

# Handbuch zur integrierten Installation

## Novell® Identity Manager

**4.0.1**

15. April 2011

[www.novell.com](http://www.novell.com)



## Rechtliche Hinweise

Novell, Inc. übernimmt für Inhalt oder Verwendung dieser Dokumentation keine Haftung und schließt insbesondere jede ausdrückliche oder implizite Garantie für Marktfähigkeit oder Eignung für einen bestimmten Zweck aus.

Novell, Inc. behält sich das Recht vor, dieses Dokument jederzeit teilweise oder vollständig zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen davon in Kenntnis zu setzen.

Novell, Inc. gibt ebenfalls keine Erklärungen oder Garantien in Bezug auf Novell-Software und schließt insbesondere jede ausdrückliche oder implizite Garantie für handelsübliche Qualität oder Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc. das Recht vor, Novell-Software jederzeit ganz oder teilweise zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen von diesen Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie erkennen alle Ausfuhrkontrollbestimmungen an und erklären sich damit einverstanden, alle für ausstehende Exporte, Re-Exporte oder Importe erforderlichen Lizenzen bzw. Klassifizierungen einzuholen. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen aufgeführte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Export von Novell-Software finden Sie auf der Webseite [Novell International Trade Services \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Copyright © 2011 Novell, Inc. Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Herausgebers darf kein Teil dieser Veröffentlichung reproduziert, fotokopiert, übertragen oder in einem Speichersystem verarbeitet werden.

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
USA.  
[www.novell.com](http://www.novell.com)

*Online-Dokumentation:* Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der [Dokumentations-Webseite von Novell \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

## Novell-Marken

Hinweise zu Novell-Marken finden Sie in der [Novell Trademark and Service Mark-Liste \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

## Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

# Inhalt

<b>Informationen zu diesem Handbuch</b>	<b>5</b>
<b>1 Überblick über das integrierte Installationsprogramm</b>	<b>7</b>
1.1 Integriertes und eigenständiges Installationsprogramm . . . . .	7
1.2 Konfigurieren von Treibern . . . . .	8
1.3 Unterschiede bei der Installation von Identity Manager 4.0.1 Standard Edition und Advanced Edition . . . . .	9
<b>2 Identity Manager-Komponenten</b>	<b>11</b>
2.1 Metaverzeichnis-Server (Identitätsdepot, Metaverzeichnis-Engine und Remote Loader) . . . . .	12
2.2 Unterstützte Prozessoren . . . . .	12
2.3 Server-Betriebssysteme . . . . .	12
2.4 Revision und Berichterstellung . . . . .	13
2.5 Benutzeranwendung . . . . .	14
2.6 Rollenzuordnungsadministrator . . . . .	14
2.7 iManager, Designer und Analyzer . . . . .	15
2.8 Webbrowser . . . . .	16
2.9 Identitätsdepot-Struktur . . . . .	16
2.9.1 Sicherheit . . . . .	17
2.9.2 Daten . . . . .	17
2.9.3 System . . . . .	17
<b>3 Systemanforderungen</b>	<b>19</b>
3.1 Unterstützte Plattformen . . . . .	19
3.2 Ressourcenanforderungen . . . . .	20
<b>4 Installation von Identity Manager</b>	<b>21</b>
4.1 Herunterladen der ISO-Datei . . . . .	21
4.2 Neuinstallation mithilfe physischer Medien oder einer ISO-Imagedatei . . . . .	23
4.2.1 Installation . . . . .	23
4.2.2 Konfiguration . . . . .	24
4.3 Verfahren nach Abschluss der Installation . . . . .	34
4.4 Automatische Installation und Konfiguration . . . . .	35
4.4.1 Automatische Installation . . . . .	36
4.4.2 Automatische Konfiguration . . . . .	36
<b>5 Aktivieren von Novell Identity Manager-Produkten</b>	<b>39</b>
5.1 Erwerb einer Produktlizenz für Identity Manager . . . . .	39
5.2 Installation einer Produktaktivierungsberechtigung . . . . .	39
5.3 Anzeigen der Produktaktivierungen für Identity Manager und Identity Manager-Treiber . . . . .	40
5.4 Aktivieren von Identity Manager-Treibern . . . . .	41
5.5 Aktivieren von Analyzer . . . . .	42
5.6 Aktivieren von Designer und dem Rollenzuordnungsadministrator . . . . .	42

<b>6</b>	<b>Aufrüsten von Identity Manager</b>	<b>43</b>
<b>7</b>	<b>Fehlerbehebung in Identity Manager</b>	<b>45</b>
<b>8</b>	<b>Deinstallation von Identity Manager</b>	<b>51</b>
8.1	GUI-Deinstallation . . . . .	51
8.2	Automatische Deinstallation . . . . .	52

# Informationen zu diesem Handbuch

Novell Identity Manager 4.0.1 ist ein Service für die Datenfreigabe und -synchronisierung, mit dessen Hilfe Anwendungen, Verzeichnisse und Datenbanken Informationen gemeinsam nutzen können. Er verbindet über mehrere Verzeichnisse verstreute Informationen und ermöglicht Ihnen das Einrichten von Richtlinien für die automatische Aktualisierung designierter Systeme bei Identitätsänderungen.

Identity Manager bietet die Grundlage für Kontenbereitstellung, Sicherheit, Single Sign-on, Benutzerselbstbedienung, Authentifizierung, Autorisierung, automatisierten Workflow und Webservices. Das Programm ermöglicht Ihnen, die verteilten Identitätsinformationen zu integrieren, zu verwalten und zu steuern, sodass Sie den richtigen Personen die richtigen Ressourcen auf sichere Weise zur Verfügung stellen können.

Dieses Handbuch enthält Informationen zur Installation, zum Aufrüsten und zur Deinstallation eines Identity Manager-Systems, das auf Ihre Umgebung zugeschnitten ist.

- ♦ [Kapitel 1, „Überblick über das integrierte Installationsprogramm“, auf Seite 7](#)
- ♦ [Kapitel 2, „Identity Manager-Komponenten“, auf Seite 11](#)
- ♦ [Kapitel 3, „Systemanforderungen“, auf Seite 19](#)
- ♦ [Kapitel 4, „Installation von Identity Manager“, auf Seite 21](#)
- ♦ [Kapitel 5, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 39](#)
- ♦ [Kapitel 6, „Aufrüsten von Identity Manager“, auf Seite 43](#)
- ♦ [Kapitel 7, „Fehlerbehebung in Identity Manager“, auf Seite 45](#)
- ♦ [Kapitel 8, „Deinstallation von Identity Manager“, auf Seite 51](#)

## Zielgruppe

Dieses Handbuch richtet sich an Administratoren, Berater und Netzwerkingenieure, die für die Planung und Implementierung von Identity Manager in einer Netzwerkkumgebung zuständig sind.

## Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Bitte verwenden Sie die Benutzerkommentarfunktion unten auf der jeweiligen Seite der Online-Dokumentation oder wählen Sie [www.novell.com/documentation/feedback.html](http://www.novell.com/documentation/feedback.html), und geben Sie dort Ihre Kommentare ein.

## Aktualisierungen der Dokumentation

Die neueste Version dieses Dokuments finden Sie auf der [Website zur Identity Manager-Dokumentation \(http://www.novell.com/documentation/idm40/index.html\)](http://www.novell.com/documentation/idm40/index.html).

## **Zusätzliche Dokumentation**

Weitere Dokumentation zu Identity Manager finden Sie auf der [Website zur Identity Manager-Dokumentation](http://www.novell.com/documentation/idm40/index.html) (<http://www.novell.com/documentation/idm40/index.html>).

Dokumentation zur Benutzeranwendung finden Sie auf der [Website zur Identity Manager-Dokumentation](http://www.novell.com/documentation/idm40/index.html) (<http://www.novell.com/documentation/idm40/index.html>).

# Überblick über das integrierte Installationsprogramm

# 1

Identity Manager 4.0.1 bietet erstklassige Unterstützung für eine unternehmensweite Richtlinieneinhaltung und geringere Kosten für das Identitätsmanagement und die Bereitstellung, von der Rechenzentrums Umgebung bis hin zur Cloud-Umgebung. Das integrierte Installationsprogramm vereinfacht die Bereitstellung von Identity Manager 4.0.1 für Administratoren und Berater. Es handelt sich um ein vereinfachtes Installationsprogramm, das Sie bei der schnellen Einrichtung eines Systems unterstützt, da es die separate Installation jeder einzelnen Komponente überflüssig macht.

- ♦ [Abschnitt 1.1, „Integriertes und eigenständiges Installationsprogramm“, auf Seite 7](#)
- ♦ [Abschnitt 1.2, „Konfigurieren von Treibern“, auf Seite 8](#)
- ♦ [Abschnitt 1.3, „Unterschiede bei der Installation von Identity Manager 4.0.1 Standard Edition und Advanced Edition“, auf Seite 9](#)

## 1.1 Integriertes und eigenständiges Installationsprogramm

*Tabelle 1-1 Vergleich zwischen dem integrierten und dem eigenständigen Installationsprogramm*

Funktionen	Integriert	Eigenständig
Baumstruktur	Die Baumstruktur ist für die meisten Identity Manager-Bereitstellungen passend vordefiniert. Weitere Informationen zur Baumstruktur finden Sie in <a href="#">Abschnitt 2.9, „Identitätsdepot-Struktur“, auf Seite 16</a> .	Die Baumstruktur ist benutzerdefinierbar.
Benutzerdefinierte Treiberinstallation	Alle Treiber werden standardmäßig installiert.	Die benutzerdefinierte Installation von Treibern wird unterstützt.
Treibersatz	Während der Metaverzeichnis-Serverkonfiguration als separate Partition erstellt.	Nicht erstellt. Kann manuell mit iManager erstellt werden.
Nicht-root-Installation	Nicht unterstützt.	Die Nicht-root-Installation mancher Komponenten wird unterstützt.
iManager-Plugin-Installation	Automatisch installiert.	Manuell installiert.
Abhängigkeiten	Verarbeitet Abhängigkeiten automatisch.	Abhängigkeiten werden manuell verarbeitet.

Funktionen	Integriert	Eigenständig
Installationsdauer	Automatisiert verschiedene manuelle Schritte für die schnelle Einrichtung des Systems.	Dauert in der Regel länger.
Benutzereingabe-Optionen	Die Benutzeroberfläche besitzt weniger Optionen und erfordert daher weniger Benutzereingaben. Verschiedene Optionen nehmen Standardwerte an.	Die Benutzeroberfläche besitzt verschiedene Optionen, daher müssen Sie mit allen Komponenten gut vertraut sein.
Prüfungen unterstützter Plattformen	Prüft die Plattformunterschiede intern.	Führt keine Plattformprüfung durch.
Behandlung von Inkonsistenzen	Konsistente Benutzerführung über verschiedene Komponenten und Plattformen hinweg.	Es können Inkonsistenzen auftreten.
Installations- und Konfigurationsphasen	Separate Installations- und Konfigurationsphasen.	Ist bei verschiedenen Komponenten unterschiedlich.

Wenn Sie eine Identity Manager-Lösung erstellen, bei der Sie eine oder mehrere der Identity Manager-Komponenten separat installieren müssen oder einen großen Umfang an benutzerdefinierten Optionen benötigen, ziehen Sie für die Installation das [Identity Manager 4.0.1 Framework Installationshandbuch](#) zu Rate. Installationsanweisungen finden Sie im Abschnitt „Installation“ im [Identity Manager 4.0.1 Framework Installationshandbuch](#).

Das integrierte Installationsprogramm wird hauptsächlich für neue Installationen von Identity Manager 4.0.1 verwendet. Informationen zum Aufrüsten einer vorhandenen Installation finden Sie in [Kapitel 6, „Aufrüsten von Identity Manager“](#), auf Seite 43.

Zurzeit unterstützt das integrierte Installationsprogramm zwei Installationsmodi: die Installation über die Benutzeroberfläche und die automatische Installation. Der Konsolenmodus wird nicht unterstützt.

## 1.2 Konfigurieren von Treibern

Die folgenden Identity Manager 4.0.1-Komponenten können mit dem integrierten Installationsprogramm installiert und konfiguriert werden:

- ◆ Metaverzeichnis-Server (Identitätsdepot, Metaverzeichnis-Engine und Remote Loader)
- ◆ Rollenbasiertes Bereitstellungsmodul
- ◆ Identitätsberichterstellungsmodul
- ◆ Event Auditing Service
- ◆ Rollenzuordnungsadministrator
- ◆ iManager
- ◆ Designer
- ◆ Analyzer



Das integrierte Installationsprogramm konfiguriert die erforderlichen Treiber für das rollenbasierte Bereitstellungsmodul und das Identitätsberichterstellungsmodul. Informationen zum Konfigurieren zusätzlicher Treiber finden Sie auf der [Website zur Identity Manager 4.0.1 Treiber-Dokumentation \(http://www.novell.com/documentation/idm401drivers/\)](http://www.novell.com/documentation/idm401drivers/).

## 1.3 Unterschiede bei der Installation von Identity Manager 4.0.1 Standard Edition und Advanced Edition

Identity Manager 4.0.1 ist in der Advanced Edition und in der Standard Edition verfügbar. Es gibt separate ISO-Imagedateien für jede Ausführung. Die Installationsprogramme für die Advanced Edition und Standard Edition weisen einige Unterschiede auf:

**Der Rollenzuordnungsadministrator ist nicht in der Standard Edition enthalten:** Der Rollenzuordnungsadministrator ist nicht in der Liste der Identity Manager-Komponenten auf der Seite „Komponenten auswählen“ des integrierten Installationsprogramms enthalten.

**Die Konfiguration des Messaging-Gateway-Treibers wird nicht unterstützt:** Sie können den Messaging-Gateway-Treiber in der Standard Edition nicht über das integrierte Installationsprogramm konfigurieren.

**Es wurden zwei weitere Administratorrollen für die Benutzeranwendung hinzugefügt:** In der Standard Edition wurden zusätzlich zum Benutzeranwendungsadministrator die Rollen „Berichtsadministrator“ und „Sicherheitsadministrator“ hinzugefügt. Sie müssen die Berechtigungsnachweise für den Berichtsadministrator und den Sicherheitsadministrator angeben, während Sie die Benutzeranwendung über das integrierte Installationsprogramm konfigurieren.

