sie einen der folgenden Abschnitte:<br>◆ **Installation:** „Installieren von iManager“, auf Seite 215<br>◆ **Upgrade:** „Aktualisieren von iManager“, auf Seite 504 |
| ❑ | 9. Rüsten Sie eDirectory auf dem Server, auf dem Identity Manager ausgeführt wird, auf die aktuelle Version und den aktuellen Patch auf.<br>Falls Sie eDirectory 9.0 (oder höher) in einer Umgebung installieren, in der der neueste 64-Bit-Remote Loader bereits aufgerüstet ist, wird die eDirectory-Installation nicht durchgeführt und der Remote Loader funktioniert nicht mehr. Führen Sie vor der Aufrüstung von eDirectory die folgenden Schritte durch, um sicherzustellen, dass der Remote Loader ordnungsgemäß funktioniert:<br>1. Stoppen Sie den Remote Loader und seine Instanzen.<br>2. Deinstallieren Sie die `novell-DXMLopensslx`-RPM.<br>3. Installieren Sie eDirectory 9.0 oder eine neuere Version.<br>Die Aufrüstung von eDirectory hält ndsd an, wodurch wiederum alle Treiber angehalten werden. Weitere Informationen finden Sie im *NetIQ eDirectory-Installationshandbuch* und in den Versionshinweisen zu NetIQ Identity Manager 4.6. |
| ❑ | 10. Aktualisieren Sie die iManager-Plugins auf dieselbe Version wie iManager. Weitere Informationen finden Sie in Abschnitt 55.2.6, „Aktualisieren von iManager-Plugins nach einer Aufrüstung oder Neuinstallation“, auf Seite 510. |
| ❑ | 11. Halten Sie die Treiber an, die mit dem Server verknüpft sind, auf dem Sie die Identity Manager-Engine (Metadirectory) installiert haben. Weitere Informationen finden Sie in Abschnitt 16.2.1, „Anhalten der Treiber“, auf Seite 148. |
| ❑ | 12. Rüsten Sie die Identity Manager-Engine auf. Weitere Informationen finden Sie in Abschnitt 55.4, „Aufrüsten der Identity Manager-Engine“, auf Seite 511.<br>**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 58.4, „Migrieren der Identity Manager-Engine auf einen neuen Server“, auf Seite 553. |
| ❑ | 13. (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 55.3, „Aufrüstung von Remote Loader“, auf Seite 510. |
| ❑ | 14. (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 55.8, „Aufrüsten der Identity Manager-Treiber“, auf Seite 532.<br>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. |
| ❑ | 15. Führen Sie eine Migration von EAS zu Sentinel for Log Management für IGA (Sentinel) durch. Weitere Informationen finden Sie in Abschnitt 55.6.2, „Migrieren des Ereignisrevisionsdiensts in Sentinel for Log Management für IGA“, auf Seite 522. |
| ❑ | 16. Rüsten Sie Tomcat und PostgreSQL auf, oder installieren Sie die aktuelle Version. Weitere Informationen finden Sie in Teil IX, „Installieren von PostgreSQL und Tomcat für Identity Manager“, auf Seite 255. |

| | Checkliste |
|---|---|
| ❑ | 17. (Bedingt) Installieren Sie OSP, falls nicht bereits installiert. Weitere Informationen finden Sie in Teil X, „Installieren der Single-Sign-on-Komponente“, auf Seite 267. |
| ❑ | 18. (Bedingt) Installieren Sie SSPR, falls nicht bereits installiert. Weitere Informationen finden Sie unter Teil XI, „Installieren der Passwortverwaltungskomponente“, auf Seite 279.<br><br>**HINWEIS:** Installieren Sie SSPR, falls Sie derzeit mit dem bisherigen Anbieter für die Passwortverwaltung arbeiten. Weitere Informationen finden Sie in Abschnitt 4.4.2, „Erläuterungen zum bisherigen Anbieter für die Passwortverwaltung“, auf Seite 41. |
| ❑ | 19. Rüsten Sie die Benutzeranwendung, das Identity Manager-Dashboard, OSP, SSPR und den Katalogadministrator mit dem Aufrüstungsprogramm auf. Weitere Informationen finden Sie unter Abschnitt 55.5, „Aufrüsten von Identitätsanwendungen und der unterstützenden Komponenten“, auf Seite 512.<br><br>Alternativ lassen sich diese Komponenten auch manuell aufrüsten. Weitere Informationen finden Sie in Teil XVII, „Migrieren der Identity Manager-Daten in eine neue Installation“, auf Seite 545. |
| ❑ | 20. Rüsten Sie die Identitätsberichterstellung und die zugehörigen Treiber auf. Weitere Informationen finden Sie in Abschnitt 55.6, „Aufrüsten der Identitätsberichterstellung“, auf Seite 522. |
| ❑ | 21. Starten Sie die Treiber für die Identitätsanwendungen und die Identity Manager-Engine. Weitere Informationen finden Sie in Abschnitt 16.2.2, „Starten der Treiber“, auf Seite 148. |
| ❑ | 22. (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 55.9, „Hinzufügen von neuen Servern zum Treibersatz“, auf Seite 534. |
| ❑ | 23. (Bedingt) Wenn Sie benutzerdefinierte Richtlinien und Regeln verwenden, stellen Sie die benutzerdefinierten Einstellungen wieder her. Weitere Informationen finden Sie in Abschnitt 55.10, „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“, auf Seite 536. |
| ❑ | 24. Aktivieren Sie die aufgerüstete Identity Manager-Lösung. Weitere Informationen finden Sie in Abschnitt 53.7, „Aktivieren von Identity Manager“, auf Seite 486. |

## 54.2 Erläuterungen zur Aufrüstung und zur Migration

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.

### Aufrüstung

Im Allgemeinen lassen sich die Identity Manager 4.5 Standard und Advanced Edition problemlos aufrüsten.

- **Identity Manager 4.5 Standard Edition:** Wenn aktuell Identity Manager 4.5 Standard Edition installiert ist, können Sie sie direkt zu Identity Manager 4.6 Standard Edition aufrüsten. Weitere Informationen finden Sie in der *Kurzanleitung für die Installation und Aktualisierung von NetIQ Identity Manager 4.6 Standard Edition*.

Wählen Sie für die Aufrüstung von Identity Manager 4.5 Standard Edition zu Identity Manager 4.6 Advanced Edition eine der folgenden Methoden:

- Rüsten Sie von Identity Manager 4.5 Standard Edition auf Identity Manager 4.6 Standard Edition auf und führen Sie dann die Aufrüstung auf Identity Manager 4.6 Advanced Edition durch. Weitere Informationen finden Sie in der *Kurzanleitung für die Installation und Aktualisierung von NetIQ Identity Manager 4.6 Standard Edition*.
- Rüsten Sie von Identity Manager 4.5 Standard Edition auf Identity Manager 4.5 Advanced Edition auf und führen Sie dann die Aufrüstung auf Identity Manager 4.6 Advanced Edition durch. Weitere Informationen finden Sie in der *Kurzanleitung für die Installation und Aktualisierung von NetIQ Identity Manager 4.6 Standard Edition*.

- **Identity Manager 4.5 Advanced Edition:** Wenn aktuell Identity Manager 4.5 Advanced Edition installiert ist, können Sie sie direkt zu Identity Manager 4.6 Advanced Edition aufrüsten. Weitere Informationen finden Sie unter Abschnitt 54.1, „Checkliste für die Aufrüstung von Identity Manager“, auf Seite 493.

### Migration

In bestimmten Fällen ist die Aufrüstung nicht möglich. Stattdessen müssen Sie eine **Migration** vornehmen. Beispiel:

- **Nicht unterstütztes Betriebssystem:** Wenn Identity Manager derzeit auf einem Server installiert ist, auf dem ein mittlerweile nicht mehr unterstütztes Betriebssystem ausgeführt wird, ist eine Migration anstelle einer Aufrüstung erforderlich.

  In der folgenden Tabelle finden Sie Informationen zu den Betriebssystemen, die die Migration oder Vor-Ort-Aufrüstung unterstützen.

| Betriebssystem | Direktaufrüstung | Migration |
|---|---|---|
| SLES 11 SP4 und 12 SP1 | Ja | nicht zutreffend |
| RHEL 6.8 und 7.3 | Ja | nicht zutreffend |
| Windows 2012 R2 | Ja | nicht zutreffend |
| Windows 2012 | Ja | nicht zutreffend |

- **Identity Manager 4.0.2:** Wenn Sie derzeit mit Identity Manager 4.0.2 mit oder ohne RBPM arbeiten, ist keine direkte Aufrüstung möglich. Führen Sie die folgenden Vorgänge aus:
  - Rüsten Sie auf Identity Manager 4.5 Advanced Edition auf.
  - Rüsten Sie auf Identity Manager 4.6 Advanced Edition auf.
  - Migrieren Sie die rollenbasierten Daten (Identitätsanwendungen). Weitere Informationen finden Sie in Abschnitt 58.7, „Aufrüsten der Identitätsanwendungen“, auf Seite 556.

Wenn Sie mehrere Server mit einem Treibersatz verknüpft haben, können Sie eine Aufrüstung oder eine Migration nur auf einem Server gleichzeitig durchführen. Wenn Sie nicht genügend Zeit haben, um die Server zum gleichen Zeitpunkt aufzurüsten, arbeiten die Treiber weiterhin mit den verschiedenen Versionen von Identity Manager, bis die Upgrades für jeden Server abgeschlossen werden können.

Die Identity Manager-Engine ist abwärtskompatibel, sodass die Identity Manager 4.6-Engine die Treiber von Identity Manager 4.5. ohne Probleme ausführen kann. Sie müssen den Rollen- und Ressourcentreiber jedoch unmittelbar nach dem Aufrüsten der Identity Manager-Engine aufrüsten.

**WICHTIG:** Wenn Sie Funktionen für Treiber aktivieren, die nur unter Identity Manager 4.6 oder höher unterstützt werden, arbeiten die Treiber nicht mehr auf den Servern mit gemischten Versionen. Die älteren Engines können die neue Funktionalität nicht verarbeiten. Dies deaktiviert die Treiber, bis alle Server auf Identity Manager 4.6 oder höher aufgerüstet wurden.

### 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. Wenn Sie die Advanced Edition bereits aktiviert haben und nun zu einer Standard Edition wechseln möchten, erhalten Sie automatisch Zugang zu allen Funktionen der Standard Edition. Falls Sie jedoch ausschließlich die Funktionen der Standard Edition nutzen möchten, müssen Sie weitere Schritte ausführen. Weitere Informationen finden Sie unter „Wechseln von der Advanced Edition zur Standard Edition“, auf Seite 498.

## 54.3 Unterstützte Aufrüstungspfade

Die folgende Tabelle zeigt die Kombinationen der Versionen von Identity Manager und eDirectory für die Aufrüstung von Identity Manager 4.5.5 oder 4.5.4 auf Version 4.6.

Die Identity Manager-Komponenten müssen in einer bestimmten Reihenfolge aufgerüstet werden. NetIQ empfiehlt, vor dem Starten der Aufrüstung die Informationen in den entsprechenden Versionshinweisen zu Ihrer aktuellen Version zu lesen:

- Versionshinweise zu NetIQ Identity Manager 4.5 Service Pack 5
- Versionshinweise zu NetIQ Identity Manager 4.5 Service Pack 4

| Basisversion | Aufgerüstete Version |
|---|---|
| Identity Manager 4.5.5 mit eDirectory 9.0.2 | Identity Manager 4.6 mit eDirectory 9.0.2 |
| Identity Manager 4.5.5 mit eDirectory 9.0.1 | Identity Manager 4.6 mit eDirectory 9.0.2 |
| Identity Manager 4.5.5 mit eDirectory 8.8.8 SP9 | Identity Manager 4.6 mit eDirectory 8.8.8 SP9 |
| | Identity Manager 4.6 mit eDirectory 9.0.2 |
| Identity Manager 4.5.5 mit eDirectory 8.8.8 SP8 | Identity Manager 4.6 mit eDirectory 8.8.8 SP9 |
| | Identity Manager 4.6 mit eDirectory 9.0.2 |
| Identity Manager 4.5.4 (oder höher) mit eDirectory 9.0.1 | Identity Manager 4.6 mit eDirectory 9.0.2 |
| Identity Manager 4.5.4 mit eDirectory 8.8.8 SP8 | Identity Manager 4.6 mit eDirectory 8.8.8 SP9 |
| | Identity Manager 4.6 mit eDirectory 9.0.2 |

### 54.3.1 Aufrüsten von Version 4.5.3 oder 4.5

Zum Aufrüsten von Identity Manager 4.5.3 oder 4.5 müssen Sie zunächst auf Version 4.5.4 aufrüsten.

Die Identity Manager-Komponenten müssen in einer bestimmten Reihenfolge aufgerüstet werden. NetIQ empfiehlt, vor dem Starten der Aufrüstung die Informationen in den entsprechenden Versionshinweisen zu Ihrer aktuellen Version zu lesen:

- 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

| Basisversion | Zwischenversion | Aufgerüstete Version |
|---|---|---|
| Identity Manager 4.5.3 mit eDirectory 8.8.8 SP7 | Identity Manager 4.5.4 mit eDirectory 9.0.1 | Identity Manager 4.6 mit eDirectory 9.0.2 |
| | Identity Manager 4.5.4 mit eDirectory 8.8.8 SP8 | Identity Manager 4.6 mit eDirectory 8.8.8 SP9 |
| Identity Manager 4.5 mit eDirectory 8.8.8 SP3 | Identity Manager 4.5.4 mit eDirectory 8.8.8 SP8 | Identity Manager 4.6 mit eDirectory 8.8.8 SP9 |

## 54.4 Wechseln von der Advanced Edition zur Standard Edition

So wechseln Sie von der Advanced Edition zur Standard Edition:

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`.

     **Linux:** `/var/opt/novell/eDirectory/data/dib`

     **Windows:** `C:\Novell\NDS\DIBFiles`
   - **2b** Erstellen Sie eine neue Datei, geben Sie den Namen `.idme` ein und tragen Sie die Zahl 2 in die Datei ein.
   - **2c** Starten Sie 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. Entfernen Sie die folgenden WAR-Dateien und den Webapps-Ordner aus dem Tomcat-Verzeichnis `Webapps`:

   **Linux:** `/opt/netiq/idm/apps/tomcat/webapps`

   **Windows:** `C:\netiq\/idm\apps\tomcat\webapps`

   - `IDMProv*`
   - `IDMRPT*`

- `dash*`
- `idmdash*`
- `landing*`
- `rra*`
- `rptdoc*`

6 Verschieben Sie die folgenden vorhandenen Ordner in ein Sicherungsverzeichnis:
   - `IDMReporting`
   - `UserApplication`

7 Kopieren Sie die Datei `ism-configuration.properties` aus dem Verzeichnis `<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. `192.99.17.22`
     - **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://192.99.17.22:8180/IDMRPT`
   - Zurücksetzen von Passwörtern per Selbstbedienung
     - **OAuth-Client-ID**. Beispiel: *sspr*
     - OAuth-Client-Geheimnis. Beispiel: <*SSPR-Client-Geheimnis*>
     - **OSP-OAuth-Umleitungs-URL**. Beispiel: `http://192.99.179.202:8180/sspr/public/oauth`

   Weitere Informationen zum Konfigurationsprogramm finden Sie in „Ausführen des Konfigurationsprogramms der Identitätsanwendungen“, auf Seite 367.

10 Speichern Sie die Änderungen und schließen Sie das Konfigurationsprogramm.

11 Starten Sie Tomcat.

12 (Bedingt) Aktivieren Sie die Standard Edition, sofern noch nicht aktiviert.

# 54.5 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 54.5.1, „Exportieren des Designer-Projekts“, auf Seite 500
- Abschnitt 54.5.2, „Exportieren der Treiberkonfiguration“, auf Seite 501

## 54.5.1 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 500
- „Erstellen eines neuen Projekts aus dem Identitätsdepot“, auf Seite 501

### 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:
   - **Hostname:** IP-Adresse oder DNS-Name des Identitätsdepot-Servers
   - **Benutzername:** DN des Benutzers, mit dem die Authentifizierung beim Identitätsdepot erfolgt
   - **Passwort:** Passwort des Authentifizierungsbenutzers
9. Klicken Sie auf **Weiter**.
10. Lassen Sie die Optionen „Identitätsdepot - Schema“ und „Standard-Benachrichtigungssammlung“ ausgewählt.
11. Erweitern Sie die Standard-Benachrichtigungssammlung, und heben Sie die Auswahl der nicht benötigten Sprachen auf.

    Die Standard-Benachrichtigungssammlungen sind in viele unterschiedliche Sprachen übersetzt. Sie können alle Sprachen importieren oder nur die Sprachen auswählen, die Sie verwenden.
12. Klicken Sie auf **Durchsuchen** , suchen Sie das Verzeichnis und wählen Sie einen Treibersatz aus, den Sie importieren möchten.
13. Wiederholen Sie Schritt 12 für jeden Treibersatz in diesem Identitätsdepot und klicken Sie anschließend auf **Fertig stellen**.
14. Klicken Sie auf **OK**, nachdem das Projekt importiert wurde.
15. Wenn Sie nur ein Identitätsdepot haben, sind Sie fertig. Wenn Sie mehrere Identitätsdepots haben, fahren Sie mit Schritt 16 fort.
16. Klicken Sie in der Symbolleiste auf **Live > Importieren**.
17. Wiederholen Sie Schritt 8 bis Schritt 14 für jedes weitere Identitätsdepot.

## 54.5.2 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 502
- „Exportieren der Treiberdaten mithilfe von iManager“, auf Seite 502

## 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.

# 55 Aufrüsten der Identity Manager-Komponenten

In diesem Abschnitt finden Sie Informationen zum Aufrüsten einzelner Komponenten in Identity Manager. So können Sie beispielsweise Designer auf die aktuelle Version aufrüsten, ohne iManager aufzurüsten. Dieser Abschnitt enthält außerdem einige Schritte, die unter Umständen nach einer Aufrüstung anfallen.



## 55.1 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 vom Identity Manager-Datenträger:
   - **Linux:** `products/Designer/install`

     Führen Sie die Binärdatei aus, indem Sie `./install` eingeben.
   - **Windows:** `products\Designer\install.exe`
4. Wählen Sie die Sprache aus, in der Sie Designer installieren möchten, und lesen und akzeptieren Sie dann die Lizenzvereinbarung.
5. Geben Sie das Verzeichnis an, in dem Designer installiert ist, und klicken Sie anschließend auf **Ja** in der Meldung, die besagt, dass Designer bereits installiert ist.
6. Wählen Sie aus, ob auf Ihrem Desktop und in Ihrem Desktop-Menü eine Verknüpfung erstellt werden soll.
7. Prüfen Sie die Zusammenfassung und klicken Sie auf **Installieren**.
8. Lesen Sie die Versionshinweise, und klicken Sie auf **Weiter**.
9. Wählen Sie, dass Designer gestartet werden soll, und klicken Sie dann auf **Fertig**.

10 Geben Sie einen Speicherort für Ihren Designer-Arbeitsbereich an und klicken Sie auf **OK**.

11 Klicken Sie in der Warnmeldung, die angibt, dass Ihr Projekt geschlossen und konvertiert werden muss, auf **OK**.

12 Erweitern Sie das Projekt in der Ansicht **Projekt** und doppelklicken Sie auf **Projekt muss konvertiert werden**.

13 Prüfen Sie die Schritte, die der Assistent zum Konvertieren des Projekts durchführt, und klicken Sie auf **Weiter**.

14 Geben Sie einen Namen für die Sicherung Ihres Projekts an und klicken Sie auf **Weiter**.

15 Lesen Sie die Zusammenfassung der Aktionen, die bei der Konvertierung durchgeführt werden, und klicken Sie anschließend auf **Konvertieren**.

16 Lesen Sie die Zusammenfassung nach der Konvertierung und klicken Sie auf **Öffnen**.

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).

## 55.2 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.

Wenn Sie mit eDirectory 8.8.8 Patch 9 arbeiten, rüsten Sie die iManager-Version auf 2.7.7 Patch 9 auf. Wenn Sie mit eDirectory 9.0.2 arbeiten, rüsten Sie die iManager-Version auf 3.0.2 Patch 1 auf. Die Installationsdateien für iManager 3.0.2 Patch 1 befinden sich im Verzeichnis `<ISO-Extraktionsverzeichnis>/products/iManager/installs/linux` und die Installationsdateien für iManager 2.7.7 Patch 9 befinden sich im Verzeichnis `<ISO-Extraktionsverzeichnis>/products/iManager277/installs/linux`.

Der Aufrüstvorgang umfasst die folgenden Aufgaben:

- Abschnitt 55.2.1, „Aufrüsten von iManager unter Linux“, auf Seite 505
- Abschnitt 55.2.2, „Aufrüsten von iManager unter Windows“, auf Seite 506
- Abschnitt 55.2.3, „Automatische Aufrüstung von iManager“, auf Seite 508
- Abschnitt 55.2.4, „Aktualisieren funktionsbasierter Services“, auf Seite 508
- Abschnitt 55.2.5, „Neuinstallieren oder Migrieren von Plugin Studio-Plugins“, auf Seite 509
- Abschnitt 55.2.6, „Aktualisieren von iManager-Plugins nach einer Aufrüstung oder Neuinstallation“, auf Seite 510

## 55.2.1 Aufrüsten von iManager unter Linux

Wenn das Setup-Programm für iManager Server eine zuvor installierte Version von iManager erkennt, haben Sie die Möglichkeit, den Installationsvorgang anzuhalten oder die vorhandenen iManager-, JRE- und Tomcat-Installationen zu entfernen.

Stellen Sie vor dem Aufrüsten von iManager sicher, dass der Computer den Voraussetzungen und Systemanforderungen entspricht. Weitere Informationen finden Sie hier:

- Versionshinweise zur Aufrüstung
- Für iManager beachten Sie Abschnitt 22.4.2, „Überlegungen für die Installation von iManager auf einer Linux-Plattform“, auf Seite 221.
- Für iManager Workstation beachten Sie Abschnitt 22.4.4, „Überlegungen für die Installation von iManager Workstation auf Linux-Clients“, auf Seite 222.

---

**HINWEIS:** Beim Aufrüsten werden die Werte für den HTTP-Port und den SSL-Port verwendet, die in der früheren iManager-Version konfiguriert waren.

---

**So rüsten Sie iManager Server unter Linux auf:**

1. Melden Sie sich als `Root` oder als `Root`-Äquivalent an dem Computer an, auf dem das Installationsprogramm ausgeführt werden soll.
2. (Bedingt) Wenn Sie die Konfigurationsdateien `server.xml` und `context.xml` geändert haben, legen Sie eine Sicherungskopie dieser Dateien in einem anderen Speicherort ab, bevor Sie die Aufrüstung vornehmen.

   Der Aufrüstungsprozess ersetzt die Konfigurationsdateien.
3. Suchen Sie auf der NetIQ Downloads-Website nach iManager-Produkten, wählen Sie die gewünschte iManager-Version aus, und laden Sie die `.tgz`-Datei in ein Verzeichnis auf dem Server herunter. Beispiel: `iMan_version_linux.tgz`.
4. Extrahieren Sie den iManager-Ordner mit dem folgenden Befehl:

   ```
   tar -zxvf iMan_Version_linux.tgz
   ```
5. Wechseln Sie in einer Shell zum Verzeichnis */Extraktionsverzeichnis*`/iManager/installs/linux`.

