NetIQ® Identity Manager

Handbuch zur integrierten Installation

Dezember 2014

www.netiq.com/documentation

Rechtliche Hinweise

Inhalt

Info zu diesem Handbuch und zur Bibliothek

Im *Handbuch zur integrierten Installation* finden Sie Anweisungen zum Installieren von NetIQ Identity Manager (Identity Manager) mit dem Programm für die integrierte Installation. In diesem Handbuch wird häufig auf das *Einrichtungshandbuch zu NetIQ Identity Manager* verwiesen, in dem Sie ausführliche Informationen zum Installieren von Identity Manager mit den Programmen für die Standalone-Installation finden.

Zielgruppe

Dieses Handbuch richtet sich an Identitätsarchitekten und Identitätsadministratoren, die Identity Manager auf die Eignung als Identitätsmanagement-Lösung in ihrer Organisation prüfen möchten.

Weitere Informationen in der Bibliothek

Weitere Informationen zur Identity Manager-Bibliothek finden Sie auf der Website der Identity Manager-Dokumentation (https://www.netiq.com/documentation/idm45/).

Info zu NetIQ Corporation

NetIQ ist ein globaler Hersteller von Unternehmenssoftware. Unser Blickpunkt 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 physikalischen, 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 große 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 Sie 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 alle Voraussetzungen verfügen, um das meiste aus den IT-Investitionen zu holen, auf die Sie sich verlassen. Weitere Informationen finden Sie im Internet unter community.netiq.com.

1 Einführung

Mit einer Lösung für die integrierte Installation und den Installationsprogrammen für einzelne Komponenten oder Komponenten bietet NetIQ zwei Möglichkeiten, wie Sie Identity Manager in Ihrer Umgebung installieren und konfigurieren. Das Programm für die **integrierte Installation** installiert und konfiguriert alle Komponenten anhand von Standardwerten für zahlreiche Einstellungen. Mit dem Programm für die integrierte Installation können Sie alle Komponenten auf einem einzigen Computer (nur unter Linux) oder in einer dezentralen Umgebung installieren. Die Programme für die **Standalone-Installation** bieten Ihnen die Möglichkeit, eine oder mehrere Identity Manager-Komponenten separat zu installieren oder einen Großteil der Einstellungen anzupassen.

Informieren Sie sich zunächst über die verschiedenen Identity Manager-Komponenten, bevor Sie den Vorgang fortsetzen. Weitere Informationen finden Sie unter „Überblick über Komponenten und Kommunikation in Identity Manager“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

1.1 Erläuterungen zu den Unterschieden zwischen der integrierten Installation und den Programmen für die Standalone-Installation

Ermitteln Sie anhand der nachfolgenden Informationen, ob das Programm für die integrierte Installation oder eines der Programme für die Standalone-Installation für Ihre Anforderungen geeignet ist.

Programm für die integrierte Installation

NetIQ empfiehlt dieses Programm, wenn Sie Identity Manager testen oder eine Testumgebung erstellen möchten. Das Programm fasst alle erforderlichen Komponenten in einem einzigen Installationsvorgang zusammen. Das Programm für die integrierte Installation weist die folgenden neuen Fähigkeiten auf:

- Wendet Standardwerte für die meisten Einstellungen an
- Installiert alle Komponenten auf einem einzigen Computer oder in einer kleinen dezentralen Umgebung
- Verwendet PostgreSQL für alle Datenbanken
- Verwendet Apache Tomcat für alle Anwendungsserver
- Sollte nicht in einer Cluster-Umgebung verwendet werden
- Sollte nicht in einer Produktionsumgebung verwendet werden

Programme für die 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. Dieser Vorgang bietet folgende Funktionen:

- Möglichkeit zum Anpassen der Einstellungen für die Komponenten
- Möglichkeit zum Installieren in dezentralen Umgebungen
- Unterstützt mehrere Datenbankplattformen

- Unterstützt mehrere Anwendungsserver
- Erstellt eine unterstützte Produktionsumgebung

Weitere Informationen zur Standalone-Installation finden Sie im *Einrichtungshandbuch zu NetIQ Identity Manager*.

1.2 Erläuterungen zur integrierten Installation

Im Rahmen der integrierten Installation werden die Installationsprogramme für die verschiedenen Identity Manager-Komponenten ausgeführt. Wenn Sie die Installation in einer dezentralen Umgebung vornehmen, können Sie die Komponenten festlegen, die auf den einzelnen Computern installiert werden sollen.

Zu Beginn des Installationsvorgangs können Sie ein Passwort festlegen, das auf alle Passwortparameter für die installierten Komponenten angewendet wird. Die installierten Komponenten werden anhand von Standardeinstellungen konfiguriert. Sie können die Standardeinstellungen direkt während des Installationsvorgangs bearbeiten oder auch nachträglich noch Änderungen vornehmen. Beim Starten des Vorgangs können Sie beispielsweise ein Passwort angeben, das für alle Passwortwerte herangezogen werden soll.

HINWEIS: Eine vorhandene Installation kann nicht mit dem integrierten Installationsvorgang aufgerüstet werden.

In den nachfolgenden Abschnitten finden Sie die Komponenten, die sich mit diesem Vorgang installieren lassen, und ihre jeweiligen Standardeinstellungen.

1.2.1 Identity Manager Server

Mit dieser Option werden die folgenden Identity Manager-Komponenten installiert:

- Identitätsdepot
- Identity Manager-Engine
- iManager-Plugins
- Identity Manager-Treiber
- Remote Loader

Das Administratorkonto für das Identitätsdepot lautet standardmäßig `Admin`. Diesen Wert können Sie bei Bedarf beim Konfigurieren der Komponenten ändern. Der Installationsvorgang legt automatisch die Baumstruktur für das Identitätsdepot an. Weitere Informationen finden Sie in Abschnitt 1.3, „Erläuterungen zur standardmäßigen Identitätsdepot-Struktur“, auf Seite 13.

1.2.2 Identitätsanwendungen

Mit dieser Option werden die folgenden Identity Manager-Komponenten und die zugehörige unterstützende Software installiert:

- Katalogadministrator
- Startseite und Bereitstellungs-Dashboard
- Rollenbasiertes Bereitstellungsmodul (RBPM)
- Rollen- und Ressourcenservice-Treiber

- Benutzeranwendung
- Benutzeranwendungstreiber
- One SSO Provider (OSP)
- PostgreSQL
- Zurücksetzen von Passwörtern per Selbstbedienung
- Tomcat

Der Installationsvorgang umfasst eine Oracle-JRE sowie Open-Source-Versionen von Apache Tomcat Web Server, Apache ActiveMQ und PostgreSQL-Datenbankserver als Grundlage für Identity Manager. Hierbei können Sie diese Komponenten installieren, ohne sie einzeln herunterladen zu müssen. NetIQ bietet allerdings keinen Enterprise-Support für diese Komponenten.

NetIQ empfiehlt, einen Enterprise-Anwendungsserver für Staging- und Produktionsumgebungen zu nutzen und Entwicklungsumgebungen mithilfe dieses Schnellinstallationsprogramms zu erstellen. NetIQ bietet keine Unterstützung und keine Aktualisierungen für diese Komponenten, außerdem keine Administration, keine Konfiguration und keine Leistungssteigerung. Wenn Sie Hilfe benötigen, wenden Sie sich an den Drittanbieter der Komponente.

Der Installationsvorgang erstellt die folgenden Konten und die folgende Datenbank:

Standardelement	Beschreibung
idmuserappdb	Datenbank für die Identitätsanwendungen
idmadmin	Administratorkonto für die Datenbank `idmuserappdb`
uaadmin	Administratorkonto für die Benutzeranwendung

Der Installationsvorgang erstellt und konfiguriert außerdem den Benutzeranwendungstreiber sowie den Rollen- und den Ressourcenservice-Treiber. Anweisungen zum Konfigurieren weiterer Treiber finden Sie auf der Website der Identity Manager-Treiberdokumentation (https://www.netiq.com/documentation/idm45drivers/).

Weitere Informationen zu den Identitätsanwendungen finden Sie unter „Erläuterungen zu den Komponenten für die Verwaltung der Benutzerbereitstellung“ und „Installieren der Identitätsanwendungen“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

1.2.3 Identitätsberichterstellung

Mit dieser Option werden die folgenden Identity Manager-Komponenten installiert:

- Identitätsberichterstellungsmodul
- Treiber „Verwaltetes System – Gateway“ (MSGW-Treiber)
- Treiber für den Datenerfassungsdienst (DCS-Treiber)

Die Identitätsberichterstellung kann nur mit einem einzigen EAS-Computer (Event Auditing Service) kommunizieren, auch wenn mehrere Ereignisrevisionssysteme vorliegen. Zum Protokollieren der Ereignisse benötigt die Identitätsberichterstellung die SIEM-Datenbank, die zusammen mit dem Event Auditing Service installiert wird.

Weitere Informationen zur Berichterstellung finden Sie unter „Berichterstellung“ und „Installieren der Komponenten für die Identitätsberichterstellung“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

1.2.4 Event Auditing Service

Mit dieser Option werden die folgenden Komponenten installiert:

- NetIQ Event Auditing Service
- SIEM-Datenbank

WICHTIG: Der Event Auditing Service kann nur auf einem Linux-Computer installiert werden.

Der Event Auditing Service und die Identitätsberichterstellung speichern Audit-, Protokoll- und Berichtereignisse in der SIEM-Datenbank. Der Installationsvorgang erstellt die folgenden Benutzerkonten in der Datenbank:

Standardelement	Beschreibung
dbauser	Administratorbenutzer für die Datenbank
idmrptsrv	Benutzerkonto für den Eigentümer der Datenbankschemas und der Objekte für die Berichterstellung
idmrptuser	Benutzerkonto mit Lesezugriff auf die Berichterstellungsdaten

Weitere Informationen zu EAS finden Sie unter „Event Auditing Services“ und „Installieren des Event Auditing Service“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

1.2.5 iManager

Mit dieser Option werden iManager und der zugehörige Arbeitsstations-Client installiert. Während der Konfiguration können Sie die Standardports für die Kommunikation in iManager ändern. Weitere Informationen zu iManager finden Sie unter „iManager“ und „Installieren von iManager“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

1.2.6 Designer

Mit dieser Option wird Designer auf dem lokalen Computer installiert. Designer umfasst keine benutzerprogrammierbaren Parameter. Weitere Informationen zu Designer finden Sie unter „Designer“ und „Planen der Installation von Designer“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

1.2.7 Analyzer

Mit dieser Option wird Analyzer auf dem lokalen Computer installiert. Analyzer umfasst keine benutzerprogrammierbaren Parameter. Weitere Informationen zu Analyzer finden Sie unter „Analyzer“ und „Installieren von Analyzer für Identity Manager“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

1.3 Erläuterungen zur standardmäßigen Identitätsdepot-Struktur

Bei der integrierten Installation wird eine standardmäßige Struktur für das Identitätsdepot angelegt, die sich für die meisten Identity Manager-Bereitstellungen eignet.

