Kurzanleitung zu NetIQ Identity Manager Standard Edition

Februar 2015

Dieses Dokument enthält Anweisungen zum Installieren, Konfigurieren und Aufrüsten von Identity Manager 4.5 Standard Edition.

1 Überblick

Identity Manager 4.5 Standard Edition bietet die folgenden Funktionen:

- Automatische regelbasierte Bereitstellung
- Passwortverwaltung (Zurücksetzen von Passwörtern per Selbstbedienung)
- Identitätsberichterstellung
- Framework zum Verpacken von Inhalten
- Single Sign-On (One SSO)
- Analyzer
- Designer

  Weitere Informationen finden Sie im *Einrichtungshandbuch zu NetIQ Identity Manager*.

WICHTIG: Beide Identity Manager-Ausführungen (Advanced und Standard) enthalten weiterhin die gleichen Integrationsmodule.

Weitere Informationen zu Verbesserungen oder zu neuen, geänderten oder nicht mehr unterstützten Funktionen in dieser Version finden Sie in den Versionshinweisen.

2 Komponenten

Identity Manager 4.5 Standard Edition umfasst die folgenden Komponenten:

- Identitätsdepot
- iManager
- Identity Manager-Engine
- Designer
- Analyzer
- Remote Loader
- Event Auditing Service (EAS)
- Tomcat (unterstützter Anwendungsserver)
- Single Sign-On (One SSO)
- Zurücksetzen von Passwörtern per Selbstbedienung (SSPR)
- Identitätsberichterstellung

Weitere Informationen zur Zusammenarbeit zwischen den Identity Manager-Komponenten finden Sie unter „Einführung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

3 Installieren von Identity Manager 4.5 Standard Edition

Laden Sie die Software von der Produkt-Website herunter. Die folgenden `.iso`-Dateien enthalten das DVD-Image zum Installieren der Identity Manager-Komponenten:

- `Identity_Manager_4.5_Linux_Standard.iso`
- `Identity_Manager_4.5_Windows_Standard.iso`

Die Installationsdateien befinden sich im Verzeichnis `products` im Identity Manager-Installationspaket. Weitere Informationen zu den standardmäßigen Installationsorten finden Sie in den Versionshinweisen unter Installationsorte.

NetIQ empfiehlt, die Voraussetzungen für die Installation in den Versionshinweisen zu lesen und anschließend die nachfolgende Checkliste in der angegebenen Reihenfolge abzuarbeiten. Zu jeder Aufgabe sind kurze Informationen und ein Verweis zu näheren Details angegeben. Weitere Informationen zum Installieren der einzelnen Identity Manager-Komponenten finden Sie im *Einrichtungshandbuch zu NetIQ Identity Manager*.

Aufgabe	Hinweise
1. Voraussetzungen	◆ Überprüfen Sie anhand der Systemanforderungen für die einzelnen Komponenten, ob der Computer oder die virtuellen Images die Installationsvoraussetzungen erfüllen. Weitere Informationen zu den installierbaren Komponenten für bestimmte Betriebssysteme finden Sie unter Auswählen einer Betriebssystemplattform für Identity Manager im *Einrichtungshandbuch zu NetIQ Identity Manager*. ◆ Weitere Informationen zu den Voraussetzungen und den Systemanforderungen sowie zur Installation, Aufrüstung oder Migration finden Sie unter Überlegungen und Voraussetzungen für die Installation im *Einrichtungshandbuch zu NetIQ Identity Manager*.
2. Installation planen	Weitere Informationen finden Sie unter „Planen der Installation von Identity Manager“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
3. Reihenfolge bei der Installation	Die Komponenten müssen in der nachstehenden Reihenfolge installiert werden, da die Installationsprogramme bestimmter Komponenten Informationen zu bereits installierten Komponenten benötigen. 1. eDirectory 2. iManager 3. Identity Manager-Engine 4. Designer 5. Analyzer 6. Event Auditing Service (EAS) 7. Tomcat (unterstützter Anwendungsserver) 8. Komponenten für Single Sign-On und Passwortverwaltung 9. Identitätsberichterstellung **WICHTIG:** Die Installationsprogramme installieren die Identity Manager-Komponenten in

Aufgabe	Hinweise
4. eDirectory installieren und konfigurieren	Installieren Sie eDirectory 8.8.8 Patch 3 oder höher. Anweisungen zur Installation finden Sie unter „Installieren des Identitätsdepots“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. ◆ Sobald Sie eDirectory installiert und konfiguriert haben, halten Sie die Directory-Dienste an. ◆ Wenden Sie den letzten veröffentlichten eDirectory-Patch an. ◆ Starten Sie die eDirectory-Dienste.
5. iManager installieren und konfigurieren	Installieren Sie iManager 2.7.7 Patch 2 oder höher. Damit die Revisionsfunktionen genutzt werden können, installieren Sie iManager 2.7.7 Patch 3 oder höher. Anweisungen zur Installation finden Sie unter „Installieren von iManager“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
6. Identity Manager-Engine, Treiber und iManager-Plugins installieren	Anweisungen zur Installation finden Sie unter „Installieren der Identity Manager-Engine, der Treiber und der iManager-Plugins“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. **HINWEIS:** Das Installationsprogramm erstellt nicht das DirMXL-PasswordPolicy-Objekt im Identitätsdepot. Sobald die Identity Manager-Engine installiert ist, starten Sie Designer und erstellen Sie den Treibersatz. Installieren Sie das Standard-Universalpasswort-Richtlinienpaket für Identity Manager, in dem sich die Richtlinie `DirMXL-PasswordPolicy` befindet. Fügen Sie diese Richtlinie zum Treibersatz hinzu. Führen Sie diesen Vorgang für alle Identity Manager-Treibersätze im Identitätsdepot aus.
7. Event Auditing Service installieren	Anweisungen zur Installation finden Sie unter „Installieren des Event Auditing Service“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
8. Tomcat installieren	Wählen Sie ausschließlich Tomcat für die Bereitstellung der Identitätsberichterstellung aus. PostgreSQL muss nicht installiert werden, da das RBPM nicht installiert wird. Anweisungen zur Installation finden Sie unter „Installieren von PostgreSQL und Tomcat“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. **HINWEIS:** Wenn Sie Tomcat auf einem Computer installieren, auf dem bereits iManager installiert ist, verwenden Sie nicht den Port 8080 für Tomcat. Falls die anderen Ports bereits in Gebrauch sind, ändern Sie sie während der Installation.