   Dieser Pfad ist relativ zu dem Verzeichnis, in das Sie die iManager-Dateien kopiert bzw. extrahiert haben.
6. (Bedingt) Wenn Sie die Installation über die Befehlszeile durchführen möchten (textbasierte Installation), geben Sie den folgenden Befehl ein:

   ```
   ./iManagerInstallLinux.bin
   ```
7. (Bedingt) Soll der Assistent für das Installationsprogramm gestartet werden, geben Sie den folgenden Befehl ein:

   ```
   ./iManagerInstallLinux.bin -i gui
   ```
8. Wählen Sie im Eröffnungsbildschirm eine Sprache aus, und klicken Sie auf **OK**.
9. Wählen Sie in der Eingabeaufforderung **Aufrüsten**.
10. Lesen Sie die Einführung, und klicken Sie auf **Weiter**.
11. Akzeptieren Sie die **Lizenzvereinbarung** und klicken Sie auf **Weiter**.
12. (Optional) Sollen IPv6-Adressen in iManager verwendet werden, klicken Sie im Fenster „IPv6 aktivieren“ auf **Ja**.

Sobald Sie iManager aufgerüstet haben, können Sie IPv6-Adressen aktivieren. Weitere Informationen finden Sie in Abschnitt 24.2, „Konfigurieren von iManager nach der Installation für die Verwendung von IPv6-Adressen“, auf Seite 243.

13 Klicken Sie auf **Weiter**.

14 Lesen Sie die Informationen auf der Seite zur **Übersicht vor der Aufrüstung** und klicken Sie dann auf **Weiter**.

Der Aufrüstungsprozess kann mehrere Minuten in Anspruch nehmen. Im Rahmen des Vorgangs werden ggf. neue Dateien für iManager-Komponenten hinzugefügt oder die iManager-Konfiguration geändert. Weitere Informationen finden Sie in den Versionshinweisen für die Aufrüstung.

15 Klicken Sie nach Abschluss des Aufrüstvorgangs auf **Fertig**.

16 Klicken Sie nach der Initialisierung von iManager auf den ersten Link auf der Einführungsseite, und melden Sie sich an. Weitere Informationen finden Sie im Abschnitt Zugreifen auf iManager im *NetIQ iManager -Verwaltungshandbuch*.

17 (Bedingt) Wenn Sie vor Beginn des Aufrüstvorgangs Sicherungskopien der Konfigurationsdateien `server.xml` und `context.xml` erstellt haben, ersetzen Sie die neuen Konfigurationsdateien durch die Sicherungskopien.

## 55.2.2 Aufrüsten von iManager unter Windows

Wenn das Setup-Programm für iManager Server eine bereits installierte Version von iManager erkennt, werden Sie aufgefordert, die installierte Version aufzurüsten. Wenn Sie die Aufrüstung bestätigen, ersetzt das Programm die vorhandenen JRE- und Tomcat-Versionen durch die jeweils aktuelle Version. Außerdem wird iManager auf die neueste Version aufgerüstet.

Stellen Sie vor dem Aufrüsten von iManager sicher, dass der Computer den Voraussetzungen und Systemanforderungen entspricht. Weitere Informationen finden Sie hier:

- Versionshinweise zur Aufrüstung
- Für iManager beachten Sie Abschnitt 22.4.2, „Überlegungen für die Installation von iManager auf einer Linux-Plattform“, auf Seite 221.
- Für iManager Workstation beachten Sie Abschnitt 22.4.4, „Überlegungen für die Installation von iManager Workstation auf Linux-Clients“, auf Seite 222.

---

**HINWEIS:** Beim Aufrüsten werden die Werte für den HTTP-Port und den SSL-Port verwendet, die in der früheren iManager-Version konfiguriert waren.

---

**So installieren Sie iManager Server unter Windows:**

1 Melden Sie sich an dem Computer, auf dem iManager aufgerüstet werden soll, als Benutzer mit Administratorrechten an.

2 (Bedingt) Wenn Sie die Konfigurationsdateien `server.xml` und `context.xml` geändert haben, legen Sie eine Sicherungskopie dieser Dateien in einem anderen Speicherort ab, bevor Sie die Aufrüstung vornehmen.

Der Aufrüstungsprozess ersetzt die Konfigurationsdateien.

3 Suchen Sie auf der NetIQ Downloads-Website nach der gewünschten iManager-Version, und laden Sie die `win.zip`-Datei in ein Verzeichnis auf dem Server herunter. Beispiel: `iMan_277_win.zip`.

4 Extrahieren Sie die `win.zip`-Datei in den iManager-Ordner.

5 Führen Sie die Datei `iManagerInstall.exe` aus (standardmäßig im Ordner *`Extraktionsverzeichnis`*`\iManager\installs\win`).

6 Wählen Sie im Begrüßungsbildschirm von iManager eine Sprache aus, und klicken Sie auf **OK**.

7 Klicken Sie im Fenster **Einführung** auf **Weiter**.

8 Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf **Weiter**.

9 (Optional) Sollen IPv6-Adressen in iManager verwendet werden, klicken Sie im Fenster **IPv6 aktivieren** auf **Ja**.

Sobald Sie iManager aufgerüstet haben, können Sie IPv6-Adressen aktivieren. Weitere Informationen finden Sie in Abschnitt 24.2, „Konfigurieren von iManager nach der Installation für die Verwendung von IPv6-Adressen“, auf Seite 243.

10 Klicken Sie auf **Weiter**.

11 Wählen Sie in der Eingabeaufforderung **Aufrüsten**.

12 (Bedingt) Lesen Sie die Angaben im Fenster **Erkennungsübersicht**.

Im Fenster **Erkennungsübersicht** wird die aktuelle Version des Servlet-Containers und der JVM-Software angezeigt, die iManager nach dem Aufrüsten verwendet.

13 Klicken Sie auf **Weiter**.

14 Lesen Sie die Informationen auf der Seite **Übersicht vor der Installation** und klicken Sie auf **Installieren**.

Der Aufrüstungsprozess kann mehrere Minuten in Anspruch nehmen. Im Rahmen des Vorgangs werden ggf. neue Dateien für iManager-Komponenten hinzugefügt oder die iManager-Konfiguration geändert. Weitere Informationen finden Sie in den Versionshinweisen für die Aufrüstung.

15 (Bedingt) Wenn die folgende Meldung im Fenster **Installation abgeschlossen** angezeigt wird, führen Sie die folgenden Schritte aus:

```
The installation of iManager version is complete, but some errors occurred
during the install.
Please see the installation log Log file path for details. Press "Done" to quit
the installer.
```

**15a** Notieren Sie den Pfad zur Protokolldatei, der in der Fehlermeldung angezeigt wird.

**15b** Klicken Sie im Fenster **Installation abgeschlossen** auf **Fertig**.

**15c** Öffnen Sie die Protokolldatei.

**15d** (Bedingt) Wenn die Protokolldatei folgende Fehlermeldung enthält, können Sie die Fehlermeldung ignorieren: Die Installation wurde erfolgreich ausgeführt und iManager funktioniert ordnungsgemäß.

```
Custom Action: com.novell.application.iManager.install.InstallDLLs
Status: ERROR
Additional Notes: ERROR - class
com.novell.application.iManager.install.InstallDLLs
NonfatalInstallException C:\WINDOWS\system32\msvcr71.dll (The process
cannot access the file because it is being used by another process)
```

**15e** (Bedingt) Wenn die Protokolldatei den in Schritt 20d aufgeführten Fehler nicht enthält, empfiehlt NetIQ, die Installation zu wiederholen.

16 Klicken Sie auf **Fertig**.

17 Klicken Sie nach der Initialisierung von iManager auf den ersten Link auf der Einführungsseite, und melden Sie sich an. Weitere Informationen finden Sie im Abschnitt Zugreifen auf iManager im *NetIQ iManager -Verwaltungshandbuch*.

18 (Bedingt) Wenn Sie vor Beginn des Aufrüstvorgangs Sicherungskopien der Konfigurationsdateien `server.xml` und `context.xml` erstellt haben, ersetzen Sie die neuen Konfigurationsdateien durch die Sicherungskopien.

## 55.2.3 Automatische Aufrüstung von iManager

Für eine standardmäßige automatische Installation auf einem Linux- oder Windows-Server verwenden Sie die standardmäßigen Installationswerte.

1 Wählen Sie auf der NetIQ Downloads-Website die gewünschte iManager-Version aus. Beispiel:

- **Linux:** `iMan_`*`Version`*`_linux.tgz`
- **Windows:** `iMan_`*`Version`*`_win.zip`

2 Laden Sie die Aufrüstungsdatei in ein Verzeichnis auf dem Server herunter.

3 (Bedingt) Auf einem Windows-Computer extrahieren Sie die `win.zip`-Datei in den iManager-Ordner.

4 Wechseln Sie in einem Konsolenfenster in das Verzeichnis, in dem sich die heruntergeladene Aufrüstungsdatei befindet.

5 Geben Sie in der Befehlszeile einen der folgenden Befehle ein:

- **Linux**: `./iManagerInstall`*`Plattform`*`.bin -i silent`
- **Windows:** `iManagerInstall.exe -i silent`

## 55.2.4 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**. Weitere Informationen finden Sie in Abschnitt 22.3, „Erläuterungen zur Installation der iManager Plugins“, auf Seite 219.
- 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**.

## 55.2.5 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.

### 55.2.6 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. Weitere Informationen finden Sie unter Abschnitt 22.3, „Erläuterungen zur Installation der iManager Plugins“, auf Seite 219.

1. Öffnen Sie iManager.
2. Navigieren Sie zu **Konfigurieren > Plugin-Installation > Verfügbare Novell-Plugin-Module**.
3. Aktualisieren Sie die Plugins.

## 55.3 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. Der Standard-Speicherort lautet:
   - **Windows:** `C:\...\RemoteLoader\`*`Remote Loader-Name`*`-config.txt`
   - **Linux:** Erstellen Sie im „rdxml“-Pfad Ihre eigene Konfigurationsdatei.
2. Stellen Sie sicher, dass alle Treiber angehalten wurden. Eine Anleitung dazu finden Sie in Abschnitt 16.2.1, „Anhalten der Treiber“, auf Seite 148.
3. Halten Sie den Remote Loader-Service bzw. den Daemon für jeden Treiber an.
   - **Windows:** Wählen Sie in der Remote Loader-Konsole die Remote Loader-Instanz aus, und klicken Sie anschließend auf **Anhalten**.
   - **Linux:** `rdxml -config` *`Pfad_zur_Konfigurationsdatei`* `-u`
   - **Java Remote Loader:** `dirxml_jremote -config` *`Pfad_zur_Konfigurationsdatei`* `-u`
4. (Bedingt) Stoppen Sie den lcache-Vorgang im Windows Task Manager.
5. (Bedingt) Soll eine automatische Installation auf einem Windows-Server vorgenommen werden, muss die Datei `silent.properties` den Pfad zum Verzeichnis enthalten, in dem sich die installierten Remote Loader-Dateien befinden. Beispiel:

   ```
   X64_CONNECTED_SYSTEM_LOCATION=c:\novell\remoteloader\64bit
   ```

   Das Installationsprogramm erkennt den Standardpfad der bisherigen Installation nicht automatisch.
6. Führen Sie das Installationsprogramm für den Remote Loader aus.

   Durch den Installationsvorgang werden die Dateien und Binärdateien auf die aktuelle Version aufgerüstet. Weitere Informationen finden Sie in Teil V, „Installieren der Identity Manager-Engine, der Treiber und der iManager-Plugins“, auf Seite 139.
7. Stellen Sie nach Abschluss der Installation sicher, dass Ihre Konfigurationsdateien die Informationen Ihrer Umgebung enthalten.
8. (Bedingt) Falls ein Problem mit der Konfigurationsdatei auftritt, kopieren Sie die Sicherungsdatei, die Sie in Schritt 1 erstellt haben. Fahren Sie anderenfalls fort mit Schritt 9 auf Seite 510.
9. Starten Sie den Remote Loader-Service bzw. den Daemon für jeden Treiber.
   - **Java Remote Loader:** `dirxml_jremote -config` *`Pfad_zur_Konfigurationsdatei`*

- **Linux:** `rdxml -config Pfad_zu_Konfigurationsdatei`
- **Windows:** Wählen Sie in der Remote Loader-Konsole die Remote Loader-Instanz aus, und klicken Sie auf **Starten**.

## 55.4 Aufrüsten der Identity Manager-Engine

Nach dem Aufrüsten des Remote Loaders und der rollenbasierten Services können Sie die Identity Manager-Engine aufrüsten. Im Rahmen des Aufrüstungsvorgangs werden die Dateien des Treiberschnittstellenmoduls aktualisiert, die im Dateisystem des Hostcomputers gespeichert sind.

---

**HINWEIS:** Wenn Sie die Identity Manager-Engine aufrüsten oder separat eine SAML-Methode aktualisieren, zeigt iMonitor für SAML-Methoden die Statusflaggen „Vorhanden“ und „Nicht vorhanden“ an. Ignorieren Sie die Statusflagge „Nicht vorhanden“; eDirectory verwendet korrekt die aktualisierte Methode. Bei der Aufrüstung der Engine wird im Rahmen des Aufrüstungsvorgangs eDirectory neu gestartet, da es intern dafür sorgt, dass die aktualisierte SAML-Methode verwendet wird. Wenn Sie eine SAML-Methode separat aktualisieren, führen Sie den Neustart des Servers manuell aus, um die aktualisierte SAML-Methode zu verwenden.

---

### 55.4.1 Ausführen einer geführten Aufrüstung

1. Stellen Sie sicher, dass alle Treiber angehalten wurden. Weitere Informationen finden Sie in Abschnitt 16.2.1, „Anhalten der Treiber“, auf Seite 148.
2. Starten Sie das Installationsprogramm für die Identity Manager-Engine:
   - **Linux:** `IDMVersion_Lin/products/IDM/install.bin`
   - **Windows:** `IDMVersion_Win:\products\IDM\Windows\setup\idm_install.exe`
3. Wählen Sie die Sprache für die Installation aus.
4. Lesen Sie die Lizenzvereinbarung durch und bestätigen Sie Ihr Einverständnis.
5. Aktualisieren Sie die Identity Manager-Engine und die Dateien der Treiberschnittstellenmodule mit den folgenden Optionen:
   - **Identity Manager Server**
   - **iManager-Plugins für Identity Manager**
   - **Treiber**
6. Geben Sie einen Benutzer und das Benutzerpasswort mit Verwaltungsrechten für eDirectory im LDAP-Format an.
7. Lesen Sie die Zusammenfassung und klicken Sie auf **Installieren**.
8. Lesen Sie die Zusammenfassung der Installation und klicken Sie auf **Fertig**.

### 55.4.2 Ausführen einer automatischen Aufrüstung

Zum Ausführen einer automatischen Aufrüstung der Identity Manager-Komponenten müssen Sie eine Eigenschaftendatei mit den erforderlichen Parametern für die Aufrüstung erstellen. Das Installations-Kit enthält eine Beispieldatei `silent.properties` im Verzeichnis `IDMVersion\products\IDM\Plattform\setup`.

**So lassen Sie eine automatische Aufrüstung ausführen:**

1. Kopieren Sie die Beispieldatei `silent.properties` in das Verzeichnis, in dem die Aufrüstung ausgeführt werden soll.
2. Bearbeiten Sie die Datei `silent.properties`. Weitere Informationen finden Sie in Abschnitt 17.2, „Ausführen einer automatischen Installation“, auf Seite 154.
3. Die Datei `silent.properties` muss die folgenden Parameter enthalten:
   - `EDIR_USER_NAME`
   - `EDIR_USER_PASSWORD`
   - `EDIR_NDS_CONF`
   - `EDIR_IP_ADDRESS`
   - `EDIR_NCP_PORT`
   - `METADIRECTORY_SERVER_SELECTED = True`
4. Starten Sie den Aufrüstvorgang. Geben Sie hierzu einen der folgenden Befehle in dem Verzeichnis an, in dem sich die Installation und die Datei `silent.properties` befinden:
   - **Linux:** `./install.bin -i silent -f silent.properties`
   - **Windows:** `idm_install.exe -i silent -f silent.properties`

## 55.5 Aufrüsten von Identitätsanwendungen und der unterstützenden Komponenten

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

Verwenden Sie zur Aufrüstung dieser Komponenten das entsprechende Aufrüstungsprogramm von NetIQ. Das Programm befindet sich im Verzeichnis `products/RBPM/` im Identity Manager-Installationspaket. Navigieren Sie zum Verzeichnis mit den folgenden Aufrüstungsdateien:

- **Linux**: `RBPM_upgrade.bin`
- **Windows**: `RBPM_upgrade.exe`

Dieser Abschnitt enthält folgende Informationen:

## 55.5.1 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.

## 55.5.2 Voraussetzungen und Überlegungen für die Aufrüstung

Lesen Sie vor einer Aufrüstung die folgenden Überlegungen:

- **Identity Manager wird auf Version 4.5.5 aufgerüstet:** Von Versionen vor Version 4.5.5 aus ist eine Aufrüstung oder Migration auf Version 4.6 nicht möglich. Weitere Informationen zur Aufrüstung auf Identity Manager 4.5 finden Sie unter Aufrüsten von Identity Manager im NetIQ Identity Manager-Einrichtungshandbuch.
- **Das Rollen- und Ressourcentreiberpaket wird aufgerüstet:** Weitere Informationen finden Sie unter Aufrüsten installierter Pakete im *Administrationshandbuch zu NetIQ Designer für Identity Manager*.
- **Tomcat als Anwendungsserver:** Diese Identity Manager-Version unterstützt lediglich Tomcat als Anwendungsserver.

  ---

  **HINWEIS:** Installieren Sie den Tomcat-Anwendungsserver mit dem beigelegten Installationsprogramm während der Installation von Identity Manager 4.5. Beim Aufrüsten können Sie nur die Tomcat-Version aufrüsten, die mit dem beigelegten Installationsprogramm installiert wurde.

  ---

  Wenn die Identitätsanwendungen auf einem anderen Anwendungsserver ausgeführt werden (also nicht auf Tomcat), migrieren Sie den Anwendungsserver zu Tomcat. Weitere Informationen finden Sie unter Abschnitt 58.6, „Migrieren aus Websphere oder JBoss in den Tomcat-Webanwendungsserver“, auf Seite 555.
- **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 „Aufrüsten der PostgreSQL-Datenbank“, auf Seite 514.
- **Prüfen Sie, ob der Kontextname der Benutzeranwendung auf den Standardnamen eingestellt ist:** Wenn Sie den Kontextnamen der Benutzeranwendung nicht auf den Standardnamen `IDMProv` eingestellt haben, müssen Sie den Kontextnamen ändern. Weitere Informationen finden Sie unter „Ändern des benutzerdefinierten Kontextnamens für die Benutzeranwendung“, auf Seite 515.
- **Zurücksetzen von Passwörtern per Selbstbedienung:** Beim Aufrüsten von SSPR 4.0 müssen die Eigenschaften `CATALINA_OPTS` und `-Dsspr.application.Path` auf den Ordner verweisen, in dem die SSPR-Konfiguration gespeichert ist.

  Beispiel:

  **Linux:** `export CATALINA_OPTS="-Dsspr.applicationPath=/home/sspr_data`

  **Windows:** `set CATALINA_OPTS="-Dsspr.applicationPath=C:\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**.

## Aufrüsten der PostgreSQL-Datenbank

Rüsten Sie die PostgreSQL-Datenbank mit den folgenden Schritten auf:

---

**WICHTIG:** Die Aufrüstung kann je nach Größe der Datenbank einige Zeit in Anspruch nehmen. Planen Sie die Aufrüstung daher entsprechend.

---

**1** Halten Sie den PostgreSQL-Dienst an, der auf dem Server ausgeführt wird.

**2** Benennen Sie den Ordner `postgres` im folgenden Speicherort um:

**Linux:** `/opt/netiq/idm/apps`

**Windows:** `C:\Netiq\IdentityManager\apps`

Benennen Sie `postgres` beispielsweise in `postgresql_9_3` um.

**3** Hängen Sie die Image-Datei `Identity_Applications_`*`Version_Plattform`*`.iso` ein und navigieren Sie zum Verzeichnis mit dem PostgreSQL-Installationsprogramm.

`<`*`ISO_Extraktionspfad`*`>/products/RBPM/postgre_tomcat_install`

**4** Installieren Sie die PostgreSQL-Anwendung. Wählen Sie in der Liste den Eintrag „PostgreSQL“:

- **Linux (GUI):** Führen Sie `./TomcatPostgreSQL.bin`
- **Linux (Konsole):** Führen Sie `./TomcatPostgreSQL.bin -i console`
- **Windows:** Führen Sie `TomcatPostgreSQL.exe` aus.

Wählen Sie während der Installation lediglich die Option **PostgreSQL**.

---

**HINWEIS:** Aktivieren Sie auf der Seite **PostgreSQL-Details** nicht die Kontrollkästchen **Datenbank-Anmeldekonto erstellen** und **Leere Datenbank erstellen**.

---

**5** Halten Sie den soeben installierten PostgreSQL-Dienst auf dem Server an.

**6** Ändern Sie den Eigentümer des PostgreSQL-Verzeichnisses mit dem folgenden Befehl:

```
chown -R postgres:postgres <Speicherort des Postgres-Verzeichnis>
```

Beispiel:

```
chown -R postgres:postgres /opt/netiq/idm/apps/postgres
```

**7** Wechseln Sie mit dem folgenden Befehl zum Benutzer `postgres`:

```
su - postgres
```

**7a** Wechseln Sie zum Verzeichnis `postgres/bin`.

**7b** Exportieren Sie den PostgreSQL-Installationspfad mit dem folgenden Befehl:

```
export PATH=/opt/netiq/idm/apps/postgres/bin:$PATH
```

**7c** Exportieren Sie das PostgreSQL-Passwort mit dem folgenden Befehl:

```
export PGPASSWORD=<Datenbankpasswort eingeben>
```

**8** Rüsten Sie PostgreSQL mit dem folgenden Befehl auf:

```
pg_upgrade --old-datadir <alter_Postgres_Speicherort\data> --new-datadir
<neuer_Postgres_Speicherort\data> --old-bindir
<alter_Postgres_Speicherort\bin> --new-bindir <neuer_Postgres_Speicherort\bin>
```

Beispiel: `. /pg_upgrade --old-datadir /opt/netiq/idm/apps/postgresql_9_3/data/ --new-datadir /opt/netiq/idm/apps/postgres/data/ --old-bindir /opt/netiq/idm/apps/postgresql_9_3/bin --new-bindir /opt/netiq/idm/apps/postgres/bin/`

Nach der erfolgreichen Aufrüstung werden Sie aufgefordert, `analyze_new_cluster.sh` und `delete_old_cluster.sh` auszuführen.

9 Starten Sie den neuen oder aufgerüsteten PostgreSQL-Datenbankdienst.

10 Wechseln Sie zum Benutzer `postgres` und führen Sie `analyze_new_cluster.sh` aus.

```
su - postgres ./analyze_new_cluster.sh
```

Prüfen Sie, ob das Skript fehlerfrei ausgeführt wird.

11 Navigieren Sie zu `/opt/netiq/idm/apps/postgres/bin` und führen Sie `delete_old_cluster.sh` als Root-Benutzer aus.

```
./delete_old_cluster.sh
```

## Ändern des benutzerdefinierten Kontextnamens für die Benutzeranwendung

Wenn Sie einen anderen Kontextnamen für die Benutzeranwendung angegeben haben (also nicht den Standardnamen `IDMProv`), ersetzen Sie den Kontextnamen mit den folgenden Schritten durch den standardmäßigen Kontextnamen `IDMProv`:

---

**HINWEIS:** Sie können den Kontextnamen in der Eigenschaft „portal.context property“ in der Datei „ism-configuration.properties“ überprüfen.