**Es wurden neue Berichte zum Identitätsberichterstellungsmodul hinzugefügt:** Drei neue Berichte wurden zum Identitätsberichterstellungsmodul hinzugefügt. Einige der Berichte für Daten wie z. B. Rollen, Ressourcen und Workflow-Prozesse sind in der Standard Edition nicht verfügbar. Weitere Informationen zu neuen Berichten finden Sie im Abschnitt „[Neue Funktionen von Identity Manager 4.0.1](#)“ im *Identity Manager 4.0.1 Übersichtshandbuch*.

Weitere Informationen zur Installation von Identity Manager finden Sie in [Kapitel 4, „Installation von Identity Manager“](#), auf Seite 21.

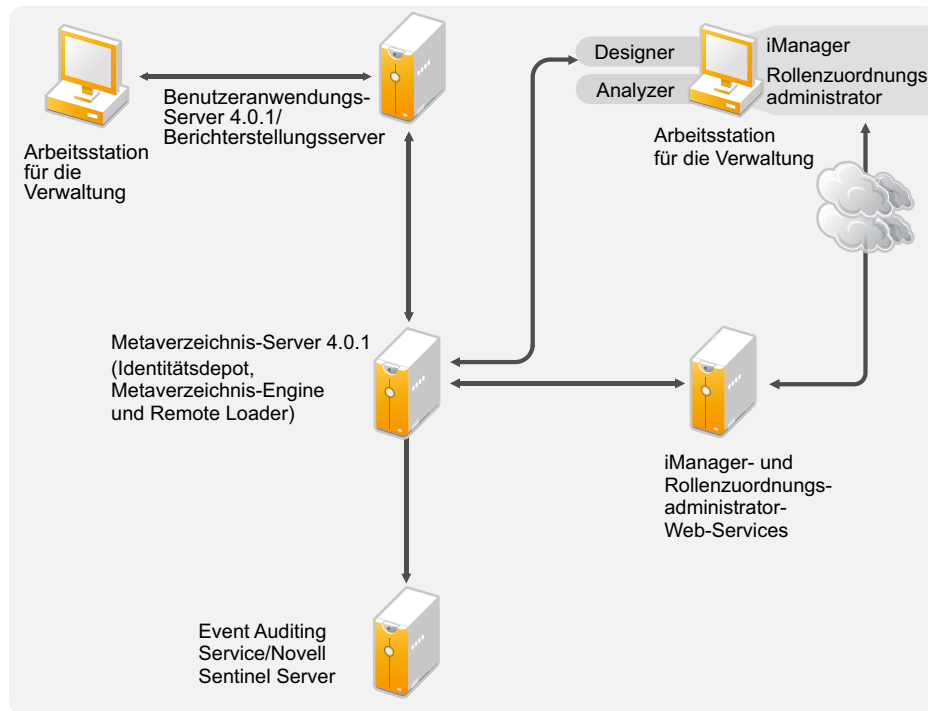


# Identity Manager-Komponenten

# 2

Mithilfe des integrierten Installationsprogramms von Identity Manager können Sie die folgenden Komponenten installieren. Die Identity Manager-Komponenten müssen nicht auf demselben System installiert werden. [Abbildung 2-1](#) zeigt, welche Plattformen und Systeme unterstützt werden.

**Abbildung 2-1** Komponenten des integrierten Installationsprogramms von Identity Manager



- ◆ [Abschnitt 2.1](#), „Metaverzeichnis-Server (Identitätsdepot, Metaverzeichnis-Engine und Remote Loader)“, auf Seite 12
- ◆ [Abschnitt 2.2](#), „Unterstützte Prozessoren“, auf Seite 12
- ◆ [Abschnitt 2.3](#), „Server-Betriebssysteme“, auf Seite 12
- ◆ [Abschnitt 2.4](#), „Revision und Berichterstellung“, auf Seite 13
- ◆ [Abschnitt 2.5](#), „Benutzeranwendung“, auf Seite 14
- ◆ [Abschnitt 2.6](#), „Rollenzuordnungsadministrator“, auf Seite 14
- ◆ [Abschnitt 2.7](#), „iManager, Designer und Analyzer“, auf Seite 15
- ◆ [Abschnitt 2.8](#), „Webbrowser“, auf Seite 16
- ◆ [Abschnitt 2.9](#), „Identitätsdepot-Struktur“, auf Seite 16

## 2.1 Metaverzeichnis-Server (Identitätsdepot, Metaverzeichnis-Engine und Remote Loader)

Der Metaverzeichnis-Server verarbeitet die Treiberereignisse, und zwar unabhängig davon, ob die Treiber für die Verwendung des Remote Loaders konfiguriert sind.

Während der Installation von Identity Manager wird das Identitätsdepot automatisch installiert.

## 2.2 Unterstützte Prozessoren

Die hier aufgelisteten Prozessoren werden auch zum Testen von Identity Manager verwendet.

Die folgenden 32-Bit-Prozessoren für Linux- (SUSE Linux Enterprise Server) und Windows-Betriebssysteme werden unterstützt:

- ♦ Intel x86-32
- ♦ AMD x86-32

Die folgenden 64-Bit-Prozessoren für Linux- (SUSE Linux Enterprise Server) und Windows-Betriebssysteme werden unterstützt:

- ♦ Intel EM64T
- ♦ AMD Athlon64
- ♦ AMD Opteron

Der SPARC-Prozessor wird für Solaris-Tests verwendet.

## 2.3 Server-Betriebssysteme

Sie können die Metaverzeichnis-Engine als 32-Bit-Anwendung auf einem 32-Bit-Betriebssystem und als 64-Bit-Anwendung auf einem 64-Bit-Betriebssystem installieren. [Tabelle 2-1](#) enthält eine Liste der unterstützten Server-Betriebssysteme, auf denen der Metaverzeichnis-Server ausgeführt werden kann.

**Tabelle 2-1** *Unterstützte Serverbetriebssysteme*

Version des Server-Betriebssystems	Hinweise
Windows Server 2003 SP2 (32 Bit)	Der Metaverzeichnis-Server läuft nur im 32-Bit-Modus.
Windows Server 2008 R2 (64 Bit)	Der Metaverzeichnis-Server läuft nur im 64-Bit-Modus.
Support-Pakete für Windows Server 2008 oder höher (32 Bit und 64 Bit)	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus.
SUSE Linux Enterprise Server 10 SP3 (32 Bit und 64 Bit)	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.

Version des Server-Betriebssystems	Hinweise
SUSE Linux Enterprise Server 11 (32 Bit und 64 Bit)	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.
SUSE Linux Enterprise Server 11 SP1 (32 Bit und 64 Bit)	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.
Solaris 10 (64 Bit)	Der Metaverzeichnis-Server läuft nur im 64-Bit-Modus.

**Tabelle 2-2** *Unterstützte Virtualisierungs-Betriebssysteme*

Version des Server-Betriebssystems	Hinweise
Xen	Xen wird unterstützt, wenn die Xen Virtual Machine als Gastbetriebssystem entweder SLES 10 oder SLES 11 im paravirtualisierten Modus ausführt.
Windows Server 2008 R2 Virtualisierung mit Hyper-V	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus.
VMware ESX	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus.

**Hinweis:** Open Enterprise Server 2 wird vom integrierten Identity Manager-Installationsprogramm nicht unterstützt.

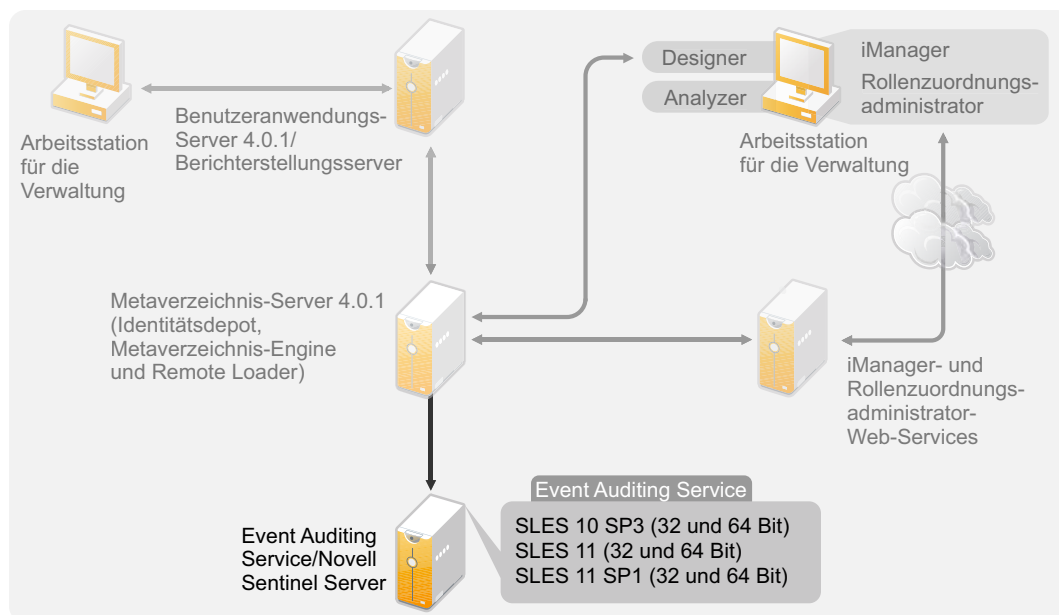
## 2.4 Revision und Berichterstellung

Durch die Erweiterung um die Funktionen für die Revision und die Berichterstellung können Sie die Konformitätsstandards erfüllen, die von vielen Unternehmen eingehalten werden müssen. Sie können Revisionsprotokolle für alle zu protokollierenden Ereignisse erstellen und Berichte erzeugen, um sicherzustellen, dass Sie alle für Ihr Unternehmen geltenden Revisionsstandards erfüllen.

Das Identitätsberichterstellungsmodul und Novell Sentinel sind zwei unterschiedliche Werkzeuge, die zum Erfassen von Revisions- und Berichtsdaten über Identity Manager verwendet werden.

Das Identitätsberichterstellungsmodul ist eine Komponente von Identity Manager 4.0.1. Novell Sentinel ist nicht im Lieferumfang von Identity Manager enthalten, sondern kann als optionale Komponente zum Identity Manager-System hinzugefügt werden.

Abbildung 2-2 Revision und Berichterstellung



Weitere Informationen zu den Systemanforderungen des Identitätsberichterstellungsmoduls finden Sie im Abschnitt „[System Requirements](#)“ (Systemanforderungen) im [Identity Reporting Module Guide](#) (Handbuch zum Identitätsberichterstellungsmodul). Informationen zur Konfiguration von Novell Sentinel mit Identity Manager finden Sie im [Identity Manager 4.0.1 Reporting Guide for Novell Sentinel](#) (Identity Manager 3.6 Berichtshandbuch für Novell Sentinel). Informationen zu den Systemanforderungen für Novell Sentinel finden Sie im [Novell Sentinel Installation Guide](http://www.novell.com/documentation/sentinel6/index.html) (<http://www.novell.com/documentation/sentinel6/index.html>) (Novell Sentinel Installationshandbuch).

## 2.5 Benutzeranwendung

Die Identity Manager-Benutzeranwendung ermöglicht Ihnen den Zugriff auf die Informationen, Rollen, Ressourcen und Funktionen von Identity Manager. Der Systemadministrator legt fest, welche Informationen Sie in der Identity Manager-Benutzeranwendung anzeigen und welche Aufgaben Sie ausführen dürfen.

Das Rollenbasierte Bereitstellungsmodul 4.0.1 verwendet JBoss 5.1 als Anwendungsserver und PostgreSQL 8.4.3 als Datenbank.

Eine Liste der Systemanforderungen für die Benutzeranwendung finden Sie im Abschnitt „[System Requirements](#)“ (Systemanforderungen) im [Identity Manager Roles Based Provisioning Module 4.0.1 User Application: Installation Guide](#) (Rollenbasiertes Bereitstellungsmodul für Identity Manager 4.0.1 Benutzeranwendung: Installationshandbuch).

## 2.6 Rollenzuordnungsadministrator

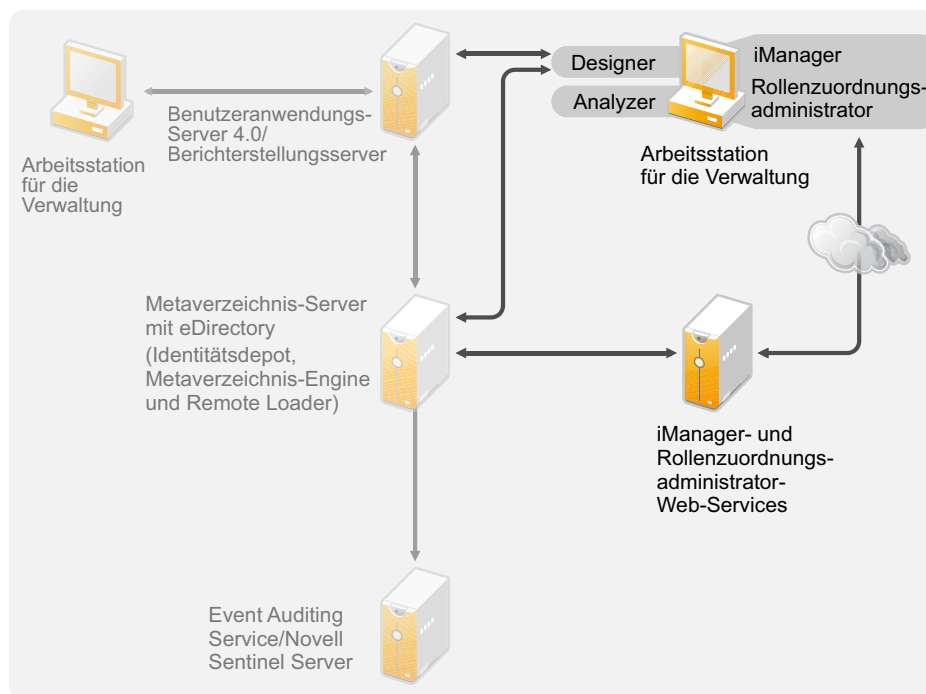
Der Novell Identity Manager-Rollenzuordnungsadministrator ermöglicht Ihnen die Zuordnung von Rollen verwalteter Systeme, zusammengefassten Rollen und Profilen (in ihrer Gesamtheit als Autorisierungen bezeichnet) zu Identity Manager-Rollen. Wenn einem Benutzer über das rollenbasierte Bereitstellungsmodul für Identity Manager eine Rolle zugewiesen wird, erhält er alle Autorisierungen, die der Rolle zugeordnet sind. Eine Liste der Systemanforderungen für den

Rollenzuordnungsadministrator finden Sie im Abschnitt „[System Requirements](#)“ (Systemanforderungen) im *Novell Identity Manager Role Mapping Administrator 4.0.1 User Guide* (Benutzerhandbuch zum Novell Identity Manager-Rollenzuordnungsadministrator 4.0.1).