Aufgabe	Hinweise

9. Komponenten für Single Sign-On und Passwortverwaltung installieren	Anweisungen zur Installation finden Sie unter „Installieren der Komponenten für Single Sign-On und Passwortverwaltung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
	
	Führen Sie nach der Installation der Komponenten für Single Sign-On und Passwortverwaltung die folgenden Schritte aus:
	
	◆ **Erweitern Sie das eDirectory-Schema.** Mithilfe dieser Aufgabe können Sie das eDirectory-Schema um Objektklassen- und Attributdefinitionen erweitern.
	1. Kopieren Sie die nachfolgenden Angaben in eine Datei und speichern Sie sie als `.ldif`-Datei.
	`dn: o="Your Organization"`
	`changetype: modify`
	`add: ACL`
	`ACL: 7#subtree#[This]#pwmResponseSet`
	2. Wechseln Sie in iManager zu **Rollen und Aufgaben > Schema > Schema erweitern** > **Daten aus Datei auf Festplatte importieren** und klicken Sie auf **Weiter**.
	3. Klicken Sie auf **Zu importierende Datei** und navigieren Sie zur `.ldif`-Datei. Überprüfen Sie, ob diese Datei den `Organization`-Containernamen `o="Your Organization"` enthält. Falls nicht, fügen Sie den vorhandenen `Organization`-Containernamen ein und klicken Sie auf **Weiter**.
	4. Geben Sie Werte für die nachfolgenden Felder ein und klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
	◆ **DNS-Name/IP-Adresse des Servers**
	◆ **Authentifizierungsanmeldung**
	◆ **Benutzer-DN**
	◆ **Password**
	HINWEIS: Der LDAP-Server akzeptiert standardmäßig keine unsicheren Verbindungen. Sie können wahlweise die SSL-Authentifizierung verwenden oder die Servereinstellungen so ändern, dass Verbindungen im Klartext zugelassen werden.
	Nach erfolgtem Import der Datei wird eine Meldung über den erfolgreichen Abschluss des Importvorgangs angezeigt.
	
	◆ **Richten Sie die SSL-Revision ein.** Wenn Sie die Revision während der SSPR-Installation aktiviert haben, erfordert die SSPR ein SSL-Zertifikat für die Revision der Ereignisse. Anweisungen zum Importieren des SSL-Zertifikats und zur Revision der Ereignisse finden Sie unter Setting Up SSL Auditing (https://www.netiq.com/documentation/sspr3/adminguide/data/b14knaes.html) (Einrichten der SSL-Revision) im *NetIQ Self Service Password Reset 3.2 Administration Guide* (NetIQ-Administrationshandbuch für SSPR 3.2 [Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung]).

Aufgabe	Hinweise
10. Identitätsberichterstellung installieren und konfigurieren	1. Allgemeine Informationen zu den erforderlichen Komponenten und zum Rahmenwerk für die Berichterstellung finden Sie unter „Installieren der Komponenten für die Identitätsberichterstellung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. 2. Anweisungen zur Installation der Identitätsberichterstellung mithilfe eines Installationsassistenten (wahlweise über die Benutzeroberfläche oder an der Konsole) finden Sie unter Abschnitt 3.1, „Installieren der Identitätsberichterstellung“, auf Seite 5. 3. Anweisungen zur automatischen Installation finden Sie in Abschnitt 3.1.2, „Automatische Installation der Identitätsberichterstellung“, auf Seite 10. 4. Anweisungen zum Konfigurieren der Treiber finden Sie unter „Konfigurieren von Treibern für die Identitätsberichterstellung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. 5. Anweisungen zum Bereitstellen der REST-APIs für die Identitätsberichterstellung finden Sie unter „Bereitstellen von REST-APIs für die Identitätsberichterstellung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. **HINWEIS:** Sie müssen die Berichtsdefinitionen in die Identitätsberichterstellung importieren. Diese finden Sie auf der Download-Seite in der Berichterstellungsanwendung.
11. Identity Manager aktivieren	Aktivieren Sie die Identity Manager-Komponenten. Weitere Informationen finden Sie unter „Aktivieren von Identity Manager“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

3.1 Installieren der Identitätsberichterstellung

Das Identity Manager-Installationspaket enthält die Installationsdateien in den Verzeichnissen `products/EAS` und `products/Reporting` in der `.iso`-Image-Datei. Standardmäßig installiert das Installationsprogramm die Komponenten in den folgenden Speicherorten:

- **Linux:** `/opt/netiq/idm/apps/IDMReporting`
- **Windows:** `C:\netiq\idm\apps\IDMReporting`

3.1.1 Geführte Installation der Identitätsberichterstellung

Im Folgenden wird beschrieben, wie Sie die Identitätsberichterstellung mithilfe eines Installationsassistenten installieren (wahlweise über die Benutzeroberfläche oder an der Konsole).

Zur Vorbereitung der Installation lesen Sie die Voraussetzungen und Systemanforderungen unter „Systemanforderungen für die Identitätsberichterstellung“ im *Einrichtungshandbuch zu NetIQ Identity Manager* sowie die Versionshinweise.