Abbildung 1-1 *Standardmäßige Identitätsdepot-Struktur*

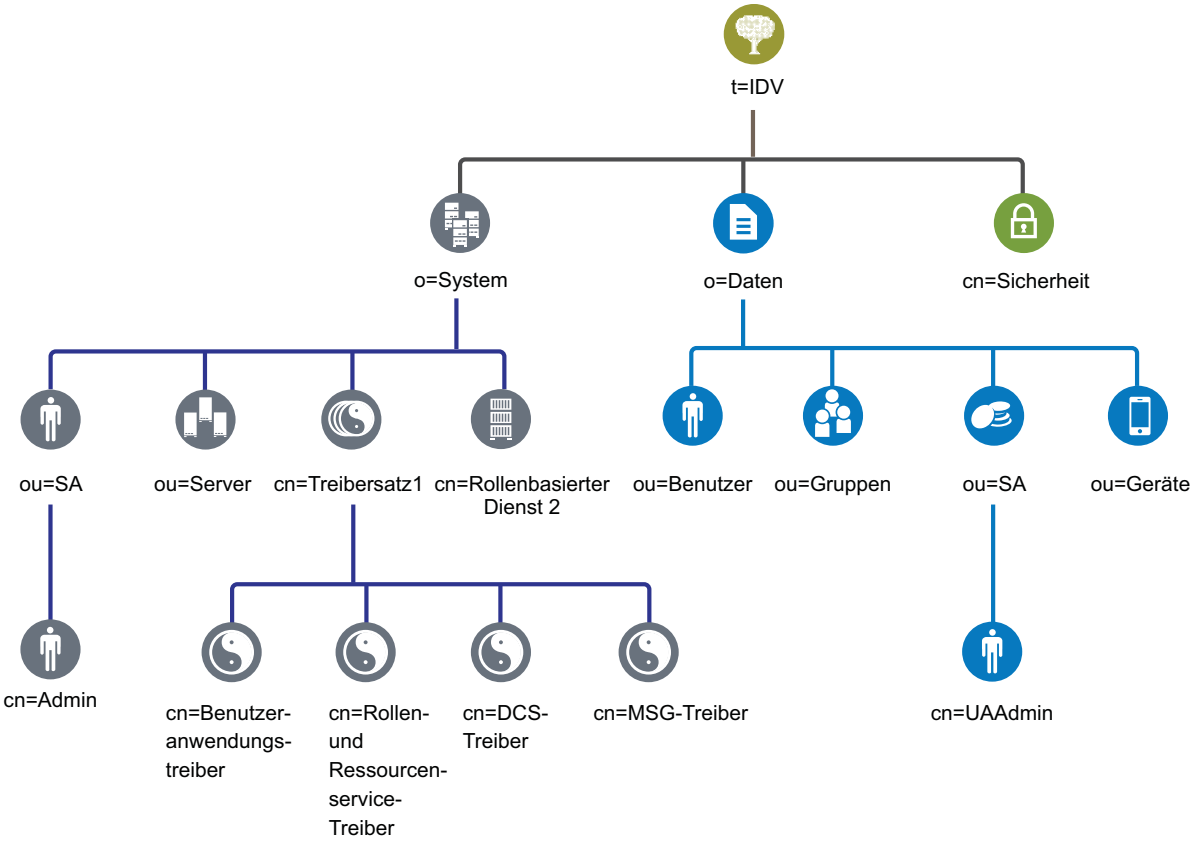

Tabelle 1-1 *Beschreibung der Objekte im Identitätsdepot*

Objekt	Beschreibung
t=idv	Der Standardname des eDirectory-Baums lautet „idv“.
o=system	Alle Systemobjekte für Identity Manager befinden sich in der Systemorganisation. Der Zugriff auf diesen Container und alle Untercontainer soll ausschließlich auf Administratoren beschränkt werden. Weitere Informationen finden Sie in Abschnitt 1.3.1, „Systemcontainer“, auf Seite 14.
ou=sa.o=system	Der Container „ou=sa.o=system“ enthält alle Systembenutzer. Zu den Systembenutzern gehören die Administratoren, die Treiberadministratoren und andere Administratoren.
cn=admin.ou=sa.o=system	Dies ist das Administratorkonto für den Baum.
ou=servers.o=system	Dieser Container enthält die Serverobjekte und alle mit den Servern verknüpften Objekte. Damit ist es möglich, die Serverobjekte von den anderen Systemobjekten zu trennen.

Objekt	Beschreibung
cn=driverset1.o=system	Das Treibersatzobjekt enthält alle Treiberobjekte. Die Treibersatzobjekte werden direkt im Systemcontainer abgelegt.
cn=User Application Driver.cn=driverset1.o=system	Der Benutzeranwendungstreiber verwaltet alle Aufgaben im Zusammenhang mit der Benutzeranwendung.
cn=Role and Resource Service Driver.cn=driverset1.o=system	Der Rollen- und Ressourcenservice-Treiber verwaltet alle Aufgaben im Zusammenhang mit dem rollenbasierten Bereitstellungsmodul.
cn=Data Collection Service Driver.cn=driverset1.o=system	Der DCS-Treiber verwaltet Aufgaben im Zusammenhang mit dem Identitätsberichterstellungsmodul.
cn=Managed System Gateway Driver.cn=driverset1.o=system	Der MSGW-Treiber verwaltet Aufgaben im Zusammenhang mit dem Identitätsberichterstellungsmodul.
cn=Role Based Service 2.o=system	Dieser Container enthält Objekte, die für die Zusammenarbeit von iManager und Identity Manager sorgen.
o=data	Alle Datenobjekte für Identity Manager befinden sich in der Datenorganisation. Die Administratoren sollen allen Benutzern den Zugriff auf diesen Container und alle Untercontainer ermöglichen. Weitere Informationen finden Sie in Abschnitt 1.3.2, „Datencontainer“, auf Seite 15.
ou=users.o=data	Standardcontainer für alle Benutzerobjekte im Identitätsdepot.
ou=groups.o=data	Standardcontainer für alle Gruppenobjekte im Identitätsdepot.
ou=sa.o=data	Standardcontainer für den Rollenadministratorbenutzer, den Superuser und die Dienstkonten für die Benutzeranwendung, das rollenbasierte Bereitstellungsmodul und das Identitätsberichterstellungsmodul.
cn=uaadmin.ou=sa.o=data	Benutzeranwendungs-Administratorobjekt.
ou=Devices.o=data	Standardcontainer für Geräte.
cn=security	Der Sicherheitscontainer enthält alle Sicherheitsobjekte für den Baum und für Identity Manager. Der Zugriff auf diesen Container und alle Untercontainer soll ausschließlich auf Administratoren beschränkt werden. Weitere Informationen finden Sie in Abschnitt 1.3.3, „Sicherheitscontainer“, auf Seite 15.

Diese Standardstruktur ist hauptsächlich für eine Installation in einer einzelnen Umgebung von Vorteil. Beispielsweise ist diese Identitätsdepotstruktur gut für kleine und mittlere Identity Manager-Bereitstellungen geeignet. Multi-Tenant-Umgebungen besitzen möglicherweise eine etwas andere Struktur. Außerdem ist es nicht möglich, große und verteilte Bäume auf diese Weise zu organisieren.

In Identity Manager 4.0 (und höher) werden überwiegend Organisationscontainer verwendet, sodass Benutzer, Gruppen und Dienstadministratoren in denselben Container platziert werden. Verwenden Sie Organisationen (o=), wenn dies möglich ist, und organisatorische Einheiten (ou=), wo dies sinnvoll ist. Die Identity Manager-Struktur ist durch ihre drei Hauptkomponenten (Systemcontainer, Datencontainer und Sicherheitscontainer) auf die spätere Skalierbarkeit ausgerichtet.

1.3.1 Systemcontainer

Der Systemcontainer ist eine Organisation. Standardmäßig wird dieser Container als `o=system` bezeichnet. Dieser Container enthält alle technischen Informationen und Konfigurationsinformationen für Ihr Identitätsdepot und für das Identity Manager-System. Der Systemcontainer enthält die folgenden Haupt-Untercontainer:

ou=sa

Der Service-Admins-Container enthält administrative Objekte für das Identitätsdepot und die Treiber. Nur Admin-Benutzer können auf den System-Teilbaum zugreifen. Der standardmäßige Identitätsdepot-Admin ist admin.sa.system. Die Objekte in diesem Container werden als „sa“ oder Dienstadministratorbenutzer, Superuser oder Dienstkonten bezeichnet.

Server

Den Serverobjekten sind viele verschiedene Objekte zugeordnet, die sich in demselben Container befinden müssen wie das Serverobjekt. Wenn Sie weitere Server zu Ihrem Baum hinzufügen, kann es letztlich sehr mühsam werden, durch all diese Objekte zu blättern.

Sie sollten alle Serverobjekte unter dem servers.system-Container anordnen. Ein Administrator kann jedoch einzelne Servercontainer für jeden der in der Umgebung bereitgestellten Server erstellen. Der Name des Containers ist der Name des Serverobjekts.

Diese Struktur ist auf die spätere Skalierbarkeit ausgerichtet. Alle dem Server zugeordneten Objekte (Volumes, Lizenzen, Zertifikate) befinden sich an der richtigen Stelle, sodass die erforderlichen Objekte rasch aufgefunden werden.

Treibersätze

Treibersätze werden während der Konfiguration der Identity Manager-Engine als separate Partition erstellt. Im Identitätsdepot werden die Treibersatzobjekte im Systemcontainer gespeichert. Diese Struktur ermöglicht Ihnen das Skalieren, indem Sie weitere Treibersätze zum Systemcontainer hinzufügen. Rollenbasierte Services für iManager werden ebenfalls im Systemcontainer gespeichert.

1.3.2 Datencontainer

Der Datencontainer enthält Gruppen, Benutzer, Rollenadministratoren, Geräte und andere Objekte. Dies sind die Daten, aus denen Ihr System besteht. Die Gruppen, Benutzer und sa-Container sind organisatorische Einheiten. Sie können zusätzliche organisatorische Einheiten verwenden, um Ihre Daten entsprechend Ihren Organisationsmethoden zu strukturieren. Der Dienstadministrator-container (`ou=sa`) enthält beispielsweise alle Benutzeranwendungsadministrator-Objekte und Dienstadministratorkonten.

1.3.3 Sicherheitscontainer

Der Sicherheitscontainer ist ein spezieller Container, der während der Installation des Identitätsdepots erstellt wird. Er wird als `cn=security` anstelle von `dc, o` oder `ou` bezeichnet. Dieser Container enthält alle Sicherheitsobjekte für das Identitätsdepot. Er enthält beispielsweise die Zertifizierungsstelle und die Passwortrichtlinien.

2 Planen der Installation von Identity Manager

In diesem Abschnitt finden Sie nützliche Informationen zur Planung der Identity Manager-Umgebung, beispielsweise die Voraussetzungen und Systemanforderungen für die einzelnen Identity Manager-Komponenten. Die Komponenten müssen dabei nicht auf demselben Computer installiert werden. Das Programm für die integrierte Installation unterstützt jedoch nicht die Installation in einer Cluster-Umgebung.

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.

2.1 Installations-Checkliste

Die nachfolgende Checkliste enthält die Hauptschritte für die Planung der Identity Manager-Installation in Ihrer Test- oder Evaluierungsumgebung.

	Checkliste
❑	1. Informieren Sie sich über die Interaktion zwischen den Identity Manager-Komponenten. Weitere Informationen finden Sie in Kapitel 1, „Einführung“, auf Seite 9.
❑	2. Lesen Sie die Überlegungen zur Installation der Komponenten, und prüfen Sie, ob die Computer den Voraussetzungen und Anforderungen entsprechen: ◆ Voraussetzungen für den integrierten Installationsvorgang: Abschnitt 2.2, „Überlegungen zur Verwendung des Programms für die integrierte Installation“, auf Seite 18. ◆ Voraussetzungen für die einzelnen Komponenten: Abschnitt 2.3, „Voraussetzungen und Systemanforderungen“, auf Seite 18. **WICHTIG:** Für die Identitätsanwendungen und die Funktionen der Identitätsberichterstellung muss der Event Auditing Service installiert werden. Der Event Auditing Service kann nur auf einem Linux-Computer installiert werden. Wenn Sie mit Windows-Computern arbeiten, müssen Sie mindestens einen Linux-Computer für den Event Auditing Service bereitstellen.
❑	3. Informieren Sie sich über die Komponenten, die Software und die Standardeinstellungen, die bei der integrierten Installation zu den Servern hinzugefügt werden. Weitere Informationen finden Sie in Kapitel 5, „Erläuterungen zu den Konfigurationsparametern“, auf Seite 33.
❑	4. Informieren Sie sich über die Standardeinrichtung des Identitätsdepots. Weitere Informationen finden Sie in Abschnitt 1.3, „Erläuterungen zur standardmäßigen Identitätsdepot-Struktur“, auf Seite 13.
❑	5. (Bedingt) Stellen Sie beim Installieren von Komponenten in einer Umgebung mit Red Hat Enterprise Linux 6.*x* sicher, dass die richtigen Bibliotheken auf dem Computer vorliegen. Weitere Informationen finden Sie unter „Installieren von Identity Manager auf einem RHEL 6.x-Server“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

	Checkliste
❑	6. Führen Sie die integrierte Installation aus: ◆ Anweisungen zur geführten Installation finden Sie in Abschnitt 3.3, „Verwenden des Installationsassistenten“, auf Seite 24. ◆ Anweisungen zur automatischen Installation finden Sie in Abschnitt 3.4, „Ausführen einer automatischen Installation“, auf Seite 25.
❑	7. Konfigurieren Sie die installierten Komponenten: ◆ Anweisungen zur geführten Konfiguration finden Sie in Abschnitt 4.2, „Verwenden des Konfigurationsassistenten“, auf Seite 28. ◆ Anweisungen zur automatischen Konfiguration finden Sie in Abschnitt 4.4, „Ausführen einer automatischen Konfiguration“, auf Seite 31.
❑	8. Schließen Sie die Installation ab. Weitere Informationen finden Sie in Kapitel 6, „Abschließende Schritte bei der integrierten Installation“, auf Seite 45.
❑	9. Aktivieren Sie Identity Manager. Weitere Informationen finden Sie in Kapitel 7, „Aktivieren von Identity Manager-Produkten“, auf Seite 47.