---

1 Halten Sie den Tomcat-Dienst an.

```
/etc/init.d/idmapps_tomcat_init stop
```

2 Navigieren Sie zum Ordner `webapps` und benennen Sie den Ordner mit dem nicht standardmäßigen Kontextnamen in `IDMProv` um.

**Linux:** `/opt/netiq/idm/apps/tomcat/webapps`

**Windows:** `C:\Netiq\IdentityManager\apps\tomcat\webapps`

Wenn der Name für `portal.context` in der Datei `ism-configuration.properties` beispielsweise `IDMDev` lautet, ersetzen Sie den Ordnernamen `IDMDev` durch `IDMProv`.

3 Führen Sie das Aufrüstungsprogramm für die Identitätsanwendungen aus. Siehe dazu Abschnitt 55.5.4, „Durchführen des geführten Aufrüstungsvorgangs“, auf Seite 516 oder Abschnitt 55.5.5, „Automatische Aufrüstung der Identity Manager-Anwendungen“, auf Seite 518.

4 Stellen Sie nach dem Aufrüsten der Identitätsanwendungen den ursprünglichen Kontextnamen für die `WAR`-Dateien wieder her. Weitere Informationen finden Sie unter „Identitätsanwendungen“, auf Seite 520.

## 55.5.3 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.

## 55.5.4 Durchführen des geführten Aufrüstungsvorgangs

In der folgenden Prozedur wird beschrieben, wie Identitätsanwendungen, OSP, SSPR, Tomcat und ActiveMQ-Anwendungen mit dem Assistenten aufgerüstet werden.

1. Melden Sie sich als `Root-` oder verwaltungsbefugter Benutzer an dem Server an, auf dem die Komponenten installiert werden sollen.
2. Hängen Sie die Imagedatei `Identity_Applications.iso` im Verzeichnis mit der ausführbaren Aufrüstungsdatei ein, die sich standardmäßig im Verzeichnis `products/RBPM/` befindet.
3. Starten Sie das Aufrüstungsprogramm. Führen Sie je nach Plattform eine der folgenden Dateien aus:
   - **Linux:** `RBPM_upgrade.bin`
   - **Windows:** `RBPM_upgrade.exe`
4. Auf der Seite **Einführung** sehen Sie die Identity Manager-Komponenten, die aufgerüstet werden. Klicken Sie dann auf **Weiter**.
5. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Weiter**.
6. Sehen Sie sich die Seite **Bereitgestellte Anwendungen** an und klicken Sie dann auf **Weiter**.

   Auf dieser Seite sind die aktuell installierten Komponenten aufgeführt. Sie finden dort auch die Version und die Installationsverzeichnisse von Tomcat und JRE. Wenn auf dem Server noch andere Anwendungen bereitgestellt sind, wird während des Aufrüstungsvorgangs eine Warnung angezeigt, dass diese Anwendungen nach der Aufrüstung möglicherweise nicht mehr korrekt funktionieren.

   Beispiel: Identitätsberichterstellung oder benutzerdefinierte WAR-Dateien. Sie müssen diese manuell aus der im Aufrüstungsvorgang erstellten Sicherung wiederherstellen.
7. Klicken Sie zum Fortsetzen der Aufrüstung auf **Weiter**.
8. Führen Sie die geführte Installation mit den folgenden Parametern aus. Dieses Programm füllt die Werte für vorhandene Komponenten automatisch aus. Für die Parameter müssen die korrekten Werte angegeben sein.
   - **One SSO-Anbieter**

     Gibt den Pfad zu einem Verzeichnis an, in dem das Aufrüstungsprogramm die Anwendungsdateien für OSP erstellen soll. Wenn der Pfad nicht korrekt ist, navigieren Sie zum Pfad, in dem OSP installiert ist.
   - **SSPR**

     Gibt den Pfad zu einem Verzeichnis an, in dem das Installationsprogramm die Anwendungsdateien für SSPR erstellen soll. Wenn der Pfad nicht korrekt ist, navigieren Sie zum Pfad, in dem SSPR installiert ist.
   - **Benutzeranwendung**

     Gibt den Pfad zu einem Verzeichnis an, in dem das Aufrüstungsprogramm die Anwendungsdateien für die Benutzeranwendung erstellen soll. Wenn der Pfad nicht korrekt ist, navigieren Sie zum Pfad, in dem die Benutzeranwendung installiert ist.

- **Datenbankverbindung**

  Gibt die Einstellungen für die Verbindung mit der Benutzeranwendungsdatenbank an. Die Identitätsanwendungen stellen ebenfalls eine Verbindung zu dieser Datenbank her. Das Aufrüstungsprogramm enthält diese Details in der Datei mit der Benutzeranwendungskonfiguration.

  **Datenbankplattform**

  Gibt die Plattform der Benutzeranwendungsdatenbank an.

  **Datenbank-Host**

  Gibt den Namen oder die IP-Adresse des Servers an, auf dem sich die Benutzeranwendung befindet.

  **Datenbankport**

  Gibt den Port an, über den der Datenbankserver mit der Benutzeranwendung kommuniziert.

  **Datenbanktreiber-JAR**

  Gibt die JAR-Datei für die Datenbankplattform an.

  Der Hersteller der Datenbank stellt die Treiber-JAR-Datei bereit, die als JAR-Datei für den Datenbankserver fungiert. Für PostgreSQL geben Sie beispielsweise `postgresql-9.4-1212.jdbc42.jar` an. Diese Datei befindet sich standardmäßig im Ordner `opt/netiq/idm/apps/postgres` unter Linux bzw. im Ordner `C:\netiq\idm\apps\postgres` unter Windows. Geben Sie auch die entsprechenden JAR-Dateien für die Datenbankplattform an.

- **Datenbank-Berechtigungsnachweise**

  **Datenbankname**

  Gibt den Namen der Datenbank an. Der Name der Datenbank lautet standardmäßig `idmuserappdb`.

  **Datenbankbenutzername**

  Gibt den Namen eines Kontos an, über das die Benutzeranwendung auf die Daten in den Datenbanken zugreifen und diese Daten bearbeiten kann. Standardmäßig lautet der Datenbankbenutzername `idmadmin`.

  **Datenbankpasswort**

  Gibt das Passwort für den angegebenen Benutzernamen an.

- **Datenbank aktualisieren**

  **Datenbank jetzt aufrüsten**

  Das Aufrüstungsprogramm aktualisiert im Rahmen des Aufrüstungsvorgangs das Schema für die Datenbanktabellen.

  **Aufrüsten der Datenbank bei Anwendungsstart**

  Das Aufrüstungsprogramm hinterlässt Anweisungen zur Aktualisierung des Schemas für die Datenbanktabellen, wenn die Benutzeranwendung zum ersten Mal nach der Aufrüstung gestartet wird.

  **SQL in eine Datei schreiben**

  Erzeugt ein SQL-Skript, mit dem der Datenbankadministrator die Datenbanken aktualisieren kann. Wenn Sie diese Option wählen, müssen Sie außerdem einen Namen für die **Schemadatei** angeben. Die Einstellung ist in der Konfiguration der Datei **SQL-Ausgabe** zu finden. Diese Option steht Ihnen für den Fall zur Verfügung, dass Sie keine Berechtigungen zur Erstellung oder Bearbeitung einer Datenbank in Ihrer Umgebung haben. Weitere Informationen zum Erzeugen der Tabellen mit der Datei finden Sie in Abschnitt 39.2, „Manuelles Erstellen der Datenbank“, auf Seite 355.

- **Datenbankadministrator**

  Gibt den Namen und das Passwort für den Datenbankadministrator an.

  **Datenbankbenutzername**

  Gibt das Konto eines Datenbankadministrators an, der Datenbanktabellen, Ansichten und andere Artefakte erstellen kann.

  **Password**

  Gibt das Passwort für den Datenbankadministrator an.

- **Sicherungsordner**

  Abhängig davon, wo Sie die Komponenten installiert haben, wird das Sicherungsverzeichnis in diesem Verzeichnis erstellt und ein Zeitstempel (mit der Uhrzeit der Sicherung) wird an das gesicherte Verzeichnis angehängt.

  Beispiel:

  - Tomcat – `/opt/netiq/idm/apps/tomcat_backup_02262017_033634`
  - OSP und SSPR – `/opt/netiq/idm/apps/osp_sspr_backup_02262017_033634`
  - ActiveMQ – `/opt/netiq/idm/apps/activemq_backup_02262017_033634`
  - Benutzeranwendung – `/opt/netiq/idm/apps/UserApplication_backup_02262017_033634`

9 Lesen Sie die **Zusammenfassung vor der Aufrüstung** und klicken Sie auf **Installieren**.

Während des Aufrüstungsvorgangs wird der Tomcat-Dienst gestoppt und die Aufrüstung wird gestartet; dies kann einige Zeit dauern.

10 Nach Abschluss des Aufrüstungsvorgangs prüfen Sie die Protokolldateien unter `/tmp/rbpm_upgrade/`. Einige Konfigurationen müssen zudem manuell aktualisiert werden (siehe Abschnitt 55.5.6, „Aufgaben nach der Aufrüstung“, auf Seite 519).

## 55.5.5 Automatische Aufrüstung der Identity Manager-Anwendungen

Bei einer automatischen (nicht interaktiven) Installation wird keine Benutzeroberfläche angezeigt.

1 Melden Sie sich als Root-Benutzer oder Administrator dort an, wo die Identity Manager-Anwendungen aufgerüstet werden sollen.

2 Öffnen Sie eine Terminalsitzung.

3 Geben Sie die Werte für die Installation in der Eigenschaftendatei an.

- **Linux**: `products/RBPM/RBPM_Upgrade_Linux.properties`
- **Windows**: `products\RBPM\RBPM_Upgrade_Win.properties`

4 Starten Sie das Aufrüstungsprogramm für Ihre Plattform mit dem folgenden Befehl:

- **Linux**: `RBPM_Upgrade.bin -i silent -f RBPM_Upgrade_Linux.properties`
- **Windows**: `RBPM_Upgrade.exe -i silent -f RBPM_Upgrade_Win.properties`

---

**HINWEIS:** Wenn sich die Datei `RBPM_Upgrade_Linux.properties` nicht in demselben Verzeichnis wie das Installationsskript befindet, müssen Sie den absoluten Pfad zu dieser Datei angeben. Das Skript entpackt die notwendigen Dateien in ein temporäres Verzeichnis und startet dann die automatische Installation.

---

## 55.5.6 Aufgaben nach der Aufrüstung

Nach Abschluss der Aufrüstung müssen Sie die benutzerdefinierten Einstellungen für Tomcat, SSPR, OSP oder die Identitätsanwendungen manuell wiederherstellen.

Führen Sie die nach der Aufrüstung vorzunehmenden Schritte für die erforderlichen Komponenten durch:


- „Java“, auf Seite 519
- „Tomcat-Anwendungsserver“, auf Seite 519
- „Identitätsanwendungen“, auf Seite 520
- „One SSO-Anbieter“, auf Seite 521
- „Self-Service Password Reset“, auf Seite 521


### Java

Überprüfen Sie die Zertifikate am aufgerüsteten JRE-Speicherort: `jre/lib/security/cacerts` im Vergleich zu Ihrem alten JRE-Speicherort. Importieren Sie die fehlenden Zertifikate manuell in `cacerts`.

1 Importieren Sie `java cacerts` mit dem Befehl `keytool`:

```
keytool -import -trustcacerts -file 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.

**Linux:** `tomcat/bin/setenv.sh`

**Windows:** `tomcat/bin/setenv.bat`

3 Starten Sie das **Konfigurationsaktualisierungsprogramm** und prüfen Sie den Pfad der `cacerts`.

### Tomcat-Anwendungsserver

1 (Bedingt) Stellen Sie die benutzerdefinierten Dateien aus der Sicherung wieder her, die vorher während des Aufrüstungsvorgangs erstellt wurden.

Beispiele:

- Angepasste HTTPS-Zertifikate. Kopieren Sie zur Wiederherstellung der Konfiguration 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 (https://tomcat.apache.org/migration.html).
- Wenn Ihnen benutzerdefinierte Keystore-Dateien vorliegen, fügen Sie den korrekten Pfad der neuen `server.xml`-Datei hinzu.

2 (Bedingt) Navigieren Sie zur Identity Manager-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 `/opt/netiq/idm/apps/UserApplication`.
2. Starten Sie das Dienstprogramm `configupdate`.

   **Linux:** `configupdate.sh`

   **Windows:** `configupdate.bat`
3. Klicken Sie auf der Registerkarte **Benutzeranwendung** auf **Erweiterte Optionen anzeigen** und führen Sie die folgenden Schritte aus:

   **3a** Aktivieren Sie das Kontrollkästchen **Namen des RBPM-Kontexts ändern**.

   **3b** Geben Sie den ursprünglichen RBPM-Kontextnamen ein.

   **3c** Wählen Sie den zugehörigen **Rollentreiber-DN** aus, und klicken Sie auf **OK**.

   **3d** 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
   ```
4. (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 Benutzeranwendungen auf verschiedenen Servern installiert sind, aktualisieren Sie den SSO-Client-Parameter mit dem Konfigurationsaktualisierungsprogramm. Weitere Informationen hierzu finden Sie in Abschnitt 40.4.3, „IDM-Dashboard“, auf Seite 386 in Abschnitt 40.4, „Parameter für SSO-Clients“, auf Seite 383.

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.

## Self-Service Password Reset

Aktualisieren Sie nach der Aufrüstung von SSPR den SSO-Client-Parameter mit dem Konfigurationsaktualisierungsprogramm. Weitere Informationen hierzu finden Sie in Abschnitt 40.4.8, „Zurücksetzen von Passwörtern per Selbstbedienung“, auf Seite 389 in Abschnitt 40.4, „Parameter für SSO-Clients“, auf Seite 383.

Aktualisieren Sie die SSPR-Konfigurationsdetails mit den folgenden Schritten:

1. Melden Sie sich beim SSPR-Portal als Administrator an.
2. Aktualisieren Sie die Audit-Serverdetails:
   - **2a** Navigieren Sie zum **Konfigurationseditor** und geben Sie das Konfigurationspasswort an.
   - **2b** Wählen Sie **Einstellungen > Revision > Audit-Weiterleitung > Syslog-Audit Server-Zertifikate** aus.
   - **2c** Importieren Sie diese Zertifikate vom Server und klicken Sie auf **Speichern**.
3. Importieren Sie die **LocalDB** in SSPR:
   - **3a** Klicken Sie oben rechts auf der Seite im Dropdown-Menü auf **Konfigurationsmanager**.
   - **3b** Klicken Sie auf **LocalDB**.
   - **3c** Klicken Sie auf **LocalDB-Archivdatei importieren (hochladen)**.
4. Konfigurieren Sie die Administratorberechtigungen für SSPR (siehe Abschnitt 32.3, „Aufgaben nach Abschluss der Installation“, auf Seite 289).

---

**HINWEIS:** Bei der Aufrüstung von SSPR 4.0 auf SSPR 4.1 wird der Standardspeicherort der SSPR-Konfiguration zum Standardspeicherort von SSPR 4.1 geändert. Weitere Informationen zu den Konfigurationsspeicherorten finden Sie in der Datei `setenv.sh`. Diese Änderung wirkt sich jedoch nicht auf das Verhalten der Komponenten aus.

Beispiel: Wenn vor der Aufrüstung der Pfad der SSPR-Konfiguration auf `-Dsspr.applicationPath='/home/sspr-data` festgelegt ist, dann verändert er sich nach der Aufrüstung zu `-Dsspr.applicationPath=/opt/netiq/idm/apps/osp_sspr/sspr/sspr_data` und alle verknüpften Konfigurationen werden an diesem Speicherort wiederhergestellt.

---

Starten Sie die aufgerüsteten Komponenten, um zu prüfen, ob die Aufrüstung erfolgreich war.

Starten Sie beispielsweise das Identity Manager-Dashboard und klicken Sie auf **Info**. Prüfen Sie, ob die Anwendung die neue Version anzeigt, zum Beispiel **4.6.0**.

## 55.6 Aufrüsten der Identitätsberichterstellung

Die Identitätsberichterstellung umfasst zwei Treiber. Unter Umständen müssen Sie auch Inhalte aus dem NetIQ-Ereignisrevisionsdienst zu Sentinel Log Management für IGA migrieren. Nehmen Sie die Aufrüstung in der nachstehenden Reihenfolge vor:

1. Rüsten Sie das Treiberpaket für die Datenerfassungsdienste (DCS-Dienste) auf.
2. Rüsten Sie das Treiberpaket für den Dienst „Verwaltetes System – Gateway“ (MSGW-Dienst) auf.
3. Migrieren zu Sentinel Log Management für IGA
4. Rüsten Sie die Identitätsberichterstellung auf

### 55.6.1 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: **Manage System Gateway Base package 2.0.0.20120509205929**.
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. Konfigurieren Sie den Treiber. Weitere Informationen finden Sie in den folgenden Abschnitten:
   - Abschnitt 44.1.2, „Konfigurieren des Treibers „Verwaltetes System – Gateway“ (MSGW-Treiber)“, auf Seite 410
   - Abschnitt 44.1.3, „Konfigurieren des Treibers für den Datenerfassungsdienst (DCS-Treiber)“, auf Seite 412
10. Wiederholen Sie Schritt 2 bis Schritt 9, und aktualisieren Sie das Paket für den DCS-Treiber.
11. Überprüfen Sie, ob der MSGW-Treiber und der DCS-Treiber mit der aufgerüsteten Version von Identity Manager verbunden sind.

### 55.6.2 Migrieren des Ereignisrevisionsdiensts in Sentinel for Log Management für IGA

In diesem Abschnitt finden Sie Informationen zum Migrieren vorhandener Daten vom NetIQ-Ereignisrevisionsdienst (Event Auditing Service, EAS) zu Sentinel Log Management für IGA.

- „Migration vorbereiten“, auf Seite 523
- „Migrieren der Daten zur neuen PostgreSQL-Datenbank“, auf Seite 524
- „Einrichten des Berichterstellungsservers“, auf Seite 527

- „Ausführen des Datensynchronisierungsprogramms“, auf Seite 527
- „Filtern der Datensynchronisierungsrichtlinie“, auf Seite 530

## Migration vorbereiten

Vor Beginn der Migration müssen Sie Sentinel und die EAS-Datenbank vorbereiten. Importieren Sie hierzu den erforderlichen Connector zum Empfangen von Ereignissen von Sentinel und rüsten Sie alle Identity Manager-Komponenten auf 4.6 auf.

Führen Sie vor der Migration der EAS-Daten zu Sentinel die nachfolgenden Aktionen aus.

1. Importieren Sie den Connector `NetIQ-Audit_2011.1r4-201701130600-release.cnz` in EAS.
2. Rüsten Sie alle vorhandenen Identity Manager-Komponenten von 4.5.4 auf 4.6 auf.
3. Sichern Sie die Datei `logevent.conf`.

   **Linux:** `/etc/logevent.conf`

   **Windows:** `C:\Windows\logevent.cfg`

   Die Datei `logevent.conf` sollte EAS-Details enthalten.
4. Prüfen Sie, ob die folgenden Identity Manager-Komponenten ausgeführt werden:
   - eDirectory
   - Identity Manager-Engine
   - iManager
   - Identitätsanwendungen (insbesondere OSP, SSPR und RBPM)
5. Aktualisieren Sie die Audit-Serverdetails für SSPR:
   - **5a** Melden Sie sich beim SSPR-Portal als Administrator an.
   - **5b** Navigieren Sie zum **Konfigurationseditor** und geben Sie das Konfigurationspasswort an.
   - **5c** Wählen Sie **Einstellungen > Revision > Audit-Weiterleitung**.
   - **5d** Geben Sie die Sentinel-Details unter **Syslog-Audit-Server** an. Beispiel: `tls,<sentinel IP>,1443`.
   - **5e** Löschen Sie die Zertifikate des Syslog-Audit-Servers mit **Löschen**.
   - **5f** Importieren Sie die Zertifikate vom aktualisierten Syslog-Audit-Server mit **Von Server importieren**.
   - **5g** Speichern Sie die Änderungen.
6. Prüfen Sie, ob der EAS-Server ausgeführt wird, bis alle im Cache befindlichen Revisionsereignisse von allen Identity Manager-Komponenten an EAS gesendet wurden.
7. Stoppen Sie die folgenden Identity Manager-Komponenten:
   - eDirectory
   - Identity Manager-Engine
   - iManager
   - Identitätsanwendungen (insbesondere OSP, SSPR und RBPM)
8. Halten Sie die Novell-Audit-Prozesse `lcache` und `jcache` an.

   ```
   kill -15 <PID für lcache>
   kill -15 <PID für jcache>
   ```

9 Erstellen Sie NAudit-Zertifikate gemäß Schritt 1 bis Schritt 6 unter Aktivieren von SSL zwischen Sentinel und Benutzeranwendung, sodass die Benutzeranwendung eine Verbindung zu Sentinel herstellen kann.

10 Bearbeiten Sie den Eintrag `LogHost` in der Datei `logevent.conf`, sodass er auf Sentinel verweist.

11 Starten Sie die nachfolgenden Identity Manager-Komponenten.

- eDirectory
- Identity Manager-Engine
- iManager
- Identitätsanwendungen (insbesondere OSP, SSPR und RBPM)

## Migrieren der Daten zur neuen PostgreSQL-Datenbank

In diesem Abschnitt finden Sie Informationen zum Migrieren der SIEM-Daten aus der EAS-Datenbank zu einer unterstützten PostgreSQL-Datenbank. Weitere Informationen zum Installieren einer PostgreSQL-Datenbank finden Sie in Kapitel 28, „Installieren von PostgreSQL und Tomcat“, auf Seite 261.

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:
     - **Linux:** `/opt/netiq/idm/apps/postgres`
     - **Windows:** `C:\NetIQ\IdentityManager\apps\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:
     - **Linux:** `psql -d SIEM -U postgres -f /opt/netiq/idm/apps/postgres/SIEM.sql`
     - **Windows:** `psql -d SIEM -U postgres –f C:\NetIQ\IdentityManager\apps\postgres\SIEM.sql`
4. Prüfen Sie, ob im Migrationsprotokoll Fehler vorhanden sind, und beheben Sie diese.

---

**HINWEIS:** Für die Identity Manager 4.6-Berichte werden keine Revisionsdaten verwendet, die aus EAS in Sentinel migriert werden. Stattdessen werden für diese Berichte die Revisionsdaten verwendet, die direkt von Sentinel synchronisiert werden.

---

## Einrichten des Berichterstellungsservers

Nach dem Importieren der EAS-Daten in die neue PostgreSQL-Datenbank konfigurieren Sie die Berichterstellungsdatenbank mit der neuen PostgreSQL-Datenbank.

In diesem Abschnitt wird vorausgesetzt, dass Sie die Identitätsberichterstellung auf demselben Server installiert haben, zu dem Sie den Datenbankserver migriert haben (Sentinel-Datenbank). Weitere Informationen zur Installation der Identitätsberichterstellung finden Sie unter Abschnitt 42.1, „Geführte Installation der Identitätsberichterstellung“, auf Seite 399.

1. Konfigurieren Sie die Details für den neuen Berichterstellungsserver mit den folgenden Schritten im Dienstprogramm `configupdate`:
   1a. Starten Sie das Dienstprogramm `configupdate` an der Eingabeaufforderung mit einem der nachfolgenden Befehle.