1. Stellen Sie sicher, dass die SIEM-Datenbank in Ihrem Ereignisrevisionsdienst ausgeführt wird.

   Das Installationsprogramm erstellt Tabellen in der Datenbank und prüft die Verbindungen. Außerdem wird eine JAR-Datei für den PostgreSQL-JDBC-Treiber installiert, die dann automatisch für die Verbindungen zur Datenbank herangezogen wird.
2. Melden Sie sich an dem Computer an, auf dem die Identitätsberichterstellung installiert werden soll.
3. Halten Sie den Anwendungsserver an. In diesem Fall ist dies Tomcat.

4 (Bedingt) Wenn Ihnen die `.iso`-Datei für das Identity Manager-Installationspaket vorliegt, navigieren Sie zum Verzeichnis, in dem sich die Installationsdateien für die Identitätsberichterstellung befinden (standardmäßig unter `products/Reporting/`).

5 (Bedingt) Wenn Sie die Installationsdateien für die Identitätsberichterstellung von der NetIQ Downloads-Website heruntergeladen haben, führen Sie die folgenden Schritte aus:

   5a Navigieren Sie zur `.tgz`-Datei für das heruntergeladene Image.

   5b Extrahieren Sie den Inhalt der Datei in einen Ordner auf dem lokalen Computer.

6 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`

7 Legen Sie im Installationsprogramm die gewünschte Sprache für die Installation fest, und klicken Sie auf **OK**.

8 Lesen Sie den Einführungstext, und klicken Sie auf **Weiter**.

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

10 Legen Sie abschließend Werte für die folgenden Parameter fest:

   - **Installationsordner**

     Gibt den Speicherort der Installationsdateien an.

   - **Identitätsdepot-Verbindungsdetails**

     Gibt die Verbindungseinstellungen für das Identitätsdepot an. Mit dem Berichterstellungskonfigurationsprogramm (`configupdate.sh`) im Verzeichnis `/opt/netiq/idm/apps/IdentityReporting/bin/lib` können Sie diese Einstellungen nach der Installation bearbeiten.

     Identitätsdepot-Server

     Gibt den DNS-Namen oder die IP-Adresse des Identitätsdepot-Servers an.

     Sicherer LDAP-Port

     Gibt den Port an, über den die Identitätsberichterstellung mit dem Identitätsdepot kommunizieren soll.

   - **Anwendungsserverplattform**

     Gibt den Anwendungsserver an, auf dem die Kern-WAR-Datei (`IDMRPT-Core.war`), die WAR-Datei für die EAS-REST-API (`easrestapi.war`) und für EAS Webstart (`easwebstart.war`) sowie die WAR-Datei für die Reporting-REST-API-Referenz (`rptdoc.war`) ausgeführt werden sollen. NetIQ unterstützt ausschließlich Tomcat für die Identitätsberichterstellung.

     HINWEIS: Ändern Sie nicht die Namen dieser WAR-Dateien. Wenn Sie die Dateinamen ändern, tritt bei der Bereitstellung ein Fehler auf.

   - **Anwendungsserver-Details**

     Gibt einen Pfad zum Bereitstellungs- oder Webapps-Verzeichnis der Tomcat-Instanz an. Beispiel: `/opt/netiq/idm/apps/tomcat/webapps`.

   - **Anwendungsserver-Verbindung**

Gibt die Einstellungen für die URL an, über die die Benutzer eine Verbindung zur Identitätsberichterstellung auf dem Anwendungsserver herstellen. Beispiel: `https:meinserver.meinefirma.de:8080`.

HINWEIS: Wenn OSP auf einer anderen Instanz des Anwendungsservers ausgeführt wird, müssen Sie außerdem die Option **Mit externen 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 erfolgen, wählen Sie `https`.

Hostname

Gibt den DNS-Namen oder die IP-Adresse des Anwendungsservers an. Verwenden Sie nicht `localhost`.

Port

Gibt den Port an, über den der Anwendungsserver mit Identity Manager kommunizieren soll.

Mit externen Authentifizierungsserver verbinden

Gibt an, ob der Authentifizierungsserver (OSP) auf einer Instanz des Anwendungsservers 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 an, mit dem der Identitätsberichterstellungsdienst eine Verbindung zum OSP-Client auf dem Authentifizierungsserver herstellen soll.

  Mit dem Berichterstellungs-Konfigurationsprogramm können Sie dieses Passwort nach der Installation bearbeiten.

- **Event Auditing Service**

  Gibt an, ob Ereignisse in der Identitätsberichterstellung mit dem NetIQ Event Auditing Service (EAS) nachverfolgt werden sollen.

  Wenn Sie diese Einstellung wählen, geben Sie außerdem den DNS-Namen oder die IP-Adresse des Servers an, auf dem der EAS gehostet wird.

- **Datenbankdetails**

  Gibt die Einstellungen für die SIEM-Datenbank an.

  Datenbank-Port

  Gibt den Port für die SIEM-Datenbank an. Der Standardwert ist 15432.

  DBA-Passwort

  Gibt das Passwort des Administratorkontos für die Datenbank an.

  Wenn Sie den EAS verwenden, erstellt das Installationsprogramm dieses Passwort für das Konto `dbauser`.

  Passwort des Benutzers 'idmrptsrv'

  Gibt das Passwort für das Konto an, das als Eigentümer des Identitätsberichterstellungsschemas und der zugehörigen Ansicht in der Datenbank fungiert.

  Das Installationsprogramm erstellt dieses Passwort für das Konto `idmrptsrv`.

Passwort des Benutzers 'idmrptuser'

Gibt das Passwort für das Konto an, das zum Ausführen von Berichten auf die Datenbank zugreift.

Das Installationsprogramm erstellt dieses Passwort für das Konto `idmrptuser`.

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.

- **Authentifizierungsdetails**

Gibt die Einstellungen für den Authentifizierungsserver an. Mit dem Berichterstellungs-Konfigurationsprogramm können Sie diese Einstellungen nach der Installation bearbeiten.

Basiscontainer

Gibt den DN des Containers an, in dem der Benutzer aufgeführt ist, der sich bei der Identitätsberichterstellung anmelden kann. Beispiel: `o=data`.