2.2 Überlegungen zur Verwendung des Programms für die integrierte Installation

In diesem Abschnitt werden die Überlegungen zur Installation aller Identity Manager-Komponenten mit dem Programm für die integrierte Installation beschrieben. Soweit nicht anderweitig angegeben, müssen Ihre Server und Arbeitsstationen auch den in Abschnitt 2.3, „Voraussetzungen und Systemanforderungen“, auf Seite 18 aufgeführten Voraussetzungen und Anforderungen entsprechen.

- ❒ Eine vorhandene Installation kann nicht mit dem integrierten Installationsvorgang aufgerüstet werden.
- ❒ Für Komponenten wie die Benutzeranwendung müssen Sie eine unterstützte Version des Apache Tomcat-Anwendungsservers verwenden. Als Arbeitserleichterung bietet das Installationsprogramm eine Option zum Installieren von Tomcat.
- ❒ Sollen alle Komponenten auf einem einzigen Computer installiert werden, müssen Sie einen Linux-Computer verwenden. Wenn Sie mit Windows-Computern arbeiten, müssen Sie mindestens einen Linux-Computer für den Event Auditing Service bereitstellen. Für die Identitätsanwendungen und das Identitätsberichterstellungsmodul muss der Event Auditing Service installiert werden.

2.3 Voraussetzungen und Systemanforderungen

Sie können alle Komponenten zur Evaluierung auf einem einzigen Computer oder verschiedene Identity Manager-Komponenten mithilfe der integrierten Installation auf unterschiedlichen Systemen und Plattformen installieren. Hierzu müssen Sie das Programm für die integrierte Installation mehrfach ausführen und jeweils die gewünschten Komponenten auswählen.

2.3.1 Voraussetzungen

Vor dem Starten des Programms für die integrierte Installation müssen die nachfolgenden Voraussetzungen erfüllt.

Alle Plattformen

WICHTIG: Der Event Auditing Service kann nur in Linux-Umgebungen ausgeführt werden. Wenn Sie die Identitätsanwendungen und die Funktionen der Identitätsberichterstellung in Identity Manager evaluieren möchten, müssen Sie zunächst den Event Auditing Service auf einem Linux-Computer installieren und dann die integrierte Installation auf einem Windows-Computer ausführen.

- ❒ 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. Weitere Informationen finden Sie unter „Auflösen von Baumnamen mit OpenSLP oder hosts.nds“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
- ❒ 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. Der DNS-Name des Computers muss aufgelöst werden können. Ist dies nicht der Fall, fügen Sie einen Eintrag für diesen Computer zur Datei `/etc/hosts` hinzu, sodass der DNS-Name aufgelöst werden kann.
- ❒ Synchronisieren Sie die Uhrzeit auf allen Netzwerkservern. NetIQ empfiehlt die NTP-Option (Network Time Protocol).

Linux

- ❒ (Bedingt) Sollen Komponenten in einer Umgebung mit Red Hat Enterprise Linux 6.x installiert werden, müssen die richtigen Bibliotheken auf dem Server vorliegen. Weitere Informationen finden Sie unter „Installieren von Identity Manager auf einem RHEL 6.x-Server“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
- ❒ (Bedingt) Bei der Installation auf einer SLES 11-Plattform (64 Bit) muss die folgende kompatible Bibliothek installiert sein:

  ```
  libgthread-2_0-0-32bit-2.17.2+2.17.3+20080708+r7171-3.1.x86_64.rpm
  ```

- ❒ Die `unzip`-RPM muss auf allen verwendeten Linux-Plattformen installiert sein.
- ❒ (Bedingt) Bei der Installation auf einer SLES 11 SP3-Plattform (64 Bit) muss die Bibliothek `libstdc++33-32 bit` installiert sein. Wenn diese Bibliothek nicht vorhanden ist, wird die integrierte Installation zwar ohne Fehlermeldung abgeschlossen, Sie können sich jedoch nicht bei iManager anmelden. Wenn Sie iManager allerdings separat installieren, fordert das iManager-Installationsprogramm Sie auf, die Bibliothek zu installieren.
- ❒ Die Datei `/etc/hosts` darf nur eine Loopback-Adresse enthalten. Falls mehrere Loopback-Adressen vorliegen, korrigieren Sie die Konfiguration. Entfernen Sie hierzu die überzähligen Adressen mit einem Editor oder mit Systemwerkzeugen. Beispiel:

  ```
  127.0.0.1 localhost.localdomain localhost #loopback
  #127.0.02 server1
  123.45.678.9 server1
  ```

Windows

- ❒ Zum Installieren von Identity Manager mit der integrierten Installation müssen Sie Administratorrechte auf dem Windows-Computer besitzen.
- ❒ Vor Beginn des Installationsvorgangs muss das Windows-Betriebssystem mit den aktuellen Service Packs aufgerüstet werden.

2.3.2 Systemanforderungen

Die nachfolgenden Anforderungen gelten dann, wenn Sie alle oder den Großteil der Komponenten auf einem einzigen Computer installieren. Die Anforderungen für bestimmte Komponenten finden Sie unter „Überlegungen und Voraussetzungen für die Installation“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

Für die fehlerfreie Installation und Konfiguration Ihres Identity Manager-Systems sind die nachfolgenden Angaben zu beachten.

Kategorie	Anforderung
Prozessor	Ein Multi-CPU-Computer mit einem 2-GHz-Prozessor.
Arbeitsspeicher	Mindestens 6 MB.
Festplattenspeicher	Mindestens 40 GB. **HINWEIS:** Zum Konfigurieren und Bereitstellen von Daten ist zusätzlicher Festplattenspeicher erforderlich. Die Menge ist abhängig von den verbundenen Systemen und der Anzahl der Objekte im Identitätsdepot.
Betriebssystem	Mindestens eines der folgenden Systeme: ◆ Red Hat 6.5 (64 Bit) ◆ SUSE Linux Enterprise Server 11 SP3 (64 Bit) ◆ Windows Server 2012 R2 (64 Bit)
Virtuelle Systeme	Es gelten folgende Voraussetzungen: ◆ Hyper-V in Windows Server 2012 R2 ◆ VMWare ESX 5.5 **WICHTIG:** NetIQ unterstützt Identity Manager auf virtuellen Enterprise-Systemen, die die Betriebssysteme, unter denen die NetIQ-Produkte ausgeführt werden können, offiziell unterstützen. Sofern die Anbieter der virtuellen Systeme diese Betriebssysteme offiziell unterstützen, unterstützt NetIQ den gesamten Identity Manager-Stack auf diesen Systemen.
Betriebssystem-Hotfixes	NetIQ empfiehlt, vor dem Installieren von Identity Manager die aktuellen Patches für das Betriebssystem mit der automatisierten Aktualisierungsfunktion des Herstellers anzuwenden.

Kategorie	Anforderung
Webbrowser	**Desktopcomputer** (ggf. höhere Version): ◆ Apple Safari 5.1.7 für Windows ◆ Apple Safari 7.0.1 ◆ Google Chrome 37 ◆ Microsoft Internet Explorer 11 ◆ Mozilla Firefox 32 **iPad** (ggf. höhere Version): ◆ Apple Safari 7 ◆ Google Chrome 37 **HINWEIS:** Für den Zugriff auf die Identitätsanwendungen müssen Cookies im Browser aktiviert sein. Wenn Cookies deaktiviert sind, ist das Produkt nicht funktionsfähig.

2.3.3 Standardmäßige Speicherorte für die Installation

Bei der integrierten Installation werden die Identity Manager-Komponenten in den Speicherorten in Tabelle 2-1 installiert. Auf Windows-Computern können Sie den Speicherort für die installierten Komponenten selbst festlegen. Auf Linux-Computern werden die Komponenten in den vordefinierten Speicherorten abgelegt.

Tabelle 2-1 *Standardmäßige Speicherorte für die Installation bei der integrierten Installation*

Identity Manager-Komponente	Standardmäßiger Installationspfad
Linux	
Identitätsdepot (eDirectory)	`/opt/novell/eDirectory`
Identity Manager-Engine	`/opt/novell/eDirectory`
Remote Loader	`/opt/novell/dirxml`
Event Auditing Service	`/opt/novell/sentinel_eas` (nur Linux)
Identitätsanwendungen	`/opt/netiq/idm/apps`
Identitätsberichterstellungsmodul	`/opt/netiq/idm/apps`
iManager und Plugins	`/var/opt/novell/iManager`
Analyzer	`/opt/netiq/idm/tools/Analyzer`
Designer	`/opt/netiq/idm/tools/Designer`
Windows	
Identitätsdepot (eDirectory)	`C:\NetIQ\IdentityManager\NDS`
Identity Manager-Engine	`C:\NetIQ\IdentityManager\NDS`
Remote Loader	`C:\NetIQ\IdentityManager\RemoteLoader`

Identity Manager-Komponente	Standardmäßiger Installationspfad
Identitätsanwendungen	`C:\NetIQ\IdentityManager\apps`
Identitätsberichterstellungsmodul	`C:\NetIQ\IdentityManager\apps`
iManager	`C:\NetIQ\IdentityManager\iManager`
Analyzer	`C:\NetIQ\IdentityManager\tools\Analyzer`
Designer	`C:\NetIQ\IdentityManager\tools\Designer`

3 Installation von Identity Manager

Das integrierte Installationsprogramm installiert die Binärdateien für die Identity Manager-Komponenten und konfiguriert die Komponenten. Sie können die Komponenten installieren und gleichzeitig konfigurieren oder auch die Konfiguration zu einem späteren Zeitpunkt nachholen.

3.1 Herunterladen der ISO-Datei

Sie müssen die Installationsdateien von der NetIQ Downloads-Website herunterladen.

So laden Sie die .iso-Datei herunter:

1. Öffnen Sie die NetIQ Downloads-Website (https://dl.netiq.com/index.jsp).
2. Wählen Sie im Menü **Produkt oder Technologie** den Eintrag **Identity Manager** aus.
3. Wählen Sie im Feld **Version auswählen** den Eintrag **Identity Manager 4.5** aus, und klicken Sie auf **Abfrage senden**.
4. Klicken Sie auf den Link **Identity Manager 4.5** und dann auf **Weiter zum Download**.
5. Melden Sie sich mit Ihrer NetIQ-Kundenzentrums-ID an.
6. Wählen Sie die entsprechende `.iso`-Datei für Ihre Plattform aus, und laden Sie die Datei gemäß den Anweisungen auf dem Bildschirm herunter.

Die integrierten Installationsdateien (`install.exe` oder `install.bin`) befinden sich an oberster Stelle der `.iso`-Dateien für Identity Manager. Greifen Sie auf die Identity Manager - Installationsdateien zu, indem Sie entweder die `.iso`-Datei mounten oder auf die DVD zugreifen, die Sie aus der `.iso`-Datei erstellt haben.

3.2 Verwenden desselben Passworts für alle Konfigurationsparameter bei der integrierten Installation

Während der Konfiguration müssen Sie für zahlreiche Identity Manager-Komponenten ein Passwort angeben. Zur Beschleunigung der Abläufe können Sie festlegen, dass ein einziges Passwort für alle Konfigurationsparameter bei der integrierten Installation verwendet werden soll.

Das Passwort muss mindestens sechs Zeichen umfassen.