   **Linux:** `./configupdate.sh`

   **Windows:** `configupdate.bat`

   1b. Bearbeiten Sie die **OAuth-Umleitungs-URL**, sodass sie auf den neuen Identitätsberichterstellungsserver und die entsprechenden Portdetails verweist. Weitere Informationen finden Sie unter Abschnitt 40.4.5, „Berichte“, auf Seite 387.
2. Tragen Sie die Details für den neuen Berichterstellungsserver mit Designer oder iManager in der DCS-Treiberkonfiguration ein.
3. Starten Sie den DCS-Treiber.

## Ausführen des Datensynchronisierungsprogramms

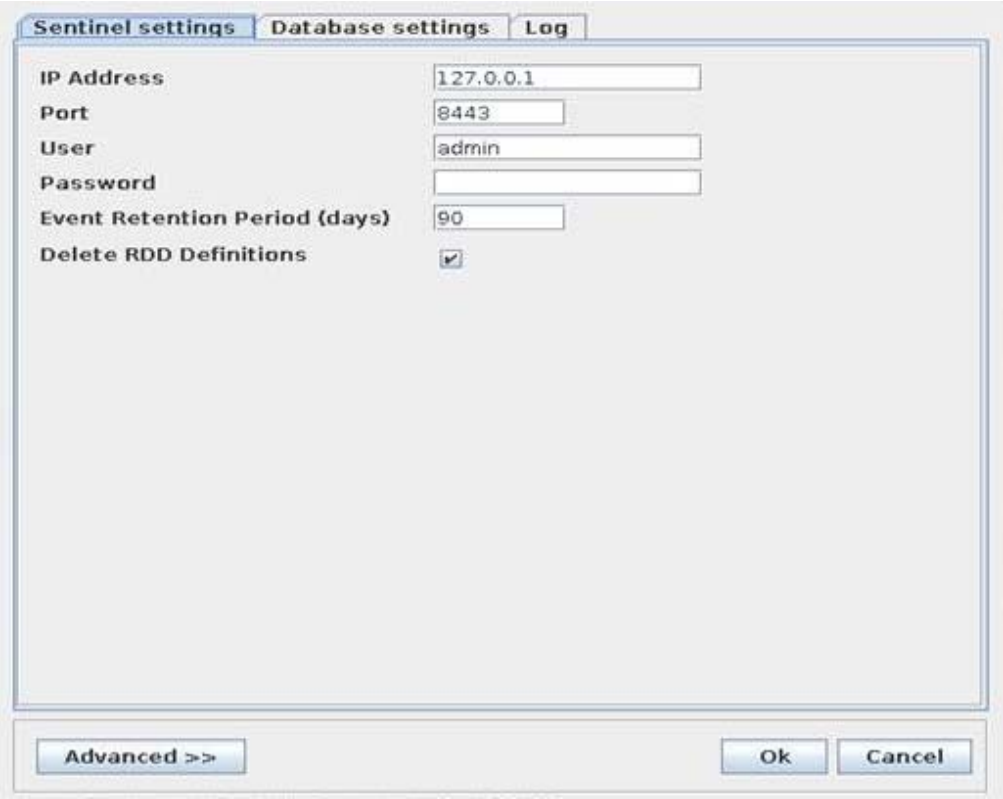
Nach dem Konfigurieren des Berichterstellungsservers aktivieren Sie die Weiterleitung der Ereignisse durch Sentinel an eine externe Datenbank. Identity Manager umfasst ein Dienstprogramm, mit dem die Datensynchronisierungsrichtlinie in Sentinel zur Weiterleitung von Ereignissen von Sentinel an eine externe Datenbank erstellt wird. Das Dienstprogramm befindet sich im Ordner `IdentityReporting/Sentinel/sentineldatasync.jar`.

Erstellen Sie die Datensynchronisierungsrichtlinie in Sentinel mit den folgenden Schritten:

1. Navigieren Sie zum Verzeichnis des Datensynchronisierungsprogramms und führen Sie den folgenden Befehl aus:

   ```
   Java –jar sentineldatasync.jar
   ```

   Hiermit wird das Datensynchronisierungsprogramm gestartet.
2. Geben Sie auf der Registerkarte **Sentinel-Einstellungen** des Dienstprogramms die folgenden Details an:




- **IP-Adresse:** Geben Sie die IP-Adresse des Computers an, auf dem Sentinel installiert ist.
- **Port:** Geben Sie die Portnummer des Sentinel-Servers an. Der Standardport ist 8443.
- **Passwort:** Geben Sie das Passwort für den Sentinel-Benutzer an.
- **Ereignisbeibehaltungszeitraum:** Geben Sie den Zeitraum an, über den die Ereignisse in der Datenbank gespeichert bleiben sollen, bevor sie gelöscht werden. Der Standardwert beträgt 90 Tage.
- **RDD-Definitionen löschen:** Beim Erstellen der Datensynchronisierungsrichtlinie in Sentinel werden die Sentinel-Standardrichtlinien standardmäßig gelöscht. Sollen Sentinel-Berichte ausgeführt werden, dürfen die Sentinel-Standardrichtlinien entsprechend nicht gelöscht werden.

  ---

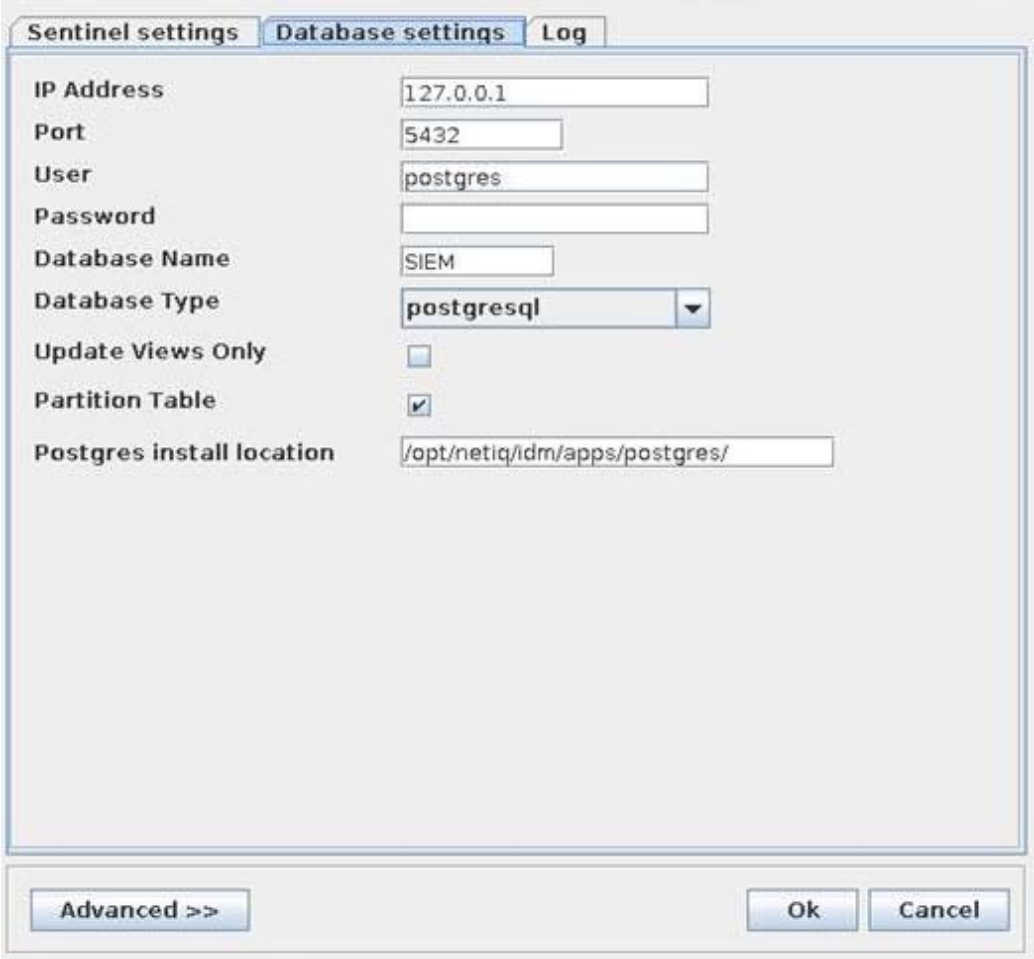
  **WICHTIG:** Deaktivieren Sie diese Option, wenn Sie mit Sentinel oder Identity Tracking arbeiten.

  ---

- **Speziell:** Im Modus **Erweitert** können Sie den folgenden Parameter bearbeiten:
  - **Nutzlast für Ereignistabelle:** Enthält ein JSON-Dokument zum Erstellen der Datensynchronisierungstabelle über REST-APIs. Die Authentifizierungsdaten werden ersetzt, sobald eine Anforderung zum Erstellen der Datensynchronisierungstabelle gesendet wird.
  - **Nutzlast für Datensynchronisierungsrichtlinie:** Enthält ein JSON-Dokument zum Erstellen der Datensynchronisierungstabelle über REST-APIs. Die Authentifizierungsdaten werden ersetzt, sobald eine Anforderung zum Erstellen der Datensynchronisierungstabelle gesendet wird.

**HINWEIS:** Sollen weitere Felder in die Datensynchronisierungsrichtlinie aufgenommen werden, bearbeiten Sie das JSON-Dokument unter **Nutzlast für Datensynchronisierungsrichtlinie**. Die Änderungen müssen sowohl in der Ereignistabelle als auch in der Datensynchronisierungsrichtlinie ausgeführt werden. Ansonsten kann die Richtlinie nicht erstellt werden.

3 Geben Sie auf der Registerkarte **Datenbankeinstellungen** die folgenden Details an:




- **IP-Adresse:** Geben Sie die IP-Adresse der Datenbank ein.
- **Port:** Geben Sie den Port für die Datenbank an.
- **Passwort:** Geben Sie ein Passwort zum Aufbau einer Verbindung zur Datenbank an.
- **Datenbankname:** Geben Sie einen Namen für die Datenbank an. Beispiel: `idmrptdb` oder `SIEM`.
- **Datenbanktyp:** Wählen Sie den Datenbanktyp in der Dropdown-Liste aus.
- **Nur Ansichten aktualisieren:** Aktivieren Sie diese Option nur dann, wenn Fehler beim Aktualisieren der Ansichten auftreten. Wenn diese Option aktiviert ist, aktualisiert das Datensynchronisierungsprogramm die Ansichten, ohne die Datensynchronisierungsrichtlinie in Sentinel zu erstellen.

- **Partitionstabelle:** Eine Partitionierung der Tabelle erhöht die allgemeine Leistung der Abfragen und erleichtert die Tabellenverwaltung. Die Datenbank speichert die von Sentinel empfangenen Ereignisse tageweise in separaten Partitionen. Es wird empfohlen, diese Einstellung unverändert beizubehalten.
- **PostgreSQL-Installationsspeicherort:** Gibt den Speicherort an, an dem PostgreSQL installiert ist. Beispiel: `/opt/netiq/idm/apps/postgres/`
- **Speziell:** Im Modus **Erweitert** können Sie den folgenden Parameter bearbeiten:

  Partitions-SQL: Enthält das SQL-Skript zur Partitionierung der Tabelle. Das Skript gilt jeweils nur für die ausgewählte Datenbank.

4 Geben Sie auf der Registerkarte **Protokolle** den Namen der Protokolldatei an.

  Die Protokolldatei befindet sich in demselben Speicherort wie das Datensynchronisierungsprogramm.

---

**WICHTIG:** Nach dem Erstellen der Datensynchronisierungsrichtlinie bearbeiten Sie den Filter, damit die Ereignisse von den angegebenen Identity Manager-Collectoren in Sentinel empfangen werden. Weitere Informationen finden Sie unter „Filtern der Datensynchronisierungsrichtlinie“, auf Seite 530.

---

## Filtern der Datensynchronisierungsrichtlinie

Damit Sentinel die Ereignisse von den angegebenen Identity Manager-Collectoren empfängt, können Sie den Filter für die Datensynchronisierungsrichtlinie bearbeiten.

1 Melden Sie sich als Administrator bei der Sentinel-Hauptoberfläche an.

2 Klicken Sie auf **Speicher** > **Datensynchronisierung**.

3 Klicken Sie auf **Bearbeiten**, um die Datensynchronisierungsrichtlinie zu konfigurieren.

4 Bearbeiten Sie die erforderlichen Informationen:

  **Kriterien:** Geben Sie eine gültige Lucene-Abfrage an.

  Die folgende Abfrage zeigt ein Beispiel für den Datenempfang ausschließlich von Identity Manager-Komponenten:

  ```
  (port:"NetIQ Identity Manager" OR port:"NetIQ Self Service Password Reset" OR port:"NetIQ eDirectory" OR port:"NetIQ NMAS" OR port:"NetIQ iManager" OR port:"NetIQ OneSSO") AND (sev:[0 TO 5]) AND NOT (evt:"Collector Internal Message" OR evt:"Starting" OR evt:"Started" OR evt:"Stopping" OR evt:"Stopped" OR evt:"CombinedRealTimeSummariesStatus" OR evt:"EnginePerformanceSummary" OR evt:"EventThroughputUtilization" OR evt:"LostConnection")
  ```

  **Richtlinienname:** Geben Sie einen Namen für die Datensynchronisierungsrichtlinie an.

  **Beibehaltungszeitraum:** Geben Sie den Zeitraum an, über den die Ereignisse in der Tabelle `sentinel_events` der Berichterstellungsdatenbank gespeichert bleiben sollen.

  **Stapelgröße:** Geben Sie die Anzahl der Ereignisse an, die in einem einzigen Stapel an die externe Datenbank gesendet werden.

  **Inaktivitätszeitraum:** Geben Sie den Zeitraum an, nach dem der Datensynchronisierungsvorgang auf weitere Ereignisse zur Verarbeitung prüft.

  **Zeitplan:** Wählen Sie eine passende Option für die Synchronisierung der Daten mit der externen Datenbank.

  - **All the time (Immer):** Wenn Sie diese Option auswählen, werden die Ereignisse sofort nach Bearbeitung eines Ereignisses mit der externen Datenbank synchronisiert.

- **Benutzerdefiniert:** Mit dieser Option konfigurieren Sie bestimmte Zeitintervalle für die Datensynchronisierung.

  Wenn Sie **Benutzerdefiniert** auswählen, müssen Sie die folgenden Informationen angeben, um die benutzerdefinierte Synchronisierungszeit festzulegen:

  - **Wochentag:** Wählen Sie den gewünschten Wochentag oder **Täglich** aus.
  - **Anfangszeit:** Geben Sie die Uhrzeit an, zu der der Datensynchronisierungsvorgang gestartet werden soll.
  - **Dauer:** Geben Sie den Synchronisierungszeitraum in Minuten an.

Wenn Sie die Daten in den Datenbanktabellen nicht sofort sehen, warten Sie bis zum nächsten Synchronisierungszyklus.

## 55.6.3 Aufrüsten der Identitätsberichterstellung

Vor der Aufrüstung der Identitätsberichterstellung müssen Sie zunächst die Identitätsanwendungen und Sentinel aufrüsten. Zum Aufrüsten der Identitätsberichterstellung von Version 4.0.2 (oder höher) installieren Sie die neue Version über die bisherige Version. Weitere Informationen finden Sie in „Installieren der Identitätsberichterstellung“, auf Seite 399.

## 55.6.4 Ändern der Verweise auf reportRunner in der Datenbank

Aktualisieren Sie die Verweise auf reportRunner in der Datenbank, nachdem Sie die Identitätsberichterstellung aufgerüstet und Tomcat zum ersten Mal gestartet haben.

1. Halten Sie Tomcat an.
2. Navigieren Sie zum Installationsverzeichnis der Identitätsberichterstellung und benennen Sie den Ordner `reportContent` in `ORG-reportContent` um.

   Beispiel: `/opt/netiq/idm/apps/IdentityReporting`
3. Löschen Sie den Inhalt der temporären Verzeichnisse und Arbeitsverzeichnisse im Tomcat-Ordner.
4. Melden Sie sich bei der PostgreSQL-Datenbank an.

   **4a** Suchen Sie die reportRunner-Verweise in den folgenden Tabellen:

   - `idm_rpt_cfg.idmrpt_rpt_params`
   - `idm_rpt_cfg.idmrpt_definition`

   **4b** Geben Sie die folgenden Löschanweisungen aus:

   ```
   DELETE FROM idm_rpt_cfg.idmrpt_rpt_params WHERE
   rpt_def_id='com.novell.content.reportRunner';

   DELETE FROM idm_rpt_cfg.idmrpt_definition WHERE
   def_id='com.novell.content.reportRunner';
   ```
5. Starten Sie Tomcat.

   Sehen Sie sich in den Protokollen an, ob die Berichte mit dem korrekten reportRunner aktualisiert wurden.
6. Melden Sie sich bei der Identitätsberichterstellung an und führen Sie die Berichte aus.

### 55.6.5 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.

## 55.7 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 Patch-Datei (z. B. `analyzer_4.6_patch1_20121128.zip`) 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** Überprüfen Sie, ob die neue Version angezeigt wird, z. B. **4.6 Update 1** und Build-ID **20121128**.

## 55.8 Aufrüsten der Identity Manager-Treiber

Ab Identity Manager 4.0.2 stellt NetIQ neue Inhalte nicht mehr über Treiberkonfigurationsdateien, sondern über **Pakete** 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).

---

**HINWEIS:** Wenn Sie die Version 3.*x* des Benutzeranwendungstreibers auf das Paket mit der Benutzeranwendungsversion 4.0.2 aufrüsten, installiert Designer sowohl die Version 3.*x* als auch die Version 4.0 derselben Treiberrichtlinien. Wenn sich sowohl die Richtlinie 3.*x* als auch die Richtlinie 4.0 im Paketkatalog befindet, funktioniert Designer nicht ordnungsgemäß. Löschen Sie die Richtlinien mit Version 3.*x* und behalten Sie die Richtlinien mit Version 4.0 bei.

---

Sie können die Treiber wie folgt auf Pakete aufrüsten:

- Abschnitt 55.8.1, „Einen neuen Treiber erstellen“, auf Seite 533
- Abschnitt 55.8.2, „Vorhandene Inhalte durch Inhalte aus Paketen ersetzen“, auf Seite 533
- Abschnitt 55.8.3, „Aktuelle Inhalte beibehalten und neue Inhalte über Pakete hinzufügen“, auf Seite 534

## 55.8.1 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.

## 55.8.2 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 54.5.2, „Exportieren der Treiberkonfiguration“, auf Seite 501.

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 55.10, „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“, auf Seite 536.

### 55.8.3 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 54.5.2, „Exportieren der Treiberkonfiguration“, auf Seite 501.

   ---

   **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.

## 55.9 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.

## 55.9.1 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 Designer verwenden, fahren Sie mit Abschnitt 58.3.1, „Kopieren der serverspezifischen Informationen in Designer“, auf Seite 552 fort. 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**.

## 55.9.2 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 535
- „Mithilfe von iManager den alten Server aus dem Treibersatz entfernen“, auf Seite 535
- „Stilllegen des alten Servers“, auf Seite 536

### 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“.

## 55.10 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 55.10.1, „Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von Designer“, auf Seite 536
- Abschnitt 55.10.2, „Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von iManager“, auf Seite 537

### 55.10.1 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 16.2.2, „Starten der Treiber“, auf Seite 148. 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.

## 55.10.2 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 16.2.2, „Starten der Treiber“, auf Seite 148. 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.

# 56 Anwenden eines Hotfix auf die Identity Manager-Komponenten

In diesem Abschnitt finden Sie Informationen zur Installation eines Hotfix für eine Identity Manager-Komponente.



## 56.1 Anwenden eines Hotfix auf die Identity Manager-Engine und den Remote Loader

Der Hotfix für die Identity Manager-Engine und den Remote Loader aktualisiert den Identity Manager-Server und den Remote Loader. Die Installation des Hotfix wird nur im geführten Modus (GUI) und im Automatikmodus durchgeführt. Der Hotfix unterstützt nicht den Konsolenmodus.

Navigieren Sie zur Anzeige der Protokolldateien für die Installation in den folgenden Speicherorten:

- **Linux**: `/tmp/logs/idmPatchInstall.log`
- **Windows**: `\%Temp%\logs`

---

**HINWEIS:** Bei Windows-Servern erstellt der Hotfix einen Sicherungsordner im Verzeichnis `\%UserProfile%\PatchInstallerBackUp<Datum><Uhrzeit>`.

---



### 56.1.1 Voraussetzungen für die Installation des Hotfix

Führen Sie vor der Installation des Hotfix die folgenden Schritte durch:

1. Halten Sie den eDirectory-Daemon an.

   Wenn Sie eDirectory nicht stoppen, versucht das Hotfix-Installationsprogramm, es zu stoppen. Wird eDirectory nicht durch das Programm angehalten, wird eine Warnmeldung angezeigt. Dann müssen Sie eDirectory manuell stoppen.

2. Stoppen Sie die Remote Loader-Services.

   Wenn der Remote Loader gerade verwendet wird, kann der Hotfix den Remote Loader nicht aktualisieren.

3 (Bedingt) Legen Sie den Java-Pfad bei einer Nicht-`Root`-Installation anhand einer der folgenden Methoden fest:

- Bearbeiten Sie die `JAVA_NONROOT`-Variable in der `install.sh`-Datei für den Hotfix.
- Exportieren Sie den Java 1.8-Pfad.

4 Navigieren Sie in einem Browser zur NetIQ-Downloads-Seite (https://dl.netiq.com/index.jsp).

5 Klicken Sie unter **Patches** auf **Search Patches** (Patches suchen).

6 Geben Sie im Suchfeld **Identity Manager *nn*-Patch** ein

7 Laden Sie den Inhalt der Datei herunter und extrahieren Sie ihn.

## 56.1.2 Installieren des Hotfix als Root-Benutzer im GUI-Modus

Führen Sie für eine `Root`-Installation die folgenden Schritte durch.

1 Vergewissern Sie sich, dass Sie die Voraussetzungen zur Installation des Hotfix erfüllen. Weitere Informationen finden Sie unter Abschnitt 56.1.1, „Voraussetzungen für die Installation des Hotfix“, auf Seite 539.

2 Melden Sie sich auf dem Server, auf dem der Hotfix ausgeführt werden soll, als `Root`-Benutzer an.

3 Navigieren Sie zum Verzeichnis `cd-image`, in das die Dateien extrahiert wurden.

Weitere Informationen finden Sie unter Abschnitt 56.1.1, „Voraussetzungen für die Installation des Hotfix“, auf Seite 539.

4 Führen Sie den entsprechenden Befehl für Ihre Plattform aus:

- **Linux** Führen Sie den Befehl `./install.sh` in einem Terminalfenster aus.
- **Windows** Starten Sie die Datei `install.bat`.

5 Wählen Sie die zu installierenden Komponenten aus, und klicken Sie auf **Installieren**.

6 (Bedingt) Führen Sie zur Aktualisierung des Remote Loaders die folgenden Schritte durch:

**6a** Klicken Sie für die Warnmeldung zum Stoppen des Remote Loaders auf **OK**.

Vergewissern Sie sich, dass Sie den Remote Loader gestoppt haben.

**6b** Wenn das Installationsprogramm auf Ihrem Computer keinen installierten 32-Bit- oder 64-Bit-Remote Loader erkennt, wählen Sie **Durchsuchen** aus, um zum Pfad für den installierten Remote Loader zu navigieren.

---

**HINWEIS:** Standardmäßig steht im Hotfix-Installationsprogramm eine **Durchsuchen**-Option für den Identity Manager-Server unter Linux zur Verfügung. Unter Windows ist sie standardmäßig nicht verfügbar.