HINWEIS: Sonderzeichen im DN müssen unter Umständen mit einem Escape-Zeichen versehen werden. Weitere Informationen finden Sie in RFC 2253/4514, Abschnitt 2.4.

Anmeldeattribut

Gibt das Attribut an, mit dem der Teilbaum des Benutzercontainers durchsucht werden soll. Beispiel: `CN`.

Zielgebietsschema

Gibt die Sprache für die Identitätsberichterstellung an. Die Anwendung nutzt das angegebene Gebietsschema in den Suchvorgängen.

- **Identitätsdepot-Berechtigungsnachweis**

Gibt den Identitätsdepot-Berechtigungsnachweis für den Identitätsdepot-Server an.

Identitätsdepot-Administrator

Gibt den DN des Admin-Benutzers an, der berechtigt ist, Rollen für Benutzer zu erteilen und zu widerrufen.

Identitätsdepot-Administratorpasswort

Gibt das Passwort für den Admin-Benutzer an.

Keystore-Pfad

Gibt den Pfad einer Keystore-Datei an, die vertrauenswürdige Zertifikate für SSL-Verbindungen enthält. Standardmäßig ist dies der Pfad, der durch das OSP-SSPR-Installationsprogramm erstellt wurde.

Keystore-Passwort

Gibt das Passwort zum Öffnen der Keystore-Datei an. Das Standardpasswort lautet *changeit*.

Container-DN der Berichtsadministratorrolle

Gibt die DN des Containers an, in dem das Installationsprogramm die reportAdmin-Rolle erstellen soll.

DN des Berichtsadministratorbenutzers

Gibt die DN des Benutzers an, dem das Installationsprogramm die reportAdmin-Rolle zuweisen soll.

HINWEIS: Der Container, in dem sich die reportAdmin-Rolle befindet, darf kein Objekt mit demselben Namen enthalten.

- **Pfad des Java JRE-Basisordners auswählen**

Gibt den Pfad der JRE für den Anwendungsserver an.

Java JRE-Basisordner

Gibt den Pfad der JRE für den Anwendungsserver an. Beispiel: `/opt/netiq/idm/apps/jre`

- **Email-Zustellung**

Gibt die Einstellungen für den SMTP-Server an, der die Berichtsbenachrichtigungen sendet. Mit dem Berichterstellungs-Konfigurationsprogramm können Sie diese Einstellungen nach der Installation bearbeiten.

Standardmäßige E-Mail-Adresse

Gibt die E-Mail-Adresse an, die die Identitätsberichterstellung 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 Standardwert 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.

Wenn Sie diese Einstellung wählen, geben Sie außerdem den Berechtigungsnachweis für den E-Mail-Server an.

- **Berichtsdetails**

Gibt die Einstellungen für das Beibehalten abgeschlossener 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 die Revisionsaktivitäten in der Identitätsberichterstellung an.

Revision für Identitätsberichterstellung aktivieren

Gibt an, ob die Protokollereignisse an einen Audit-Server 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 die Identitätsberichterstellung aktivieren.

Gibt den Speicherort des Cache-Verzeichnisses für die Revision an. Beispiel: `/opt/novell/Identity Reporting`.

HINWEIS: Wenn Sie die Revision aktivieren, muss die Datei `logevent` einen gültigen Pfad zum Cache-Verzeichnis und zur Datei „nauditpa.jar“ enthalten. Falls diese Einstellungen nicht ordnungsgemäß konfiguriert sind, wird die Identitätsberichterstellung nicht gestartet.

- **NAudit-Zertifikate**

  Gilt nur dann, wenn Sie die Revision für die Identitätsberichterstellung aktivieren.

  Gibt die Einstellungen für den NAudit-Dienst an, der Ereignisse aus der Identitätsberichterstellung an den EAS sendet.

  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 an den EAS 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 an den EAS gesendeten Revisionsmeldungen authentifizieren soll.

11. Überprüfen Sie die Angaben im Fenster „Zusammenfassung vor der Installation“, und klicken Sie auf **Installieren**.

3.1.2 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.

Zur Vorbereitung der Installation lesen Sie die Voraussetzungen und Systemanforderungen unter „Systemanforderungen für die Identitätsberichterstellung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. 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:

NETIQ_DB_RPT_USER_PASSWORD

Gibt das Passwort des Administrators für die SIEM-Datenbank an.

NETIQ_IDM_SRV_PWD

Gibt das Passwort des Eigentümers der Datenbankschemas und der Objekte für die Berichterstellung an.

NETIQ_IDM_USER_PWD

Gibt das Passwort für den Benutzer „idmrptuser“ an, der über den schreibgeschützten Zugriff auf Berichterstellungsdaten verfügt.

NETIQ_EAS_SYSTEM_PASSWORD

Gibt das Passwort für den EAS-Server an.

Sie können das Systempasswort aus der Systemeigenschaft in der Datei `activemqusers.properties` auf dem Computer, auf dem der EAS installiert ist, kopieren.

NETIQ_ADMIN_PWD

(Bedingt) Gibt das Passwort eines LDAP-Administrators an, sodass Suchvorgänge in Untercontainern während der Laufzeit ausgeführt werden können.

NETIQ_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 10 auf Seite 6.

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.

3.1.3 Aufgaben nach Abschluss der Installation

- Mit dem Konfigurationsaktualisierungsprogramm für Ihre Plattform können Sie die Installationseigenschaften nach der Installation ändern.
  - **Linux:** Führen Sie die Datei `configupdate.sh` im Verzeichnis `/opt/netiq/idm/apps/IdentityReporting/bin/lib` aus.
  - **Windows:** Führen Sie die Datei `configupdate.bat` im Verzeichnis `C:\netiq\idm\apps\IdentityReporting\bin\lib` aus.