Linux

Führen Sie den folgenden Befehl aus, bevor Sie das Installations- oder Konfigurationsprogramm starten:

```
export USER_SUPPLIED_PASSWORD=password
```

Beispiel:

```
export USER_SUPPLIED_PASSWORD=test123
```

Windows

Führen Sie einen der folgenden Schritte aus:

- Fügen Sie unter **Systemeigenschaften > Umgebungsvariablen** den Eintrag `USER_SUPPLIED_PASSWORD` hinzu, und geben Sie einen Wert für die Variable an.
- Führen Sie den folgenden Befehl aus, bevor Sie das Installations- oder Konfigurationsprogramm starten:

  ```
  set USER_SUPPLIED_PASSWORD=password
  ```

  Beispiel:

  ```
  set USER_SUPPLIED_PASSWORD=test123
  ```

HINWEIS: Auf Windows-Servern übernimmt der Installationsvorgang die angegebene Passwortvariable nicht für **EAS-Systempasswort**. Geben Sie für diesen Parameter stattdessen das vom System generierte Passwort für die EAS-Installation auf dem Remote-Linux-Server an.

3.3 Verwenden des Installationsassistenten

Im folgenden Verfahren wird die Installation von Identity Manager auf einer Linux- oder Windows-Plattform mit dem Installationsassistenten beschrieben. Anweisungen für die automatische, unbeaufsichtigte Installation finden Sie in Abschnitt 3.4, „Ausführen einer automatischen Installation“, auf Seite 25.

Überprüfen Sie in Vorbereitung auf die Installation die Voraussetzungen und Systemanforderungen in Abschnitt 2.1, „Installations-Checkliste“, auf Seite 17. Beachten Sie außerdem die zugehörigen Installationsinformationen in den aktuellen Versionshinweisen.

Zur Arbeitserleichterung können Sie ein Passwort angeben, das der Installationsvorgang für den Großteil der Passwörter übernimmt, die für Identity Manager konfiguriert werden müssen.

So installieren Sie Identity Manager mit dem Assistenten:

1. Melden Sie sich als root oder als verwaltungsbefugter Benutzer an dem Computer an, auf dem die Komponenten installiert werden sollen.
2. Hängen Sie die `.iso`-Datei ein, oder erstellen Sie eine DVD aus der `.iso`-Datei. Weitere Informationen finden Sie in Abschnitt 3.1, „Herunterladen der ISO-Datei“, auf Seite 23.
3. (Optional) Legen Sie fest, dass ein einziges Passwort für alle Konfigurationsparameter bei der integrierten Installation verwendet werden soll. Weitere Informationen finden Sie in Abschnitt 3.2, „Verwenden desselben Passworts für alle Konfigurationsparameter bei der integrierten Installation“, auf Seite 23.
4. Greifen Sie im Stammverzeichnis der `.iso`-Datei auf die Installationsdateien zu, und führen Sie einen der folgenden Schritte aus:
   - **Linux** – Geben Sie Folgendes ein: `./install.bin`
   - **Windows** – Führen Sie `install.exe` aus.
5. Wählen Sie auf der Startseite die gewünschte Sprache in der Dropdown-Liste aus, und klicken Sie auf **OK**.
6. Lesen Sie auf der Einführungsseite die Liste der Identity Manager-Komponenten, die installiert werden können, und klicken Sie auf **Weiter**.
7. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Weiter**.

HINWEIS: Sie müssen die gesamte Lizenzvereinbarung lesen und bis an ihr Ende blättern, damit Sie sie akzeptieren können.

8 Geben Sie die Komponenten an, die auf dem lokalen Server installiert werden sollen, und klicken Sie auf **Weiter**.

Weitere Informationen zu den Komponentenoptionen finden Sie in Abschnitt 1.2, „Erläuterungen zur integrierten Installation“, auf Seite 10.

9 (Bedingt) Auf einem Windows-Server legen Sie den Installationsordner fest, und klicken Sie auf **Weiter**.

10 Lesen Sie die Zusammenfassung vor der Installation, und klicken Sie auf **Installieren**.

HINWEIS: Der Installationsvorgang kann einige Zeit in Anspruch nehmen, abhängig von den ausgewählten Komponenten.

11 Nach Abschluss der Installation konfigurieren Sie die installierten Komponenten mit einem der folgenden Schritte:

- **Sofortige Konfiguration:** Wählen Sie **Jetzt fortsetzen**.
- **Spätere Konfiguration:** Deaktivieren Sie die Option **Jetzt fortsetzen**.

Sie können die Konfigurationsparameter jederzeit ändern. Identity Manager kann jedoch erst dann ausgeführt werden, wenn ein Großteil der Parameter festgelegt ist. Weitere Informationen finden Sie in Kapitel 4, „Konfigurieren der Identity Manager-Komponenten“, auf Seite 27.

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

12 Klicken Sie auf **Fertig**.

3.4 Ausführen einer automatischen Installation

Bei der automatischen (nicht interaktiven) Installation wird keine Benutzeroberfläche angezeigt, und der Benutzer muss keinerlei Fragen beantworten. Stattdessen ruft das System die Daten aus der Eigenschaftendatei ab. Anweisungen zur geführten Installation finden Sie in Abschnitt 3.3, „Verwenden des Installationsassistenten“, auf Seite 24. Überprüfen Sie in Vorbereitung auf die Installation die Voraussetzungen und Systemanforderungen in Abschnitt 2.1, „Installations-Checkliste“, auf Seite 17. Beachten Sie außerdem die zugehörigen Installationsinformationen in den aktuellen Versionshinweisen.

Zur Arbeitserleichterung können Sie ein Passwort angeben, das der Installationsvorgang für die Single-Sign-On-Passwörter übernimmt, die für Identity Manager konfiguriert werden müssen. Weitere Informationen finden Sie in Abschnitt 4.1, „Überlegungen zur Konfiguration der Komponenten“, auf Seite 27.

So lassen Sie eine automatische Installation ausführen:

1 Melden Sie sich als `root` oder Administrator an dem Computer an, auf dem die Komponenten installiert werden sollen.

2 Sobald Sie die `.iso`-Datei gemountet haben, navigieren Sie zum Verzeichnis, in dem sich die Installationsdateien befinden (standardmäßig unter `osp_sspr`).

3 Öffnen Sie die Datei `install.properties` für die automatische Installation, die sich standardmäßig in einem der folgenden Verzeichnisse befindet:

- **Linux:** `install/propfiles`
- **Windows:** `install\propfiles`

4 (Optional) Legen Sie fest, dass ein einziges Passwort für alle Konfigurationsparameter bei der integrierten Installation verwendet werden soll. Weitere Informationen finden Sie in Abschnitt 3.2, „Verwenden desselben Passworts für alle Konfigurationsparameter bei der integrierten Installation“, auf Seite 23.

5 Starten Sie die automatische Installation mit einem der folgenden Befehle:

- **Linux:** `install.bin -i silent -f` *`Pfad_zur_install.properties_Datei`*
- **Windows:** `install.exe -i silent -f` *`Pfad_zur_install.properties_Datei`*

6 Fahren Sie mit der Konfigurationsphase des Vorgangs fort. Weitere Informationen finden Sie in Kapitel 4, „Konfigurieren der Identity Manager-Komponenten“, auf Seite 27.

4 Konfigurieren der Identity Manager-Komponenten

Sie können sich wahlweise von der integrierten Installation durch die Konfiguration der installierten Identity Manager-Komponenten führen oder auch eine automatische Konfiguration vornehmen lassen. Bei einigen Komponenten wie Designer oder Analyzer ist keine Konfiguration erforderlich. Weitere Informationen zu den Konfigurationsparametern finden Sie in Kapitel 5, „Erläuterungen zu den Konfigurationsparametern“, auf Seite 33.

HINWEIS: Der Konfigurationsvorgang weist eine Beispiel-Passwortrichtlinie zu `admin.sa.system`, `uaadmin.sa.data` und `users.data` zu, damit die Benutzer sich bei den Identitätsanwendungen anmelden können. Im Rahmen dieses Vorgangs wird auch die Einstellung **Administrator darf Passwörter abrufen** in den Optionen zum Abrufen der Passwörter aktualisiert.

4.1 Überlegungen zur Konfiguration der Komponenten

Lesen Sie die folgenden Überlegungen, bevor Sie die installierten Komponenten mit der integrierten Installation konfigurieren:

- Sie können nur die Komponenten konfigurieren, die auf dem lokalen Computer installiert sind.
- Vor Beginn der Installation oder Konfiguration können Sie festlegen, dass ein einziges Passwort für alle Konfigurationsparameter bei der integrierten Installation verwendet werden soll. Weitere Informationen finden Sie in Abschnitt 3.2, „Verwenden desselben Passworts für alle Konfigurationsparameter bei der integrierten Installation“, auf Seite 23.
- Die Datei `/etc/hosts` muss Einträge für die Loopback-Adresse 127.0.0.1 und die tatsächliche IP-Adresse enthalten. Weitere Informationen finden Sie in Abschnitt 2.3, „Voraussetzungen und Systemanforderungen“, auf Seite 18.
- Wenn Sie die Identitätsanwendungen und die Komponenten der Identitätsberichterstellung konfigurieren, müssen Sie die Option **Erweiterte Einstellungen** wählen und alle Felder, die den Eintrag `localhost` enthalten, in eine gültige IP-Adresse oder einen gültigen DNS-Namen ändern. Wenn Sie den Eintrag `localhost` unverändert beibehalten, schlägt die Konfiguration fehl.
- Wenn Sie lediglich den Identity Manager-Server konfigurieren, fügen Sie die Protokollierungsserverdetails manuell zur Datei `logevent.conf` (Linux) bzw. `logevent.cfg` (Windows) hinzu. Die integrierte Installation aktualisiert die Datei nur dann mit den Protokollierungsserverdetails, wenn Sie die Identitätsanwendungen oder die Identitätsberichterstellung konfigurieren.
- Bevor Sie einen Sekundärserver in einen vorhandenen Baum einfügen, sollten Sie eine Zustandsprüfung ausführen. Diese Zustandsprüfung wird nicht automatisch im Rahmen der integrierten Installation vorgenommen.

- Wenn Sie einen Sekundärserver zum Baum hinzufügen, 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 unter „Konfigurieren des Treibers für den Datenerfassungsdienst (DCS-Treiber)“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.
  - Wenn der DCS-Treiber sich auf diesem Sekundärserver befindet, muss der Server auch eine Kopie der Stammpartition enthalten, damit er ordnungsgemäß funktioniert.

Weitere Informationen zu den Konfigurationswerten finden Sie in Kapitel 5, „Erläuterungen zu den Konfigurationsparametern“, auf Seite 33.

4.2 Verwenden des Konfigurationsassistenten

Der Konfigurationsassistent führt Sie durch die Konfiguration aller Identity Manager-Komponenten, die Sie bei der Installation ausgewählt hatten.

So konfigurieren Sie die Identity Manager-Komponenten:

1. (Bedingt) Zum Hinzufügen eines Sekundärservers zu einem vorhandenen Baum führen Sie die folgenden Schritte aus:
   - **1a** Verwenden Sie das ndscheck-Dienstprogramm, das sich standardmäßig in den folgenden Verzeichnissen befindet:
     - **Linux:** `/opt/novell/eDirectory/bin/ndscheck`
     - **Windows:** *`Installationsort`*`\NDS`
   - **1b** Geben Sie die erforderlichen Parameter an und führen Sie den folgenden Befehl aus:

     `ndscheck [-h Hostname Port] [-a admin_FDN] [-w Passwort]`
2. (Bedingt) Wenn Sie ab Schritt 12 auf Seite 25 im Installationsverfahren fortfahren, gehen Sie zu Schritt 6 auf Seite 28.
3. (Optional) Legen Sie fest, dass ein einziges Passwort für alle Konfigurationsparameter bei der integrierten Installation verwendet werden soll. Weitere Informationen finden Sie in Abschnitt 3.2, „Verwenden desselben Passworts für alle Konfigurationsparameter bei der integrierten Installation“, auf Seite 23.
4. (Bedingt) Starten Sie die Konfiguration manuell mit einem der folgenden Schritte:
   - **Linux (Benutzeroberfläche)** – Geben Sie Folgendes ein: `/configure.bin`
   - **Windows** – Führen Sie `configure.exe` aus.
5. Wählen Sie auf der Startseite die gewünschte Sprache in der Dropdown-Liste aus, und klicken Sie auf **OK**.
6. Prüfen Sie die Komponenten, die auf dem System installiert sind, und klicken Sie auf **Weiter**.
7. Wählen Sie die Komponenten aus, die auf dem lokalen Server konfiguriert werden sollen, und klicken Sie auf **Weiter**.
8. Konfigurieren Sie die verschiedenen Komponenten mithilfe der folgenden Informationen:
   - **Identitätsdepot:** Geben Sie an, ob ein neuer Baum im Identitätsdepot erstellt oder ein vorhandener Baum bearbeitet werden soll, und konfigurieren Sie den Baum für Ihre Umgebung. Weitere Informationen finden Sie in Abschnitt 5.1, „Identitätsdepot“, auf Seite 33.