---

7 Sehen Sie sich den Installationsstatus der ausgewählten Komponenten an und klicken Sie auf **Fertig**.

8 (Bedingt) **Linux**: Führen Sie die folgenden Schritte durch, um zu überprüfen, ob der Hotfix erfolgreich auf die Identity Manager-Komponenten angewendet wurde, die Sie in Schritt 5 ausgewählt haben:

**8a** Prüfen Sie anhand der Identity Manager-Server-Trace, ob die Identity Manager-Version aktualisiert wurde. Im Trace-Fenster wird Folgendes angezeigt:

```
<product version="4.5.n.n">DirXML</product>
```

wobei *n* für die Version des Identity Manager-Hotfix steht.

**8b** Führen Sie folgenden Befehl aus, um zu überprüfen, ob die Identity Manager-RPMs auf Ihrem Computer installiert sind:

```
rpm -qa | grep nov | grep 4.5
```

**9** (Bedingt) **Windows**: Führen Sie die folgenden Schritte durch, um zu überprüfen, ob der Hotfix erfolgreich auf die Identity Manager-Komponenten angewendet wurde, die Sie in Schritt 5 ausgewählt haben:

**9a** Prüfen Sie das Änderungsdatum der Dateien, die durch das Hotfix-Installationsprogramm aktualisiert wurden.

**9b** Starten Sie den Remote Loader.

**9c** Klicken Sie auf **Eigenschaften** und dann mit der rechten Maustaste auf `rlconsole.exe`.

**9d** Klicken Sie auf **Eigenschaften > Details**.

**9e** Überprüfen Sie, ob der Wert in der Dateiversion 4.5.*n.n* lautet, wobei *n* für die Version des Identity Manager-Hotfix steht.

## 56.1.3 Installieren des Hotfix als Nicht-Root-Benutzer im GUI-Modus

Führen Sie die folgenden Schritte durch, um eine Nicht-`Root`-Installation im geführten Modus auszuführen.

1. Vergewissern Sie sich, dass Sie die Voraussetzungen zur Installation des Hotfix erfüllen. Weitere Informationen finden Sie unter Abschnitt 56.1.1, „Voraussetzungen für die Installation des Hotfix“, auf Seite 539.
2. Melden Sie sich am Server, auf dem der Hotfix ausgeführt werden soll, als Nicht-`Root`-Benutzer an.
3. Führen Sie die Datei `install.sh` aus.
4. Navigieren Sie zum Stammverzeichnis von eDirectory. Beispiel: `/home/<Benutzer>/eDirectory`.
5. Klicken Sie auf **Installieren**.

## 56.1.4 Installieren des Hotfix im Automatikmodus

Zur Ausführung des Identity Manager-Hotfix-Installationsprogramms im Automatikmodus benötigen Sie eine `patchUpgradeSilent.Properties`-Datei. NetIQ stellt Ihnen eine Beispieldatei zur Verfügung, die sich standardmäßig im Verzeichnis `cd-image` befindet. Diese Vorgehensweise ist sowohl für eine `Root`-Installation als auch eine Nicht-`Root`-Installation geeignet.

1. Vergewissern Sie sich, dass Sie die Voraussetzungen zur Installation des Hotfix erfüllen. Weitere Informationen finden Sie unter Abschnitt 56.1.1, „Voraussetzungen für die Installation des Hotfix“, auf Seite 539.
2. Bearbeiten Sie den Inhalt der Datei `patchUpgradeSilent.Properties`.

   Die Beispieldatei enthält folgende Informationen:

```
#Silent Properties File IDMPatchInstaller
#eDirectory and RemoteLoader services should be stopped before installation
#Set this property to true/false for Engine Upgrade for root and non root
install
install_Engine=true
#Set this property to true/false for Remote Loader32 Upgrade
install_RL32=true
#Set this property to true/false for Remote Loader64 Upgrade
install_RL64=true
#Set this property for Engine Upgrade for NON ROOT user
#eg: If the engine location is /home/eDirectoryNonRoot/eDirectory/opt/novell/
eDirectory select till eDirectory(parent directory of /opt)
engine_Location=/home/eDirectoryNonRoot/eDirectory/
#Set this property for Remote Loader 32-Bit Install location
#Only for Windows
RL32_Location=C:\\Novell\\IdentityManager\\RemoteLoader\\32bit
#Set this property for Remote Loader 64-Bit Install location
#Only for Windows
RL64_Location=C:\\Novell\\IdentityManager\\RemoteLoader\\64bit
```

**HINWEIS:** Auf Windows-Servern wird für die Hotfix-Installation der Installationspfad für den Identity Manager-Engine-Server verwendet, der bei der Installation von Identity Manager 4.5 angegeben wurde.

3 (Bedingt) Bei einer Nicht-`Root`-Installation müssen Sie die Eigenschaft `engine_Location` auskommentieren, um auf den genauen Speicherort der Identity Manager-Engine zu verweisen.

4 Starten Sie den Installationsvorgang mit einem der folgenden Befehle:

- **Linux**: `<Hotfix-Speicherort>/install.sh -i silent -f <Dateiname>`
- **Windows**: `<Hotfix-Speicherort>\install.bat -i silent -f <Dateiname>`

**HINWEIS:** Wenn Sie die Nicht-`Root`-Installation von Identity Manager als `Root`-Benutzer ausführen, zeigt das Installationsprogramm folgende Warnung an:

```
NetIQ recommends that you apply only patches pertaining to the installed IDM
version. If you understand the risk and want to proceed, type yes else no.
```

Ignorieren Sie die Warnmeldung, und wählen Sie **Ja** zum Fortfahren.

## 56.2 Anwenden eines Hotfix auf einen Identity Manager-Treiber

In diesem Abschnitt finden Sie Informationen zur Installation eines Hotfix für einen Identity Manager-Treiber.


- Abschnitt 56.2.1, „Anwenden des Identity Manager-Treiber-Hotfix als Root-Benutzer“, auf Seite 543
- Abschnitt 56.2.2, „Anwenden des Identity Manager-Treiber-Hotfix als Nicht-Root-Benutzer“, auf Seite 543

## 56.2.1 Anwenden des Identity Manager-Treiber-Hotfix als Root-Benutzer

In einer Root-Installation installiert der Treiber-Hotfix die Treiber-RPMs am Standardspeicherort im Pfad /opt/novell/eDirectory.

## 56.2.2 Anwenden des Identity Manager-Treiber-Hotfix als Nicht-Root-Benutzer

1. Überprüfen Sie, ob das Verzeichnis <*Nicht-Root-eDirectory-Speicherort*>/rpm vorhanden ist und die _db.000-Datei enthält.

   Falls _db.000 in diesem Verzeichnis nicht vorhanden ist, wird die Installation nicht erfolgreich durchgeführt.

2. Geben Sie folgenden Befehl bei der Eingabeaufforderung ein, um das Root-Verzeichnis an einem Nicht-Root-eDirectory-Speicherort festzulegen:

   ROOTDIR=<*non-root eDirectory location*>

   Dadurch werden die Umgebungsvariablen in dem Verzeichnis festgelegt, in dem eDirectory als Nicht-Root-Benutzer installiert ist.

3. Laden Sie den Hotfix herunter und extrahieren Sie die heruntergeladene TAR- oder ZIP-Datei.

4. Installieren Sie die Treiberdateien mit folgendem Befehl:

   ```
   rpm --dbpath $ROOTDIR/rpm -Uvh --relocate=/usr=$ROOTDIR/opt/novell/eDirectory
   --relocate=/etc=$ROOTDIR/etc --relocate=/opt/novell/eDirectory=$ROOTDIR/opt/
   novell/eDirectory --relocate=/opt/novell/dirxml=$ROOTDIR/opt/novell/dirxml --
   relocate=/var=$ROOTDIR/var --badreloc --nodeps --replacefiles <rpm-location>
   ```

   Beispiel: Installieren Sie die ssop-RPM mit folgendem Befehl:

   ```
   rpm --dbpath $ROOTDIR/rpm -Uvh --relocate=/usr=$ROOTDIR/opt/novell/eDirectory
   --relocate=/etc=$ROOTDIR/etc --relocate=/opt/novell/eDirectory=$ROOTDIR/opt/
   novell/eDirectory --relocate=/opt/novell/dirxml=$ROOTDIR/opt/novell/dirxml --
   relocate=/var=$ROOTDIR/var --badreloc --nodeps --replacefiles /home/user/
   novell-DXMLssop.rpm
   ```

# XVI 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 XVI, „Aufrüsten von Identity Manager“, auf Seite 491. Weitere Informationen zum Unterschied zwischen Aufrüstung und Migration finden Sie in Abschnitt 54.2, „Erläuterungen zur Aufrüstung und zur Migration“, auf Seite 495.

# 57 Vorbereiten der Migration von Identity Manager

In diesem Abschnitt wird die Vorbereitung Ihrer Identity Manager-Lösung auf die Migration in die neue Installation beschrieben.

## 57.1 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 54.2, „Erläuterungen zur Aufrüstung und zur Migration“, auf Seite 495. |
| ❑ | 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 23. |
| ❑ | 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 Kapitel 6, „Überlegungen und Voraussetzungen für die Installation“, auf Seite 61 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 7.2, „Voraussetzungen und Überlegungen für die Installation des Identitätsdepots“, auf Seite 71. |
| ❑ | 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 58.4, „Migrieren der Identity Manager-Engine auf einen neuen Server“, auf Seite 553. |
| ❑ | 7. Installieren Sie Identity Manager auf dem neuen Server. Weitere Informationen finden Sie in „Planen der Installation von Identity Manager“, auf Seite 45. |
| ❑ | 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 55.3, „Aufrüstung von Remote Loader“, auf Seite 510. |
| ❑ | 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 58.1, „Checkliste für die Migration von Identity Manager“, auf Seite 549. |
| ❑ | 10. Fügen Sie den neuen Server zum Treibersatz hinzu. Weitere Informationen finden Sie in Abschnitt 55.9.1, „Hinzufügen des neuen Servers zum Treibersatz“, auf Seite 535. |
| ❑ | 11. Ändern Sie die serverspezifischen Informationen für jeden Treiber. Weitere Informationen finden Sie in Abschnitt 58.3.1, „Kopieren der serverspezifischen Informationen in Designer“, auf Seite 552. |

| | Checkliste |
|---|---|
| ❑ | 12. (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 58.3, „Kopieren von serverspezifischen Informationen für den Treibersatz“, auf Seite 551 |
| ❑ | 13. Aktualisieren Sie die Treiber auf das Paketformat. Weitere Informationen finden Sie in Abschnitt 55.8, „Aufrüsten der Identity Manager-Treiber“, auf Seite 532. |
| ❑ | 14. (Bedingt) Wenn Sie benutzerdefinierte Richtlinien und Regeln verwenden, stellen Sie die angepassten Einstellungen wieder her. Weitere Informationen finden Sie in Abschnitt 55.10, „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“, auf Seite 536. |
| ❑ | 15. Entfernen Sie den alten Server aus dem Treibersatz. Weitere Informationen finden Sie in Abschnitt 55.9.2, „Entfernen des alten Servers aus dem Treibersatz“, auf Seite 535. |
| ❑ | 16. Aktivieren Sie die aufgerüstete Identity Manager-Lösung. Weitere Informationen finden Sie in Abschnitt 53.7, „Aktivieren von Identity Manager“, auf Seite 486. |

## 57.2 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 16.2.1, „Anhalten der Treiber“, auf Seite 148
- Abschnitt 16.2.2, „Starten der Treiber“, auf Seite 148

# 58 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:



## 58.1 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 5.3.4, „Empfohlene Servereinrichtung“, auf Seite 53 sowie in den aktuellen Versionshinweisen für die Komponenten.<br><br>**HINWEIS:** Soll die aktuelle Datenbank der Benutzeranwendung weiterhin genutzt werden, wählen Sie im Installationsprogramm die Option **Vorhandene Datenbank**. Weitere Informationen finden Sie in Teil XII, „Installieren der Identitätsanwendungen“, auf Seite 295. |
| ❑ | 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 58.2, „Vorbereiten des Designer-Projekts auf die Migration“, auf Seite 550. |

| | 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 58.4, „Migrieren der Identity Manager-Engine auf einen neuen Server“, auf Seite 553. |
| ❑ | 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 58.5, „Migrieren des Benutzeranwendungstreibers“, auf Seite 553. |
| ❑ | 9. Erstellen Sie einen neuen Rollen- und Ressourcenservice-Treiber.<br><br>Ein vorhandener Rollen- und Ressourcenservice-Treiber kann nicht migriert werden. Weitere Informationen finden Sie in Abschnitt 38.3, „Erstellen des Rollen- und Ressourcenservice-Treibers“, auf Seite 352. |
| ❑ | 10. Stellen Sie die beiden Treiber im Identitätsdepot bereit. Weitere Informationen finden Sie in Abschnitt 38.4, „Bereitstellen der Treiber für die Benutzeranwendung“, auf Seite 353. |
| ❑ | 11. Rüsten Sie die Identitätsanwendungen auf. Weitere Informationen finden Sie in Abschnitt 55.5, „Aufrüsten von Identitätsanwendungen und der unterstützenden Komponenten“, auf Seite 512. |
| ❑ | 12. (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 58.8.1, „Vorbereiten einer Oracle-Datenbank für die SQL-Datei“, auf Seite 557. |
| ❑ | 13. Stellen Sie sicher, dass die Browser keine Inhalte aus früheren Versionen von Identity Manager enthalten. Weitere Informationen finden Sie in Abschnitt 58.8.2, „Leeren des Browsercache“, auf Seite 558. |
| ❑ | 14. (Bedingt) Stellen Sie Ihre benutzerdefinierten Einstellungen für das SharedPagePortlet wieder her. Weitere Informationen finden Sie in Abschnitt 58.8.4, „Aktualisieren der Einstellung für die maximale Zeitüberschreitung für das SharedPagePortlet“, auf Seite 558. |
| ❑ | 15. 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 58.8.5, „Deaktivieren der Einstellung für automatische Abfragen für Gruppen“, auf Seite 559. |

## 58.2 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.

## 58.3 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 58.3.1, „Kopieren der serverspezifischen Informationen in Designer“, auf Seite 552
- Abschnitt 58.3.2, „Ändern der serverspezifischen Informationen in iManager“, auf Seite 552
- Abschnitt 58.3.3, „Ändern der serverspezifischen Informationen für die Benutzeranwendung“, auf Seite 553

### 58.3.1 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 16.2.2, „Starten der Treiber“, auf Seite 148.

### 58.3.2 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.

### 58.3.3 Ändern der serverspezifischen Informationen für die Benutzeranwendung

Sie müssen die Benutzeranwendung neu konfigurieren, damit der neue Server erkannt wird. Führen Sie die Datei `configupdate.sh` bzw. `configupdate.bat` 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:

- **Linux:** `configupdate.sh`
- **Windows:** `configupdate.bat`

3 Geben Sie die Werte aus Kapitel 40, „Konfigurieren der Einstellungen für die Identitätsanwendungen“, auf Seite 367 an.

## 58.4 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 Teil V, „Installieren der Identity Manager-Engine, der Treiber und der iManager-Plugins“, auf Seite 139.

## 58.5 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.

### 58.5.1 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**.

### 58.5.2 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**.

### 58.5.3 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.

## 58.6 Migrieren aus Websphere oder JBoss in den Tomcat-Webanwendungsserver

Vor dem Aufrüsten auf Identity Manager 4.6 (oder höher) müssen Sie einen vorhandenen JBoss- oder Websphere-Anwendungsserver zum Tomcat-Anwendungsserver migrieren.

In diesem Abschnitt finden Sie Anleitungen zum Migrieren der Identitätsanwendungen aus Ihren vorhandenen Webanwendungsservern wie Websphere oder JBoss in den Tomcat-Anwendungsserver. Dazu müssen Sie Identitätsanwendungen auf Tomcat installieren und die Einstellungen mit dem Konfigurationsprogramm konfigurieren.

Führen Sie die folgenden Schritte durch, um aus Websphere oder JBoss in Tomcat zu migrieren:

1 Stoppen Sie den Websphere- oder JBoss-Server.

2 (Bedingt) Falls Tomcat noch nicht installiert ist, installieren Sie Tomcat und JRE mit dem Installationsprogramm Ihrer Wahl.

- **Linux**: `products/RBPM/postgre_tomcat_install/TomcatPostgreSQL.bin`
- **Windows**: `products\RBPM\postgre_tomcat_install\TomcatPostgreSQL.exe`

---

**HINWEIS:** Verwenden Sie den Tomcat-Anwendungsserver aus dem Bundle mit der `.iso`-Datei für IDM 4.5.

---

3 (Bedingt) Wenn Sie eine vorhandene JRE-Datei verwenden, werden Sie vom Installationsprogramm aufgefordert, bestimmte Dateien zu überschreiben. Klicken Sie auf **Ja, alle**.

4 Installieren Sie die Identitätsanwendungen mit dem Installationsprogramm Ihrer Wahl unter:

`Produkte/RBPM/user_app_install/IdmUserApp.bin`

4a Wählen Sie **Tomcat** als Webanwendungsserver aus.

4b Wählen Sie die Option **Vorhandene Datenbank** aus, und geben Sie die Host-Berechtigung ein. Die standardmäßige **Benutzer-ID** lautet `idmadmin`.

4c Geben Sie den Installationspfad von Tomcat und JRE an.

4d (Bedingt) Geben Sie in einer Cluster-Umgebung die **Engine-ID** an, die bei der JBoss/Websphere-Installation genannt wurde.

---

**HINWEIS:** Wenn eine einzige Instanz auf dem Anwendungsserver ausgeführt wird, lassen Sie das Feld **Engine-ID** leer, sofern Sie dieses Feld bei der JBoss- oder Websphere-Installation nicht ausgefüllt haben.

---

4e (Bedingt) Wählen Sie zum Importieren des Master-Schlüsselwerts in Ihrer Clusterumgebung **Ja** aus, und geben Sie den Master-Schlüsselwert an. Sie finden den Master-Schlüsselwert in Ihren früheren Konfigurationen der JBoss- oder Websphere-Anwendungsserver.

4f Wählen Sie auf der Seite **IDM konfigurieren** die Option **Später konfigurieren** aus, und klicken Sie auf **Weiter**.

4g Lesen Sie die Seite **Übersicht vor der Installation** und klicken Sie dann auf **Installieren**.

5 Öffnen Sie das Dienstprogramm **Konfigurationsaktualisierung**:

`/opt/netiq/idm/apps/UserApplication`

Weitere Informationen zum Festlegen der Werte für die Einstellungen finden Sie in Kapitel 40, „Konfigurieren der Einstellungen für die Identitätsanwendungen“, auf Seite 367.

6 Klicken Sie auf **Speichern**.

7 (Bedingt) Rüsten Sie auf das aktuelle Service Pack für Identity Manager 4.5 auf.

---

**HINWEIS:** Soll auf Identity Manager 4.6 aufgerüstet werden, müssen Sie nicht auf das aktuelle Service Pack für Identity Manager aufrüsten.

---

8 Starten Sie den Tomcat-Anwendungsserver und überprüfen Sie, ob die Identitätsanwendungen korrekt bereitgestellt wurden.

Rüsten Sie die Identitätsanwendungen nach der Migration auf. Weitere Informationen finden Sie unter Abschnitt 55.5, „Aufrüsten von Identitätsanwendungen und der unterstützenden Komponenten“, auf Seite 512.

## 58.7 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 58.8.1, „Vorbereiten einer Oracle-Datenbank für die SQL-Datei“, auf Seite 557.
- 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 finden Sie in Abschnitt 4.4, „Verwenden von Self-Service Password Management in Identity Manager“, auf Seite 40.

Weitere Informationen zum Aufrüsten der Identitätsanwendungen finden Sie in Abschnitt 55.5, „Aufrüsten von Identitätsanwendungen und der unterstützenden Komponenten“, auf Seite 512.

## 58.8 Abschließen der Migration der Identitätsanwendungen

Nach dem Aufrüsten oder Migrieren der Identitätsanwendungen schließen Sie den Migrationsvorgang ab.

### 58.8.1 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/ojdbc6.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.

   Weitere Informationen zum Ausführen der SQL-Datei finden Sie in Abschnitt 39.2, „Manuelles Erstellen der Datenbank“, auf Seite 355.

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

## 58.8.2 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.

## 58.8.3 Verwalten der Passwörter mit dem bisherigen Anbieter oder einem externen Anbieter

Standardmäßig erfolgt die Passwortverwaltung in Identity Manager mit SSPR. Wenn jedoch die vorhandenen Passwortrichtlinien weiterhin gelten sollen, verwenden Sie den internen bisherigen Anbieter in Identity Manager. Alternativ können Sie einen externen Anbieter nutzen. Zum Konfigurieren von Identity Manager für diese Anbieter befolgen Sie die Anweisungen in einem der folgenden Abschnitte:

- Abschnitt 39.6.2, „Verwenden des bisherigen Anbieters für die „Passwort vergessen“-Verwaltung“, auf Seite 361
- Abschnitt 39.6.3, „Verwenden eines externen Systems für die „Passwort vergessen“-Verwaltung“, auf Seite 363

## 58.8.4 Aktualisieren der Einstellung für die maximale Zeitüberschreitung für das SharedPagePortlet

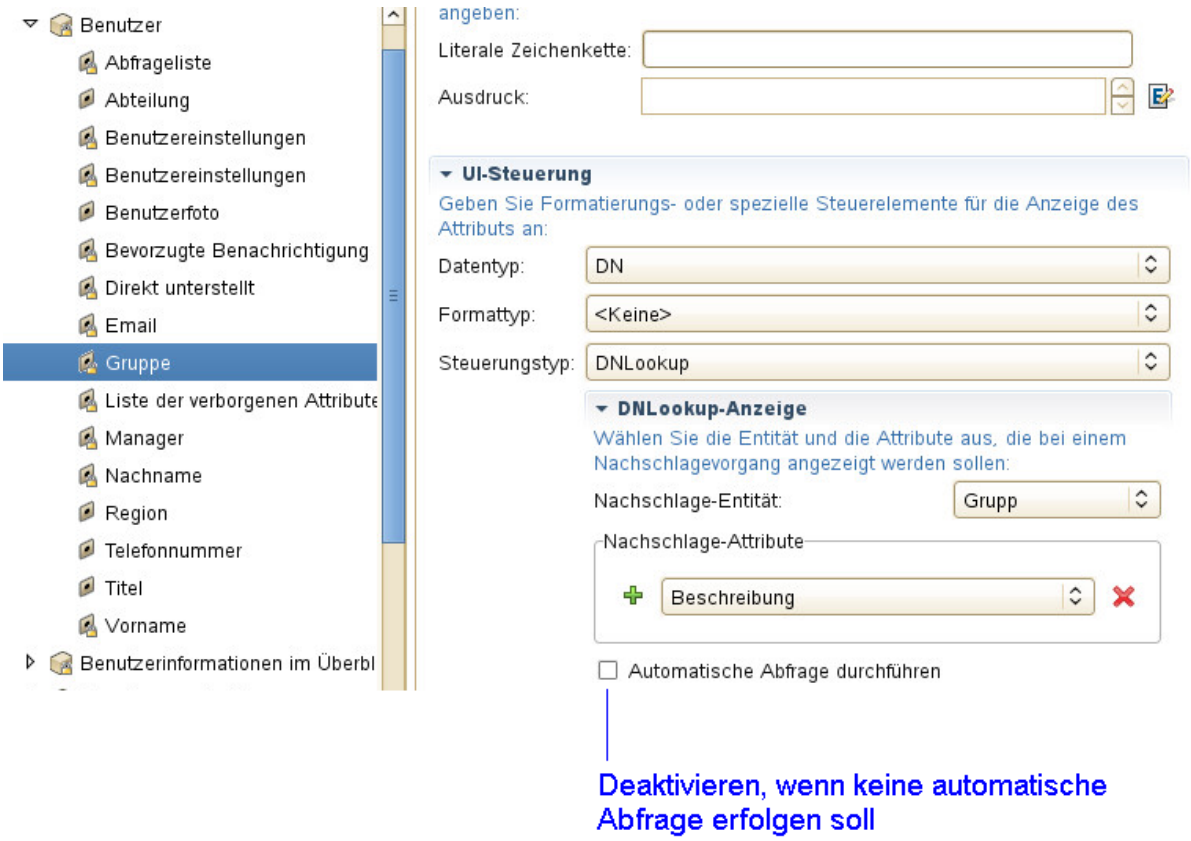
Falls Sie die Standardeinstellungen für das SharedPagePortlet angepasst haben, wurden diese Änderungen in der Datenbank gespeichert, und diese Einstellung wird überschrieben. Wenn Sie zur Registerkarte „Identitätsselbstbedienung“ navigieren, wird daher unter Umständen nicht die richtige freigegebene 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**.