  Wenn Sie eine Einstellung für die Identitätsberichterstellung mit dem Konfigurationsprogramm ändern, müssen Sie den Anwendungsserver 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.
- Greifen Sie als Berichtadministrator auf die Berichterstellungs-URL zu. Für die URL gilt das folgende Format: `http://Server:Port/IDMRPT/`. Stellen Sie sicher, dass die Authentifizierung und die Autorisierung erfolgreich ausgeführt werden. NetIQ empfiehlt, die Anmeldung nicht ohne ausreichende Verwaltungsrechte vorzunehmen.

WICHTIG: Wenn Sie sich als Benutzer ohne Rechte bei der Berichterstellungsanwendung anmelden, werden die Option zum Abmelden und der Link zur Startseite nicht angezeigt.

---

4 Aufrüsten von Identity Manager

NetIQ unterstützt die folgenden Aufrüstungspfade für Identity Manager 4.0.2 Standard Edition:

- Identity Manager 4.0.2 Standard Edition auf Identity Manager 4.5 Standard Edition
- Identity Manager 4.5 Standard Edition auf Identity Manager 4.5 Advanced Edition

Eine direkte Aufrüstung von Identity Manager 4.0.2 Standard Edition auf Identity Manager 4.5 Advanced Edition ist nicht möglich. Sie können die Aufrüstung jedoch mit einem der folgenden Verfahren vornehmen:

- Rüsten Sie von Identity Manager 4.0.2 Standard Edition auf Identity Manager 4.5 Standard Edition auf und führen Sie dann die Aufrüstung auf Identity Manager 4.5 Advanced Edition durch.
- Rüsten Sie von Identity Manager 4.0.2 Standard Edition auf Identity Manager 4.0.2 Advanced Edition auf und führen Sie dann die Aufrüstung auf Identity Manager 4.5 Advanced Edition durch.

4.1 Aufrüsten von Identity Manager 4.0.2 Standard Edition auf Identity Manager 4.5 Standard Edition

Zur Vorbereitung der Aufrüstung empfiehlt NetIQ, die Voraussetzungen für die Aufrüstung in den Versionshinweisen zu lesen und anschließend die nachfolgenden Aufgaben in der angegebenen Reihenfolge abzuarbeiten.

Aufgabe	Hinweise
1. Unterschiede zwischen Aufrüstung und Migration ermitteln	Weitere Informationen finden Sie unter „Erläuterungen zur Aufrüstung und zur Migration“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

Aufgabe	Hinweise
2. Auf Identity Manager 4.0.2 aufrüsten	Es ist nicht möglich, von Versionen vor 4.0.2 direkt auf Identity Manager Version 4.5 aufzurüsten oder zu migrieren. Weitere Informationen finden Sie im *Einrichtungshandbuch zu NetIQ Identity Manager 4.0.2*.
3. Erforderliche Dateien für Aufrüstung/ Migration beschaffen	Stellen Sie sicher, dass das aktuelle Installations-Kit für die Aufrüstung/ Migration von Identity Manager auf 4.5 Standard Edition vorliegt.
4. Interaktion zwischen Identity Manager-Komponenten	Weitere Informationen finden Sie unter „Einführung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
5. Systemvoraussetzungen	Stellen Sie sicher, dass die Computer die Hardware- und Software-Anforderungen für eine höhere Version von Identity Manager erfüllen. Weitere Informationen finden Sie unter „Überlegungen und Voraussetzungen für die Installation“ im *Einrichtungshandbuch zu NetIQ Identity Manager* und in den zugehörigen Versionshinweisen.
6. Sicherungskopie des aktuellen Treibers, der Treiberkonfiguration und der Datenbanken anlegen	Weitere Informationen finden Sie unter „Sichern der aktuellen Konfiguration“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
7. Analyzer aufrüsten	Rüsten Sie Analyzer auf die aktuelle Version auf. Weitere Informationen finden Sie unter „Aufrüsten von Analyzer“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
8. Designer aufrüsten	Rüsten Sie Designer auf die aktuelle Version auf. Weitere Informationen finden Sie unter „Aufrüsten von Designer“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
9. eDirectory aufrüsten	Rüsten Sie eDirectory auf dem Server, auf dem Identity Manager ausgeführt wird, auf die aktuelle Version und den aktuellen Patch auf. Weitere Informationen finden Sie im *NetIQ eDirectory 8.8-Installationshandbuch* und in den Versionshinweisen zu Identity Manager.
10. iManager aufrüsten	Rüsten Sie iManager auf die aktuelle Version und den aktuellen Patch auf. Anweisungen zur Aufrüstung finden Sie unter „Aufrüsten von iManager“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
11. Treiber anhalten	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 unter „Anhalten der Treiber“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
12. Identity Manager-Engine aufrüsten	Weitere Informationen finden Sie unter „Aufrüsten der Identity Manager-Engine“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. **HINWEIS:** Wenn Sie die Identity Manager-Engine auf einen neuen Server migrieren, können Sie die eDirectory-Reproduktionen verwenden, die sich auf dem aktuellen Identity Manager-Server befinden. Weitere Informationen finden Sie unter „Migrieren von Identity Manager auf einen neuen Server“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
13. (Bedingt) Remote Loader aufrüsten	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 unter „Aufrüsten von Remote Loader“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