## 2.7 iManager, Designer und Analyzer

Wählen Sie zur Installation von iManager, Designer, Analyzer und dem Rollenzuordnungsadministrator diese Komponenten mithilfe der entsprechenden Kontrollkästchen auf der Seite „Komponenten auswählen“ der Installation einzeln aus. [Abbildung 2-3](#) veranschaulicht diese Komponenten.

**Abbildung 2-3** Werkzeuge für Identity Manager



Informationen zu den Systemanforderungen finden Sie in der jeweiligen Komponentendokumentation.

- ♦ iManager: Siehe Abschnitt [Installieren von iManager](http://www.novell.com/documentation/imanager27/imanager_install_274/data/alw39eb.html) ([http://www.novell.com/documentation/imanager27/imanager\\_install\\_274/data/alw39eb.html](http://www.novell.com/documentation/imanager27/imanager_install_274/data/alw39eb.html)) im *Novell iManager 2.7 Installationshandbuch*.
- ♦ Designer: Siehe Abschnitt „[System Requirements](#)“ (Systemanforderungen) im *Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide* (Administrationshandbuch zu Designer 4.0.1 für Identity Manager 4.0.1).
- ♦ Analyzer: Siehe Abschnitt „[Installing Analyzer](#)“ (Analyzer installieren) im *Analyzer 4.0.1 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.1 für Identity Manager).
- ♦ Rollenzuordnungsadministrator: Siehe Abschnitt „[System Requirements](#)“ (Systemanforderungen) im *Identity Manager Role Mapping Administrator 4.0.1 Installation and Configuration Guide* (Identity Manager Rollenzuordnungsadministrator 4.0.1 Installations- und Konfigurationshandbuch).

## 2.8 Webbrowser

Zur Verwaltung von Identity Manager werden die folgenden Webbrowser unterstützt:

- ♦ Internet Explorer 6 SP2
- ♦ Internet Explorer 7 und 8
- ♦ Firefox 3, 3.5.x und 3.6.x

## 2.9 Identitätsdepot-Struktur

Die Identitätsdepot-Struktur ist für die meisten Identity Manager-Bereitstellungen passend vordefiniert.

Abbildung 2-4 Identitätsdepot-Struktur

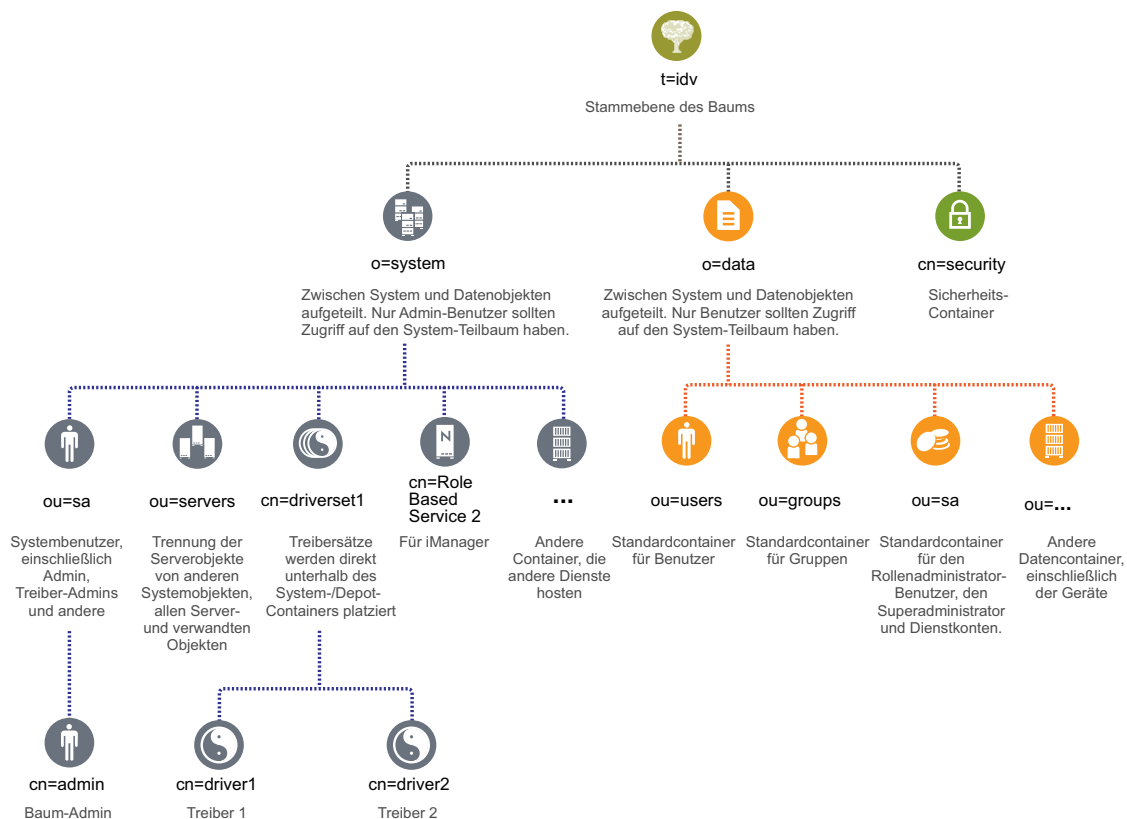


Abbildung 2-4 stellt die Identitätsdepot-Struktur für Identity Manager dar. Diese Struktur ist hauptsächlich für eine Installation in einer einzelnen Umgebung nützlich. Dies ist die Standardstruktur für kleine und mittlere Identity Manager-Bereitstellungen. Multi-Tenant-Umgebungen besitzen möglicherweise eine etwas andere Struktur. Außerdem ist es nicht möglich, große und verteilte Bäume auf diese Weise zu organisieren. Diese Art von Baumstruktur wird erstellt, wenn Sie über das integrierte Installationsprogramm einen neuen Baum erstellen.



Identity Manager 4.0.1 verwendet hauptsächlich Organisationscontainer, sodass Benutzer, Gruppen und Service-Admins in demselben Container platziert werden. Sie sollten Organisationen verwenden, wenn möglich, und organisatorische Einheiten, wo dies sinnvoll ist. Die Identity Manager 4.0.1-Struktur ist auf Skalierbarkeit ausgerichtet, da sie drei Hauptkomponenten hat:

- ♦ [Abschnitt 2.9.1, „Sicherheit“, auf Seite 17](#)
- ♦ [Abschnitt 2.9.2, „Daten“, auf Seite 17](#)
- ♦ [Abschnitt 2.9.3, „System“, auf Seite 17](#)

## 2.9.1 Sicherheit

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.

## 2.9.2 Daten

Der Datencontainer enthält Gruppen, Benutzer, Rollenadministratoren, Geräte u. a. 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.

### **ou=sa**

Der Service-Admins-Container (`ou=sa`) enthält alle Benutzeranwendungsadministrator-Objekte und Service-Administratorkonten.

## 2.9.3 System

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

- ♦ `sa` oder Service-Admin-Benutzer/Superuser/Servicekonten
- ♦ Server
- ♦ Treibersätze
- ♦ Services

### **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`.

### **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. Alle dem Server zugeordneten Objekte (Volumes, Lizenzen, Zertifikate) befinden sich an der richtigen Stelle und es ist viel einfacher, die benötigten Objekte zu finden.

Diese Struktur ist auf Skalierbarkeit ausgelegt. Wenn Sie 10 oder 100 Server haben, ist es daher einfach, die einem einzelnen Server zugeordneten Objekte zu finden.

### **Treibersätze**

Treibersätze werden während der Metaverzeichnis-Serverkonfiguration als separate Partition erstellt. Alle Treibersatzobjekte werden im Systemcontainer gespeichert. Ihr Identity Manager 4.0.1-System kann mehrere Treibersätze haben. Diese Struktur ermöglicht Ihnen das Skalieren, indem Sie weitere Treibersätze zum Systemcontainer hinzufügen. Rollenbasierte Services für iManager werden ebenfalls im Systemcontainer gespeichert.

# Systemanforderungen

# 3

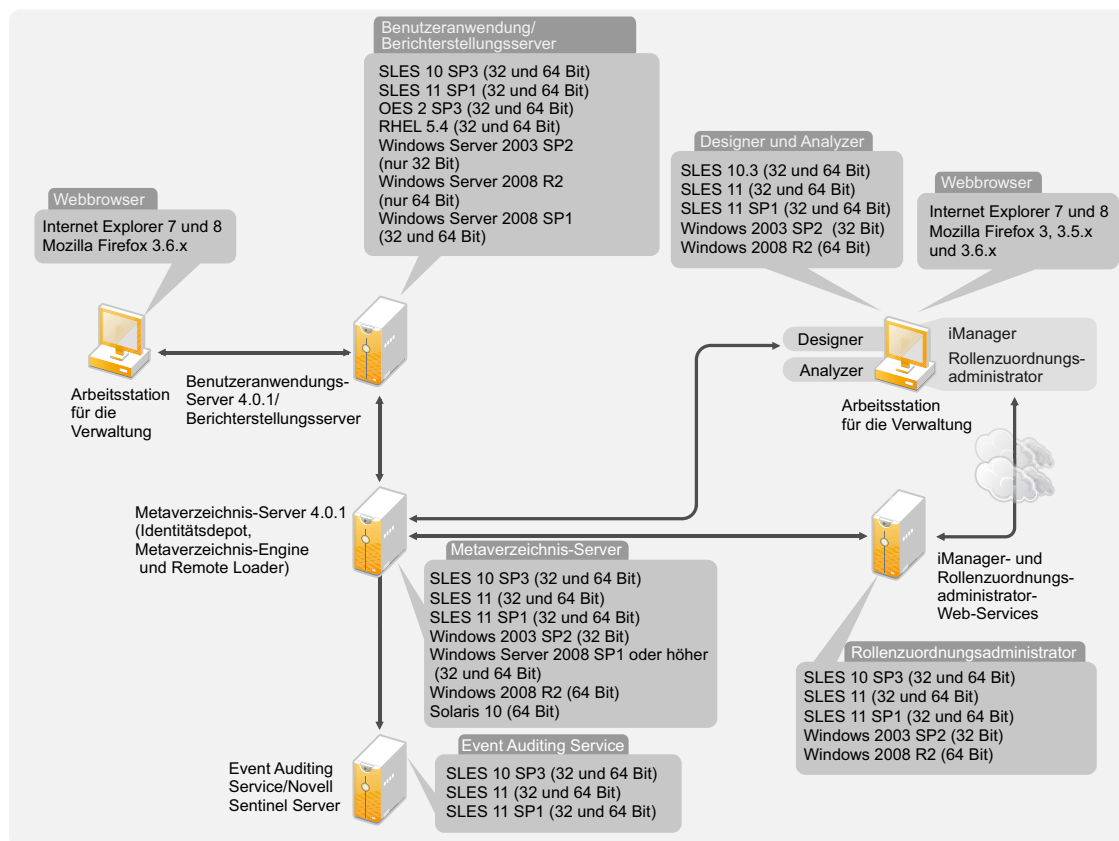
Die Komponenten von Novell Identity Manager können mithilfe des integrierten Installationsprogramms auf mehreren Systemen und Plattformen installiert werden.

- ♦ [Abschnitt 3.1, „Unterstützte Plattformen“](#), auf Seite 19
- ♦ [Abschnitt 3.2, „Ressourcenanforderungen“](#), auf Seite 20

## 3.1 Unterstützte Plattformen

Abbildung 3-1 zeigt Plattformen, die vom integrierten Installationsprogramm von Novell Identity Manager 4.0.1 unterstützt werden.

Abbildung 3-1 Systemanforderungen für das integrierte Installationsprogramm von Identity Manager



- ♦ Bei Identity Manager 4.0.1 wird der Event Auditing Service nur auf SLES-Plattformen unterstützt. Der Event Auditing Service wird unter Windows und RHEL nicht unterstützt. Der Event Auditing Service-Server wird auf einem Remote-Computer installiert. Das Installationsprogramm zeigt ein zusätzliches Feld für die Identitätsberichterstellungskonfiguration an, in dem Sie das Event Auditing Service-Systempasswort für den Server angeben können. Kopieren Sie das Systempasswort in der Datei

`/etc/opt/novell/sentinel_eas/config/activemqusers.properties` auf dem Computer, auf dem der Event Auditing Service installiert ist, und fügen Sie es in das Event Auditing Service-Systempasswortfeld ein.

- ♦ Bei Identity Manager 4.0.1 wird auf Solaris nur der Metaverzeichnis-Server unterstützt.
- ♦ Nicht alle Identity Manager-Komponenten können auf allen Plattformen installiert werden. Zum Beispiel wird der Metaverzeichnis-Server nur unter Solaris und der Event Auditing Service nur auf SLES-Plattformen unterstützt.

## 3.2 Ressourcenanforderungen

Zusätzlich zu den oben angegebenen Plattformanforderungen müssen Sie sicherstellen, dass die folgenden Ressourcenanforderungen erfüllt sind, damit alle Identity Manager-Komponenten installiert und konfiguriert werden können:

- ♦ Mindestens 3072 MB RAM
- ♦ 10 GB freier Festplattenspeicher, um alle Komponenten zu installieren.
- ♦ Weiterer Festplattenspeicher für die Konfiguration und Bereitstellung von Daten. Dies kann je nach Ihren verbundenen Systemen und der Anzahl der Objekte im Identitätsdepot variieren.
- ♦ Ein Multi-CPU-Server mit einem 2 GHz-Prozessor wird bevorzugt.