## 58.8.5 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**:



# 59 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.

---

## 59.1 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.

## 59.2 Deinstallieren der Identity Manager-Engine

Beim Installieren der Identity Manager-Engine wird ein Deinstallationsskript auf dem Identity Manager-Server gespeichert. Mithilfe dieses Skripts können Sie alle Dienste, Pakete und Verzeichnisse entfernen, die während der Installation erstellt wurden.

---

**HINWEIS:** Bevor Sie die Identity Manager-Engine deinstallieren können, muss zunächst das Identitätsdepot entsprechend vorbereitet werden. Weitere Informationen finden Sie in Abschnitt 59.1, „Entfernen von Objekten aus dem Identitätsdepot“, auf Seite 561.

---

### 59.2.1 Deinstallieren der Identity Manager-Engine unter Linux/UNIX

Navigieren Sie auf dem Linux- oder UNIX-Server, auf dem die Identity Manager-Engine gehostet wird, zum Skript `Uninstall_Identity_Manager` (standardmäßig im Verzeichnis `/root/idm/Uninstall_Identity_Manager`).

Führen Sie das Skript mit dem folgenden Befehl aus:

```
./Uninstall_Identity_Manager
```

### 59.2.2 Deinstallieren der Identity Manager-Engine als Nicht-Root-Benutzer

Wenn Sie Identity Manager als Nicht-`Root`-Benutzer installiert haben, wird das `idm`-Verzeichnis in das Verzeichnis des Benutzers gestellt, der Identity Manager installiert hat.

**So deinstallieren Sie die Identity Manager-Engine:**

1. Melden Sie sich als der Benutzer an, der die Identity Manager-Engine installiert hat.
2. Navigieren Sie zum Installationsverzeichnis der Identity Manager-Engine (standardmäßig `/`*`eDirectory_Basisverzeichnis`*`/opt/novell/eDirectory/bin/idm-uninstall`).
3. Führen Sie das Deinstallationsskript mit dem folgenden Befehl aus:

   ```
   ./Uninstall_Identity_Manager
   ```

### 59.2.3 Deinstallieren der Identity Manager-Engine unter Windows

Auf einem Windows-Server deinstallieren Sie die Identity Manager-Engine über die Option „Software“ in der Systemsteuerung. Unter Windows 2012 R2 klicken Sie beispielsweise auf **Programme und Funktionen**. Klicken Sie mit der rechten Maustaste auf **Identity Manager**, und klicken Sie auf **Deinstallieren**.

## 59.3 Deinstallieren von Remote Loader

Beim Installieren des Remote Loaders wird ein Deinstallationsskript auf dem Identity Manager-Server gespeichert. Mithilfe dieses Skripts können Sie alle Dienste, Pakete und Verzeichnisse entfernen, die während der Installation erstellt wurden.

### 59.3.1 Deinstallieren des Remote Loaders unter Linux/UNIX

Zum Deinstallieren des Remote Loaders auf einem Linux- oder UNIX-Server navigieren Sie zum Deinstallationsskript (standardmäßig im Verzeichnis `/root/idm/Uninstall_Identity_Manager`). Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./Uninstall_Identity_Manager`.

Wenn Sie den Remote Loader als Nicht-`Root`-Benutzer installiert haben, wird das `idm`-Verzeichnis in das Verzeichnis des Benutzers gestellt, der die Installation vorgenommen hat.

### 59.3.2 Deinstallieren des Remote Loaders als Nicht-Root-Benutzer

Wenn Sie den Remote Loader als Nicht-`Root`-Benutzer installiert haben, wird das `idm`-Verzeichnis in das Verzeichnis des Benutzers gestellt, der Identity Manager installiert hat.

1. Melden Sie sich als der Benutzer an, der den Remote Loader installiert hat.
2. Navigieren Sie zum Installationsverzeichnis des Remote Loaders (standardmäßig `/`*`Benutzerverzeichnis`*`/idm/Uninstall_Identity_Manager`).
3. Führen Sie das Deinstallationsskript mit dem folgenden Befehl aus:

   ```
   ./Uninstall_Identity_Manager
   ```

### 59.3.3 Deinstallieren des Remote Loaders unter Windows

Auf einem Windows-Server deinstallieren Sie den Remote Loader über die Option „Software“ in der Systemsteuerung.

## 59.4 Deinstallation des rollenbasierten Bereitstellungsmoduls

Sie müssen alle Komponenten des rollenbasierten Bereitstellungsmoduls (RBPM) deinstallieren, beispielsweise die Treiber und die Datenbank.

Wenn Sie die mit dem RBPM verknüpften Laufzeitkomponenten deinstallieren müssen, startet das Deinstallationsprogramm den Server automatisch neu, sofern Sie das Deinstallationsprogramm nicht im Automatikmodus unter Windows ausführen. Der Windows-Server muss manuell neu gebootet werden. Soll Identity Manager außerhalb des integrierten Installationsprogramms deinstalliert werden, halten Sie außerdem den *nds-Dienst* an, bevor Sie das Deinstallationsprogramm starten.

---

**HINWEIS:** Vor der Deinstallation des RBPM deinstallieren Sie die Identity Manager-Engine. Weitere Informationen finden Sie in Abschnitt 59.2, „Deinstallieren der Identity Manager-Engine“, auf Seite 562.

---

## 59.4.1 Löschen der Treiber für das rollenbasierte Bereitstellungsmodul

Sie können den Benutzeranwendungstreiber und den Rollen- und Ressourcenservice-Treiber wahlweise in Designer oder in iManager löschen.

1. Halten Sie den Benutzeranwendungstreiber, den Rollen- und den Ressourcenservice-Treiber an. Führen Sie den entsprechenden Vorgang für die verwendete Komponente aus:
   - **Designer:** Klicken Sie mit der rechten Maustaste auf die Treiberzeile und klicken Sie anschließend auf **Live > Treiber anhalten**.
   - **iManager:** Klicken Sie auf der Seite „Treibersatz-Überblick“ auf die obere rechte Ecke des Treiberabbilds und dann auf **Treiber anhalten**.
2. Löschen Sie den Benutzeranwendungstreiber und den Rollen- und Ressourcenservice-Treiber. Führen Sie den entsprechenden Vorgang für die verwendete Komponente aus:
   - **Designer:** Klicken Sie mit der rechten Maustaste auf die Treiberzeile und wählen Sie **Löschen**.
   - **iManager:** Klicken Sie auf der Seite „Treibersatz-Überblick“ auf **Treiber > Treiber löschen** und dann auf den zu löschenden Treiber.

## 59.4.2 Deinstallieren der Benutzeranwendung unter Linux/UNIX

Sie müssen die Benutzeranwendung und die zugehörige Datenbank von Tomcat deinstallieren. In diesem Verfahren wird das Entfernen der Benutzeranwendung und der zugehörigen Datenbank aus Tomcat und PostgreSQL beschrieben. Wenn Sie einen anderen Anwendungsserver und eine andere Datenbank verwenden, beachten Sie die Dokumentation für diese Produkte.

---

**WICHTIG:** Gehen Sie beim Entfernen der Benutzeranwendung vorsichtig vor. Hierbei werden alle Ordner und Dateien aus dem Ordner gelöscht, in dem die Skripte und die unterstützenden installiert wurden. Beim Entfernen der Dateien könnten Sie gleichzeitig unbeabsichtigt Tomcat oder PostgreSQL deinstallieren. Der Name des Deinstallationsordners lautet beispielsweise in der Regel `/opt/netiq/idm/apps/UserApplication`. Dieser Ordner enthält auch die Ordner für Tomcat und PostgreSQL.

---

1. Melden Sie sich bei dem Server an, auf dem Sie die Benutzeranwendung installiert haben.
2. Deinstallieren Sie die Benutzeranwendung mit den folgenden Schritten:
   - **2a** Navigieren Sie zum Skript `Uninstall_UserApp` (standardmäßig im Verzeichnis `/opt/netiq/idm/apps/UserApplication/RemoveUserApp`).
   - **2b** Führen Sie den folgenden Befehl aus:

     ```
     ./Uninstall_UserApp
     ```
3. Deinstallieren Sie die Datenbank mit dem folgenden Befehl:

   ```
   ./Uninstall_TomcatPostgreSQL
   ```

## 59.4.3 Deinstallieren der Benutzeranwendung unter Windows

Sie müssen die Benutzeranwendung und die zugehörige Datenbank von Tomcat deinstallieren. In diesem Verfahren wird das Entfernen der Benutzeranwendung und der zugehörigen Datenbank aus Tomcat und PostgreSQL beschrieben. Wenn Sie einen anderen Anwendungsserver und eine andere Datenbank verwenden, beachten Sie die Dokumentation für diese Produkte.

**WICHTIG:** Gehen Sie beim Entfernen der Benutzeranwendung vorsichtig vor. Hierbei werden alle Ordner und Dateien aus dem Ordner gelöscht, in dem die Skripte und die unterstützenden installiert wurden. Beim Entfernen der Dateien könnten Sie gleichzeitig unbeabsichtigt Tomcat oder PostgreSQL deinstallieren. Der Name des Deinstallationsordners lautet beispielsweise in der Regel `C:\NetIQ\IdentityManager\apps\UserApplication`. Dieser Ordner enthält auch die Ordner für Tomcat und PostgreSQL.

1. Melden Sie sich bei dem Server an, auf dem Sie die Benutzeranwendung installiert haben.
2. Öffnen Sie die Option „Software“ in der Systemsteuerung. Unter Windows Server 2012 R2 klicken Sie beispielsweise auf **Programme und Funktionen**.
3. Klicken Sie mit der rechten Maustaste auf **Identity Manager-Benutzeranwendung**, und klicken Sie auf **Deinstallieren**.

## 59.5 Deinstallieren der Identitätsberichterstellung

Die Komponenten der Identitätsberichterstellung müssen in der nachstehenden Reihenfolge deinstalliert werden:

1. Löschen Sie die Treiber. Weitere Informationen finden Sie in Abschnitt 59.5.1, „Löschen der Berichterstellungstreiber“, auf Seite 565.
2. Löschen Sie die Identitätsberichterstellung. Weitere Informationen finden Sie in Abschnitt 59.5.2, „Deinstallieren der Identitätsberichterstellung“, auf Seite 566.
3. Löschen Sie Sentinel. Weitere Informationen finden Sie unter Abschnitt 59.5.3, „Deinstallieren von Sentinel“, auf Seite 566.

**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.

### 59.5.1 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.

### 59.5.2 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 59.5.1, „Löschen der Berichterstellungstreiber“, auf Seite 565.

---

**WICHTIG:** Bevor Sie das Deinstallationsprogramm für die Identitätsberichterstellung starten, müssen Sie die generierten Berichte aus dem Installationsverzeichnis der Identitätsberichterstellung in einen anderen Speicherort auf dem Computer kopieren. Bei der Deinstallation werden alle Dateien und Ordner aus dem Verzeichnis entfernt, in dem die Berichterstellung installiert war. Beispiel: Berichterstellungs-Installationsordner `C:\NetIQ\IdentityManager\apps\IDMReporting` oder `/opt/netiq/idm/apps/IDMReporting`.

---

Deinstallieren Sie die Identitätsberichterstellung mit dem entsprechenden Vorgang für Ihr Betriebssystem:

**Linux und UNIX**

Navigieren Sie zum Skript `Uninstall_Identity Reporting` (standardmäßig im Verzeichnis `/opt/netiq/idm/apps/IDMReporting/`).

Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./Uninstall_IdentityReporting`.

**Windows**

Öffnen Sie die Option „Software“ in der Systemsteuerung. Unter Windows Server 2012 R2 klicken Sie beispielsweise auf **Programme und Funktionen**. Klicken Sie mit der rechten Maustaste auf **Identitätsberichterstellung**, und klicken Sie auf **Deinstallieren**.

### 59.5.3 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–sentinel`
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.

## 59.6 Deinstallieren von eDirectory

Vor dem Deinstallieren von eDirectory müssen Sie sich über die eDirectory-Baumstruktur und die Speicherorte der Reproduktionen informieren. Beispielsweise müssen Sie feststellen, ob sich gleich mehrere Server im Baum befinden.

1. (Bedingt) Wenn der eDirectory-Baum mehrere Server enthält, führen Sie die folgenden Schritte aus:

   **1a** (Bedingt) Wenn sich Masterreproduktionen auf dem Server befinden, müssen Sie einen anderen Server in diesem Reproduktionsring zum Master bestimmen, bevor Sie eDirectory entfernen können.

Weitere Informationen finden Sie unter „Managing Partitions and Replicas“ (Verwalten von Partitionen und Reproduktionen) im *NetIQ eDirectory Administration Guide* (eDirectory-Administrationshandbuch).

**1b** (Bedingt) Wenn der Baum auf dem Server, auf dem eDirectory installiert ist, die einzige Kopie einer Partition enthält, führen Sie entweder diese Partition mit der übergeordneten Partition zusammen, oder kopieren Sie eine Reproduktion dieser Partition auf einen anderen Server, und machen Sie diesen Server zum Masterreproduktionsserver.

Weitere Informationen finden Sie unter „Managing Partitions and Replicas“ (Verwalten von Partitionen und Reproduktionen) im *NetIQ eDirectory Administration Guide* (eDirectory-Administrationshandbuch).

**1c** Führen Sie eine Zustandsüberprüfung der eDirectory-Datenbank aus. Beheben Sie alle eventuell auftretenden Probleme, bevor Sie den Vorgang fortsetzen.

Weitere Informationen hierzu finden Sie unter „Keeping eDirectory Healthy“ (Funktionsfähigkeit von eDirectory aufrechterhalten) im *NetIQ eDirectory - Administrationshandbuch*.

**2** Deinstallieren Sie eDirectory mit dem entsprechenden Verfahren für Ihr Betriebssystem:

**Linux und UNIX**

Navigieren Sie zum Skript `nds-unistall` (standardmäßig im Verzeichnis `/opt/novell/eDirectory/sbin`).

Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./nds-uninstall`.

**Windows**

Öffnen Sie die Option „Software“ in der Systemsteuerung. Unter Windows Server 2012 R2 klicken Sie beispielsweise auf **Programme und Funktionen**. Klicken Sie mit der rechten Maustaste auf **NetIQ eDirectory**, und klicken Sie auf **Deinstallieren**.

**3** (Bedingt) Wenn der eDirectory-Baum mehrere Server enthält, führen Sie die folgenden Schritte aus:

**3a** Löschen Sie alle serverspezifischen Objekte, die noch im Baum verblieben sind.

**3b** Führen Sie eine weitere Zustandsprüfung durch, damit gewährleistet ist, dass der Server ordnungsgemäß aus dem Baum entfernt wurde.

Weitere Informationen hierzu finden Sie unter „Keeping eDirectory Healthy“ (Funktionsfähigkeit von eDirectory aufrechterhalten) im *NetIQ eDirectory - Administrationshandbuch*.

## 59.7 Deinstallation von Analyzer

**1** Schließen Sie Analyzer.

**2** Deinstallieren Sie Analyzer mit dem entsprechenden Verfahren für Ihr Betriebssystem:

**Linux und UNIX**

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: `./Uninstall\ Analyzer\ for\ Identity\ Manager`.

**Windows**

Öffnen Sie die Option „Software“ in der Systemsteuerung. Unter Windows Server 2008 klicken Sie beispielsweise auf **Programme und Funktionen**. Klicken Sie mit der rechten Maustaste auf **Analyzer für Identity Manager**, und klicken Sie auf **Deinstallieren**.

## 59.8 Deinstallieren von iManager

In diesem Abschnitt wird die Deinstallation von iManager und iManager Workstation beschrieben. Beim Deinstallieren von iManager und den zugehörigen Drittanbieter-Komponenten ist keine besondere Reihenfolge zu beachten. NetIQ empfiehlt, die Überlegungen zur Deinstallation dieser Komponenten zu lesen:

- Wenn Sie entweder den Webserver oder den Servlet-Container deinstallieren, können Sie iManager nicht mehr ausführen.
- Auf allen Plattformen gilt: Bei der Deinstallation werden nur die Dateien entfernt, die im Rahmen der Installation installiert wurden. Dateien, die im laufenden Betrieb der Anwendung erstellt wurden, werden bei der Deinstallation nicht entfernt. Beispiel: Protokolldateien und automatisch generierte Konfigurationsdateien, die während der Ausführung von Tomcat angelegt wurden.
- Bei der Deinstallation werden weder neu erstellte Dateien entfernt noch Dateien, die im Rahmen der Installation in der ursprünglichen Verzeichnisstruktur gespeichert und später geändert wurden. Damit ist sichergestellt, dass Daten nicht unbeabsichtigt gelöscht werden.
- Die Deinstallation von iManager hat keine Auswirkungen auf die RBS-Konfigurationen, die Sie in Ihrem Baum eingerichtet haben. Bei der Deinstallation werden keine Protokolldateien und keine benutzerdefinierten Inhalte entfernt.

Überprüfen Sie nach dem Deinstallieren von iManager, ob die folgenden Verzeichnisse entfernt wurden:

- `/var/opt/novell/iManager/`
- `/etc/opt/novell/iManager/`
- `/var/opt/novell/tomcat8/`
- `/etc/opt/novell/tomcat8/`

Wenn diese Verzeichnisse noch vorhanden sind und Sie dann versuchen, iManager neu zu installieren, schlägt die Installation fehl, und das Installationsprogramm gibt Fehlermeldungen zurück.

---

**WICHTIG:** Sichern Sie vor dem Deinstallieren von iManager alle benutzerdefinierten Inhalte oder bestimmte iManager-Dateien, die beibehalten werden sollen. Beispiel: Benutzerdefinierte Plugins.

---

### 59.8.1 Deinstallieren von iManager unter Linux

Bei der Deinstallation von iManager wird NICI nicht deinstalliert. Sie können NICI bei Bedarf separat deinstallieren.

---

**WICHTIG:** Wenn eDirectory auf demselben Computer wie iManager installiert ist, wird NICI benötigt, um eDirectory weiterhin ausführen zu können.

---

1. Melden Sie sich an dem Computer, auf dem iManager deinstalliert werden soll, als `Root` an.
2. Geben Sie in einer Shell den folgenden Befehl ein:

   ```
   /var/opt/novell/iManager/nps/UninstallerData/UninstalliManager
   ```

### 59.8.2 Deinstallieren von iManager unter Windows

Zum Deinstallieren von iManager-Komponenten öffnen Sie die Option „Software“ in der Systemsteuerung. Bei der Deinstallation gelten die folgenden Bedingungen:

- In der Systemsteuerungsoption werden Tomcat und NICI getrennt von iManager aufgeführt. Wenn Sie die Programme nicht mehr verwenden, können Sie sie deinstallieren.
- Wenn eDirectory auf demselben Server wie iManager installiert ist, deinstallieren Sie NICI nicht. NICI ist für die Ausführung von eDirectory erforderlich.
- Bei der Deinstallation werden Sie gefragt, ob alle iManager-Dateien entfernt werden sollen. Mit **Ja** entfernt das Programm sämtliche Dateien (auch benutzerdefinierte Inhalte). Es werden jedoch keine 2.7-RBS-Objekte aus dem eDirectory-Baum entfernt, und der Zustand des Schemas ändert sich nicht.

### 59.8.3 Deinstallieren von iManager Workstation

Wenn Sie iManager Workstation deinstallieren möchten, löschen Sie das Verzeichnis, in dem Sie die Dateien extrahiert haben.

## 59.9 Deinstallation von Designer

1. Schließen Sie Designer.
2. Deinstallieren Sie Designer mit dem entsprechenden Verfahren für Ihr Betriebssystem:

   **Linux und UNIX**

   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\ Designer\ for\ Identity\ Manager`.

   **Windows**

   Öffnen Sie die Option „Software“ in der Systemsteuerung. Unter Windows Server 2008 klicken Sie beispielsweise auf **Programme und Funktionen**. Klicken Sie mit der rechten Maustaste auf **Designer für Identity Manager**, und klicken Sie auf **Deinstallieren**.

# 60 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.

## 60.1 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 |
|---|---|
| Sie möchten eine oder mehrere Konfigurationseinstellungen für die Benutzeranwendung ändern, die Sie während der Installation vorgenommen haben:<br>◆ Identitätsdepot-Verbindungen und -Zertifikate<br>◆ Email-Einstellungen<br>◆ Benutzeridentität und Benutzergruppen in der Identity Manager-Engine<br>◆ Access Manager- oder iChain-Einstellungen | Das Dienstprogramm für die Konfiguration kann unabhängig vom Installationsprogramm ausgeführt werden.<br>**Linux:** Führen Sie im Installationsverzeichnis (standardmäßig `/opt/netiq/idm/apps/UserApplication/`) den folgenden Befehl aus:<br>`configupdate.sh`<br>**Windows:** Führen Sie im Installationsverzeichnis (standardmäßig `C:\NetIQ\IdentityManager\apps\UserApplication\`) den folgenden Befehl aus:<br>`configupdate.bat` |
| Beim Starten von Tomcat tritt die folgende Ausnahme auf:<br>`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). |

| Problem | Empfohlene Vorgehensweise |
|---|---|
| Beim Starten des Anwendungsservers treten Keystore-Fehler auf. | Ihr Anwendungsserver verwendet nicht das bei der Installation der Benutzeranwendung angegebene JDK.<br><br>Importieren Sie die Zertifikatsdatei mithilfe des Befehls `keytool`:<br><br>`keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit`<br><br>◆ Ersetzen Sie *aliasName* durch einen beliebigen eindeutigen Namen für dieses Zertifikat.<br>◆ Ersetzen Sie *certFile* durch den vollständigen Pfad und Namen der Zertifikatsdatei.<br>◆ Das Keystore-Standardpasswort lautet `changeit` (falls Sie ein anderes Passwort festgelegt haben, geben Sie es an). |
| Es werden keine E-Mail-Benachrichtigungen gesendet. | Überprüfen Sie mit dem `configupdate`-Dienstprogramm, ob Sie Werte für die Benutzeranwendungs-Konfigurationsparameter **Email-Von** und **Email-Host** angegeben haben.<br><br>**Linux:** Führen Sie im Installationsverzeichnis (standardmäßig `/opt/netiq/idm/apps/UserApplication/`) den folgenden Befehl aus:<br><br>`configupdate.sh`<br><br>**Windows:** Führen Sie im Installationsverzeichnis (standardmäßig C:\NetIQ\IdentityManager\apps\UserApplication\) den folgenden Befehl aus:<br><br>`configupdate.bat` |

## 60.2 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. |

## 60.3 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-E-Mail-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. |

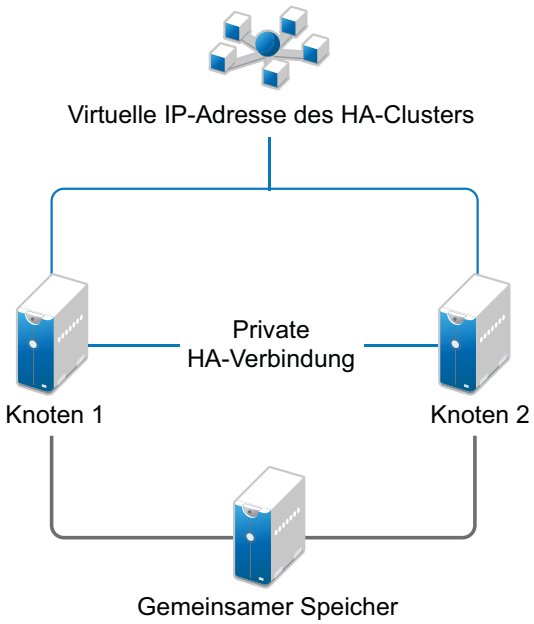
# A Beispiellösung für eine Identity Manager-Clusterbereitstellung

In diesem Anhang finden Sie schrittweise Anweisungen zum Konfigurieren von eDirectory und Identity Manager in einer Cluster-Umgebung 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 A-1 zeigt eine Beispiellösung für die Clusterbereitstellung.