- **Event Auditing Service:** Geben Sie die Konfigurationsinformationen für den Event Auditing Service an. Weitere Informationen finden Sie in Abschnitt 5.3, „Event Auditing Service“, auf Seite 37.

  WICHTIG: Der Event Auditing Service kann nur auf Linux-Computern installiert werden. Für die Konfiguration des Identitätsberichterstellungsmoduls ist jedoch ein funktionsfähiger Event Auditing Service erforderlich.

- **Identitätsanwendungen:** Geben Sie die Konfigurationsinformationen für die Identitätsanwendungen an. Sie müssen die IP-Adresse oder den DNS-Namen eines Audit-Servers angeben; ansonsten schlägt die Konfiguration fehl. Weitere Informationen finden Sie in Abschnitt 5.4, „Identitätsanwendungen“, auf Seite 38.

  WICHTIG: Sie müssen die Option **Erweiterte Einstellungen** wählen und alle Felder, die den Eintrag `localhost` enthalten, in eine gültige IP-Adresse oder einen gültigen DNS-Namen ändern. Wenn Sie den Standardparameter `localhost` unverändert beibehalten, schlägt die Konfiguration fehl.

- **(Bedingt) Identity Manager-Server:** Wenn Sie die Installation in einem vorhandenen eDirectory-Baum vornehmen, geben Sie die vorhandenen Identity Manager-Serverinformationen an. Weitere Informationen finden Sie in Abschnitt 5.2, „Identity Manager Server“, auf Seite 37.
- **Identitätsberichterstellungsmodul:** Das Identitätsberichterstellungsmodul kann nur dann genutzt werden, wenn der Event Auditing Service installiert und konfiguriert ist. Der Event Auditing Service kann nur auf einem Linux-Computer installiert werden. Wenn Sie mit einem Windows-Computer arbeiten, müssen Sie den Event Auditing Service auf einem Linux-Computer installieren, bevor Sie das Identitätsberichterstellungsmodul auf einem Windows-Computer konfigurieren können.

  Geben Sie die Konfigurationsinformationen für das Identitätsberichterstellungsmodul an. Weitere Informationen finden Sie in Abschnitt 5.5, „Identitätsberichterstellungsmodul“, auf Seite 40.
- **Werkzeuge:** nur Linux. Wählen Sie **Erweiterte Einstellungen**, und ändern Sie die standardmäßigen HTTP-Ports. Weitere Informationen finden Sie in Abschnitt 5.6, „Werkzeuge“, auf Seite 43.

9 Klicken Sie auf **Weiter**, und konfigurieren Sie die verschiedenen Komponenten.

10 Prüfen Sie die Zusammenfassung der Konfigurationsinformationen, und klicken Sie auf **Konfigurieren**.

11 Lesen Sie die Zusammenfassung der Konfiguration, und klicken Sie auf **Fertig**.

HINWEIS: Falls Fehler während der Konfiguration aufgetreten sind, zeigt die integrierte Installation den Speicherort der Installationsprotokolle an. Ermitteln Sie anhand der Installationsprotokolle, warum die Konfiguration fehlgeschlagen ist.

4.3 Bearbeiten der Eigenschaftendatei zum Ausführen einer automatischen Konfiguration

Soll eine automatische Konfiguration der Identity Manager-Komponenten ausgeführt werden, erstellen oder bearbeiten Sie für jede Konfiguration eine Eigenschaftendatei mit den erforderlichen Parametern für die Konfiguration. Der Identity Manager-Datenträger enthält zwei Beispieldateien, die Sie verwenden können, wenn Sie alle Komponenten auf einem einzigen Server installiert haben.

So bearbeiten Sie die Eigenschaftendatei:

1. (Bedingt) Wenn Sie alle Komponenten auf demselben Server installiert haben, bearbeiten Sie eine der Beispiel-Eigenschaftendateien für die automatische Konfiguration, die sich standardmäßig in den folgenden Verzeichnissen befinden:
   - **Linux:** `install/propfiles`
   - **Windows:** `install\propfiles`

   Mit der Datei `configure_new_tree.properties` erstellen Sie beispielsweise einen neuen Baum.
2. (Bedingt) Falls Sie nicht alle Komponenten auf demselben Server installiert haben, erzeugen Sie mit den folgenden Schritten eine Eigenschaftendatei für die installierten Komponenten:

   2a Führen Sie den folgenden Befehl aus:

   ```
   ./install.bin -i silent -DSELECTED_PRODUCTS=components_to_be_configured -f
   filename.properties
   ```

   Dateiname`.properties` bezeichnet hierbei eine der Beispiel-Eigenschaftendateien.

   Das Programm überprüft, ob die angegebenen Komponenten installiert sind, und generiert dann eine Liste der obligatorischen Parameter für die betreffenden Komponenten.

   2b Erstellen Sie anhand der Ausgabe des Befehls in Schritt 2a eine neue Eigenschaftendatei.

   2c Fügen Sie die Variable `SELECTED_PRODUCTS` in die Datei ein, und geben Sie die zu konfigurierenden Komponenten an.
3. Legen Sie in der Eigenschaftendatei die Einstellungen für die installierten Komponenten fest. Weitere Informationen finden Sie in Kapitel 5, „Erläuterungen zu den Konfigurationsparametern“, auf Seite 33.
4. Fügen Sie der Eigenschaftendatei die folgenden Passwortvariablen hinzu:

Passwortvariable	Zugehöriges Benutzerkonto bzw. zugehöriger Dienst
IA_IDVAULT_ADMIN_PASSWORD	Identitätsdepot-Administrator
IA_RBPM_POSTGRESQL_DB_PASSWORD	Administrator der Datenbank für die Identitätsanwendungen (idmadmin)
IA_RBPM_USERAPPADMIN_PASSWORD	Administrator der Benutzeranwendung (uaadmin)
IA_REPORTING_NOVL_DB_USER_PASSWORD	Administrator für die Datenbank der Identitätsberichterstellung
IA_REPORTING_IDM_SERVER_PASSWORD	Benutzer des Identitätsberichterstellungsservers (idmrptsrv)
IA_REPORTING_IDM_USER_PASSWORD	Benutzer der Identitätsberichterstellung (idmrptuser)
IA_EAS_DBA_PWD	Administrator der Datenbank für den Event Auditing Service (dbauser)
IA_EAS_ADMIN_PWD	Administrator des Event Auditing Service (admin)
-DUSER_SUPPLIED_PASSWORD	Single-Sign-On-Dienst

   Wenn Sie die Variable `duser_supplied_password` beim Starten der automatischen Installation angegeben hatten, übernimmt das Programm diesen Wert für die Single-Sign-On-Passwörter.
5. Speichern und schließen Sie die Datei.

4.4 Ausführen einer automatischen Konfiguration

Soll eine automatische Konfiguration der Identity Manager-Komponenten ausgeführt werden, erstellen Sie für jede Konfiguration eine Eigenschaftendatei mit den erforderlichen Parametern für die Konfiguration. Der Identity Manager-Datenträger enthält zwei Beispieldateien, die Sie verwenden können, wenn Sie alle Komponenten auf einem einzigen Server installiert haben.

Weitere Informationen zu den konfigurierbaren Parametern finden Sie in Kapitel 5, „Erläuterungen zu den Konfigurationsparametern“, auf Seite 33.

So lassen Sie eine automatische Konfiguration ausführen:

1. (Bedingt) Zum Hinzufügen eines Sekundärservers zu einem vorhandenen Baum führen Sie die folgenden Schritte aus:

   1a. Verwenden Sie das ndscheck-Dienstprogramm, das sich standardmäßig in den folgenden Verzeichnissen befindet:

   - **Linux:** `/opt/novell/eDirectory/bin/ndscheck`
   - **Windows:** *`Installationsort`*`\NDS`

   1b. Geben Sie die erforderlichen Parameter an und führen Sie den folgenden Befehl aus:

   ```
   ndscheck [-h Hostname Port] [-a admin_FDN] [-w Passwort]
   ```

2. (Optional) Legen Sie fest, dass ein einziges Passwort für alle Konfigurationsparameter bei der integrierten Installation verwendet werden soll. Weitere Informationen finden Sie in Abschnitt 3.2, „Verwenden desselben Passworts für alle Konfigurationsparameter bei der integrierten Installation“, auf Seite 23.

3. Starten Sie die automatische Konfiguration mit einem der folgenden Befehle:

   - **Linux:** `configure.bin -i silent -f` *`Pfad_zur_Eigenschaftendatei`*
   - **Windows:** `configure.exe -i silent -f` *`Pfad_zur_Eigenschaftendatei`*

5 Erläuterungen zu den Konfigurationsparametern

In diesem Abschnitt werden die Parameter definiert, die zur ordnungsgemäßen Konfiguration der Identity Manager-Installation erforderlich sind. Sie können im Installationsprogramm angeben, dass die Komponenten direkt nach ihrer Installation konfiguriert werden.

HINWEIS: Für zahlreiche Komponenten muss ein Passwort angegeben werden. Sie können dasselbe Passwort für alle Parameter verwenden. Geben Sie hierzu das Passwort beim Starten des Installationsvorgangs an. Weitere Informationen finden Sie in den Anweisungen zur Installation.

5.1 Identitätsdepot

In diesem Abschnitt werden die Einstellungen für den eDirectory-Baum für das Identitätsdepot definiert. Einige Parameter betreffen die Konfiguration eines neuen Baums im Vergleich zur Konfiguration eines vorhandenen Baums. Im Programm werden zudem nur die grundlegenden Parameter angezeigt. Sollen alle Parameter eingeblendet werden, klicken Sie auf **Erweiterte Einstellungen**.

5.1.1 Erstellen eines neuen Baums

Verwenden Sie die nachfolgenden Parameter, wenn noch kein eDirectory-Baum vorhanden ist. Alle Parameter in diesem Abschnitt sind zum Erstellen eines neuen Baums erforderlich.

Neuen Baum erstellen

Mit dieser Option wird ein neuer eDirectory-Baum für das Identitätsdepot erstellt.

Baumname

Gibt den Namen des zu erstellenden Baums an. Der Baumname muss den folgenden Anforderungen entsprechen:

- Der Baumname muss im Netzwerk eindeutig sein.
- Der Baumname muss 2 bis 32 Zeichen lang sein.
- Der Baumname darf nur Buchstaben (a-z, A-Z), Ziffern (0-9), Bindestriche (-) und Unterstriche (_) enthalten.

Wenn Sie separate Bäume nutzen, sollten Sie einen Unternehmensstandard für die Baumnamen festlegen, sodass die Bäume künftig leichter zusammengeführt werden können.

Administratorpasswort

Gibt das Passwort für das Administratorobjekt an. Beispiel: `netiq123`. Das Installationsprogramm konfiguriert das Passwort für das erstellte Administratorobjekt.

Erweiterte Einstellungen

Alle verbleibenden Einstellungen sind unter **Erweiterte Einstellungen** aufgeführt. Wenn Sie keine Änderungen unter **Erweiterte Einstellungen** vornehmen, werden die aufgeführten Standardeinstellungen im Konfigurationsprogramm herangezogen.

Identitätsdepot-Administrator

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). Der Standardname lautet `admin`.

Mit diesem Konto führt das Installationsprogramm alle Vorgänge im Baum aus.

NCP-Port

Gilt nur für Linux-Server

Gibt den NCP-Port (NetWare Core Protocol) an, über den das Identitätsdepot mit den Identity Manager-Komponenten kommuniziert. Der Standardwert ist 524.

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 unter „Kommunizieren mit dem Identitätsdepot über LDAP“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

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 unter „Kommunizieren mit dem Identitätsdepot über LDAP“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

HTTP-Port

Gibt den Port an, an dem der HTTP-Stack im Klartext arbeitet. Der Standardwert ist 8028.