---

**Hinweis:** Diese Spezifikationen können abhängig von der Bereitstellungsumgebung variieren.

---

# Installation von Identity Manager

# 4

Sie können mithilfe des integrierten Installationsprogramms alle Komponenten gleichzeitig oder nacheinander installieren und konfigurieren. Wenn Sie jede Komponente einzeln installieren möchten, verwenden Sie das Identity Manager Framework-Installationsprogramm, das separate Installationsprogramme für die verschiedenen Komponenten hat, und installieren Sie die Komponenten in der Reihenfolge, die im Abschnitt „[Installation von Identity Manager](#)“ im *Identity Manager 4.0.1 Framework Installationshandbuch* angegeben ist. Eine Erklärung der verschiedenen Komponenten finden Sie im Handbuch *Überblick über Identity Manager 4.0.1*.

Eine Liste der verschiedenen Komponenten, die das integrierte Installationsprogramm von Identity Manager installiert, finden Sie in [Kapitel 1](#), „[Überblick über das integrierte Installationsprogramm](#)“, auf [Seite 7](#). Ausführliche Informationen zu jeder Komponente finden Sie im Handbuch *Überblick über Identity Manager 4.0.1*.

Die folgenden Abschnitte enthalten keine detaillierten Installationsanweisungen, da die Installationsoberfläche größtenteils selbsterklärend ist. Sie enthalten jedoch Informationen zu wichtigen Schritten des Prozesses, bei denen Sie möglicherweise Hilfe benötigen.

- ♦ [Abschnitt 4.1](#), „[Herunterladen der ISO-Datei](#)“, auf [Seite 21](#)
- ♦ [Abschnitt 4.2](#), „[Neuinstallation mithilfe physischer Medien oder einer ISO-Imagedatei](#)“, auf [Seite 23](#)
- ♦ [Abschnitt 4.3](#), „[Verfahren nach Abschluss der Installation](#)“, auf [Seite 34](#)
- ♦ [Abschnitt 4.4](#), „[Automatische Installation und Konfiguration](#)“, auf [Seite 35](#)

Informationen zum Aufrüsten einer vorhandenen Identity Manager-Installation finden Sie in [Kapitel 6](#), „[Aufrüsten von Identity Manager](#)“, auf [Seite 43](#).

## 4.1 Herunterladen der ISO-Datei

Identity Manager 4.0.1 ist in der Advanced Edition und in der Standard Edition verfügbar. Es gibt separate ISO-Imagedateien für jede Ausführung. Die Identity Manager 4.0.1 Advanced Edition enthält einen vollständigen Satz an Funktionen der Unternehmensklasse zur Bereitstellung von Benutzern. Um die verschiedenen Anforderungen der Kunden zu erfüllen, enthält die Identity Manager Standard Edition nur eine Auswahl der Funktionen, die in der Identity Manager Advanced Edition verfügbar sind. Die Standard Edition bietet auch weiterhin alle Funktionen, die in älteren Versionen von Identity Manager vorhanden sind. Weitere Informationen zur Identity Manager 4.0.1 Advanced Edition und Standard Edition finden Sie im Abschnitt „[Funktionen von Identity Manager 4.0.1](#)“ im *Identity Manager 4.0.1 Übersichtshandbuch*.

Kaufen Sie die Edition, die Ihren Geschäftsanforderungen am ehesten entspricht. Sie können auch eine Testversion von Identity Manager herunterladen und 90 Tage lang kostenlos nutzen. Die Komponenten von Identity Manager müssen jedoch innerhalb von 90 Tagen nach der Installation aktiviert werden, anderenfalls wird ihre Funktion eingestellt. Sie können Identity Manager zu einem beliebigen Zeitpunkt während oder nach Ablauf der 90 Tage durch den Kauf einer Produktlizenz aktivieren. Weitere Informationen finden Sie in [Kapitel 5](#), „[Aktivieren von Novell Identity Manager-Produkten](#)“, auf [Seite 39](#).

So können Sie Identity Manager und -Services herunterladen:

- 1 Rufen Sie die [Download-Website von Novell \(http://download.novell.com\)](http://download.novell.com) auf.
- 2 Wählen Sie im Menü *Product or Technology* (Produkt oder Technologie) den Eintrag *Identity Manager* aus und klicken Sie auf *Search* (Suchen).
- 3 Klicken Sie auf der Download-Website von Novell Identity Manager auf die Schaltfläche *Download* neben der gewünschten Datei. [Tabelle 4-1](#) enthält eine Beschreibung zu jeder Datei.
- 4 Wählen Sie eine ISO-Imagedatei gemäß Ihren Anforderungen aus. Jede ISO-Imagedatei enthält die 32-Bit- und 64-Bit-Version des Produkts.
- 5 Befolgen Sie die Bildschirmanweisungen, um die Datei in einen Ordner auf Ihrem Computer herunterzuladen.
- 6 Wiederholen Sie die Schritte ab [Schritt 3](#), bis Sie alle erforderlichen Dateien heruntergeladen haben.
- 7 Mounten Sie die heruntergeladene *.iso*-Datei als Volume oder verwenden Sie die *.iso*-Datei zum Erstellen einer DVD der Software. Wenn Sie noch nicht geprüft haben, ob der gebrannte Datenträger gültig ist, können Sie dies mit Hilfe der Option *Medienprüfung* tun.

---

**Hinweis:** Die Linux ISO-Dateien sollten aufgrund der Größe der ISO-Dateien auf eine Doppel-DVD kopiert werden.

---

**Tabelle 4-1** Identity Manager-ISO-Imagedateien

ISO	Plattform	Beschreibung
Identity_Manager_4.0.1_Linux_Advanced.iso	Linux	Enthält das DVD-Image für den Metaverzeichnis-Server, Event Auditing Service, Designer, iManager, Rollenzuordnungsadministrator, Analyzer, das Identitätsberichterstellungsmodul und das rollenbasierte Bereitstellungsmodul.
Identity_Manager_4.0.1_Linux_Standard.iso	Linux	Enthält das DVD-Image für den Metaverzeichnis-Server, Event Auditing Service, Designer, iManager, Analyzer, das Identitätsberichterstellungsmodul und das rollenbasierte Bereitstellungsmodul.
Identity_Manager_4.0.1_Windows_Advanced.iso	Windows	Enthält das DVD-Image für den Metaverzeichnis-Server, Designer, iManager, Rollenzuordnungsadministrator, Analyzer, das Identitätsberichterstellungsmodul und das rollenbasierte Bereitstellungsmodul.
Identity_Manager_4.0.1_Windows_Standard.iso	Windows	Enthält das DVD-Image für den Metaverzeichnis-Server, Designer, iManager, Analyzer, das Identitätsberichterstellungsmodul und das rollenbasierte Bereitstellungsmodul.
Identity_Manager_4.0.1_Solaris_Advanced.iso	Solaris	Enthält das DVD-Image für den Metaverzeichnis-Server. Andere Komponenten werden auf der Solaris-Plattform nicht unterstützt.

ISO	Plattform	Beschreibung
Identity_Manager_4.0.1_Solaris_Standard.iso	Solaris	Enthält das DVD-Image für den Metaverzeichnis-Server. Andere Komponenten werden auf der Solaris-Plattform nicht unterstützt.

**Wichtig:** Wenn Sie von der Identity Manager Advanced Edition zur Standard Edition wechseln möchten, deinstallieren Sie die Advanced Edition und installieren Sie die Standard Edition. Wenn Sie von der Standard Edition zur Advanced Edition aufrüsten möchten, verwenden Sie die Identity Manager Advanced Edition-ISO-Imagedatei. Sie müssen die richtige Aktivierung anwenden, um auf die Advanced Edition aufrüsten zu können. Weitere Informationen zum Aufrüsten von der Standard Edition auf die Advanced Edition finden Sie im [Identity Manager 4.0.1 Aufrüstungs- und Migrationshandbuch](#).

## 4.2 Neuinstallation mithilfe physischer Medien oder einer ISO-Imagedatei

Das integrierte Installationsprogramm unterstützt Sie bei der Installation der Binärdateien für die Identity Manager-Komponenten und der Konfiguration der Komponenten.

- ♦ [Abschnitt 4.2.1, „Installation“, auf Seite 23](#)
- ♦ [Abschnitt 4.2.2, „Konfiguration“, auf Seite 24](#)

**Wichtig:** Wenn Sie Identity Manager über ein integriertes Installationsprogramm auf einem 64-Bit-System installieren, stellen Sie sicher, dass die compat-Bibliothek `libgthread-2_0-0-32bit-2.17.2+2.17.3+20080708+r7171-3.1.x86_64.rpm` vor der Installation von Identity Manager installiert wird.

### 4.2.1 Installation

- 1 Greifen Sie auf die Identity Manager 4.0.1-Installationsdateien zu, indem Sie entweder die `.iso`-Datei mounten oder auf die DVD zugreifen, die Sie aus der `.iso`-Datei erstellt haben.

Weitere Informationen finden Sie in [Abschnitt 4.1, „Herunterladen der ISO-Datei“, auf Seite 21](#).

- 2 Navigieren Sie zum Mount-Verzeichnis und starten Sie die Installation, indem Sie das entsprechende Programm für Ihre Plattform verwenden.

**Linux/Solaris:** `./install.bin`

Führen Sie die Binärdatei aus, indem Sie `./install.bin` eingeben.

**Windows:** `install.exe`

- 3 Mithilfe der folgenden Informationen wird die Installation ausgeführt:

**Einführung:** Wählen Sie die Sprache für Ihre Installation aus und überprüfen Sie anschließend die Komponenten, die Sie installieren können.

**Lizenzvereinbarung:** Lesen Sie die Lizenzvereinbarung durch und bestätigen Sie Ihr Einverständnis.

**Komponenten auswählen:** Wählen Sie die gewünschten Komponenten zur Installation aus. Die Optionen sind:

- ◆ Metaverzeichnis-Server
- ◆ Rollenbasiertes Bereitstellungsmodul
- ◆ Identitätsberichterstellungsmodul
- ◆ Event Auditing Service
- ◆ Rollenzuordnungsadministrator
- ◆ iManager
- ◆ Designer
- ◆ Analyser

---

**Hinweis:** Das rollenbasierte Bereitstellungsmodul und das Identitätsberichterstellungsmodul können auf einem System installiert werden, auf dem das Identitätsdepot nicht vorhanden ist. Sie müssen das rollenbasierte Bereitstellungsmodul und das Identitätsberichterstellungsmodul immer auf demselben Computer installieren. Das rollenbasierte Bereitstellungsmodul verwendet JBoss und PostgreSQL als Anwendungsserver bzw. Datenbank.

---

**Installationsverzeichnis auswählen:** Geben Sie den Basisordner an, in dem Identity Manager und alle Komponenten installiert werden. Diese Option gilt nur für Windows.

Linux/UNIX-Installationen haben einen vordefinierten Installationspfad. Das integrierte Installationsprogramm installiert Komponenten unter den folgenden vordefinierten Installationspfaden:

- ◆ eDirectory und Identity Manager: `/opt/novell/eDirectory`
- ◆ Rollenbasiertes Bereitstellungsmodul, Berichterstellungsmodul, Rollenzuordnungsadministrator, Designer und Analyser: `/opt/novell/idm`
- ◆ Event Auditing Service: `/opt/novell/sentinel_eas`

**Zusammenfassung vor der Installation:** Überprüfen Sie die Seite „Zusammenfassung vor der Installation“, die Informationen zu den ausgewählten Komponenten enthält. Wenn Sie eine Einstellung ändern möchten, klicken Sie auf *Zurück*.

**Installation abgeschlossen:** Überprüfen Sie in der Zusammenfassung nach der Installation den Installationsstatus der ausgewählten Komponenten und den Speicherort der Protokolldatei für jede Komponente. In [Tabelle 4-2 auf Seite 35](#) finden Sie Informationen zum Speicherort der Protokolldateien.

**Fortfahren zum Konfigurieren:** (Bedingt) Dieses Kontrollkästchen ist nur aktiviert, wenn die ausgewählten Komponenten konfigurierbar sind. Wenn Sie mit der Konfiguration fortfahren möchten, fahren Sie mit [Abschnitt 4.2.2, „Konfiguration“](#), auf [Seite 24](#) fort. Wenn Sie nicht mit der Konfiguration fortfahren möchten, deaktivieren Sie dieses Kontrollkästchen.

## 4.2.2 Konfiguration

Sie können die Identity Manager-Komponenten, die Sie bereits installiert haben, mithilfe des integrierten Installationsprogramms konfigurieren. Stellen Sie sicher, dass Sie [Abschnitt 4.2.1, „Installation“](#), auf [Seite 23](#) abgeschlossen haben, bevor Sie mit der Konfiguration fortfahren.



---

**Wichtig:** Wenn Sie einen neuen Baum erstellen oder Elemente zu einem vorhandenen Baum hinzufügen und die Datei `/etc/hosts` den Eintrag „127.0.0.2“ enthält, schlägt die Konfiguration fehl, da das Standard-IP-Zertifikat für die Loopback-Adresse 127.0.0.2 erstellt wird. Um eine fehlerfreie Konfiguration zu ermöglichen, kommentieren Sie die Loopback-Adresse 127.0.0.2 aus und stellen Sie sicher, dass die Loopback-Adresse 127.0.0.1 und die echte IP-Adresse in der Datei enthalten sind.

---

So konfigurieren Sie die Identity Manager-Komponenten:

- 1 Wenn Sie von [Schritt 3 auf Seite 23](#) im Installationsverfahren fortfahren, gehen Sie zu [Schritt 2](#). Beginnen Sie anderenfalls die Konfiguration mit dem entsprechenden Programm für Ihre Plattform:

**Linux:** `./configure.bin`

**Solaris:** `./configure.bin`

Führen Sie die Binärdatei aus, indem Sie eingeben `./configure.bin`.

**Windows:** `configure.exe`

- 2 Wählen Sie die zu konfigurierenden Komponenten aus und klicken Sie auf *Weiter*.
- 3 Wählen Sie eine der folgenden Optionen aus, um die Konfiguration der Identity Manager-Komponenten abzuschließen:
  - ♦ „[Neuen Baum erstellen](#)“ auf Seite 26
  - ♦ „[Zu einem vorhandenen Baum hinzufügen](#)“ auf Seite 31

---

**Hinweis:** ♦ Wenn Sie Objekte zu einem vorhandenen Baum hinzufügen, führen Sie das Dienstprogramm „`NrfCaseUpdate`“ auf dem Primärserver aus, um Suchen von Rollen und Ressourcen unter Berücksichtigung der Groß-/Kleinschreibung zu ermöglichen, wenn der Primärserver über Identity Manager 3.6 oder höher verfügt.