***Abbildung A-1*** *Beispiellösung für eine Clusterbereitstellung*




## A.1 Voraussetzungen

- Zwei Server mit SuSE Linux Enterprise Server (SLES) 12 SP1 (64-Bit) für Knoten
- Ein Server mit SLES 12 SP1 (64 Bit) für iSCSI-Server
- ISO-Image zur HA-Erweiterung für SLES12 SP1 (64 Bit)
- Sechs statische IP-Adressen:
  - Je zwei statische IP-Adressen pro Knoten. Eine IP-Adresse wird für das öffentliche Netzwerk verwendet, die andere für den Heartbeat.

- 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.

## A.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 Extention*.

### A.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 SP1 auf den beiden anderen Knoten.

Beachten Sie Folgendes während der Installation von SLES 12 SP1:

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 im Terminal den Befehl `yast2 iscsi-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. Klicken Sie auf **Fertig stellen**.
10. Überprüfen Sie, ob das iSCSI-Ziel installiert wurde. Geben Sie hierzu den Befehl `cat /proc/net/iet/volume` im Terminal ein.

## A.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.

## A.2.3 Partitionieren des freigegebenen Speichers

Erstellen Sie im freigegebenen Speicher je eine Partition für SBD und für OCFS2 (Oracle Cluster File System 2).

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“ aus.
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 10 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**.

## A.2.4 Installieren der HA-Erweiterung

So installieren Sie die HA-Erweiterung:

1. Gehen Sie zur NetIQ Downloads-Website.
2. Wählen Sie im Menü **Produkt oder Technologie** den Eintrag **SUSE Linux Enterprise-HA-Erweiterung**, und klicken Sie auf **Suchen**.

   **HINWEIS:** Wählen Sie die entsprechende ISO-Datei mit der HA-Erweiterung für Ihre Systemarchitektur aus.
3. Laden Sie die ISO-Datei auf die einzelnen Server herunter.
4. Öffnen Sie das Dialogfeld **YaST-Kontrollzentrum**, und klicken Sie auf **Zusatzprodukte > Hinzufügen**.
5. Klicken Sie auf **Durchsuchen**, wählen Sie das lokale ISO-Image aus, und klicken Sie auf **Weiter**.
6. Wählen Sie im Dialogfeld **Software-Auswahl und Systemaufgaben** die Option **Hochverfügbarkeit**. Wiederholen Sie diesen Schritt auf dem anderen Server.

## A.2.5 Konfigurieren des HA-Clusters

Konfigurieren Sie die Unicast-IP-Adressen für Heartbeat:

1. Konfigurieren Sie die andere Schnittstelle auf beiden Knoten mit der statischen IP-Adresse, die für die Knotenkommunikation (Heartbeat) verwendet werden soll. In diesem Beispiel erhält Knoten1 die IP-Adresse 10.10.10.13 und Knoten2 die IP-Adresse 10.10.10.14.
2. Testen Sie die Verbindung zwischen den Servern. Senden Sie hierzu über die Hostnamen einen Ping-Befehl an die beiden Server.

   **WICHTIG:** Wenn die Computer sich gegenseitig keinen Ping-Befehl senden können, bearbeiten Sie die lokale Datei `/etc/hosts`, und fügen Sie die Hostnamen und die IP-Adressen der anderen Knoten hinzu. In diesem Beispiel enthält die Datei `/etc/hosts` Folgendes:

   - 10.10.10.13 sles11sp2-idm1
   - 10.10.10.14 sles11sp2-idm2
3. Führen Sie auf Knoten1 im Terminal den Befehl `yast2 cluster` aus.
4. Geben Sie im Dialogfeld **Cluster – Kommunikationskanäle** die folgenden Details an:
   - **4a** Legen Sie das Transportprotokoll UDPU fest.
   - **4b** Geben Sie die **Bindungs-Netzwerkadresse** an (Netzwerkadresse der Unicast-IP-Adressen). In diesem Beispiel lautet die Bindungs-Netzwerkadresse 10.10.10.0.
   - **4c** Geben Sie den **Multicast-Port** an. In diesem Beispiel lautet der Multicast-Port 5405.
   - **4d** Klicken Sie auf **Hinzufügen**, und geben Sie die IP-Adresse der einzelnen Knoten unter der Mitgliedadresse an. In diesem Beispiel erhält Knoten1 die IP-Adresse 10.10.10.13 und Knoten2 die IP-Adresse 10.10.10.14.
   - **4e** Wählen Sie **Knoten-ID automatisch generieren**, und klicken Sie auf **Weiter**.
5. Wählen Sie im Dialogfeld **Cluster – Sicherheit** die Option **Sicherheitsauthentifizierung aktivieren**, legen Sie unter **Threads** den Wert **1** fest, und klicken Sie auf **Authentifizierungsschlüsseldatei generieren**.

Hiermit wird ein Authentifizierungsschlüssel erstellt, über den andere Knoten dem Cluster beitreten können. Dieser Schlüssel wird unter `/etc/corosync/authkey` gespeichert. Kopieren Sie diese Datei auf den anderen Knoten.

6 Wählen Sie im Dialogfeld **Cluster – Dienst** die Option **Ein – OpenAIS beim Booten starten**, und klicken Sie auf **OpenAIS jetzt starten**.

7 Wählen Sie **Verwaltung ebenfalls starten**, damit der Cluster über crm_gui verwaltet werden kann. Weitere Informationen finden Sie in Abschnitt A.2.2, „Konfigurieren des iSCSI-Initiators auf allen Knoten“, auf Seite 577.

8 Führen Sie in der Kontrollleiste **Host synchronisieren** die folgenden Schritte aus:

**8a** Klicken Sie auf **Hinzufügen**, und fügen Sie Hostnamen für die Clusterknoten hinzu.

**8b** Synchronisieren Sie die Konfigurationsdatei zwischen den Knoten mit **Preshared-Keys generieren**, und kopieren Sie die Datei dann auf den anderen Knoten. Die Schlüsseldatei ist unter `/etc/csync2/key_hagroup` gespeichert.

**8c** Klicken Sie im Bereich **Datei synchronisieren** auf **Vorgeschlagene Dateien hinzufügen**. Hiermit wird automatisch eine Liste der gemeinsamen Dateien generiert, die zwischen den Knoten synchronisiert werden sollen.

**8d** Klicken Sie auf **csync2 aktivieren** und dann auf **Weiter**.

**8e** Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

9 Legen Sie mit dem Befehl `passwd hacluster` das Passwort für den hacluster-Benutzer auf allen Knoten fest.

---

**HINWEIS:** Geben Sie auf allen Knoten dasselbe Passwort für den hacluster-Benutzer an.

---

10 Kopieren Sie die Konfigurationsdateien und Authentifizierungsschlüssel mit den folgenden Befehlen auf den anderen Knoten:

- `# scp /etc/csync2/csync2.cfg node2:/etc/csync2/`
- `# scp /etc/csync2/key_hagroup node2:/etc/csync2/`
- `# scp /etc/corosync/authkey node2:/etc/corosync/`
- `# scp /etc/corosync/corosync.conf node2:/etc/corosync/`

11 Sobald alle Konfigurationsdateien auf Knoten2 kopiert wurden, booten Sie alle Knoten neu.

12 Führen Sie den Befehl `csync2 -xv` aus.

13 Hängen Sie den freigegebenen Speicher ein. Erstellen Sie hierzu das Verzeichnis `mkdir -p /share`.

14 Führen Sie auf Knoten2 die folgenden Schritte aus:

**14a** Führen Sie im Terminal den Befehl `yast cluster` aus.

---

**HINWEIS:** Das Fenster des Assistenten wird nicht geöffnet, da die Konfigurationsdatei bereits kopiert wurde.

---

**14b** Wählen Sie auf der Registerkarte **Dienst** die Option **Prüfung aktiviert – OpenAIS beim Booten starten**, und klicken Sie auf **OpenAIS jetzt starten**.

**14c** Klicken Sie auf der Registerkarte **csync2 konfigurieren** auf **csync2 aktivieren** und dann auf **Fertig stellen**.

**14d** Hängen Sie den freigegebenen Speicher ein. Erstellen Sie hierzu das Verzeichnis `mkdir -p /share`.

Der Cluster sollte ausgeführt werden.

15 Überprüfen Sie den Status. Führen Sie hierzu im Terminal den Befehl `crm_mon` aus. Im Folgenden finden Sie ein Beispiel für die Ausgabe:

```
============
Last updated: Fri Aug 5 16:38:36 2011
Stack: openais
Current DC: node1 - partition with quorum
Version: 1.1.2-2e096a41a5f9e184a1c1537c82c6da1093698eb5
2 Nodes configured, 2 expected votes
0 Resources configured.
============
Online: [node1 node2]
```

## A.2.6 Konfigurieren der globalen Cluster-Optionen

Eine Ressource ist ein Dienst oder eine Anwendung, die von einem Cluster verwaltet wird. Der Cluster-Software-Stack überwacht die Ressourcen und überprüft, ob sie ordnungsgemäß ausgeführt werden. Falls die Ressourcen aus jeglichen Ursachen angehalten werden, erkennt der Cluster den Fehler. Die betreffende Ressource wird dann auf dem jeweils anderen Knoten gestartet oder neu gestartet, sodass die Hochverfügbarkeit gewährleistet ist. In diesem Beispiel werden die globalen Cluster-Optionen auf Knoten1 konfiguriert.

So konfigurieren Sie die HA-Ressource auf Knoten1:

1 Führen Sie im Terminal den Befehl `crm_gui` aus.

2 Klicken Sie auf **Verbindung > Anmelden**. Melden Sie sich mit der IP-Adresse für einen der beiden Knoten an.

3 Klicken Sie auf die Registerkarte **CRM-Konfiguration**, und ändern Sie den Wert für **Standardmäßige Ressourcenbeibehaltung** in einen positiven Wert.

   Damit ist gewährleistet, dass die Ressourcen im Cluster im aktuellen Speicherort verbleiben. In diesem Beispiel ist der Wert gleich 1.

4 Ändern Sie den Eintrag für **Keine Quorumrichtlinie** in **Ignorieren**.

   Damit ist gewährleistet, dass die Clusterdienste selbst dann ausgeführt werden, wenn einer der Knoten ausfällt.

5 Klicken Sie auf **Anwenden**.

## A.2.7 Konfigurieren der OCFS-Ressourcen

Bevor Sie das OCFS2-Volume erstellen können, müssen Sie die folgenden Ressourcen als Dienste im Cluster konfigurieren:

- Distributed Lock Manager (DLM)
- O2CB
- STONITH-Ressource

Für OCFS2 muss auf allen Knoten im Cluster eine DLM-Ressource ausgeführt werden, die in der Regel als Klon konfiguriert wird. In diesem Beispiel werden die OCFS-Ressourcen auf Knoten1 konfiguriert.

## Konfigurieren der DLM- und O2CB-Ressourcen

So konfigurieren Sie die DLM- und O2CB-Ressourcen auf Knoten1:

1. Starten Sie eine Shell, und melden Sie sich als Root oder als äquivalenter Benutzer an.
2. Führen Sie im Terminal den Befehl `crm configure` aus.
3. Erstellen Sie mit dem folgenden Befehl Primitive-Ressourcen für DLM und O2CB:

   ```
   primitive dlm ocf:pacemaker:controld op monitor interval="60" timeout="60"
   primitive o2cb ocf:ocfs2:o2cb op monitor interval="60" timeout="60"
   ```

   **HINWEIS:** Der DLM-Ressourcenklon steuert den DLM-Dienst, sodass der Dienst auf allen Knoten im Cluster gestartet wird. Aufgrund der internen Co-Location und Anordnung der Basisgruppe wird der O2CB-Dienst nur auf Knoten gestartet, auf denen bereits ein Exemplar des DLM-Dienstes ausgeführt wird.

4. Erstellen Sie die Basisgruppe und den Basisklon mit dem folgenden Befehl:

   ```
   group base-group dlm o2cb clone base-clone base-group meta interleave="true"
   target-role="Started"
   ```

5. Rufen Sie die Änderungen mit dem Befehl `show` ab.
6. Führen Sie den Befehl `commit` aus, und geben Sie dann **Exit** ein.

## Konfigurieren von STONITH-Ressourcen

Es wird empfohlen, eine 10 MB große Partition am Anfang des Geräts anzulegen. (In diesem Beispiel wird die SBD-Partition als `/dev/sdb1` bezeichnet.)

**WICHTIG:** Verwenden Sie ausschließlich Gerätenamen, die sich nicht ändern. Zum Bearbeiten eines Geräts müssen Sie `/dev/disk/by-id` am Anfang des Gerätenamens angeben. Soll beispielsweise das Gerät `/dev/disk/by-id/scsi-149455400000000000000000030000002506000000f000000` als SBD-STONITH-Gerät zugewiesen werden, geben Sie den Befehl `sbd -d /dev/disk/by-id/scsi 149455400000000000000000030000002506000000f000000 create` ein.

Überprüfen Sie den Gerätenamen mit dem Befehl `ls -l`.

1. Initialisieren Sie das SBD-Gerät auf Knoten1. Führen Sie hierzu den folgenden Befehl in einem Terminal aus:

   ```
   sbd -d /dev/sdb1 create
   ```

2. Überprüfen Sie mit dem Befehl `sbd -d /dev/sdb1 dump`, ob die folgenden Details auf das Gerät geschrieben wurden:
   - `Header-Version:` 2
   - `Anzahl der Steckplätze:` 255
   - `Sektorgröße:` 512
   - `Zeitüberschreitung (Überwachung):` 5
   - `Zeitüberschreitung (Zuordnung):` 2
   - `Zeitüberschreitung (Schleife):` 1
   - `Zeitüberschreitung (msgwait):` 10

## Einrichten der Software-Überwachung

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.

Softdog ist der am stärksten generisch ausgelegte Treiber. Die Name der meisten Überwachungstreiber enthalten Zeichenfolgen wie „wd“, „wdt“ oder „dog“. Überprüfen Sie daher mit dem folgenden Befehl, welcher Treiber derzeit geladen ist:

```
lsmod | grep wd
```

## Starten des SBD-Daemons

So starten Sie den SBD-Daemon auf Knoten1:

1. Halten Sie OpenAIS an. Führen Sie hierzu in einem Terminal den Befehl `rcopenais stop` aus.
2. Erstellen Sie die Datei `/etc/sysconfig/sbd`, und fügen Sie Folgendes hinzu:

   ```
   SBD_DEVICE="/dev/sdb1"

   #The next line enables the watchdog support:

   SBD_OPTS="-W"
   ```

   **HINWEIS:** Wenn der Zugriff auf das SBD-Gerät nicht möglich ist, kann der Daemon nicht gestartet werden, sodass der Start von OpenAIS verhindert wird.
3. Führen Sie im Terminal den Befehl `yast cluster` aus.
4. Klicken Sie auf der Registerkarte **csync2 konfigurieren** im Bereich **Datei synchronisieren** auf **Hinzufügen**, und geben Sie den Pfad zur SBD-Datei wie folgt ein:

   ```
   /etc/sysconfig/sbd
   ```
5. Klicken Sie auf **OK**.
6. Klicken Sie im Bereich **Datei synchronisieren** auf **Vorgeschlagene Dateien hinzufügen**. Hiermit wird automatisch eine Liste der gemeinsamen Dateien generiert, die zwischen den Knoten synchronisiert werden sollen.
7. Führen Sie den Befehl `csync2 -xv` aus.
8. Ordnen Sie die Knoten mit dem Befehl `sbd -d /dev/sdb1 allocate <Knotenname>` zu. Zum Zuordnen der Knotennamen zum SBD-Gerät führen Sie diesen Befehl zweimal aus. In diesem Beispiel werden die folgenden Befehle ausgeführt.

   ```
   sbd -d/dev/sdb1 allocate sles11sp2-idm1
   sbd -d/dev/sdb1 allocate sles11sp2-idm2
   ```
9. Starten Sie OpenAIS mit dem Befehl `rcopenais start`.

## Testen des SBD

So testen Sie den SBD auf Knoten1:

1. Rufen Sie mit dem Befehl `sbd -d /dev/sdb1 list` die Knotensteckplätze und ihre aktuellen Meldungen vom SBD-Gerät ab.
2. Senden Sie mit dem Befehl `sbd -d /dev/sdb1 message SLES11SP2-idm2 test` eine Testmeldung an einen der Knoten.

   Der Knoten bestätigt den Empfang der Nachricht in den Systemprotokollen. Im Folgenden finden Sie ein Beispiel für eine Meldung:

   ```
   Aug 29 14:10:00 SLES11SP2-idm2 sdb1: [13412]: info: Received command test from
   SLES11SP2-idm1 on disk /dev/sdb1
   ```

---

**WICHTIG:** Aus der Bestätigung geht hervor, dass der SBD auf dem Knoten ausgeführt wird und dass der SBD zum Empfangen von Meldungen bereit ist.

---

## Konfigurieren der Fencing-Ressource

Zum Abschluss der SBD-Einrichtung aktivieren Sie den SBD als STONITH-/Fencing-Mechanismus in der CIB (Cluster Information Base). Führen Sie die folgenden Befehle in einem Terminal auf Knoten1 aus:

```
node1# crm configure

crm(live)configure# property stonith-enabled="true"

crm(live)configure# property stonith-timeout="60s"

crm(live)configure# primitive stonith_sbd stonith:external/sbd params
sbd_device="/dev/sdb1"  meta is-managed="true"

crm(live)configure# commit

crm(live)configure# quit
```

---

**HINWEIS:** Der Wert für `stonith-timeout` ist abhängig vom Wert für `msgwait timeout`. Wenn Sie für `default msgwait timeout` beispielsweise einen Zeitraum von 10 Sekunden festlegen, legen Sie 60 Sekunden für `stonith-timeout` fest.

---

## Erstellen eines OCFS2-Volumes

Bereiten Sie zunächst die Blockgeräte vor, die für das OCFS2-Volume verwendet werden sollen. Behalten Sie die Geräte unverändert bei, wenn das OCFS2-Volume als nicht zugeordneter freier Speicherplatz verwendet werden soll, und erstellen und formatieren Sie dann das OCFS2-Volume mit dem mkfs.ocfs2-Dienstprogramm.

So erstellen Sie das OCFS2-Volume auf Knoten1:

1. Öffnen Sie ein Terminalfenster, und melden Sie sich als Root an.
2. Überprüfen Sie mit dem Befehl `crm_mon`, ob der Cluster online ist.
3. Erstellen Sie ein OCFS2-Dateisystem unter `/dev/sdb2`, das zwei Clusterknoten unterstützt, und führen Sie den Befehl `mkfs.ocfs2 -N 2 /dev/sdb2` aus.

### Einhängen eines OCFS2-Volumes

So hängen Sie das OCFS2-Volume auf Knoten1 ein:

1. Starten Sie eine Shell, und melden Sie sich als Root oder als äquivalenter Benutzer an.
2. Führen Sie den Befehl `crm configure` aus.
3. Konfigurieren Sie Pacemaker für das Einhängen des OCFS2-Dateisystems auf allen Knoten im Cluster:

   ```
   primitive ocfs2-1 ocf:heartbeat:Filesystem params device="/dev/sdb2"
   directory="/share" fstype="ocfs2" options="acl" op monitor interval="20"
   timeout="40"
   ```

4. Fügen Sie das Dateisystem-Primitive mit den folgenden Schritten zur Basisgruppe hinzu, die Sie in „Konfigurieren der DLM- und O2CB-Ressourcen“, auf Seite 581 konfiguriert haben:

   **4a** Wählen Sie **Basisgruppe bearbeiten**.

   **4b** Bearbeiten Sie die Gruppe im vi-Editor wie folgt, und speichern Sie die Änderungen:

   ```
   group base-group dlm o2cb ocfs2-1 meta target-role = „Started"
   ```

   **HINWEIS:** Aufgrund der internen Co-Location und Anordnung der Basisgruppe startet Pacemaker die OCFS2-1-Ressource nur auf Knoten, auf denen bereits eine O2CB-Ressource ausgeführt wird.

5. Überprüfen Sie mit dem Befehl `show`, ob alle erforderlichen Ressourcen konfiguriert wurden.
6. Führen Sie den Befehl `commit` aus, und geben Sie dann **Exit** ein.

## A.2.8 Konfigurieren der IP-Ressource

Konfigurieren Sie die IP-Ressource mit den folgenden Befehlen auf Knoten1:

```
node1# crm configure

crm(live)configure# primitive clusterip ocf:heartbeat:IPaddr operations $id="clusterip-
operations" op monitor interval="5s" timeout="60s" params ip="10.52.190.15" meta
resource-stickiness="100" target-role="Started"   crm(live)configure# group eDir_group
clusterip meta is-managed="true" target-role="Started"   crm(live)configure# show
crm(live)configure# commit
```

## A.2.9 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 HA-Clustern finden Sie unter „Deploying eDirectory on High Availability Clusters“ (Bereitstellen von eDirectory in Hochverfügbarkeitsclustern) im *eDirectory 8.8-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.