Die angegebenen HTTP-Stack-Ports dürfen nicht mit den HTTP-Stack-Ports für iManager identisch sein. Weitere Informationen finden Sie im *iManager-Administrationshandbuch* (http://www.netiq.com/documentation/imanager27/imanager_admin_275/data/hk42s9ot.html).

Sicherer HTTP-Port

Gibt den Port an, an dem der HTTP-Stack mit dem TLS/SSL-Protokoll arbeitet. Der Standardwert ist 8030.

Die angegebenen HTTP-Stack-Ports dürfen nicht mit den HTTP-Stack-Ports für iManager identisch sein. Weitere Informationen finden Sie im *iManager-Administrationshandbuch* (http://www.netiq.com/documentation/imanager27/imanager_admin_275/data/hk42s9ot.html).

Pfad der eDirectory-Instanz

Gilt nur für Linux-Server

Gibt den Pfad dieser eDirectory-Instanz auf diesem Server an. Der Standardpfad ist `/var/opt/novell/eDirectory`. Sie können mehrere Instanzen von eDirectory auf einem einzigen Server ausführen.

DIB-Pfad

Gibt den Pfad im lokalen System an, in dem die DIB-Dateien (Directory Information Base) installiert werden sollen. Standardmäßig legt das Installationsprogramm die Dateien in den folgenden Speicherorten ab:

- **Linux:** `/var/opt/novell/eDirectory/data/dib`
- **Windows:** `C:\NetIQ\IdentityManager\NDS\DIBFiles\`

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

WICHTIG: Die DIB-Dateien müssen sich im Verzeichnis `\NDS` unter Windows befinden. Wenn Sie den standardmäßigen Speicherort der DIB-Dateien unter Windows ändern, schlägt die Konfiguration der Identity Manager-Engine fehl.

TLS für einfache Bindung mit Passwort erforderlich

(Optional) Geben Sie an, ob das Identitätsdepot das TLS-Protokoll (Transport Layer Security) für den Empfang von LDAP-Anforderungen im Klartext benötigt. Diese Option ist standardmäßig aktiviert.

Secretstore aktivieren

Gilt nur für Windows-Server

(Optional) Geben Sie an, ob SecretStore bei der Konfiguration von eDirectory aktiviert werden soll. Weitere Informationen finden Sie unter SecretStore Integration with eDirectory (https://www.netiq.com/documentation/edir88/edirin88/data/bv50u8n.html) (SecretStore-Integration in eDirectory).

5.1.2 Hinzufügen zu einem vorhandenen Baum

Wenn bereits ein eDirectory-Baum vorhanden ist, fügen Sie diesen neuen Server mit den nachfolgenden Parametern in den vorhandenen Baum ein.

WICHTIG: Informieren Sie sich über die Auswirkungen, die beim Hinzufügen eines neuen Servers zu einem vorhandenen Baum zu beachten sind. Weitere Informationen finden Sie in Abschnitt 4.1, „Überlegungen zur Konfiguration der Komponenten“, auf Seite 27.

Zu einem vorhandenen Baum hinzufügen

Mit dieser Option wird ein vorhandener Baum für das Identitätsdepot bearbeitet.

Name des vorhandenen Baums

Geben Sie den Namen des vorhandenen eDirectory-Baums ein.

Adresse des vorhandenen Servers

Geben Sie die IP-Adresse des Servers ein, auf dem sich das Masterreplikat der Stammpartition befindet.

Vorhandene Portnummer

Geben Sie den NCP-Port des oben angegebenen Servers an. Der Standardport für NCP ist 524.

Kontext-DN des vorhandenen Servers

Geben Sie den LDAP-DN des Kontexts an, in dem dieser Server im vorhandenen Baum platziert werden soll. Der Standardwert lautet „ou=servers,o=system“ aus der Identitätsdepotstruktur, die mit der integrierten Installation erstellt wurde. Weitere Informationen finden Sie in Abschnitt 1.3, „Erläuterungen zur standardmäßigen Identitätsdepot-Struktur“, auf Seite 13.

Name des Administrators des vorhandenen Servers

Geben Sie den Namen des eDirectory-Administrators an. Der Standardname lautet „admin“. Weitere Informationen finden Sie in Abschnitt 1.3, „Erläuterungen zur standardmäßigen Identitätsdepot-Struktur“, auf Seite 13.

Kontext-DN des Administrators des vorhandenen Servers

Geben Sie den LDAP-DN des Kontexts an, in dem sich der eDirectory-Administrator im vorhandenen Baum befindet. Der Standardwert lautet „ou=sa,o=system“ aus der Identitätsdepotstruktur, die mit der integrierten Installation erstellt wurde. Weitere Informationen finden Sie in Abschnitt 1.3, „Erläuterungen zur standardmäßigen Identitätsdepot-Struktur“, auf Seite 13.

Administratorpasswort des vorhandenen Servers

Geben Sie das Passwort des eDirectory-Administrators an.

Erweiterte Einstellungen

Alle verbleibenden Einstellungen sind unter **Erweiterte Einstellungen** aufgeführt. Wenn Sie keine Änderungen unter **Erweiterte Einstellungen** vornehmen, werden die aufgeführten Standardeinstellungen im Konfigurationsprogramm herangezogen.

LDAP-Port

Gibt den Port an, den der vorhandene eDirectory-Baum auf LDAP-Anforderungen im Klartext überwachen soll. Der Standardwert ist 389.

Weitere Informationen zur Verwendung von LDAP finden Sie unter „Kommunizieren mit dem Identitätsdepot über LDAP“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

Sicherer LDAP-Port

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

Weitere Informationen zur Verwendung von LDAP finden Sie unter „Kommunizieren mit dem Identitätsdepot über LDAP“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

HTTP-Port

Gibt den Port an, an dem der HTTP-Stack im Klartext arbeitet. Der Standardwert ist 8028.

Die angegebenen HTTP-Stack-Ports dürfen nicht mit den HTTP-Stack-Ports für iManager identisch sein. Weitere Informationen finden Sie im *iManager-Administrationshandbuch* (http://www.netiq.com/documentation/imanager27/imanager_admin_275/data/hk42s9ot.html).

Sicherer HTTP-Port

Gibt den Port an, an dem der HTTP-Stack mit dem TLS/SSL-Protokoll arbeitet. Der Standardwert ist 8030.

Die angegebenen HTTP-Stack-Ports dürfen nicht mit den HTTP-Stack-Ports für iManager identisch sein. Weitere Informationen finden Sie im *iManager-Administrationshandbuch* (http://www.netiq.com/documentation/imanager27/imanager_admin_275/data/hk42s9ot.html).

DIB-Pfad

Gibt den Pfad im lokalen System an, in dem die DIB-Dateien (Directory Information Base) installiert werden sollen. Standardmäßig legt das Installationsprogramm die Dateien in den folgenden Speicherorten ab:

- **Linux:** `/var/opt/novell/eDirectory/data/dib`
- **Windows:** `C:\NetIQ\IdentityManager\NDS\DIBFiles\`

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

WICHTIG: Die DIB-Dateien müssen sich im Verzeichnis `\NDS` unter Windows befinden. Wenn Sie den standardmäßigen Speicherort der DIB-Dateien unter Windows ändern, schlägt die Konfiguration der Identity Manager-Engine fehl.

TLS für einfache Bindung mit Passwort erforderlich

(Optional) Geben Sie an, ob das Identitätsdepot das TLS-Protokoll (Transport Layer Security) für den Empfang von LDAP-Anforderungen im Klartext benötigt. Diese Option ist standardmäßig aktiviert.

Secretstore aktivieren

Gilt nur für Windows-Server

(Optional) Geben Sie an, ob SecretStore bei der Konfiguration von eDirectory aktiviert werden soll. Weitere Informationen finden Sie unter SecretStore Integration with eDirectory (https://www.netiq.com/documentation/edir88/edirin88/data/bv50u8n.html) (SecretStore-Integration in eDirectory).

5.2 Identity Manager Server

Die Felder unter **Identity Manager-Server** werden nur dann in der integrierten Installation angezeigt, wenn Sie den Server zu einem vorhandenen eDirectory-Baum hinzufügen.

WICHTIG: Die integrierte Installation unterstützt keine Aufrüstung. Wenn bereits eine Identity Manager-Bereitstellung vorhanden ist, müssen Sie die Identity Manager-Lösung mit den normalen Installationsprogrammen aufrüsten. Weitere Informationen finden Sie unter „Aufrüsten von Identity Manager“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

Name des Treibersatzes

Geben Sie einen Namen für ein neues Identity Manager-Treibersatzobjekt an. Dieses Objekt muss erstellt werden, damit Identity Manager ordnungsgemäß funktioniert. Wenn Sie einen neuen Baum anlegen, wird dieses Objekt durch die integrierte Installation erstellt.

Kontext-DN des Treibersatzes

Geben Sie den LDAP-DN für den Container an, in dem das Treibersatzobjekt erstellt werden soll. Der Standardwert lautet „o=system“ aus der Identitätsdepotstruktur, die mit der integrierten Installation erstellt wurde. Weitere Informationen finden Sie in Abschnitt 1.3, „Erläuterungen zur standardmäßigen Identitätsdepot-Struktur“, auf Seite 13.

5.3 Event Auditing Service

Mit der EAS-Funktion (Event Auditing Service) in Identity Manager können Sie die Revision der Identity Manager-Komponenten vornehmen. Der Event Auditing Service kann allerdings nur auf Linux-Computern installiert werden. Der Event Auditing Service muss installiert sein und ausgeführt werden, bevor Sie die Identitätsanwendungen und die Funktionen der Identitätsberichterstellung konfigurieren können. Ansonsten schlägt die Konfiguration der Identitätsanwendungen und der Funktionen der Identitätsberichterstellung fehl.

Administratorpasswort

Geben Sie das Passwort für den Administrator der EAS-Dienstprogramme an. Dieses Konto wird während der Installation erstellt.

HINWEIS: Auf einem SLES-Server (SUSE Linux) muss das Passwort der Systempasswortrichtlinie für SLES entsprechen.

dbauser-Passwort

Gibt das Passwort für das `admin`-Konto an, mit dem das Identity Information Warehouse (Datenbank auf dem EAS-Server) bearbeitet werden kann. Dieses Konto wird während der Installation erstellt.

HINWEIS: Auf einem SLES-Server (SUSE Linux) muss das Passwort der Systempasswortrichtlinie für SLES entsprechen.

Erweiterte Einstellungen

Alle verbleibenden Einstellungen sind unter **Erweiterte Einstellungen** aufgeführt. Wenn Sie keine Änderungen unter **Erweiterte Einstellungen** vornehmen, werden die aufgeführten Standardeinstellungen im Konfigurationsprogramm herangezogen.

PostgreSQL-Port

Geben Sie den Port an, über den die PostgreSQL-Datenbank kommuniziert. Der Standardport ist 15432.

Portweiterleitung aktivieren

Geben Sie an, ob die Portweiterleitung von Paketen mit dem Event Auditing Service aktiviert werden soll. Standardmäßig ist diese Option aktiviert.

5.4 Identitätsanwendungen

In diesem Abschnitt werden die Einstellungen für die Identitätsanwendungen (z. B. für die Benutzeranwendung) definiert. Im Programm werden nur die grundlegenden Parameter angezeigt. Sollen alle Parameter eingeblendet werden, klicken Sie auf **Erweiterte Einstellungen**.

WICHTIG: Sie müssen die Option **Erweiterte Einstellungen** wählen und alle Felder, die den Eintrag `localhost` enthalten, in eine gültige IP-Adresse oder einen gültigen DNS-Namen ändern. Wenn Sie den Standardparameter `localhost` unverändert beibehalten, schlägt die Konfiguration fehl.

OSP-Server-Host

Gibt den DNS-Namen oder die IP-Adresse des Servers an, auf dem OSP installiert werden soll und der als LDAP-Authentifizierungsserver fungiert. Verwenden Sie nicht `localhost`.

Weitere Informationen zu OSP finden Sie unter „Single-Sign-On-Zugriff in Identity Manager“ im *Einrichtungshandbuch zu NetIQ Identity Manager*.

OSP-Keystore-Passwort

Gibt das Passwort an, das zum Laden des neuen Keystores auf dem OAuth-Server erstellt werden soll.

Das Passwort muss mindestens sechs Zeichen umfassen.