Aufgabe	Hinweise
14. (Bedingt) Pakete aufrüsten	Wenn Sie Pakete anstelle von Treiberkonfigurationsdateien verwenden, rüsten Sie die Pakete auf die vorhandenen Treiber auf, um neue Richtlinien zu erhalten. Weitere Informationen finden Sie unter „Aufrüsten der Identity Manager-Treiber“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. 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. Aktivierungsschlüssel für Identity Manager 4.5 Standard Edition anwenden	Stellen Sie sicher, dass in iManager die Aktivierung der Identity Manager 4.5 Standard Edition angewendet wird. Wenn Sie die Aktivierung nicht anwenden, werden die Identity Manager-Engine und die Treiber im Evaluierungsmodus ausgeführt.
16. Dateien und Ordner für RBPM und Identitätsberichterstellung entfernen	Entfernen Sie die Dateien und Ordner für das RBPM und die Identitätsberichterstellung vom aktuellen Anwendungsserver. Führen Sie hierzu die folgenden Schritte aus: 1. (Bedingt) Deinstallieren Sie die WAR-Dateien für das RBPM und die Identitätsberichterstellung vom Anwendungsserver. Beachten Sie hierzu die Anweisungen in der Dokumentation Ihres Anwendungsservers. 2. Halten Sie den Anwendungsserver an, auf dem das RBPM und die Identitätsberichterstellung installiert sind. 3. Entfernen Sie die Installationsdateien und Ordner für die Identitätsberichterstellung mit dem Identitätsberichterstellungs-Deinstallationsprogramm. Weitere Informationen finden Sie unter „Deinstallieren der Identitätsberichterstellung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. 4. Entfernen Sie die Installationsdateien und Ordner für das RBPM mit dem RBPM-Deinstallationsprogramm. Weitere Informationen finden Sie unter „Deinstallation des rollenbasierten Bereitstellungsmoduls“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
17. Benutzeranwendungstreiber und Rollen- und Ressourcenservice-Treiber entfernen	Entfernen Sie den Benutzeranwendungstreiber und den Rollen- und Ressourcenservice-Treiber aus dem Treibersatz der aufgerüsteten Einrichtung und aus dem Designer-Projekt. Weitere Informationen finden Sie unter „Löschen der Treiber für das rollenbasierte Bereitstellungsmodul“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

Aufgabe	Hinweise
18. Komponenten für die Identitätsberichterstellung installieren	Installieren Sie die Komponenten für die Identitätsberichterstellung. Führen Sie hierzu die folgenden Schritte aus: 1. Erstellen Sie eine Sicherung der EAS-Daten. Weitere Informationen finden Sie unter „Sichern des Schemas für die Treiber“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. 2. Rüsten Sie den Event Auditing Service (EAS) auf. Zum Aufrüsten des EAS installieren Sie die neue Version über die bisherige Version. Weitere Informationen finden Sie unter „Aufrüsten des Event Auditing Service“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. 3. Das Installationsprogramm bietet Optionen zum Installieren von Tomcat und PostgreSQL. Installieren Sie ausschließlich Tomcat. Weitere Informationen finden Sie unter „Installieren von PostgreSQL und Tomcat für Identity Manager“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. 4. Installieren und konfigurieren Sie NetIQ SSO-Anbieter (OSP) und SSPR (Zurücksetzen von Passwörtern per Selbstbedienung). Weitere Informationen finden Sie unter „Installieren der Komponenten für Single Sign-On und Passwortverwaltung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. 5. Installieren Sie die Identitätsberichterstellung. Geben Sie während der Installation den DNS-Namen oder die IP-Adresse des Servers an, auf dem sich der aufgerüstete EAS befindet. Weitere Informationen finden Sie unter „Installieren der Identitätsberichterstellung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. 6. (Bedingt) Aktualisieren Sie die DCS-Treiberkonfiguration für den neuen Anwendungsserver (Tomcat). 7. Löschen Sie die Verweise auf `reportRunner` aus der PostgreSQL-Datenbank, bevor Sie den Anwendungsserver nach erfolgter Installation der Berichterstellung starten. a. (Bedingt) Halten Sie Tomcat an. b. Benennen Sie den Ordner `reportContent` im Hauptordner der Identitätsberichterstellung um. Beispiel: `/opt/netiq/idm/apps/IdentityReporting` c. Leeren Sie im Tomcat-Hauptordner die Verzeichnisse `temp` und `work`. d. Melden Sie sich in EAS bei der PostgreSQL-Datenbank an und löschen Sie die Verweise auf `reportRunner` mit den folgenden Anweisungen: ◆ `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';` e. Starten Sie Tomcat.
19. Treiber starten	Starten Sie die Treiber für die Identitätsberichterstellung und die Identity Manager-Engine. Weitere Informationen finden Sie unter „Starten der Treiber“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

Aufgabe	Hinweise
20. (Bedingt) Benutzerdefinierte Einstellungen wiederherstellen	(Bedingt) Wenn Sie benutzerdefinierte Richtlinien und Regeln verwenden, stellen Sie die angepassten Einstellungen wieder her. Weitere Informationen finden Sie unter „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
21. (Bedingt) Sentinel aufrüsten	(Bedingt) Wenn Sie NetIQ Sentinel verwenden, stellen Sie sicher, dass das neueste Service Pack ausgeführt wird. Weitere Informationen zum Aufrüsten von Sentinel finden Sie im *NetIQ Sentinel Installations- und Konfigurationshandbuch*.

4.2 Aufrüsten von Identity Manager 4.5 Standard Edition auf Identity Manager 4.5 Advanced Edition

Beim Aufrüsten von Identity Manager 4.5 Standard Edition auf Identity Manager 4.5 Advanced Edition muss die Konfiguration der Identity Manager-Komponenten bearbeitet werden. Für diese Aufrüstung müssen Sie nicht das Identity Manager-Installationsprogramm ausführen.

Identity Manager 4.5 Advanced Edition umfasst alle Funktionen aus der Standard Edition sowie einige zusätzliche Funktionen, beispielsweise die Identitätsanwendungen. Unter Neue Funktionen in den Versionshinweisen zu Identity Manager 4.5 Advanced Edition finden Sie eine kurze Übersicht über die neuen Funktionen in dieser Version. Werfen Sie einen kurzen Blick in diesen Abschnitt und informieren Sie sich .