Wenn Sie das Dienstprogramm „`NrfCaseUpdate`“ nicht ausführen, schlägt die Konfiguration des Metaverzeichnis-Servers fehl. Weitere Informationen zum Ausführen des Dienstprogramms „`NrfCaseUpdate`“ finden Sie unter „[Ausführen des NrfCaseUpdate-Dienstprogramms](#)“ im *Rollenbasiertes Bereitstellungsmodul für Identity Manager 4.0.1 Benutzeranwendung: Installationshandbuch*.

- ♦ Das integrierte Installationsprogramm führt keine Zustandsüberprüfung durch, bevor es den Sekundärserver hinzufügt. Sie müssen „`ndscheck`“ ausführen, bevor Sie den Sekundärserver mithilfe des integrierten Installationsprogramms hinzufügen. Führen Sie „`ndscheck`“ unter Windows im Verzeichnis `<Installationsverzeichnis>\NDS` aus. Unter Linux/Solaris starten Sie den Befehl vom Verzeichnis `/opt/novell/eDirectory/bin/ndscheck` aus. Geben Sie die obligatorischen Parameter an und führen Sie den Befehl wie folgt aus:

```
ndscheck [-h <Hostname Port>] [-a <admin FDN>] [[-w <Passwort>]
```

- ♦ Die Datei `logevent.cfg` wird mit den Protokollierungsserverdetails sowohl auf Windows- als auch auf Linux-Plattformen geändert, wenn das rollenbasierte Bereitstellungsmodul oder das Identitätsberichterstellungsmodul über das integrierte Installationsprogramm konfiguriert wird. Wenn Sie nur den Metaverzeichnis-Server konfigurieren, fügen Sie die Protokollierungsserverdetails manuell zur Datei `logevent.cfg` hinzu.
-

## Neuen Baum erstellen

Welche Felder angezeigt werden, hängt davon ab, welche Komponenten Sie auf der vorherigen Seite zum Konfigurieren ausgewählt haben.

- 1 Wenn Sie ausgewählt haben, dass ein neuer Baum erstellt werden soll, verwenden Sie die folgenden Informationen zum Konfigurieren Ihrer Identity Manager-Komponenten.
  - ♦ „Identitätsdepot“ auf Seite 26
  - ♦ „Identitätsdepot > Erweitert“ auf Seite 26
  - ♦ „Rollenbasiertes Bereitstellungsmodul (RBPM)“ auf Seite 27
  - ♦ „Rollenbasiertes Bereitstellungsmodul (RBPM) > Erweitert“ auf Seite 28
  - ♦ „Identitätsberichterstellungsmodul“ auf Seite 28
  - ♦ „Identitätsberichterstellungsmodul > Erweitert“ auf Seite 29
  - ♦ „Event Auditing Service“ auf Seite 30
  - ♦ „Event Auditing Service > Erweitert“ auf Seite 30
  - ♦ „iManager > Erweitert“ auf Seite 30
- 2 Überprüfen Sie die Zusammenfassung vor der Konfiguration und klicken Sie anschließend auf *Konfigurieren*.
- 3 Überprüfen Sie die Seite mit der Konfigurationszusammenfassung und klicken Sie anschließend auf *Fertig*.

Falls während der Konfiguration Probleme aufgetreten sind, überprüfen Sie die Konfigurationsprotokolle. Weitere Informationen finden Sie in „[Speicherorte der Protokolldateien und Eigenschaftendateien](#)“ auf Seite 35.

### Identitätsdepot

Füllen Sie die folgenden Felder aus, um einen neuen Baum zu erstellen:

**Neuer Baumname:** Geben Sie einen Namen für den neuen Baum an.

**Admin-Passwort:** Geben Sie ein Passwort für den Identitätsdepot-Administrator an.

**Admin-Passwort bestätigen:** Geben Sie das Passwort für den Identitätsdepot-Administrator erneut an.

### Identitätsdepot > Erweitert

Wählen Sie *Erweitert*, wenn Sie den Baum, der erstellt wird, anpassen möchten. Füllen Sie die folgenden Felder aus, um den Baum anzupassen:

**Administratorname:** Geben Sie den Namen des verwaltungsbefugten Benutzers des Identitätsdepots an.

**NCP-Port:** Behalten Sie entweder den Standardwert von 524 für den NCP-Port bei oder ändern Sie den Wert des Ports. NCP ist das Kern-Kommunikationsprotokoll von eDirectory.

**LDAP-Port:** Behalten Sie entweder den Standardwert von 389 für den LDAP-Port bei oder ändern Sie den Wert des Ports.

**Sicherer LDAP-Port:** Behalten Sie entweder den Standardwert von 636 für den sicheren LDAP-Port bei oder ändern Sie den Wert des Ports.

**HTTP-Port:** Behalten Sie entweder den Standardwert von 8028 für den HTTP-Port bei oder ändern Sie den Wert des Ports.

**Sicherer HTTP-Port:** Behalten Sie entweder den Standardwert von 8030 für den sicheren HTTP-Port bei oder ändern Sie den Wert des Ports.

**Instanzpfad:** Wenn Sie einen Linux/UNIX-Server verwenden, können Sie mehrere Instanzen von eDirectory auf einem Server ausführen. Geben Sie den Pfad dieser eDirectory-Instanz auf diesem Server an. Der Standardpfad ist `/var/opt/novell/eDirectory`.

**DIB-Pfad:** Geben Sie den Pfad für Ihre eDirectory-Datenbank (DIB) an. Der Standardspeicherort der DIB ist:

- ♦ **Linux/UNIX:** `/var/opt/novell/eDirectory/data/dib`
- ♦ **Windows:** `c:\Novell\IdentityManager\NDS\DIBFiles\`

---

**Hinweis:** DIB-Dateien müssen sich immer im `\NDS`-Ordner befinden. Wenn Sie den Standardspeicherort der DIB unter Windows, z. B. `\NDS\DIBFiles\`, ändern, schlägt die Konfiguration des Metaverzeichnis-Servers fehl.

---

**TLS für einfache Bindung mit Passwort erforderlich:** Wählen Sie diese Option aus, wenn alle LDAP-Verbindungen auf dem sicheren Port (Standard-Portnummer 636) sein müssen. Wenn Sie diese Option deaktivieren, übergeben Benutzer, die sich auf dem Klartext-Port (Standard-Portnummer 389) beim LDAP-Server authentifizieren, ihre Passwörter in Klartext. Weitere Informationen hierzu finden Sie unter „Communicating with eDirectory through LDAP“ (<http://www.novell.com/documentation/edir88/edirin88/data/a7f08y1.html>) (Kommunizieren mit eDirectory über LDAP) im *Novell eDirectory 8.8 Installation Guide* (<http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html>) (Novell eDirectory 8.8 Installationshandbuch).

#### Rollenbasiertes Bereitstellungsmodul (RBPM)

Füllen Sie die folgenden Felder aus, um das RBPM und Ihren Event Auditing Service (EAS) zu konfigurieren, der Teil des Identitätsberichterstellungsmoduls ist:

**EAS-Serveradresse:** Geben Sie den DNS-Namen oder die IP-Adresse des Servers an, auf dem sich der EAS befindet. Sie können diesen Server verwenden oder einen anderen Server hinzufügen. Das Identitätsberichterstellungsmodul kann nur auf einem einzigen EAS-Server konfiguriert werden.

**Passwort des idmadmin-Datenbankbenutzers:** Geben Sie das Passwort für den Datenbankbenutzer an. In dieser Datenbank werden Informationen für Berichte gespeichert.

**Passwort des idmadmin-Datenbankbenutzers bestätigen:** Geben Sie das Passwort für den Datenbankbenutzer erneut an.

**Benutzeranwendungspasswort:** Geben Sie das Passwort für die Benutzeranwendung an.

**Benutzeranwendungspasswort bestätigen:** Geben Sie das Passwort für die Benutzeranwendung erneut an.

**(Bedingt) Passwort des Sicherheitsadministrators:** Geben Sie das Passwort für den Sicherheitsadministrator an.

Dieses Feld ist nur für die Identity Manager Standard Edition erforderlich.

**(Bedingt) Passwort des Sicherheitsadministrators bestätigen:** Geben Sie das Passwort für den Sicherheitsadministrator erneut an.

Dieses Feld ist nur für die Identity Manager Standard Edition erforderlich.

**(Bedingt) Berichtsadministrator-Passwort:** Geben Sie das Passwort für den Identitätsberichterstellungsadministrator an.

Dieses Feld ist nur für die Identity Manager Standard Edition erforderlich.

**(Bedingt) Berichtsadministrator-Passwort bestätigen:** Geben Sie das Passwort für den Identitätsberichterstellungsadministrator erneut an.

Dieses Feld ist nur für die Identity Manager Standard Edition erforderlich.

Rollenbasiertes Bereitstellungsmodul (RBPM) > Erweitert

Wählen Sie *Erweitert*, wenn Sie die Konfiguration des RBPMs anpassen möchten.

**Adresse der Benutzeranwendung:** Geben Sie den DNS-Namen oder die IP-Adresse des Servers an, auf dem sich die Benutzeranwendung befindet.

**Benutzer der Benutzeranwendung:** Geben Sie den Namen für den verwaltungsbefugten Benutzer für die Benutzeranwendung an.

**Name des Benutzeranwendungsadministrators:** Geben Sie den Namen des Benutzeranwendungsadministrators an. Ein Benutzeranwendungsadministrator ist berechtigt, alle Verwaltungsfunktionen der Identity Manager-Benutzeranwendung durchzuführen. Dies umfasst den Zugriff auf die Registerkarte „Administration“ der Identity Manager-Benutzeroberfläche zur Durchführung von unterstützten Administrationsaktionen.

**(Bedingt) Name des Sicherheitsadministrators:** Geben Sie den Namen des Sicherheitsadministrators für die Benutzeranwendung an. Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Sicherheitsdomäne. Der Sicherheitsadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Sicherheitsdomäne durchführen.

Dieses Feld ist nur für die Identity Manager Standard Edition erforderlich.

**(Bedingt) Name des Berichtsadministrators:** Geben Sie den Namen des Berichtsadministrators an. Dieser Benutzer kann alle Funktionen in der Berichterstellungsdomäne verwenden. Der Berichtsadministrator kann für alle Objekte alle Aktionen innerhalb der Berichterstellungsdomäne durchführen.

Dieses Feld ist nur für die Identity Manager Standard Edition erforderlich.

Identitätsberichterstellungsmodul

Füllen Sie die folgenden Felder aus, um das Identitätsberichterstellungsmodul zu konfigurieren:

**Passwort des Benutzers 'idmrptsrv':** Geben Sie das Passwort für den Benutzer „idmrptsrv“ an. Der Benutzer „idmrptsrv“ ist der Eigentümer der Datenbankschemas und Objekte für die Berichterstellung.

**Passwort des Benutzers 'idmrptuser':** Geben Sie das Passwort für den Benutzer „idmrptuser“ an. Dies ist ein Benutzer mit Lesezugriff auf die Berichterstellungsdaten.

**dbauser-Passwort:** Geben Sie das Passwort für den dbauser (Datenbankadministrator) an.

**Gateway-Port des verwalteten Systems:** Geben Sie den Port an, auf dem der Treiber „Verwaltetes System - Gateway“ kommuniziert.

Dieses Feld ist nur für die Identity Manager Advanced Edition erforderlich.

**Adresse des Datenerfassungsdiensts:** Geben Sie die IP-Adresse oder den DNS-Namen des Datenerfassungsdienst-Servers an.

Identitätsberichterstellungsmodul > Erweitert

Wählen Sie *Erweitert*, um die Konfiguration des Identitätsberichterstellungsmoduls anzupassen. Füllen Sie die folgenden Felder aus, um das Identitätsberichterstellungsmodul anzupassen:

**Untercontainersuche aktivieren:** Wählen Sie diese Option aus, um dem Identitätsberichterstellungsmodul das Ausführen von Untercontainer-Suchvorgängen zum Sammeln von Informationen für Berichte zu ermöglichen.

**Anwendungsserverplattform:** Geben Sie den Typ des Anwendungsservers an, den Sie mit dem rollenbasierten Bereitstellungsmodul verwenden. Die unterstützten Plattformen sind JBoss, WebSphere und WebLogic.

**Datenbank-Hostadresse:** Geben Sie den DNS-Namen oder die IP-Adresse des Servers an, auf dem Ihre Datenbank ausgeführt wird.

**Dateiname des PostgreSQL-JDBC-Treibers:** Geben Sie `postgresql-8.4-701.jdbc4.jar` als Dateinamen des PostgreSQL-JDBC-Treibers an.

**Speicherort des PostgreSQL-JDBC-Treibers:** Geben Sie den Speicherort der `.jar`-Datei des PostgreSQL JDBC-Treibers an. Standardmäßig befindet sich diese Datei unter:

- ♦ **Linux/UNIX:** `/opt/novell/sentinel_eas/lib/`
- ♦ **Windows:** `c:\Novell\idm\sentinel_eas\lib`

**Sicheres LDAP:** Wählen Sie aus, ob der Server über eine sichere LDAP-Verbindung kommuniziert.

**LDAP-Port:** Wenn Sie sicheres LDAP für die Kommunikation ausgewählt haben, geben Sie den sicheren LDAP-Port an. Geben Sie Anderenfalls den Klartext-Port an.

**Tokenablaufwert (Minuten):** Geben Sie den Zeitraum in Minuten an, für den das Token für die Authentifizierung aufbewahrt werden soll.

**Berichtseinheit:** Wählen Sie *Tag*, *Woche* oder *Monat* aus.

**Berichtsaufbewahrungswert:** Geben Sie an, wie lange ein Bericht aufbewahrt werden soll. Wenn die Berichtseinheit auf „Tag“ gesetzt wurde und der Berichtsaufbewahrungswert 1 ist, werden die Berichte 1 Tag lang aufbewahrt, bevor sie gelöscht werden.

**Anmeldeattribut für Untercontainer:** Wenn Sie Untercontainer-Suchvorgänge aktivieren, müssen Sie das Anmeldeattribut angeben, das zum Durchsuchen des Teilbaums des Benutzercontainers verwendet wird.

**SMTP-Serveradresse:** Geben Sie den DNS-Namen oder die IP-Adresse des SMTP-Servers an, um Emails für die Berichtsbenachrichtigungen zu konfigurieren.