SSPR-Konfigurationspasswort

Gibt das Passwort an, mit dem die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung (SSPR) konfiguriert werden soll.

Standardmäßig umfasst SSPR kein Konfigurationspasswort. Ohne Passwort kann jeder Benutzer, der sich bei SSPR anmeldet, auch die Konfigurationseinstellungen bearbeiten.

Dienstpasswort

Gibt das Passwort für den Single-Sign-On-Client für SSPR, die Identitätsanwendungen und die Identitätsberichterstellung an.

Das Passwort muss mindestens sechs Zeichen umfassen.

Passwort für Identitätsanwendungs-Administrator

Gibt das Passwort des Administrators für die Benutzeranwendung an. Dieses Konto wird während des Installationsvorgangs im Identitätsdepot erstellt und erhält die Rechte zum Ausführen von administrativen Tätigkeiten für den angegebenen Benutzercontainer für die Benutzeranwendung. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- Der Kontoname lautet standardmäßig `uaadmin`.
- Wenn Sie den Anwendungsserver, 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 Anwendung über die Seite **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* (https://www.netiq.com/documentation/idm45/agpro/data/agpropartadminapp.html) (Benutzeranwendung: Administrationshandbuch).

Passwort des idmadmin-Datenbankbenutzers

Gibt das Passwort des Administrators für die Datenbank der Identitätsanwendungen an.

Das Konto lautet standardmäßig `idmadmin`.

Port zum Herunterfahren von Tomcat

Gibt den Port an, über den alle Webapps und Tomcat sauber heruntergefahren werden sollen. Der Standardwert ist 8105.

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 8543.

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 8109.

Mit diesem Parameter geben Sie an, dass der Anwendungsserver den statischen Inhalt in der Web-Anwendung verwalten oder die SSL-Verarbeitung des Anwendungsservers nutzen soll.

Audit-Server-Host

Gibt den DNS-Namen oder die IP-Adresse des Servers an, auf dem die SIEM-Datenbank gehostet wird, die vom Event Auditing Service und von der Identitätsberichterstellung verwendet wird (Identity Information Warehouse). Verwenden Sie nicht `localhost`.

Sie können den Server für einen alternativen Revisionsdienst angeben, z. B. Event Auditing Service oder NetIQ Sentinel.

WICHTIG: Der Audit-Server muss installiert sein und ausgeführt werden, bevor Sie die Identitätsanwendungen konfigurieren können. Wenn die integrierte Installation nicht mit dem Audit-Server kommunizieren kann, schlägt die Konfiguration fehl.

Erweiterte Einstellungen

Alle verbleibenden Einstellungen sind unter **Erweiterte Einstellungen** aufgeführt. Sie müssen den Eintrag `localhost` im Feld **Identitätsanwendungs-Host** in eine IP-Adresse oder einen DNS-Namen ändern. Wenn Sie keine Änderungen unter **Erweiterte Einstellungen** vornehmen, werden die aufgeführten Standardeinstellungen im Konfigurationsprogramm herangezogen, und die Konfiguration schlägt fehl.

Identitätsanwendungs-Administrator

Gibt den Namen des Administratorkontos für die Identitätsanwendungen an. Der Standardwert lautet „uaadmin“.

Identitätsanwendungs-Host

Gibt die URL an, über die eine Verbindung zum Benutzeranwendungs-Client auf dem Anwendungsserver hergestellt werden soll. Verwenden Sie nicht `localhost`.

5.5 Identitätsberichterstellungsmodul

In diesem Abschnitt werden die Einstellungen für das Identitätsberichterstellungsmodul definiert. Im Programm werden nur die grundlegenden Parameter angezeigt. Sollen alle Parameter eingeblendet werden, klicken Sie auf **Erweiterte Einstellungen**.

WICHTIG: Für das Identitätsberichterstellungsmodul ist ein Event Auditing Service erforderlich. Der Event Auditing Service kann nur auf Linux-Computern ausgeführt werden. Wenn Sie die Installation auf einem Windows-Computer vornehmen, müssen Sie zunächst den Event Auditing Service auf einem Linux-Computer installieren, bevor Sie das Identitätsberichterstellungsmodul unter Windows konfigurieren können.

EAS-Systempasswort

Gilt nur für Windows-Server bzw. nur dann, wenn der Event Auditing Service nicht auf dem lokalen Computer ausgeführt wird.

Geben Sie das Systempasswort für das EAS-System an, das auf einem Linux-Computer installiert ist. Das Systempasswort befindet sich auf dem Linux-Computer in der Datei `activemqusers.properties` im Verzeichnis `/etc/opt/novell/sentinel_eas/config`.

Passwort des Benutzers 'idmrptsrv'

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

Das `idmrptsrv`-Konto wird während der Installation erstellt.

Passwort des Benutzers 'idmrptuser'

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

Das `idmrptuser`-Konto wird während der Installation erstellt.

dbauser-Passwort

Gibt das Passwort für den Administrator der SIEM-Datenbank an, die vom Event Auditing Service und von der Identitätsberichterstellung verwendet wird (Identity Information Warehouse).

Das `dbauser`-Konto wird während der Installation erstellt.

EAS-Server-Host

Gilt nur für Windows-Server bzw. nur dann, wenn der Event Auditing Service nicht auf dem lokalen Computer ausgeführt wird.

Geben Sie die IP-Adresse oder den DNS-Namen des Servers an, auf dem der Event Auditing Service und die PostgreSQL-Datenbank ausgeführt werden.

Datenbank-Port

Gilt nur für Windows-Server bzw. nur dann, wenn der Event Auditing Service nicht auf dem lokalen Computer ausgeführt wird.

Geben Sie den Port an, über den die PostgreSQL-Datenbank kommuniziert. Der Standardport ist 15432.

EAS dbauser-Passwort

Geben Sie das Passwort für den „dbauser“ der PostgreSQL-Datenbank an.

Gateway-Port des verwalteten Systems

Gibt den Port an, über den der MSGW-Treiber mit dem Identitätsdepot kommunizieren soll.

Der Standardwert ist 7707.

Data Collection Service-Host

Gibt den DNS-Namen oder die IP-Adresse des Servers an, auf dem der Datenerfassungsdienst gehostet wird. Verwenden Sie nicht `localhost`.

Erweiterte Einstellungen

Alle verbleibenden Einstellungen sind unter **Erweiterte Einstellungen** aufgeführt. Wenn Sie keine Änderungen unter **Erweiterte Einstellungen** vornehmen, werden die aufgeführten Standardeinstellungen im Konfigurationsprogramm herangezogen.

Untercontainersuche aktivieren

Geben Sie an, ob die Identitätsberichterstellungsmodule Suchvorgänge in Untercontainern unterstützen sollen. Standardmäßig ist diese Option aktiviert.

Sichere LDAP-Verbindungen verwenden

Geben Sie an, ob der Server über eine sichere LDAP-Verbindung kommunizieren soll.

Sie müssen außerdem den **LDAP-Port** angeben.

LDAP-Port

Gibt den Port für die Kommunikation mit dem Anwendungsserver an, auf dem das Identitätsdepot gehostet wird. Legen Sie hier denselben Wert fest, den Sie für **Sicherer LDAP-Port** in Abschnitt 5.1, „Identitätsdepot“, auf Seite 33 angegeben haben.

Alternativ können Sie einen Klartext-Port für die nicht sichere Kommunikation angeben. In diesem Fall wählen Sie nicht die Option **Sichere LDAP-Verbindungen verwenden**.

Tokenablaufswert (Minuten)

Geben Sie den Zeitraum ein, über den ein Token für die Authentifizierung aufbewahrt werden soll. Der Standardwert ist 60 Minuten.

Dauer und Einheiten für Beibehaltung abgeschlossener Berichte

Geben Sie den Zeitraum an, über den die abgeschlossenen Berichte im Identitätsberichterstellungsmodul beibehalten werden sollen, bevor sie gelöscht werden. Für einen Zeitraum von sechs Monaten wählen Sie beispielsweise die Option **Monat** als Dauer, und geben Sie den Wert `6` als Einheiten ein.

Anmeldeattribut für Untercontainer

Gibt das Anmeldeattribut an, mit dem Identity Manager den Teilbaum eines angegebenen Benutzercontainers beim Erfassen von Daten für Berichte durchsuchen soll. Der Standardwert lautet `cn`.

HINWEIS: Wenn Sie einen DN mit Sonderzeichen angeben, müssen diese unter Umständen mit einem Escape-Zeichen versehen werden. Weitere Informationen finden Sie in RFC 2253/4514, Abschnitt 2.

SMTP-Server-Host

Gibt den DNS-Namen oder die IP-Adresse des E-Mail-Servers an, über den das Identitätsberichterstellungsmodul die Benachrichtigungen senden soll. Der Standardwert lautet `localhost`. Ersetzen Sie diesen Eintrag durch eine gültige IP-Adresse oder einen gültigen DNS-Namen.

SMTP-Server-Port

Gibt die Portnummer für den E-Mail-Server an. Der Standardwert ist 435.

SMTP-Benutzer-ID

(Bedingt) Gibt die E-Mail-Adresse für die Authentifizierung an, wenn die Kommunikation mit dem E-Mail-Server authentifiziert werden soll.

Sie müssen außerdem die Option **Serverauthentifizierung für SMTP erforderlich** angeben.

SMTP-Benutzerpasswort

Gibt das Passwort für die E-Mail-Adresse an, die für die Authentifizierung herangezogen werden soll.

Standardmäßige E-Mail-Adresse

Gibt die E-Mail-Adresse an, die die Identitätsberichterstellung als Absender für E-Mail-Benachrichtigungen verwenden soll.

SSL für SMTP verwenden

Gibt an, ob die Kommunikation mit dem E-Mail-Server über SSL erfolgen soll. Die Option ist standardmäßig nicht aktiviert.

Serverauthentifizierung für SMTP erforderlich

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

Sie müssen außerdem Werte für **SMTP-Benutzer-ID** und **SMTP-Benutzerpasswort** angeben. Die Option ist standardmäßig nicht aktiviert.

5.6 Werkzeuge

In diesem Abschnitt werden die Einstellungen für die Identity Manager-Werkzeuge iManager, Analyzer und Designer definiert. Derzeit sind lediglich die Parameter für iManager programmierbar. Diese Parameter werden ausschließlich auf Linux-Computern während der Konfiguration aufgeführt. Sollen die Parameter eingeblendet werden, klicken Sie auf **Erweiterte Einstellungen**.

HINWEIS: Die angegebenen HTTP-Stack-Ports dürfen nicht mit den HTTP-Stack-Ports für das Identitätsdepot identisch sein. Weitere Informationen finden Sie im *iManager-Administrationshandbuch* (https://www.netiq.com/documentation/imanager27/imanager_admin/data/hk42s9ot.html).

HTTP-Port

Gibt die Nummer des Stack-Ports an, über den iManager im Klartext kommuniziert. Der Standardwert ist 8080.

Sicherer HTTP-Port

Gibt die Nummer des Stack-Ports an, über den iManager über das TLS/SSL-Protokoll kommuniziert. Der Standardwert ist 8443.

6 Abschließende Schritte bei der integrierten Installation

Nach Abschluss der integrierten Installation sind die Identity Manager-Komponenten installiert, und die grundlegende Konfiguration wurde vorgenommen. Sie müssen jedoch noch Treiber installieren und zusätzliche Konfigurationsschritte ausführen, damit die verschiedenen Komponenten voll funktionsfähig sind. Schließen Sie die Konfiguration Ihres Identity Manager-Systems mit den folgenden Schritten ab:

- **Treiber:** Für die Treiber steht jeweils ein eigenes Handbuch bereit, in dem die Installation und Konfiguration dieses Treibers erläutert wird. Weitere Informationen finden Sie auf der Website der Identity Manager 4.5-Treiberdokumentation (https://www.netiq.com/documentation/idm45drivers/).
- **Identitätsanwendungen:** Sie müssen die verschiedenen Identitätsanwendungen für Ihre Umgebung konfigurieren. Weitere Informationen finden Sie im *NetIQ Identity Manager User Application: Administration Guide* (https://www.netiq.com/documentation/idm45/agpro/data/bookinfo.html) (NetIQ Identity Manager-Benutzeranwendung: Administrationshandbuch).
- **Identitätsberichterstellung:** Sie müssen das Identitätsberichterstellungsmodul für Ihre Umgebung konfigurieren. Weitere Informationen finden Sie im *NetIQ Identity Reporting Module Guide* (https://www.netiq.com/documentation/idm45/reporting/data/bookinfo.html) (Handbuch zum NetIQ-Identitätsberichterstellungsmodul).