NetIQ empfiehlt, die Schritte in der nachfolgenden Checkliste für die Aufrüstung in der angegebenen Reihenfolge auszuführen:

Aufgabe	Beschreibung
1. Unterschiede zwischen Aufrüstung und Migration ermitteln	Informieren Sie sich über die Unterschiede zwischen Aufrüstung und Migration. Weitere Informationen finden Sie unter „Erläuterungen zur Aufrüstung und zur Migration“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
2. Auf Identity Manager 4.5 Standard Edition aufrüsten	Es ist nicht möglich, von Versionen vor 4.0.2 auf Identity Manager Version 4.5 aufzurüsten oder zu migrieren. Weitere Informationen finden Sie im Einrichtungshandbuch zu NetIQ Identity Manager 4.0.2.
3. Erforderliche Dateien für Aufrüstung/Migration beschaffen	Stellen Sie sicher, dass das aktuelle Installations-Kit für die Aufrüstung von Identity Manager auf 4.5 Advanced Edition vorliegt.
4. Interaktion zwischen den Identity Manager-Komponenten ermitteln	Weitere Informationen finden Sie unter „Einführung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
5. Systemvoraussetzungen	Stellen Sie sicher, dass die Computer die Hardware- und Software-Anforderungen für eine höhere Version von Identity Manager erfüllen. Weitere Informationen finden Sie unter „Überlegungen und Voraussetzungen für die Installation“ im *Einrichtungshandbuch zu NetIQ Identity Manager* sowie in den Versionshinweisen für die Version, auf die aufgerüstet werden soll.
6. Anwendungsserver anhalten, auf dem die Identitätsberichterstellung installiert ist	In diesem Fall ist der Anwendungsserver Tomcat.

Aufgabe	Beschreibung
7. Identitätsberichterstellung deinstallieren	Deinstallieren Sie die WAR-Dateien für die Identitätsberichterstellung vom Anwendungsserver. Beachten Sie hierzu die Anweisungen in der Dokumentation Ihres Anwendungsservers. Weitere Informationen finden Sie unter „Deinstallieren der Identitätsberichterstellung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
8. Aktivierungsschlüssel für Identity Manager 4.5 Advanced Edition anwenden	Stellen Sie sicher, dass in iManager der Aktivierungsschlüssel für Identity Manager 4.5 Advanced Edition angewendet wird. Ansonsten wird die Aufrüstung der Identity Manager-Engine nicht fortgesetzt. **WICHTIG:** Damit Identity Manager nach der Aufrüstung die richtige Version und den richtigen Markennamen anzeigt, wenden Sie Patch 2 für Identity Manager 4.5 von der NetIQ Downloads-Website (http://download.novell.com/Download?buildid=vNsTfMo9g-4~) an. Weitere Informationen zum Herunterladen und Anwenden des Patches finden Sie unter „Anwenden des Patches für Identity Manager 4.5“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
9. Benutzeranwendung, Rollen- und Ressourcenservice-Treiber und MSG-Treiber erstellen und bereitstellen	Weitere Informationen finden Sie unter „Erstellen und Bereitstellen der Treiber für die Identitätsanwendungen“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
10. (Bedingt) Anwendungsserver installieren	Installieren Sie WebSphere oder JBoss als Anwendungsserver. Soll Tomcat als Anwendungsserver fungieren, können Sie die vorhandene Tomcat-Instanz weiterverwenden.
11. Identitätsanwendungen installieren und konfigurieren	**HINWEIS:** Bei der Aufrüstung werden die vorhandenen Rollen, die den Benutzern in eDirectory zugewiesen sind, nicht entfernt. Falls die Berichtadministrator-Benutzerrolle in der aufgerüsteten Software noch vorhanden ist, löschen Sie diese Rolle aus Sicherheitsgründen. Das Installationsprogramm installiert die folgenden Komponenten: ◆ Katalogadministrator ◆ Startseite und Bereitstellungs-Dashboard ◆ Rollenbasiertes Bereitstellungsmodul (RBPM) Weitere Informationen finden Sie unter „Installieren der Identitätsanwendungen“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
12. Anwendungsserver starten	Wenn der Anwendungsserver nicht Tomcat ist, starten Sie den Anwendungsserver (WebSphere oder JBoss) und Tomcat. Tomcat muss ausgeführt werden, weil NetIQ die OSP-Installation ausschließlich auf Tomcat unterstützt.
13. DCS-Treiberkonfiguration aktualisieren	(Bedingt) Aktualisieren Sie die DCS-Treiberkonfiguration für den neuen Anwendungsserver. Aktualisieren Sie die DCS-Treiberkonfiguration, so dass der MSG-Treiber registriert wird. Weitere Informationen finden Sie unter Abschnitt 4.3, „Aktualisieren der Konfigurationsinformationen für den DCS-Treiber“, auf Seite 18.

Aufgabe	Beschreibung
14. Identitätsberichterstellung installieren und konfigurieren	Geben Sie die Details zum vorhandenen EAS-Server während der Installation an. Weitere Informationen finden Sie unter „Installieren des Berichterstellungsmoduls“ im *Einrichtungshandbuch zu NetIQ Identity Manager*. Protokollieren Sie die Identitätsberichterstellungsereignisse mit den folgenden Schritten auf dem EAS-Server: 1. Halten Sie den Anwendungsserver an. Beispiel: `/etc/init.d/idmapps_tomcat_init stop` 2. Halten Sie den Revisions-Thread mit dem folgenden Befehl an: `ps -eaf | grep naudit` 3. Aktivieren Sie die Berichterstellung, um das Auditing zu verwenden. a. (Optional) Aktualisieren Sie das ConfigUpdate-Dienstprogramm, damit es im GUI-Modus ausgeführt wird. b. Starten Sie das ConfigUpdate-Dienstprogramm und wählen Sie die Registerkarte **Berichterstellung**. c. Aktivieren Sie das Kontrollkästchen **Audit mit EAS aktivieren**. Falls diese Option bereits aktiviert ist, deaktivieren Sie sie und klicken Sie auf **OK**. d. Starten Sie das ConfigUpdate-Dienstprogramm erneut und wählen Sie die Registerkarte **Berichterstellung**. e. Aktivieren Sie das Kontrollkästchen **Audit mit EAS aktivieren** und klicken Sie auf **OK**. 4. Starten Sie den Anwendungsserver. Beispiel: `/etc/init.d/idmapps_tomcat_init start`
15. Treiber starten	Starten Sie die Treiber für die Identitätsberichterstellung und die Identity Manager-Engine. Weitere Informationen finden Sie unter „Starten der Treiber“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
16. (Bedingt) Benutzerdefinierte Einstellungen wiederherstellen	(Bedingt) Wenn Sie benutzerdefinierte Richtlinien und Regeln verwenden, stellen Sie die angepassten Einstellungen wieder her. Weitere Informationen finden Sie unter „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
17. (Bedingt) Sentinel aufrüsten	(Bedingt) Wenn Sie NetIQ Sentinel verwenden, stellen Sie sicher, dass das neueste Service Pack ausgeführt wird. Weitere Informationen zum Aufrüsten von Sentinel finden Sie im *NetIQ Sentinel Installations- und Konfigurationshandbuch*.