## A.2.10 Konfigurieren der eDirectory-Ressource

Konfigurieren Sie die eDirectory-Ressource mit den folgenden Befehlen auf Knoten1:

```
node1# crm configure    crm(live)configure# primitive eDirectory ocf:heartbeat:eDir88
operations $id="eDirectory-operations" op monitor interval="15s" enabled="true"
timeout="60s" on-fail="restart" start-delay="30s" params eDir_config_file="/etc/opt/
novell/eDirectory/conf/nds.conf" meta resource-stickiness="100" target-role="Started"
crm(live)configure# edit eDir_group
```

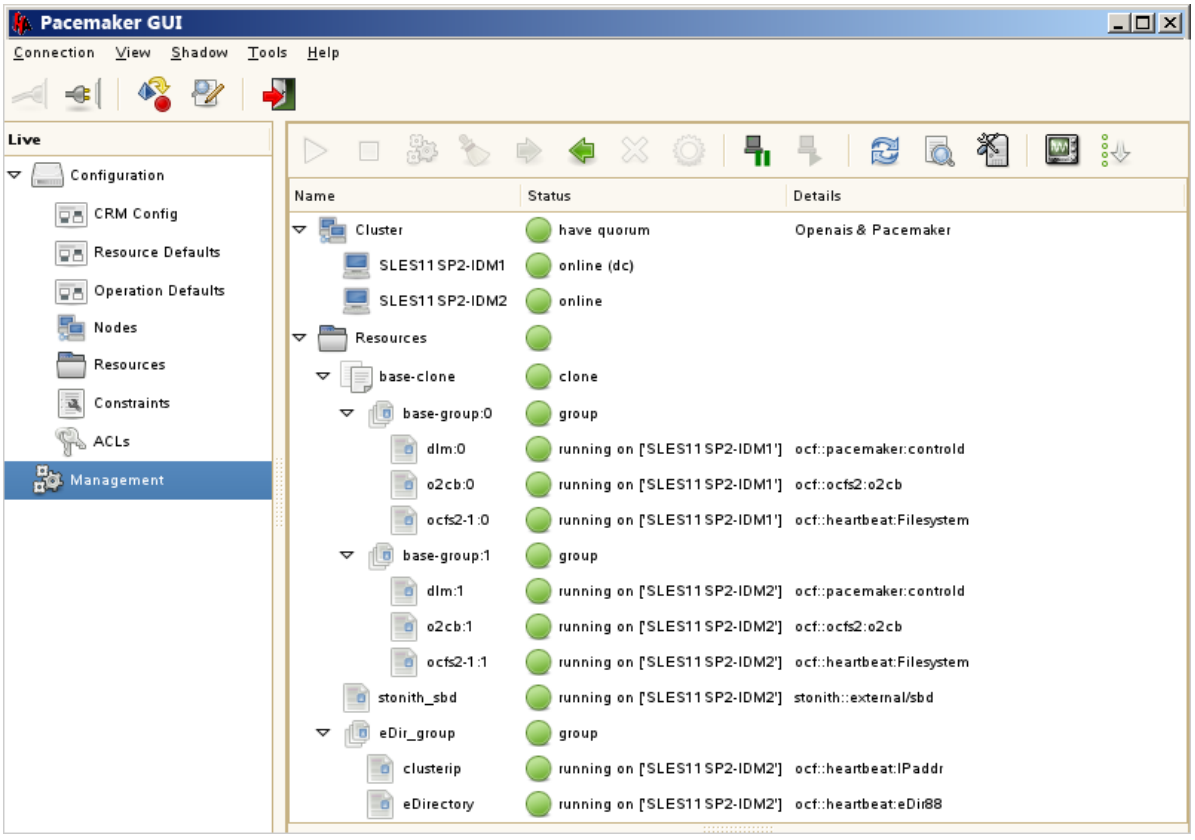
Bearbeiten Sie die Gruppe im vi-Editor, und fügen Sie den Text „eDirectory“ nach „clusterip“ ein, damit die Änderungen gespeichert werden:

```
group eDir_group clusterip eDirectory \

meta is-managed="true" target-role="Started"

crm(live)configure# show   crm(live)configure# commit
```

Klicken Sie im Hauptfenster der Pacemaker-Benutzeroberfläche auf die Registerkarte „Verwaltung“, und starten Sie **eDir_group**, falls die Ressourcen nicht bereits ausgeführt werden. In der nachfolgenden Abbildung werden die Ressourcen dargestellt, die in der Cluster-Einrichtung ausgeführt werden.



# B Beispiel einer Bereitstellungslösung für Identity Manager in einem Cluster

In diesem Anhang finden Sie schrittweise Anleitungen zum Konfigurieren von Identity Manager in einer Cluster-Umgebung auf einer Plattform mit Windows 2012 R2.



## B.1 Voraussetzungen

eDirectory 8.8.8 SP9 oder 9.0.2 (oder höher) wird in einer Cluster-Umgebung unter Windows 2012 R2 ausgeführt. Weitere Informationen zum Einrichten eines eDirectory-Clusters finden Sie unter Clustering von eDirectory-Diensten unter Windows im *NetIQ eDirectory-Installationshandbuch*.

## B.2 Konfigurieren von NetIQ Identity Manager in einem eDirectory-Cluster

In diesem Abschnitt wird vorausgesetzt, dass Sie bereits einen eDirectory-Cluster eingerichtet haben.

Konfigurieren Sie Identity Manager mit dem nachfolgenden Verfahren in einer eDirectory-Cluster-Umgebung.

1. Stellen Sie im **Cluster Manager** die Priorität der eDirectory-Clusterrollen auf dem primären Knoten auf **Kein Autostart** ein.
2. Halten Sie den sekundären Knoten an.
3. Installieren Sie die Identity Manager-Engine auf dem primären Knoten. Aktivieren Sie hierzu im Identity Manager-Installationsassistenten die Option **Metaverzeichnis-Server**.

   **WICHTIG:** Die Identity Manager-Engine muss im lokalen Speicher installiert werden.
4. Der Identity Manager-Installationsassistent hält die eDirectory-Clusterrolle während der Installation an. Wenn diese Rolle angehalten ist, wird sie unter Umständen als fehlerhaft gemeldet. Starten Sie die eDirectory-Clusterrolle nach der Installation über den **Cluster Manager**.
5. Legen Sie die erforderliche Priorität für die eDirectory-Clusterrolle fest und aktivieren Sie den sekundären Knoten.

6 Installieren Sie die Identity Manager-Engine mit dem Befehl `DCLUSTER_INSTALL` auf einem sekundären Knoten.

Beispiel: `. /idm_install.exe -DCLUSTER_INSTALL="true"`

## B.3 Clustering für Remote Loader

1 Installieren Sie den Remote Loader auf dem primären und dem sekundären Clusterknoten.

**HINWEIS:** Der Remote Loader muss auf dem primären und dem sekundären Clusterknoten jeweils in demselben freigegebenen Speicherpfad installiert werden.

2 (Bedingt) Wenn die sichere Kommunikation für den Remote Loader gilt, speichern Sie alle SSL-Zertifikate in einem freigegebenen Speicher.

3 Bevor Sie die Remote Loader-Clusterrolle erstellen, öffnen Sie die Remote Loader-Konsole und wählen Sie **Remote Loader als Windows-Dienst**.

4 Erstellen Sie unter **Cluster Manager > Rollen** eine neue Remote Loader-Clusterrolle.

Geben Sie die folgenden Informationen für die Rolle an:

**Rollentyp:** Generischer Dienst

**Dienst auswählen:** Remote Loader-Instanz (als Windows-Dienst registriert)

**Name:** Name der Clusterrolle

**Adresse:** Geben Sie eine eindeutige IP-Adresse an

**Speicher auswählen:** Freigegebener Clusterspeicher

**Registrierungseinstellungen replizieren**

1. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\RLConsole`
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\DirXML Remote Loader\Command port 8000`

   Geben Sie den Registrierungspfad der Remote Loader-Instanz an, die in den Cluster aufgenommen werden soll.
3. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\PassSync`

**HINWEIS**

- Standardmäßig nimmt jede Clusterrolle nur genau einen Windows-Dienst an. Geben Sie daher für jede Remote Loader-Instanz jeweils einen eindeutigen Befehlsport und einen zugehörigen Registrierungspfad an.
- Der Passwortfilter des Active Directory-Treibers wird in einem Windows-Cluster nicht unterstützt.

# 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.

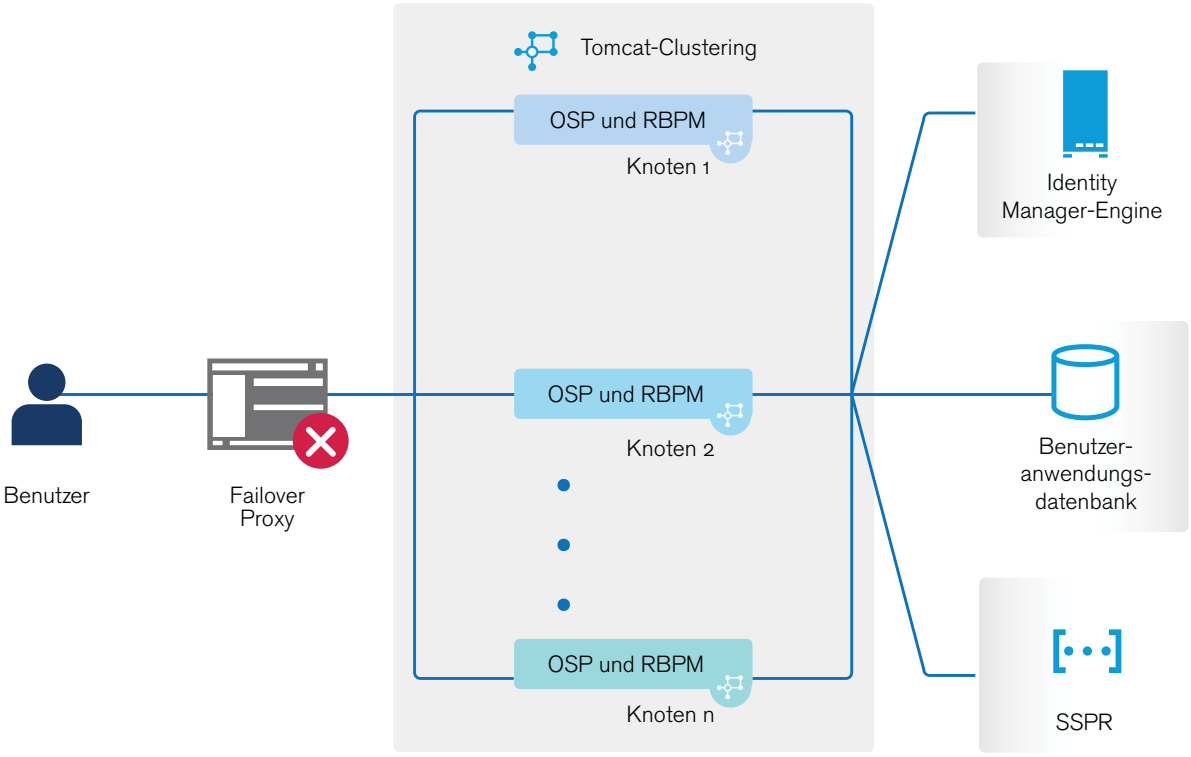
Durch das Clustering ist es möglich, Identitätsanwendungen auf verschiedenen parallelen Servern (Clusterknoten) auszuführen und dadurch hohe Verfügbarkeit zu erzielen. Zum Aufbau eines Clusters müssen verschiedene Tomcat-Instanzen (Knoten) gruppiert werden. Die Last wird auf verschiedene Server verteilt. 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.
- OSP (One Single-Sign On Provider) und die Benutzeranwendung sind auf demselben Clusterknoten installiert. OSP kann jedoch auch auf einem anderen Server in der Produktionsumgebung installiert werden. In diesem Fall müssen Sie einige Änderungen an der Konfiguration durchführen. Diese finden Sie in Abschnitt C.2, „Installationsvorgang“, auf Seite 591.
- SSPR (Single Sign-On Password Reset) wird auf separaten Computern installiert. Dies ist der empfohlene Ansatz für eine Bereitstellung auf Produktionsebene.
- PostgreSQL wird als Datenbank für die Benutzeranwendung verwendet. Alle anderen Datenbanken, die von unterstützt werden – wie Oracle, SQL-Server oder PostgreSQL – 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 (SLES) 12 SP1 (64-Bit), SLES 11 SP4 (64-Bit) oder RedHat Enterprise Linux (RHEL) 6.8 (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 4.6-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 4.6-Engine. Schrittweise Anleitungen finden Sie unter Kapitel 7, „Planen der Installation des Identitätsdepots“, auf Seite 69. Für eine Bereitstellung auf Produktionsebene empfiehl es sich, die Identity Manager-Engine auf einem separaten Server zu installieren.
2. Installieren Sie PostgreSQL über das beigelegte Installationsprogramm.

   Identity Manager unterstützt PostgreSQL 9.4.10 unter SLES 11 SP4 sowie PostgreSQL 9.6.1 auf anderen unterstützten Plattformen.

   Schrittweise Anleitungen finden Sie unter Kapitel 28, „Installieren von PostgreSQL und Tomcat“, auf Seite 261. Für eine Bereitstellung auf Produktionsebene empfiehl es sich, PostgreSQL auf einem separaten Server zu installieren.
3. Erstellen Sie die folgenden Treiber und stellen Sie sie für die Identitätsanwendungen bereit:
   - Benutzeranwendungstreiber
   - Rollen- und Ressourcenservice-Treiber

   Schrittweise Anleitungen finden Sie unter Kapitel 38, „Erstellen und Bereitstellen der Treiber für die Identitätsanwendungen“, auf Seite 351.
4. Installieren Sie die folgenden Identity Manager-Komponenten auf Knoten1:
   a. Tomcat

      Installieren Sie Tomcat mit einem Installationsprogramm Ihrer Wahl und wählen Sie während des Installationsvorgangs nur Tomcat aus. Schrittweise Anleitungen finden Sie unter Kapitel 28, „Installieren von PostgreSQL und Tomcat“, auf Seite 261.

   b. OSP

      Weitere Informationen zum Installieren des OSP finden Sie in Kapitel 32, „Installieren der Passwortverwaltung für Identity Manager“, auf Seite 285.

      Geben Sie während des Installationsvorgangs die IP-Adresse und Portnummer des Identity Manager-Engine(eDirectory)-Servers auf der Seite mit den Authentifizierungsdetails an.

   c. Benutzeranwendung

      Konfigurieren Sie die folgenden Einstellungen während des Installationsvorgangs:

      i. Wählen Sie **Tomcat** als Anwendungsserver aus.

      ii. Wählen Sie **PostgreSQL** als Datenbankplattform aus.

      ---

      **HINWEIS:** Es ist möglich, eine der von Identity Manager 4.6 unterstützten Datenbanken zu verwenden.

      ---

      iii. Geben Sie die erforderlichen Datenbankdetails auf den folgenden Seiten an.

      iv. Kopieren Sie die JAR-Datei mit dem Datenbanktreiber (`postgresql-9.4.1212jdbc42.jar`) vom PostgreSQL-Server auf alle Benutzeranwendungsknoten im Cluster.

**HINWEIS:** Wenn Sie andere von unterstützte Datenbanken wie Oracle oder SQL Server verwenden, müssen Sie die entsprechenden JAR-Dateien mit dem Treiber vom Server, auf dem die Datenbank installiert ist, auf alle Benutzeranwendungsknoten im Cluster kopieren. Weitere Informationen finden Sie unter Kapitel 35, „Konfigurieren der Datenbank für die Identitätsanwendungen“, auf Seite 315.

v. Suchen Sie die kopierte JAR-Datei mit dem Datenbanktreiber und wählen Sie sie aus.

vi. Wählen Sie in den Details der Seite „Neue Datenbank“ oder „Vorhandene Datenbank“ die Option **Neue Datenbank** aus.

vii. Geben Sie auf der Seite „Identity Manager-Konfiguration“ einen eindeutigen Namen im Feld **Workflow-Engine-ID** an. Beispiel: Der eindeutige Name kann Engine1 für Knoten1 lauten.

viii. Wählen Sie auf der Seite „Sicherheit – Master-Schlüssel die Option **Nein** aus, um einen neuen Master-Schlüssel zu erstellen.

Die Identitätsanwendungen verschlüsseln vertrauliche Daten mit einem Master-Schlüssel. Da es sich hierbei um die erste Instanz der Identitätsanwendungen in einem Cluster handelt, müssen Sie das Installationsprogramm anweisen, einen neuen Master-Schlüssel zu erstellen. Wählen Sie hierzu **Nein** aus. In einem Cluster muss für das Benutzeranwendungs-Clustering jede Instanz der Benutzeranwendung denselben Master-Schlüssel verwenden. Wählen Sie während der Konfiguration dieser Instanzen die Option **Ja** aus. Dadurch wird der vorhandene Schlüssel importiert und es wird immer derselbe Master-Schlüssel verwendet.

**HINWEIS:** Detaillierte Anweisungen und weitere Informationen zur Installation der Benutzeranwendung finden Sie in Kapitel 37, „Installieren der Identitätsanwendungen“, auf Seite 325.

5. Führen Sie in Knoten2 die folgenden Schritte durch:

a. Installieren Sie Tomcat mit einem Installationsprogramm Ihrer Wahl (wählen Sie während des Installationsvorgangs nur Tomcat aus).

Schrittweise Anleitungen finden Sie unter Kapitel 28, „Installieren von PostgreSQL und Tomcat“, auf Seite 261.

b. Installieren Sie OSP.

Weitere Informationen zur Installation von OSP finden Sie in Kapitel 32, „Installieren der Passwortverwaltung für Identity Manager“, auf Seite 285.

Geben Sie während des Installationsvorgangs die IP-Adresse und Portnummer des Identity Manager-Engine(eDirectory)-Servers auf der Seite mit den Authentifizierungsdetails an.

c. Installieren Sie die Benutzeranwendung.

Konfigurieren Sie die folgenden Einstellungen während des Installationsvorgangs:

i. Wählen Sie **Tomcat** als Anwendungsserver aus.

ii. Wählen Sie **PostgreSQL** als Datenbankplattform aus.

**HINWEIS:** Sie können eine beliebige unterstützte Datenbank verwenden.

iii. Geben Sie auf den folgenden Seiten während des Installationsvorgangs die erforderlichen Datenbankdetails an.

iv. Kopieren Sie die JAR-Datei mit dem Datenbanktreiber (`postgresql-9.4.1212jdbc42.jar`) vom PostgreSQL-Server auf Knoten2.

**HINWEIS:** Wenn Sie eine andere von Identity Manager 4.5.1 unterstützte Datenbank wie Oracle oder SQL Server verwenden, müssen Sie die entsprechenden JAR-Dateien mit dem Treiber vom Server, auf der die Datenbank installiert ist, auf alle Benutzeranwendungsknoten im Cluster kopieren. Weitere Informationen finden Sie unter Kapitel 35, „Konfigurieren der Datenbank für die Identitätsanwendungen“, auf Seite 315.

v. Suchen Sie die kopierte JAR-Datei mit dem Datenbanktreiber und wählen Sie sie aus.

vi. Wählen Sie in den Details der Seite „Neue Datenbank“ oder „Vorhandene Datenbank“ die Option **Vorhandene Datenbank** aus.

vii. Geben Sie auf der Seite „Identity Manager-Konfiguration“ einen eindeutigen Namen im Feld **Workflow-Engine-ID** an. Beispiel: Der eindeutige Name kann Engine2 für Knoten2 lauten.

viii. Wählen Sie zum Erstellen eines neuen Master-Schlüssels auf der Seite „Sicherheit – Master-Schlüssel“ die Option **Ja** aus.

Für das Benutzeranwendungs-Clustering muss jede Instanz der Benutzeranwendung denselben Master-Schlüssel verwenden. Wählen Sie die Option **Ja** aus. Dadurch wird der vorhandene Schlüssel importiert und es wird immer derselbe Master-Schlüssel verwendet. Dieser Schlüssel wird erstellt, wenn Sie die erste Instanz der Benutzeranwendung in Knoten1 installiert haben.

Der Master-Schlüssel befindet sich in der Datei mit den ISM-Konfigurationseigenschaften, die sich unter`/TOMCAT_INSTALLED_HOME/conf/` in Knoten1 befindet. Der Parameter mit dem Master-Schlüssel lautet `com.novell.idm.masterkey`.

ix. Klicken Sie auf **Installieren**, um die Installation abzuschließen.

**HINWEIS:** Detaillierte Informationen zum Installieren der Benutzeranwendung finden Sie in Kapitel 37, „Installieren der Identitätsanwendungen“, auf Seite 325.

6. Installieren Sie SSPR auf einem separaten Computer.

Notieren Sie sich vor der Installation die folgenden Einstellungen und geben Sie diese während des Installationsvorgangs an:

a. Installieren Sie **Tomcat**. Installationsanleitungen finden Sie in Schritt 4a.

b. Installieren Sie **SSPR**.

Führen Sie während der SSPR-Installation die folgenden Schritte durch:

i. Wählen Sie auf der Seite „Anwendungsserver-Verbindung“ die Option **Connect to external authentication server** (Mit externem Authentifizierungsserver verbinden) und geben Sie den DNS-Namen des Servers an, auf dem der Lastausgleich installiert ist.

ii. Geben Sie auf der Seite „Authentifizierungsdetails“ die **IP-Adresse** und den **Port** des Identity Manager-Engine-Servers an. Das Passwort für die Zertifikate der Zertifizierungsstelle lautet „changeit“.

c. 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**.

i. Klicken Sie auf **Wert hinzufügen** und geben Sie die folgende URL an:

OSP: `http://<DNS_für_Failover><Port>/osp`

ii. Speichern Sie die Änderungen.

iii. Klicken Sie auf der Seite „SSPR-Konfiguration“ auf **Einstellungen** > **OAuth-SSO** und bearbeiten Sie die OSP-Links; ersetzen Sie dazu die IP-Adressen durch den DNS-Namen des Servers, auf dem die Lastausgleichsoftware installiert ist.

iv. Klicken Sie auf **Einstellungen** > **Anwendung** und aktualisieren Sie die Weiterleitungs- und Abmeldungs-URLs; ersetzen Sie dazu die IP-Adressen durch den DNS-Namen des Servers, auf dem die Lastausgleichsoftware installiert ist.

d. Starten Sie zur Aktualisierung der SSPR-Informationen auf Knoten1 das Konfigurationsprogramm unter `/opt/netiq/idm/apps/UserApplication/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.

---

**HINWEIS:** Vergewissern Sie sich, dass die Werte für diese Parameter in Knoten2 aktualisiert werden.

---

7. Führen Sie die folgenden Konfigurationsaufgaben in den Clusterknoten durch:

a. Starten Sie Tomcat in allen Clusterknoten neu.

b. Melden Sie sich zur Aktualisierung des Links „Passwort vergessen“ mit der SSPR-IP-Adresse bei der Benutzeranwendung in Knoten1 an und klicken Sie auf **Verwaltung** > **Passwort vergessen**.

Weitere Informationen zur SSPR-Konfiguration finden Sie unter Abschnitt 39.6, „Konfigurieren der „Passwort vergessen“-Verwaltung“, auf Seite 359.

c. Weitere Informationen zum Link „Passwort ändern“ finden Sie in Abschnitt 39.6.4, „Aktualisieren der SSPR-Links im Dashboard für eine dezentrale Umgebung oder eine Cluster-Umgebung“, auf Seite 364.

d. Überprüfen Sie, ob die Links „Passwort vergessen“ und „Passwort ändern“ mit der SSPR-IP-Adresse in Knoten2 aktualisiert sind.

---

**HINWEIS:** Wenn die Links „Passwort vergessen“ und „Passwort ändern“ bereits mit der SSPR-IP-Adresse aktualisiert sind, brauchen Sie keine Änderungen vorzunehmen.

---

8. Stoppen Sie Tomcat in Knoten1 und generieren Sie eine neue `osp.jks`-Datei. Geben Sie dazu den DNS-Namen des Lastausgleichservers an und führen Sie den folgenden Befehl aus:

```
/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.

---

9. (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
```

10. 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 in diesen Speicherort. Die neue `osp.jks`-Datei wurde in Schritt 8 erstellt.

11. 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.
12. 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 Datei mit den ISM-Konfigurationseigenschaften 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.

    ---
13. 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.
14. 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. Falls Sie lieber TCP anstatt dieses Protokolls verwenden möchten, finden Sie die entsprechenden Anleitungen unter Konfigurieren der Benutzeranwendung zur Verwendung von TCP.

15. Aktivieren Sie den Berechtigungsindex für das Clustering.
    a. Melden Sie sich bei iManager in 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**.
16. 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-7.0-doc/cluster-howto.html.
17. Starten Sie Tomcat in allen Knoten neu.
18. 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.
19. 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.

20. Vergewissern Sie sich, dass die Sitzungstreue für den Cluster aktiviert ist, der in der Lastausgleichsoftware für die Benutzeranwendungsknoten erstellt wurde.
21. 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.

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

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