7 Aktivieren von Identity Manager-Produkten

In diesem Abschnitt wird erläutert, wie die Aktivierung der Identity Manager-Komponenten erfolgt. Die Komponenten von Identity Manager müssen innerhalb von 90 Tagen nach der Installation aktiviert werden, anderenfalls wird ihre Funktion eingestellt. Sie können Identity Manager-Produkte zu einem beliebigen Zeitpunkt während oder nach Ablauf der 90 Tage aktivieren. Aktivieren Sie die Identity Manager-Komponenten anhand der Angaben in den nachfolgenden Abschnitten.

7.1 Erwerb einer Produktlizenz für Identity Manager

Informationen zum Kauf einer Identity Manager-Produktlizenz für die Aktivierung des Produkts finden Sie auf der NetIQ Identity Manager-Bestellwebseite (https://www.netiq.com/products/identity-manager/advanced/how-to-buy/).

Wenn Sie eine Produktlizenz erworben haben, wird Ihnen von NetIQ die Kunden-ID zugesendet. Die E-Mail 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.

7.2 Installation einer Produktaktivierungsberechtigung

Die Produktaktivierungsberechtigung muss über iManager installiert werden.

So installieren Sie die Produktaktivierungsberechtigung:

1. Nach dem Erwerb einer Lizenz erhalten Sie von NetIQ eine E-Mail mit Ihrer Kunden-ID. Die E-Mail enthält 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:
   - Speichern Sie die Datei mit der Produktaktivierungsberechtigung an einem geeigneten Ort.

     oder
   - Öffnen Sie die Datei mit der Produktaktivierungsberechtigung und kopieren Sie ihren Inhalt in die Zwischenablage.

     Achten Sie darauf, dass in der Kopie keine zusätzlichen Zeilen oder Leerzeichen eingefügt werden. Markieren Sie den zu kopierenden Text vom ersten Gedankenstrich (-) der Berechtigung (----BEGINN DER PRODUKTAKTIVIERUNGSBERECHTIGUNG) bis zum letzten Gedankenstrich (-) der Berechtigung (ENDE DER PRODUKTAKTIVIERUNGSBERECHTIGUNG-----).
3. Öffnen Sie iManager.
4. Wählen Sie **Identity Manager > Identity Manager-Überblick**.

5 Navigieren Sie in der Baumstruktur zu einem Treibersatz, und wählen Sie diesen Treibersatz aus.

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 anschließend auf **Weiter**.

9 Führen Sie einen der folgenden Vorgänge aus:

- Geben Sie an, wo Sie den Identity Manager-Berechtigungsnachweis gespeichert haben, und klicken Sie auf **Weiter**.

  oder

- Kopieren Sie den Inhalt der Datei in den Textbereich und klicken Sie auf **Weiter**.

10 Klicken Sie auf **Fertig stellen**.

HINWEIS: Sie müssen jeden Treibersatz aktivieren, in dem ein Treiber vorhanden ist. Sie können mit dem Berechtigungsnachweis jeden Baum aktivieren.

7.3 Anzeigen der Produktaktivierungen für Identity Manager und Identity Manager-Treiber

Für die Treibersätze werden jeweils die Produktaktivierungsberechtigungen angezeigt, die Sie für die Identity Manager-Engine und die Identity Manager-Treiber installiert haben.

1 Öffnen Sie iManager.

2 Klicken Sie auf **Identity Manager** > **Identity Manager-Überblick**.

3 Navigieren Sie in der Baumstruktur zu einem Treibersatz, wählen Sie diesen Treibersatz aus, und starten Sie die Suche mit ▶.

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.

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 sollte dann nicht mehr angezeigt werden.

7.4 Aktivieren von Identity Manager-Treibern

Mit dem Kauf von Identity Manager haben Sie auch Aktivierungen für Service-Treiber und verschiedene allgemeine Treiber erworben.

- **Service-Treiber:** Beim Aktivieren der Identity Manager-Engine werden die folgenden Diensttreiber aktiviert:
  - Datenerfassungsdienst

    - Berechtigungsservices
    - ID-Provider
    - Loopback-Service
    - Verwaltetes System - Gateway
    - 'Manuelle Aufgabe'-Service
    - Null-Service
    - Rollenservice
    - Benutzeranwendung
    - Auftrag
- **Allgemeine Treiber:** Beim Aktivieren der Identity Manager-Engine werden die folgenden allgemeinen Treiber aktiviert:
    - Active Directory
    - ADAM
    - eDirectory
    - GroupWise
    - LDAP
    - Lotus Notes

Aktivierungen für alle anderen Identity Manager-Treiber müssen separat erworben werden. Die Aktivierungen für die Treiber sind als Identity Manager-Integrationsmodule erhältlich. Ein Identity Manager-Integrationsmodul kann einen oder mehrere Treiber enthalten. Sie erhalten für jedes erworbene Identity Manager-Integrationsmodul eine Produktaktivierungsberechtigung.

Sie müssen die Schritte in Abschnitt 7.2, „Installation einer Produktaktivierungsberechtigung“, auf Seite 47 für jedes Identity Manager-Integrationsmodul ausführen, um die Treiber zu aktivieren.

7.5 Aktivieren von Analyzer

Wenn Sie Analyzer zum ersten Mal starten, werden Sie zur Aktivierung aufgefordert. Wenn Sie die Aktivierung nicht vornehmen, können Sie Analyzer nicht verwenden.

7.6 Aktivieren von Designer und dem Rollenzuordnungsadministrator

Für Designer und den Rollenzuordnungsadministrator sind keine weiteren Aktivierungen neben der Aktivierung der Identity Manager-Engine und der Treiber erforderlich.

8 Deinstallation von Identity Manager

Sie können alle installierten Identity Manager-Komponenten wahlweise mit dem Assistenten für die integrierte Deinstallation oder im Rahmen einer automatischen Deinstallation wieder deinstallieren.

8.1 Verwenden des Deinstallationsassistenten

Bevor Sie die integrierte Deinstallation starten, stellen Sie sicher, dass die Umgebungsvariablen `JAVA_HOME` und `PATH` auf Java verweisen.

So deinstallieren Sie die Identity Manager-Komponenten:

1. Führen Sie die Deinstallation aus, indem Sie das entsprechende Programm für Ihre Plattform verwenden:
   - **Linux:** `./Uninstall_Identity_Manager`

     Die Binärdatei befindet sich standardmäßig im Verzeichnis `/root/idm/Uninstall_Identity_Manager`.
   - **Windows:** `Uninstall_Identity Manager Components.exe`

     Das Deinstallationsprogramm befindet sich standardmäßig im Verzeichnis `C:/Programme/NetIQ/Identity Manager` directory. Alternativ klicken Sie auf **Software**, und deinstallieren Sie die Identity Manager-Komponenten.

     HINWEIS: Durch die Deinstallation des Identitätsdepots werden nicht alle Dateien entfernt. Weitere Informationen finden Sie in der Dokumentation zur Deinstallation von eDirectory (https://www.netiq.com/documentation/edir88/edirin88/data/bnn8twh.html).
2. Aktivieren Sie die Kontrollkästchen neben den Komponenten, die Sie deinstallieren möchten, und klicken Sie anschließend auf **Weiter**.
3. Geben Sie die Berechtigungsnachweise für die einzelnen Komponenten im LDAP-Format an, und klicken Sie auf **Weiter**.

   Das Deinstallationsprogramm benötigt die Berechtigungsnachweise für die Dekonfiguration der Komponenten vor der Deinstallation.
4. Lesen Sie die Zusammenfassung für die Deinstallation der Komponenten und klicken Sie anschließend auf **Deinstallieren**.

   Falls Änderungen an Ihren Komponenten erforderlich sind, klicken Sie auf **Zurück** und nehmen Sie die entsprechenden Änderungen vor.
5. Überprüfen Sie die Seite mit der Zusammenfassung der abgeschlossenen Deinstallation, die die Liste der Komponenten enthält, die erfolgreich deinstalliert wurden, und klicken Sie anschließend auf **Fertig**, um den Deinstallationsprozess abzuschließen.

8.2 Ausführen einer automatischen Deinstallation

Zum Ausführen einer automatischen Deinstallation der Identity Manager-Komponenten müssen Sie eine Eigenschaftendatei mit den für die Deinstallation erforderlichen Parametern erstellen. Auf dem Identity Manager-Datenträger ist eine Beispieldatei vorhanden:

- **Linux:** `./install/propfiles/uninstall.properties`
- **Windows:** `\install\propfiles\uninstall.properties`

Starten Sie die automatische Deinstallation, indem Sie das entsprechende Programm für Ihre Plattform ausführen:

- **Linux:** `/root/idm/Uninstall_Identity Manager/Uninstall_Identity_Manager.bin -i silent -f` *`Dateiname`*`.properties`
- **Windows:** *`Installationsort`*`\Uninstall_Identity Manager Components/Uninstall Identity Manager Components.exe -i silent -f` *`Dateiname`*`.properties`

9 Fehlersuche

Nehmen Sie die Fehlersuche beim Programm zur integrierten Installation anhand der nachfolgenden Informationen vor.

9.1 Speicherorte der Protokolldateien und Eigenschaftendateien

Die folgende Tabelle enthält den Speicherort für das Installationsprotokoll (`ii_install.log`), das Konfigurationsprotokoll (`ii_configure.log`) und die Eigenschaftsdateien. Für jede installierte Komponente ist eine Eigenschaftendatei vorhanden.

Plattform	Protokolldateien	Installationseigenschaftendateien
Windows	*<Installationsverzeichnis>*`\install\logs` Der standardmäßige Speicherort lautet `C:\netiq\IdentityManager\install\logs`	*<Installationsverzeichnis>*`\install\propfiles` Der standardmäßige Speicherort lautet `C:\netiq\IdentityManager\install\logs\propfiles\`
Linux	`/var/opt/netiq/idm/install/logs`	`/var/opt/netiq/idm/install/logs/propfiles/`

9.2 Fehlersuche bei der Konfiguration

Nehmen Sie die Fehlersuche bei der Konfiguration von Komponenten anhand der folgenden Informationen vor:

Problem: Die Konfiguration der Identitätsanwendungen schlägt fehl.

Vorgeschlagene Gegenmaßnahme: Greifen Sie auf die Protokolldateien zu. Suchen Sie das Wort `localhost`. Wenn dieses Wort in den Protokollen vorliegt, haben Sie den Standardwert `localhost` unter **Erweiterte Einstellungen** während der Konfiguration nicht durch eine gültige IP-Adresse oder einen gültigen DNS-Namen ersetzt. Führen Sie die Konfiguration erneut aus, und geben Sie unter **Erweiterte Einstellungen** eine gültige IP-Adresse oder einen gültigen DNS-Namen ein.

9.3 Fehlersuche bei Problemen mit Remote Loader unter Windows

Standardmäßig werden alle Identity Manager-Komponenten bei der integrierten Installation im Verzeichnis `C:\NetIQ` installiert. Für alle Treiber gilt das Standardverzeichnis `C:\Novell`. Sie können jedoch das Verzeichnis für die Treiber manuell ändern, sodass die Treiber ordnungsgemäß funktionieren.

So sorgen Sie für die Funktionsfähigkeit der Remote Loader-Treiber:

1. Starten Sie die Remote Loader-Konsole.

2 Fügen Sie eine Instanz des entsprechenden Treibers hinzu.

3 Ändern Sie den Standardpfad von `C:\Novell` in `C:\NetIQ`.

4 Fahren Sie mit den normalen Konfigurationsschritten fort.

9.4 Fehlersuche bei der Deinstallation

Informieren Sie sich anhand der nachfolgenden Informationen über die Fehlersuche bei Problemen während der Deinstallation. Falls das Problem weiterhin auftritt, wenden Sie sich an Ihren zuständigen NetIQ-Ansprechpartner.

Problem: Die Deinstallation meldet, dass der Deinstallationsvorgang nicht abgeschlossen wurde, in der Protokolldatei sind jedoch keine Fehler vermerkt.

Vorgeschlagene Gegenmaßnahme: 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 manuell löschen.