**SMTP-Server-Port:** Behalten Sie entweder 456 als Standardport für den SMTP-Server-Port bei oder ändern Sie den Wert.

**SMTP-Benutzer-Email:** Geben Sie die Email-Adresse an, die für die Authentifizierung verwendet werden soll, wenn die Authentifizierung aktiviert ist.

**SMTP-Benutzerpasswort:** Geben Sie das Passwort für den SMTP-Benutzer an.

**SMTP-Benutzerpasswort bestätigen:** Geben Sie das Passwort für den SMTP-Benutzer erneut an.

**Standard-Email-Adresse:** Geben Sie eine Standard-Email-Adresse an, die verwendet werden soll, wenn für die Person, die den Bericht ausführt, keine Email-Adresse im Identitätsdepot vorhanden ist.

**SMTP verwendet SSL:** Wählen Sie diese Option aus, wenn der SMTP-Server eine SSL-Verbindung verwendet.

**Server benötigt Authentifizierung:** Wählen Sie diese Option aus, wenn der SMTP-Server eine Authentifizierung erfordert.

### Event Auditing Service

Füllen Sie die folgenden Felder aus, um den Event Auditing Service zu konfigurieren:

**Admin-Passwort:** Geben Sie das Passwort für den verwaltungsbefugten Benutzer an.

**Admin-Passwort bestätigen:** Geben Sie das Passwort für den verwaltungsbefugten Benutzer erneut an.

**Administratorpasswort der Datenbank:** Geben Sie das Passwort für den Datenbank-Administrator an.

**Administratorpasswort der Datenbank bestätigen:** Geben Sie das Passwort für den Datenbank-Administrator erneut an.

### Event Auditing Service > Erweitert

Wählen Sie *Erweitert*, um die Konfiguration des Event Auditing Services anzupassen:

**PostgreSQL-Port:** Behalten Sie entweder den Standardwert von 15432 für den PostgreSQL-Port bei oder ändern Sie ihn.

**Portweiterleitung aktivieren:** Wählen Sie diese Option aus, um die Portweiterleitung zu aktivieren, oder deaktivieren Sie sie, um die Portweiterleitung zu deaktivieren.

### iManager > Erweitert

Für iManager gibt es nur erweiterte Konfigurationsoptionen. Wählen Sie *Erweitert*, um diese Optionen anzuzeigen:

**HTTP-Port:** Behalten Sie entweder den Standardwert von 8080 für den nicht sicheren Port bei oder ändern Sie ihn.

**Sicherer HTTP-Port:** Behalten Sie entweder den Standardwert von 8443 für den sicheren Port bei oder ändern Sie ihn.

## Zu einem vorhandenen Baum hinzufügen

Welche Felder angezeigt werden, hängt davon ab, welche Komponenten Sie auf der vorherigen Seite zum Konfigurieren ausgewählt haben.

- 1 Wenn Sie ausgewählt haben, dass dieser Server zu einem vorhandenen Baum hinzugefügt werden soll, verwenden Sie die folgenden Informationen zum Konfigurieren der Identity Manager-Komponenten.
  - ♦ „Identitätsdepot“ auf Seite 31
  - ♦ „Identitätsdepot > Erweitert“ auf Seite 31
  - ♦ „Metaverzeichnis-Server“ auf Seite 32
  - ♦ „Rollenbasiertes Bereitstellungsmodul (RBPM)“ auf Seite 33
  - ♦ „Rollenbasiertes Bereitstellungsmodul (RBPM) > Erweitert“ auf Seite 34
  - ♦ „Identitätsberichterstellungsmodul“ auf Seite 34
  - ♦ „Event Auditing Service“ auf Seite 34
  - ♦ „iManager > Erweitert“ auf Seite 34
- 2 Überprüfen Sie die Seite mit der Konfigurationszusammenfassung und klicken Sie anschließend auf *Fertig*.

Falls während der Konfiguration Probleme aufgetreten sind, überprüfen Sie die Konfigurationsprotokolle. Weitere Informationen finden Sie in „[Speicherorte der Protokolldateien und Eigenschaftendateien](#)“ auf Seite 35.

### Identitätsdepot

Füllen Sie die folgenden Felder aus, um zu ermöglichen, dass Ihr Server zu einem vorhandenen Identitätsdepot hinzugefügt wird:

**Adresse des vorhandenen Servers:** Geben Sie die IP-Adresse eines Servers in Ihrem vorhandenen Baum an.

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

**Kontext-DN des vorhandenen Servers:** Geben Sie den DN des Containers an, in dem dieser Server in Ihrem vorhandenen Baum platziert werden soll. Beispiel: ou=server,o=system.

**Serveradministrator-DN des vorhandenen Servers:** Geben Sie den DN des Benutzers an, der vollständige Verwaltungsrechte für Ihren Baum hat.

Unter Windows ist der Administraturname des vorhandenen Servers gleich dem Administraturnamen des vorhandenen Baums und der Admin-Kontext-DN des vorhandenen Servers gleich dem Administratorkontext-DN des vorhandenen Baums.

**Administratorpasswort des vorhandenen Servers:** Geben Sie das Passwort für den oben angegebenen verwaltungsbefugten Benutzer an.

### Identitätsdepot > Erweitert

Wählen Sie *Erweitert*, wenn Sie dieses Identitätsdepot anpassen möchten. Füllen Sie die folgenden Felder aus, um das Identitätsdepot anzupassen:

**NCP-Port:** Behalten Sie entweder den Standardwert von 524 für den NCP-Port bei oder ändern Sie den Wert des Ports. NCP ist das Kern-Kommunikationsprotokoll von eDirectory.

**LDAP-Port:** Behalten Sie entweder den Standardwert von 389 für den LDAP-Port bei oder ändern Sie den Wert des Ports.

**Sicherer LDAP-Port:** Behalten Sie entweder den Standardwert von 636 für den sicheren LDAP-Port bei oder ändern Sie den Wert des Ports.

**HTTP-Port:** Behalten Sie entweder den Standardwert von 8028 für den HTTP-Port bei oder ändern Sie den Wert des Ports.

**Sicherer HTTP-Port:** Behalten Sie entweder den Standardwert von 8030 für den sicheren HTTP-Port bei oder ändern Sie den Wert des Ports.

**Instanzpfad:** Wenn Sie einen Linux/UNIX-Server verwenden, können Sie mehrere Instanzen von eDirectory auf einem Server ausführen. Geben Sie den Pfad dieser eDirectory-Instanz auf diesem Server an. Der Standardpfad ist `/var/opt/novell/eDirectory/data`.

**DIB-Pfad:** Geben Sie den Pfad für Ihre eDirectory-Datenbank (DIB) an. Der Standardspeicherort der DIB ist:

- ♦ **Linux/UNIX:** `/var/opt/novell/eDirectory/data/DIB`
- ♦ **Windows:** `c:\Novell\Identity Manager\NDS\DIBfiles\`

---

**Hinweis:** DIB-Dateien müssen sich immer im `\NDS`-Ordner befinden. Wenn Sie den Standardspeicherort der DIB unter Windows, z. B. `\NDS\DIBfiles\`, ändern, schlägt die Konfiguration des Metaverzeichnis-Servers fehl.

---

**TLS für einfache Bindung mit Passwort erforderlich:** Wählen Sie diese Option aus, wenn alle LDAP-Verbindungen auf dem sicheren Port (Standard-Portnummer 636) sein müssen. Wenn Sie diese Option deaktivieren, übergeben Benutzer, die sich auf dem Klartext-Port (Standard-Portnummer 389) beim LDAP-Server authentifizieren, ihre Passwörter in Klartext. Weitere Informationen hierzu finden Sie unter „Communicating with eDirectory through LDAP“ (<http://www.novell.com/documentation/edir88/edirin88/data/a7f08y1.html>) (Kommunizieren mit eDirectory über LDAP) im *Novell eDirectory 8.8 Installation Guide* (<http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html>) (Novell eDirectory 8.8 Installationshandbuch).

**Verschlüsselte Reproduktion aktivieren:** Wählen Sie diese Option aus, wenn die Reproduktion Ihres Baums verschlüsselt werden soll. Weitere Informationen hierzu finden Sie unter „Encrypted Replication“ (<http://www.novell.com/documentation/edir88/edir88/data/bs6rydy.html>) (Verschlüsselte Reproduktion) im *Administrationshandbuch zu Novell eDirectory 8.8* (<http://www.novell.com/documentation/edir88/edir88/data/a2iii88.html>).

## Metaverzeichnis-Server

**Name des Treibersatzes:** Geben Sie den Namen für den neuen Treibersatz an, der während der Konfiguration des Metaverzeichnis-Servers erstellt wird. Stellen Sie sicher, dass Sie keinen vorhandenen Treibersatz verwenden.

**Kontext-DN des Treibersatzes:** Geben Sie den Kontext an, in dem der neue Treibersatz in Ihrem Baum erstellt wird.



## Rollenbasiertes Bereitstellungsmodul (RBPM)

Füllen Sie die folgenden Felder aus, um das RBPM und Ihren Event Auditing Service (EAS) zu konfigurieren, der Teil des Identitätsberichterstellungsmoduls ist:

**EAS-Serveradresse:** Geben Sie den DNS-Namen oder die IP-Adresse des Servers an, auf dem sich der EAS befindet. Sie können diesen Server verwenden oder einen anderen Server hinzufügen. Das Identitätsberichterstellungsmodul kann nur auf einem einzigen EAS-Server konfiguriert werden.

**Passwort des idmadmin-Datenbankbenutzers:** Geben Sie das Passwort für den Datenbankbenutzer an. In dieser Datenbank werden Informationen für Berichte gespeichert.

**Benutzeranwendung - Admin-DN:** Geben Sie den DN für den Benutzeranwendungsadministrator im LDAP-Format an. Der Benutzeranwendungsadministrator ist berechtigt, alle Verwaltungsfunktionen der Identity Manager-Benutzeranwendung durchzuführen. Dies umfasst den Zugriff auf die Registerkarte „Administration“ der Identity Manager-Benutzeroberfläche zur Durchführung von unterstützten Administrationsaktionen.

---

**Wichtig:** Stellen Sie sicher, dass Sie unterschiedliche DNs in den Feldern *Benutzeranwendungsadministrator-DN*, *Sicherheitsadministrator-DN* und *Berichtsadministrator-DN* angeben. Wenn diese DNs auf dem primären Server bereits vorhanden sind, schlägt die Konfiguration der Benutzeranwendung fehl.

---

**Administratorpasswort der Benutzeranwendung:** Geben Sie das Passwort für die Benutzeranwendung an.

**Container-DN des Benutzeranwendungstreibers:** Geben Sie den Stammcontainer-DN für den Benutzeranwendungsadministrator im LDAP-Format an.

**(Bedingt) Sicherheitsadministrator-DN:** Geben Sie den DN für den Sicherheitsadministrator im LDAP-Format an. Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Sicherheitsdomäne. Der Sicherheitsadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Sicherheitsdomäne durchführen.

Dieses Feld ist nur für die Identity Manager Standard Edition erforderlich.

**(Bedingt) Sicherheitsadministrator-Passwort:** Geben Sie das Passwort für den Sicherheitsadministrator an.

Dieses Feld ist nur für die Identity Manager Standard Edition erforderlich.

**(Bedingt) Berichtsadministrator-DN:** Geben Sie den DN für den Berichtsadministrator im LDAP-Format an. Dieser Benutzer hat innerhalb der Berichterstellungsdomäne Zugriff auf alle Funktionen. Der Berichtsadministrator kann für alle Objekte alle Aktionen innerhalb der Berichterstellungsdomäne durchführen.

Dieses Feld ist nur für die Identity Manager Standard Edition erforderlich.

**(Bedingt) Berichtsadministrator-Passwort:** Geben Sie das Passwort des Berichtsadministrators an.

Dieses Feld ist nur für die Identity Manager Standard Edition erforderlich.

## Rollenbasiertes Bereitstellungsmodul (RBPM) > Erweitert

Die erweiterten Konfigurationsoptionen des RBPMs sind für die Konfiguration neuer und vorhandener Bäume gleich. Weitere Informationen finden Sie in [„Rollenbasiertes Bereitstellungsmodul \(RBPM\) > Erweitert“ auf Seite 28](#).

Bei der Installation des Sekundärserverns nach der RBPM-Konfiguration müssen Sie die *Authentifizierungs-ID* des Benutzeranwendungstreibers ändern:

- 1 Melden Sie sich über iManager beim vorhandenen Baum an.
- 2 Wählen Sie *Identity Manager-Verwaltung > Identity Manager-Überblick* und wählen Sie dann den Treibersatz aus.
- 3 Klicken Sie auf die Option *Eigenschaften bearbeiten* des Benutzeranwendungstreibers, ändern Sie den Wert der *Authentifizierungs-ID* in den Wert des Benutzeranwendungsadministrators im LDAP-Format.

## Identitätsberichterstellungsmodul

Die Konfigurationsoptionen des Identitätsberichterstellungsmoduls sind für die Konfiguration neuer und vorhandener Bäume gleich. Weitere Informationen finden Sie in [„Identitätsberichterstellungsmodul“ auf Seite 28](#) und [„Identitätsberichterstellungsmodul > Erweitert“ auf Seite 29](#).

## Event Auditing Service

Die Konfigurationsoptionen des Event Auditing Services sind für die Konfiguration neuer und vorhandener Bäume gleich. Weitere Informationen finden Sie in [„Event Auditing Service“ auf Seite 30](#) und [„Event Auditing Service > Erweitert“ auf Seite 30](#).

## iManager > Erweitert

Die Konfigurationsoptionen von iManager sind für die Konfiguration neuer und vorhandener Bäume gleich. Weitere Informationen finden Sie in [„iManager > Erweitert“ auf Seite 30](#).