4.3 Aktualisieren der Konfigurationsinformationen für den DCS-Treiber

1. Starten Sie Designer und wählen Sie **DCS-Treiber-Konfiguration > Treiberparameter > Treiberoptionen**.
2. Ändern Sie im Abschnitt „Verwaltetes System - Gateway-Registrierung“ die Einstellungen wie folgt:
   - Setzen Sie **'Verwaltetes System – Gateway' registrieren** auf **Ja**.

- Ändern Sie den MSGW-Treiber-DN. Beispiel: `CN=Treiber „Verwaltetes System - Gateway",cn=driverset1,o=system`.
- Ändern Sie den Benutzer-DN. Beispiel: `cn=admin,ou=sa,o=system`.
- Geben Sie das Passwort für den Benutzer-DN an.

  Weitere Informationen zum Konfigurieren des Treibers finden Sie unter „Konfigurieren des Treibers für den Datenerfassungsdienst (DCS-Treiber)“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

3 Speichern Sie die Einstellungen und stellen Sie anschließend den DCS-Treiber bereit.

4 Starten Sie den DCS-Treiber neu.

  Nach dem Aufrüsten der Identitätsberichterstellung wird die Advanced Edition möglicherweise nicht sofort angezeigt. Die Versionsänderung erfolgt erst, nachdem der nächste Stapel an Ereignissen verarbeitet wurde.

5 Deinstallieren von Identity Manager 4.5 Standard Edition

Bei einigen Identity Manager-Komponenten sind gewisse Voraussetzungen für die Deinstallation zu beachten. Lesen Sie jeweils den gesamten Abschnitt für eine Komponente, bevor Sie die Deinstallation starten. Weitere Informationen finden Sie unter „Deinstallieren der Identity Manager-Komponenten“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

6 Rechtliche Hinweise

DIESES DOKUMENT UND DIE HIER BESCHRIEBENE SOFTWARE WERDEN GEMÄSS EINER LIZENZVEREINBARUNG ODER EINER VERSCHWIEGENHEITSVERPFLICHTUNG BEREITGESTELLT UND UNTERLIEGEN DEN JEWEILIGEN BESTIMMUNGEN DIESER VEREINBARUNGEN. SOFERN NICHT AUSDRÜCKLICH IN DER LIZENZVEREINBARUNG ODER VERSCHWIEGENHEITSVERPFLICHTUNG ERKLÄRT, STELLT DIE NETIQ CORPORATION DIESES DOKUMENT UND DIE IN DIESEM DOKUMENT BESCHRIEBENE SOFTWARE OHNE MÄNGELGEWÄHR UND OHNE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNGEN JEGLICHER ART BEREIT, BEISPIELSWEISE UNTER ANDEREM STILLSCHWEIGENDE GEWÄHRLEISTUNGEN HINSICHTLICH DER MARKTGÄNGIGKEIT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. IN EINIGEN LÄNDERN SIND HAFTUNGSAUSSCHLÜSSE FÜR AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNGEN IN BESTIMMTEN TRANSAKTIONEN NICHT ZULÄSSIG. AUS DIESEM GRUND HAT DIESE BESTIMMUNG FÜR SIE UNTER UMSTÄNDEN KEINE GÜLTIGKEIT.

Der Klarheit halber werden alle Module, Adapter und anderes Material („Modul“) gemäß den Bestimmungen der Endbenutzer-Lizenzvereinbarung (EULA) für die jeweilige Version des NetIQ-Produkts oder der NetIQ-Software lizenziert, zu dem/der diese Module gehören oder mit dem/der sie zusammenarbeiten. Durch den Zugriff auf ein Modul bzw. durch das Kopieren oder Verwenden eines Moduls erklären Sie sich an diese Bestimmungen gebunden. Falls Sie den Bestimmungen der Endbenutzer-Lizenzvereinbarung nicht zustimmen, sind Sie nicht berechtigt, ein Modul zu verwenden oder zu kopieren bzw. auf ein Modul zuzugreifen, und Sie sind verpflichtet, jegliche Kopien des Moduls zu vernichten und weitere Anweisungen bei NetIQ zu erfragen.

Ohne vorherige schriftliche Genehmigung der NetIQ Corporation dürfen dieses Dokument und die in diesem Dokument beschriebene Software nicht vermietet, verkauft oder verschenkt werden, soweit dies nicht anderweitig gesetzlich gestattet ist. Ohne vorherige schriftliche Genehmigung der NetIQ Corporation darf dieses Dokument oder die in diesem Dokument beschriebene Software weder ganz noch teilweise reproduziert, in einem Abrufsystem gespeichert oder auf jegliche Art oder auf jeglichem Medium (elektronisch, mechanisch oder anderweitig) gespeichert werden, soweit dies nicht