# 4.3 Verfahren nach Abschluss der Installation

Das integrierte Installationsprogramm erstellt nicht das DirXML-PasswordPolicy-Objekt im Identitätsdepot. Diese Richtlinie wird jedem Identity Manager-Treibersatz in einem Baum zugewiesen. Führen Sie nach Abschluss der Identity Manager-Installation folgende Schritte aus, um das DirXML-PasswordPolicy-Objekt zu erstellen:

- 1 Erstellen Sie eine LDIF-Datei mit folgenden Attributen:

```
dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: add
nsimPwdRuleEnforcement: FALSE
nspmSpecialAsLastCharacter: TRUE
nspmSpecialAsFirstCharacter: TRUE
nspmSpecialCharactersAllowed: TRUE
nspmNumericAsLastCharacter: TRUE
nspmNumericAsFirstCharacter: TRUE
nspmNumericCharactersAllowed: TRUE
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
```

```

passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy

dn: cn=driverset1,o=system #(driver-set dn, which the policy is assigned
to)
changetype: modify
add: objectclass
objectclass: nsimPasswordPolicyAux

dn: cn=driverset1,o=system #(driver-set dn, which the policy is assigned
to)
changetype: modify
add: nspmPasswordPolicyDN
nspmPasswordPolicyDN: cn=DirXML-PasswordPolicy,cn=Password
Policies,cn=Security

dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: modify
add: nsimAssignments
nsimAssignments: cn=driverset1,o=system #(driver-set dn, which the policy
is assigned to)

```

**2** Verwenden Sie „ldapmodify“ für den Import von Attributen aus der LDIF-Datei.

```

ldapmodify -x -ZZ -c -h <hostname> -p 389 -D "cn=admin,ou=sa,o=system" -w
<password> -f <ldif_file_name>

```

---

**Hinweis:** Verwenden Sie bei Windows die Datei ldapmodify.exe aus dem ISO-Image des integrierten Installationsprogramms. (z. B. <II\_ISO\_Path>/install/utilities)

---

## Speicherorte der Protokolldateien und Eigenschaftendateien

Die folgende Tabelle enthält den Speicherort für das Installationsprotokoll (ii\_install.log), die Konfigurationsprotokolle (ii\_configure.log) und die Eigenschaftendateien. Für jede installierte Komponente ist eine Eigenschaftendatei vorhanden.

**Tabelle 4-2** Speicherort von Protokolldateien und Eigenschaftendateien nach der Installation und Konfiguration

Plattform	Protokolldateien	Installationseigenschaftendateien
Windows	<Installationsverzeichnis>\install \logs  Der Standard-Speicherort ist C:\Novell\IdentityManager\install\ logs	<Installationsverzeichnis>\install\propf iles  Der Standard-Speicherort ist C:\Novell\IdentityManager\install \logs\propfiles\
Linux/ Solaris	/var/opt/novell/idm/install/logs	/var/opt/novell/idm/install/logs/ propfiles/

## 4.4 Automatische Installation und Konfiguration

- ♦ [Abschnitt 4.4.1, „Automatische Installation“, auf Seite 36](#)
- ♦ [Abschnitt 4.4.2, „Automatische Konfiguration“, auf Seite 36](#)

## 4.4.1 Automatische Installation

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

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

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

- ♦ **Linux:** `./install.bin -i silent -f <Dateiname>.properties`
- ♦ **Solaris:** `./install.bin -i silent -f <Dateiname>.properties`  
Führen Sie die Binärdatei aus, indem Sie eingeben `./install.bin -i silent -f <Dateiname>.properties`.
- ♦ **Windows:** `\install.exe -i silent -f <Dateiname>.properties`

Die automatische Installation unterstützt die folgenden Passwortvariablen als Umgebungsvariablen. Wenn die Passwortvariablen nicht über die Umgebung übergeben werden, müssen Sie sie zur Eigenschaftendatei für die automatische Installation hinzufügen.

**Metaverzeichnis-Server:** `IA_IDVAULT_ADMIN_PASSWORD`.

**Rollenbasiertes Bereitstellungsmodul:** `IA_RBPM_POSTGRESQL_DB_PASSWORD` und `IA_RBPM_USERAPPADMIN_PASSWORD`.

**Identitätsberichterstellungsmodul:** `IA_REPORTING_NOVL_DB_USER_PASSWORD`, `IA_REPORTING_IDM_USER_PASSWORD` und `IA_REPORTING_IDM_SERVER_PASSWORD`.

**Event Auditing Service:** `IA_EAS_ADMIN_PWD` und `IA_EAS_DBA_PWD`.

## 4.4.2 Automatische Konfiguration

Sie können auch eine automatische Konfiguration der Identity Manager-Komponenten ausführen, indem Sie eine Eigenschaftendatei mit den für die Konfiguration erforderlichen Parametern erstellen. Auf dem Identity Manager-Datenträger sind zwei Beispieldateien vorhanden. Eine der Dateien wird verwendet, wenn Sie einen neuen Baum erstellen, und die andere, wenn Sie den Server zu einem vorhandenen Baum hinzufügen möchten.

- ♦ **Linux:** Navigieren Sie zum folgenden Speicherort:
  - ♦ `./install/propfiles/configure_new_tree.properties`
  - ♦ `./install/propfiles/configure_existing_tree.properties`
- ♦ **Solaris:** Navigieren Sie zum folgenden Speicherort:
  - ♦ `./install/propfiles/configure_new_tree.properties`
  - ♦ `./install/propfiles/configure_existing_tree.properties`

- ♦ **Windows:** Navigieren Sie zum folgenden Speicherort:
  - ♦ `\install\propfiles\configure_new_tree.properties`
  - ♦ `IDM4.0.1_Win:\install\propfiles\configure_existing_tree.properties`

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

- ♦ **Linux:** `./configure.bin -i silent -f <Dateiname>.properties`
- ♦ **Solaris:** `./configure.bin -i silent -f <Dateiname>.properties`  
Führen Sie die Binärdatei aus, indem Sie eingeben `./configure.bin -i silent -f <Dateiname>.properties`.
- ♦ **Windows:** `\configure.exe -i silent -f <Dateiname>.properties`

Die Beispiel-Eigenschaftendateien, die unter `install\propfiles` verfügbar sind, können nur verwendet werden, wenn alle Komponenten in einem Durchlauf konfiguriert werden.

Wenn Sie die obligatorischen Parameter sehen möchten, führen Sie folgenden Befehl aus:

```
./install/bin -i silent -DSELECTED_PRODUCTS=<Zu konfigurierende Komponenten>
```

Die Beschreibung der IDs für die Identity Manager-Komponenten ist in der Eigenschaftendatei enthalten.

Erstellen Sie eine Eigenschaftendatei mit der Ausgabe des oben genannten Befehls, fügen Sie `SELECTED_PRODUCTS` mit den zu konfigurierenden Komponenten hinzu, führen Sie dann den Befehl für die automatische Installation erneut aus, um eine automatische Konfiguration der ausgewählten Komponenten durchzuführen.



# Aktivieren von Novell Identity Manager-Produkten

# 5

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.

Führen Sie zur Aktivierung der Identity Manager-Komponenten folgende Schritte aus:

- ♦ [Abschnitt 5.1, „Erwerb einer Produktlizenz für Identity Manager“](#), auf Seite 39
- ♦ [Abschnitt 5.2, „Installation einer Produktaktivierungsberechtigung“](#), auf Seite 39
- ♦ [Abschnitt 5.3, „Anzeigen der Produktaktivierungen für Identity Manager und Identity Manager-Treiber“](#), auf Seite 40
- ♦ [Abschnitt 5.4, „Aktivieren von Identity Manager-Treibern“](#), auf Seite 41
- ♦ [Abschnitt 5.5, „Aktivieren von Analyzer“](#), auf Seite 42
- ♦ [Abschnitt 5.6, „Aktivieren von Designer und dem Rollenzuordnungsadministrator“](#), auf Seite 42

## 5.1 Erwerb einer Produktlizenz für Identity Manager

Informationen zum Kauf einer Identity Manager-Produktlizenz für die Aktivierung des Produkts finden Sie auf der [Novell Identity Manager-Bestellwebseite \(http://www.novell.com/products/identitymanager/howtobuy.html\)](http://www.novell.com/products/identitymanager/howtobuy.html).

Wenn Sie eine Produktlizenz erworben haben, wird Ihnen von Novell die Kunden-ID per Email zugesendet. Die Email enthält außerdem die URL der Website, auf der Sie eine Produktaktivierungsberechtigung erhalten. Wenn Sie Ihre Kunden-ID vergessen oder sie keine erhalten haben, rufen Sie bitte beim Novell Activation Center unter +1-800-418-8373 in den USA an. An allen anderen Standorten rufen Sie bitte unter +1-801-861-8373 an. Sie können auch [online mit uns chatten \(http://support.novell.com/chat/activation\)](http://support.novell.com/chat/activation).

## 5.2 Installation einer Produktaktivierungsberechtigung

Die Produktaktivierungsberechtigung muss über iManager installiert werden.

- 1 Nach dem Erwerb einer Lizenz erhalten Sie von Novell eine Email mit Ihrer Kunden-ID. Die Email 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-----).

---

**Warnung:** Wenn die Aktivierung der Standard Edition auf ein vorhandenes, nicht aktiviertes Advanced Edition-System angewendet wird, werden der Identity Manager-Metaverzeichnis-Server und die Treiber angehalten.

---

- 3 Öffnen Sie iManager.
- 4 Wählen Sie *Identity Manager > Identity Manager-Überblick*.
- 5 Klicken Sie auf , um in der Baumstruktur nach einem Treibersatz zu suchen und diesen auszuwählen.
- 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.

---

## 5.3 Anzeigen der Produktaktivierungen für Identity Manager und Identity Manager-Treiber

Für jeden Treibersatz werden die Produktaktivierungsberechtigungen angezeigt, die Sie für die Metaverzeichnis-Engine- und Identity Manager-Treiber installiert haben:

- 1 Öffnen Sie iManager.
- 2 Klicken Sie auf *Identity Manager > Identity Manager-Überblick*.
- 3 Klicken Sie auf , um in der Baumstruktur nach einem Treibersatz zu suchen und diesen auszuwählen, und klicken Sie anschließend auf , um den Suchvorgang auszuführen.
- 4 Klicken Sie auf der Seite „Identity Manager-Überblick“ auf den Treibersatz, dessen Aktivierungsinformationen Sie anzeigen möchten.



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.

---

## 5.4 Aktivieren von Identity Manager-Treibern

Im Lieferumfang von Identity Manager sind Aktivierungen von Service-Treibern und verschiedenen allgemeinen Treibern enthalten.

- ♦ **Service-Treiber:** Folgende Service-Treiber werden aktiviert, wenn Sie den Metaverzeichnis-Server aktivieren:
  - ♦ Datenerfassungsdienst
  - ♦ Berechtigungsservices
  - ♦ ID-Provider
  - ♦ Loopback-Service
  - ♦ Verwaltetes System - Gateway
  - ♦ 'Manuelle Aufgabe'-Service
  - ♦ Null-Service
  - ♦ Rollenservice
  - ♦ Benutzeranwendung
  - ♦ Auftrag
- ♦ **Allgemeine Treiber:** Folgende allgemeine Treiber werden aktiviert, wenn Sie den Metaverzeichnis-Server aktivieren:
  - ♦ 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 5.2, „Installation einer Produktaktivierungsberechtigung“](#), auf [Seite 39](#) für jedes Identity Manager-Integrationsmodul ausführen, um die Treiber zu aktivieren.

## 5.5 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. Weitere Informationen finden Sie unter „[Activating Analyzer](#)“ (Aktivieren von Analyzer) im *Analyzer 4.0.1 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.1 für Identity Manager).

## 5.6 Aktivieren von Designer und dem Rollenzuordnungsadministrator

Designer und der Rollenzuordnungsadministrator erfordern keine weiteren Aktivierungen zusätzlich zur Aktivierung des Metaverzeichnis-Servers oder der Treiber.

# Aufrüsten von Identity Manager

# 6

Sie können Identity Manager-Komponenten nicht durch das integrierte Installationsprogramm aktualisieren. Verwenden Sie die individuellen Produktinstallationsprogramme für die Aufrüstung auf Identity Manager 4.0.1. Für die Aufrüstung von der Identity Manager 4.0.1 Standard Edition auf die Advanced Edition gibt es ein anderes Verfahren, das nur Konfigurationsänderungen beinhaltet. Für diese Aufrüstung müssen Sie nicht das Identity Manager-Installationsprogramm ausführen. Weitere Informationen zu Aufrüstungen von Identity Manager finden Sie im Abschnitt „[Aufrüsten](#)“ im *Identity Manager 4.0.1 Aufrüstungs- und Migrationshandbuch*.



# Fehlerbehebung in Identity Manager

# 7

Beachten Sie die folgenden Informationen, wenn Sie Identity Manager mithilfe des integrierten Installationsprogramms installieren:

- ♦ „Probleme bei der Installation“ auf Seite 45
- ♦ „Übergeben obligatorischer Parameter während der Konfiguration“ auf Seite 46
- ♦ „Die Konfiguration schlägt fehl, wenn die Datei „hosts“ den Eintrag „127.0.0.2“ enthält“ auf Seite 46
- ♦ „Das Installationsprogramm gibt „java.io.FileNotFoundException“ aus“ auf Seite 47
- ♦ „Der Baumname wird automatisch generiert, wenn der Baumname bereits vorhanden ist“ auf Seite 47
- ♦ „Sekundärserver-Installation“ auf Seite 47
- ♦ „Dienste werden nicht ausgeführt“ auf Seite 47
- ♦ „Erkennung des aktuellen Systemstatus“ auf Seite 47
- ♦ „Das integrierte Installationsprogramm hängt sich unter Windows möglicherweise während der Identity Manager-Deinstallation auf“ auf Seite 48
- ♦ „Beim Installieren der Windows-Laufzeit-Distribution wird möglicherweise aufgrund eines Installationsfehlers ein Neustart erzwungen“ auf Seite 48
- ♦ „Konfiguration der ISO, die unter UNIX über Drittanbieter-ISO-Extraktionswerkzeuge extrahiert wurde“ auf Seite 48
- ♦ „Das Aktivieren von XDAS beeinträchtigt die Leistung“ auf Seite 48
- ♦ „Deinstallationsprobleme bei Identity Manager-Komponenten“ auf Seite 49

## Probleme bei der Installation

**Aktion:** Falls während der Installation von Identity Manager Fehler auftreten, stellen Sie sicher, dass Sie je nach Plattform wie folgt auf die Protokolldateien verweisen:

- ♦ **Linux/Solaris:** /var/opt/novell/idm/install/logs/
- ♦ **Windows:** Der Standard-Speicherort ist C:\novell\IdentityManager\install\logs\. Sie können den Speicherort der Protokolldateien basierend auf dem von Ihnen angegebenen Installationspeicherort ändern.

**Aktion:** Typische Fehler können Sie mithilfe der Datei `ii_install.log` bei Installationsproblemen, der Datei `ii_configure.log` bei Konfigurationsproblemen, der Datei `ii_upgrade.log` bei Aufrüstungsproblemen und der Datei `ii_uninstall.log` bei Deinstallationsproblemen ermitteln. Suchen Sie in den Protokolldateien nach dem Text „exit value = xxx“. Wenn der Wert ungleich 0 ist, ist die Ausführung

eines bestimmten Befehls fehlgeschlagen, wodurch eine Protokolldatei generiert wird. In dieser Protokolldatei finden Sie weitere Details zu dem Fehler.

Beispiel:

```
"/home/siva/build/products/Reporting/IDMReport.bin" -  
DIA_USER_JRE_HOME="/opt/nov  
ell/idm/jre" -i silent -f "/tmp/  
idmreporting_configure.properties"  
execute command  
  exitValue = 1  
log file location  :/tmp/idmreporting_configure.properties  
log file location  :/opt/novell/idm/rbpm/IDMReporting//  
RPT_Install.log
```

Das oben stehende Snippet aus der Datei `ii_install.log` gibt an, dass der Befehl fehlgeschlagen ist, da der Wert von „exitValue“ 1 (also ungleich Null) ist. Ziehen Sie zur weiteren Analyse wie im Befehl angezeigt die Datei `/opt/novell/idm/rbpm/IDMReporting/RPT_Install.log` heran.

## Übergeben obligatorischer Parameter während der Konfiguration

Ursprung: Während der Konfiguration zeigt das Installationsprogramm nach der Angabe der Konfigurationsparameter möglicherweise die folgende Fehlermeldung an:

```
Some of the inputs are not proper. They are highlighted in  
Red.
```

Mögliche Ursache: Basierend auf dem markierten Parameter könnte die Fehlermeldung eine der folgenden Ursachen haben:

- ♦ Die Portnummer wird bereits verwendet.
- ♦ Der übergebene DNS-Hostname ist ungültig.
- ♦ Das DN-Format ist falsch.

Aktion: Führen Sie folgende Schritte aus:

- ♦ Wenn der Port bereits verwendet wird, verwenden Sie eine andere Portnummer.
- ♦ Geben Sie einen gültigen DNS-Namen oder, wenn Sie keinen DNS-Namen angeben möchten, eine gültige IP-Adresse an.
- ♦ Überprüfen Sie, ob ein gültiger DN im LDAP-Format angegeben ist.

## Die Konfiguration schlägt fehl, wenn die Datei „hosts“ den Eintrag „127.0.0.2“ enthält

Mögliche Ursache: Wenn die Datei `/etc/hosts` einen Eintrag mit der Loopback-Adresse 127.0.0.2 enthält, wird das Standard-IP-Zertifikat für die Loopback-Adresse 127.0.0.2 erstellt.

Aktion: Es gibt zwei mögliche Ausweichlösungen:

- ♦ Bearbeiten Sie die Datei `/etc/hosts`, wenn die Datei „hosts“ einen Eintrag mit der Loopback-Adresse 127.0.0.2 enthält.

Beispiel: 127.0.0.2 Hostname. Kommentieren Sie den Eintrag aus und stellen Sie sicher, dass der richtige IP-Adresseneintrag in der Datei enthalten ist.

### Das Installationsprogramm gibt „`java.io.FileNotFoundException`“ aus

Mögliche Ursache: Wenn das Systemverzeichnis `tmp` nicht vorhanden ist, gibt das Installationsprogramm diese Ausnahme kurz nach dem Aufrufen des Installationsprogramms aus.

Aktion: Erstellen Sie das Systemverzeichnis `tmp`.

### Der Baumname wird automatisch generiert, wenn der Baumname bereits vorhanden ist

Ursprung: Das integrierte Installationsprogramm versucht, den Baumnamen automatisch zu generieren, falls der entsprechende Baumname bereits vorhanden ist.

### Sekundärserver-Installation

Erklärung: Das integrierte Installationsprogramm fügt die Reproduktion, die das Serverobjekt enthält, zu allen Sekundärserver-Installationen hinzu. Es wartet darauf, dass die Reproduktion eingeschaltet wird.

### Dienste werden nicht ausgeführt

Erklärung: Einige Dienste werden möglicherweise nicht ausgeführt, weil die von ihnen benötigten Ports belegt sind.

Aktion: Stellen Sie sicher, dass die folgenden Ports frei sind, bevor Sie die Installation starten. Führen Sie den Befehl `netstat -anp | egrep` aus, um zu überprüfen, ob diese Ports frei sind.

```
netstat -anp | egrep
': (524 | 389 | 636 | 8028 | 8030 | 8090 | 8000 | 7707 | 8006
| 8009 | 8081 | 8443 | 8009 | 8080 | 8443 | 1199 | 1198 | 119
0 | 3973 | 4544 | 4545 | 4546 | 4557 | 4812 | 4813 | 8109 | 81
83 | 8180 | 8543 | 29007 | 37022 | 8180 | 10013 | 10014 | 61
616 | 61617 | 1514 | 15432 | 5556 | 1289 | 1443 | 1468) '
```

### Erkennung des aktuellen Systemstatus

Erklärung: Stellen Sie sicher, dass Sie die Statusdatei des Installationsprogramms sichern. Die integrierte Statusdatei ist eine wichtige Konfigurationsdatei, die vom Installationsprogramm für Informationen wie den aktuellen Status des Systems, die installierten Komponenten, die konfigurierten Komponenten oder die deinstallierten Komponenten verwendet wird.

Aktion: Sichern Sie die Statusdatei wie folgt:

- ♦ **Linux/Solaris:** Führen Sie `/etc/opt/novell/idm/install/conf/install_state.conf` aus.

- ♦ **Windows:** Führen Sie C:\Novell\conf\install\_state.conf aus.

### **Das integrierte Installationsprogramm hängt sich unter Windows möglicherweise während der Identity Manager-Deinstallation auf**

**Mögliche Ursache:** Das Installationsprogramm versucht, alle abhängigen Dienste vor der Deinstallation von Identity Manager anzuhalten. Manchmal ist das Installationsprogramm nicht in der Lage, den DHost-Dienst anzuhalten, da einige Dienste vom DHost-Dienst abhängig sind.

**Aktion:** Führen Sie folgende Schritte aus, um zu prüfen, ob sich das Installationsprogramm während der Deinstallation des Identitätsdepots aufgehängt hat:

- 1** Wechseln Sie zur *Systemsteuerung*, öffnen Sie *Novell eDirectory Services* und klicken Sie auf die Schaltfläche *Start*. Falls sich das Installationsprogramm aufhängt, wird folgende Meldung angezeigt:

```
Novell eDirectory Service is in a NT service Stop Pending State.
```

- 2** Halten Sie den DHost-Dienst manuell über den Task-Manager an, um mit der Deinstallation fortzufahren.

### **Beim Installieren der Windows-Laufzeit-Distribution wird möglicherweise aufgrund eines Installationsfehlers ein Neustart erzwungen**

**Erklärung:** Die Metaverzeichnis-Installation schlägt mit der folgenden Meldung in der Datei <Installationsverzeichnis>\ii\_install.log fehl:

```
: \Users\Administrator\IDM4\products\eDirectory\x64\windows\x64\redist_pkg\vcredist_x86.exe" /q:a /c:"msiexec /i vcredist.msi /qn /l C:\Users\ADMINI~1\AppData\Local\Temp\vcredist32_Windows_x64_Install.log" execute command exitValue = 3010
```

**Aktion:** Der von der Programmdatei „vcredist“ zurückgegebene Fehlercode 3010 gibt einen Erfolg an, was bedeutet, dass Sie den Windows-Computer neu starten müssen. Starten Sie nach dem Neustartvorgang das Installationsprogramm neu. Die Installation wird normal fortgesetzt. Der Neustart des Computers wirkt sich nicht auf die früheren, erfolgreichen Installationen aus.

### **Konfiguration der ISO, die unter UNIX über Drittanbieter-ISO-Extraktionswerkzeuge extrahiert wurde**

**Erklärung:** Die Konfiguration des integrierten Installationsprogramms von Identity Manager 4.0.1 schlägt fehl, wenn die ISO unter UNIX über Drittanbieter-ISO-Extraktionswerkzeuge extrahiert wird.

**Aktion:** Verwenden Sie für eine erfolgreiche Konfiguration den Befehl `mount -o loop`.

### **Das Aktivieren von XDAS beeinträchtigt die Leistung**

**Mögliche Ursache:** Wenn die XDAS-Ereignisprotokollierung aktiviert ist, wird die Leistung der Identity Manager-Engine ohne SLP-Konfiguration verringert.



Aktion: SLP muss korrekt konfiguriert sein und ausgeführt werden, um sicherzustellen, dass die Leistung nicht beeinträchtigt wird.

## Deinstallationsprobleme bei Identity Manager-Komponenten

Ursprung: Wenn während der Deinstallation eine oder mehrere Komponenten nicht deinstalliert werden konnten, ist die Option *Deinstallieren* deaktiviert, wenn Sie versuchen, die Deinstallation zu wiederholen. Ein Grund für den Deinstallationsfehler unter Windows kann darin liegen, dass die Umgebungsvariablen JAVA\_HOME und PATH nicht festgelegt sind.

Aktion: Führen Sie die Deinstallationsprogramme für die einzelnen Komponenten wie folgt aus:

- ♦ **Linux/Solaris:** Führen Sie den folgenden Befehl aus, um die einzelnen Komponenten zu deinstallieren:
  - ♦ **Metaverzeichnis:** Deinstallieren Sie das Identity Manager-Framework:

```
/root/idm/Uninstall_Identity_Manager/  
Uninstall_Identity_Manager
```

Deinstallieren Sie das Identitätsdepot:

```
/opt/novell/eDirectory/sbin/nds-uninstall
```
  - ♦ **JBoss:** Führen Sie den folgenden Befehl aus:

```
$IA_RBPM_POSTGRESQL_INSTALL_PATH$/  
JBossPostgreSQL_Uninstaller/Uninstall_JBossPostgreSQL
```
  - ♦ **Rollenbasiertes Bereitstellungsmodul:** Führen Sie den folgenden Befehl aus:

```
java -jar /opt/novell/idm/rbpm/RemoveUserApp/  
uninstaller.jar
```
  - ♦ **Identitätsberichterstellungsmodul:** Führen Sie den folgenden Befehl aus:

```
/opt/novell/idm/rbpm/Uninstall_Identity_Reporting/  
Uninstall_Identity_Reporting
```
  - ♦ **Event Auditing Service:** Führen Sie den folgenden Befehl aus:

```
/opt/novell/sentinel_eas/Uninstall_Event_Auditing  
Service/Uninstall_Event_Auditing_Service
```
  - ♦ **Rollenzuordnungsadministrator:** Führen Sie den folgenden Befehl aus:

```
/opt/novell/idm/rma/rma-uninstall.sh -s
```
  - ♦ **Designer:** Führen Sie den folgenden Befehl aus:

```
/opt/novell/idm/Designer/UninstallDesigner/Uninstall  
Designer_for_Identity_Manager
```
  - ♦ **Analyzer:** Führen Sie den folgenden Befehl aus:

```
/opt/novell/idm/Analyzer/UninstallAnalyzer/Uninstall  
Analyzer_for_Identity_Manager
```
  - ♦ **iManager:** Führen Sie den folgenden Befehl aus:

```
/var/opt/novell/tomcat5/webapps/nps/UninstallerData/  
UninstalliManager
```

- ♦ **Windows:** Deinstallieren Sie alle Komponenten mit Ausnahme des Rollenzuordnungsadministrators über *Windows > Software*. Führen Sie zum Deinstallieren des Rollenzuordnungsadministrators den Befehl `C:\novell\IdentityManager\RMA\rma-uninstall.bat` über die Befehlszeile aus.

# Deinstallation von Identity Manager

# 8

Das Deinstallationskript deinstalliert alle Identity Manager-Komponenten, die mit dem integrierten Installationsprogramm installiert wurden. Informationen zum Deinstallieren einzelner Komponenten finden Sie unter „[Deinstallation von Identity Manager](#)“ im *Identity Manager 4.0.1 Framework Installationshandbuch*.

## 8.1 GUI-Deinstallation

Stellen Sie sicher, dass die Umgebungsvariablen JAVA\_HOME und PATH auf Java verweisen, bevor das integrierte Deinstallationsprogramm aufgerufen wird.

So deinstallieren Sie die Identity Manager-Komponenten:

- 1 Führen Sie die Deinstallation aus, indem Sie das entsprechende Programm für Ihre Plattform verwenden:

- ♦ **Linux/Solaris:** `./Uninstall_Identity Manager Components.bin`

Die Binärdatei befindet sich unter `/opt/novell/idm/Uninstall_Identity Manager Components/Uninstall Identity Manager Components.bin`.

- ♦ **Windows:** `Uninstall_Identity Manager Components.exe`

Das Deinstallationsprogramm befindet sich unter `<Installationsordner>\Uninstall_Identity Manager Components\Uninstall_Identity Manager Components.exe`. Klicken Sie auf *Software* und deinstallieren Sie die Identity Manager-Komponenten.

---

**Hinweis:** Durch die Deinstallation des Identitätsdepos werden nicht alle Dateien entfernt. Weitere Informationen hierzu finden Sie in der [Dokumentation zur Deinstallation von eDirectory](http://www.novell.com/documentation/edir88/edirin88/data/bnn8twh.html) (<http://www.novell.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 jede dieser Komponenten im LDAP-Format an und klicken Sie anschließend 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 Automatische 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`
- ♦ **Solaris:** `./install/propfiles/uninstall.properties`
- ♦ **Windows:** `\install\propfiles\uninstall.properties`

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

- ♦ **Linux:** `/opt/novell/idm/Uninstall_Identity Manager Components/Uninstall Identity Manager Components.bin -i silent -f <Dateiname>.properties`
- ♦ **Solaris:** `/opt/novell/idm/Uninstall_Identity Manager Components/Uninstall Identity Manager Components.bin -i silent -f <Dateiname>.properties`
- ♦ **Windows:** `<Installationsordner>\Uninstall_Identity Manager Components/Uninstall Identity Manager Components.exe -i silent -f <Dateiname>.properties`