

Handbuch zur integrierten Installation

Novell® Identity Manager

4.0

15. Oktober 2010

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 © 2010, 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

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

Informationen zu diesem Handbuch	7
1 Überblick über das integrierte Installationsprogramm	9
1.1 Integriertes und eigenständiges Installationsprogramm	9
1.2 Konfigurieren von Treibern	10
2 Identity Manager-Komponenten	13
2.1 Metaverzeichnis-Server (Identitätsdepot, Metaverzeichnis-Engine und Remote Loader)	14
2.1.1 Unterstützte Prozessoren	14
2.1.2 Server-Betriebssysteme	14
2.2 Revision und Berichterstellung	16
2.3 Benutzeranwendung	16
2.4 Rollenzuordnungsadministrator	17
2.5 iManager, Designer und Analyzer	17
2.6 Webbrowser	18
2.7 Identitätsdepot-Struktur	18
2.7.1 Sicherheit	20
2.7.2 Daten	20
2.7.3 System	20
3 Systemanforderungen	23
3.1 Unterstützte Plattformen	23
3.2 Anforderungen	24
4 Installation von Identity Manager	25
4.1 Herunterladen der ISO-Datei von der Download-Site	25
4.2 Neuinstallation mithilfe physischer Medien oder eines ISO-Images	26
4.2.1 Installation	26
4.2.2 Konfiguration	28
4.3 Automatische Installation und Konfiguration	35
4.3.1 Automatische Installation	36
4.3.2 Automatische Konfiguration	36
5 Aktivieren von Novell Identity Manager-Produkten	39
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	41
5.6 Aktivieren von Designer und dem Rollenzuordnungsadministrator	42
6 Aufrüsten von Identity Manager	43
6.1 Backup der aktuellen Konfiguration erstellen	43

6.1.1	Sicherstellen, dass Ihr Designer-Projekt aktuell ist	43
6.1.2	Exportieren der Treiberdaten	45
6.2	Anhalten der Treiber	46
6.2.1	Anhalten der Treiber mithilfe von Designer	46
6.2.2	Anhalten der Treiber mithilfe von iManager	46
6.3	Aufrüstung von Designer	46
6.4	Aufrüsten des Metaverzeichnis-Servers (Identitätsdepot, Metaverzeichnis-Engine und Remote Loader)	47
6.5	Aufrüsten von Treibern auf Pakete	49
6.5.1	Einen neuen Treiber erstellen	49
6.5.2	Vorhandene Inhalte durch Inhalte aus Paketen ersetzen	49
6.5.3	Aktuelle Inhalte beibehalten und neue Inhalte über Pakete hinzufügen	50
6.6	Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber	50
6.6.1	Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von Designer	51
6.6.2	Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von iManager	52
6.7	Bereitstellen des konvertierten Projekts	53
6.8	Starten der Treiber	53
6.8.1	Starten der Treiber mithilfe von Designer	53
6.8.2	Starten der Treiber mithilfe von iManager	53
7	Fehlerbehebung in Identity Manager	55
8	Deinstallation von Identity Manager	61

Informationen zu diesem Handbuch

Novell Identity Manager 4.0 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 9](#)
- ♦ [Kapitel 2, „Identity Manager-Komponenten“, auf Seite 13](#)
- ♦ [Kapitel 3, „Systemanforderungen“, auf Seite 23](#)
- ♦ [Kapitel 4, „Installation von Identity Manager“, auf Seite 25](#)
- ♦ [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 55](#)
- ♦ [Kapitel 8, „Deinstallation von Identity Manager“, auf Seite 61](#)

Zielgruppe

Dieses Handbuch richtet sich an Administratoren, Berater und Netzwerkengineure, 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, und geben Sie dort Ihre Kommentare ein.

Aktualisierungen für Dokumentationen

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 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 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 9
- ♦ [Abschnitt 1.2, „Konfigurieren von Treibern“](#), auf Seite 10

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 Abschnitt 2.7, „Identitätsdepot-Struktur“ , auf Seite 18.	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.
Installationsdauer	Automatisiert verschiedene manuelle Schritte für die schnelle Einrichtung des Systems.	Dauert in der Regel länger.

Funktionen	Integriert	Eigenständig
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 Framework Installationshandbuch](#) zu Rate. Installationsanweisungen finden Sie im Abschnitt „Installation“ im [Identity Manager 4.0 Framework Installationshandbuch](#).

Das integrierte Installationsprogramm wird hauptsächlich für neue Installationen von Identity Manager 4.0 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-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

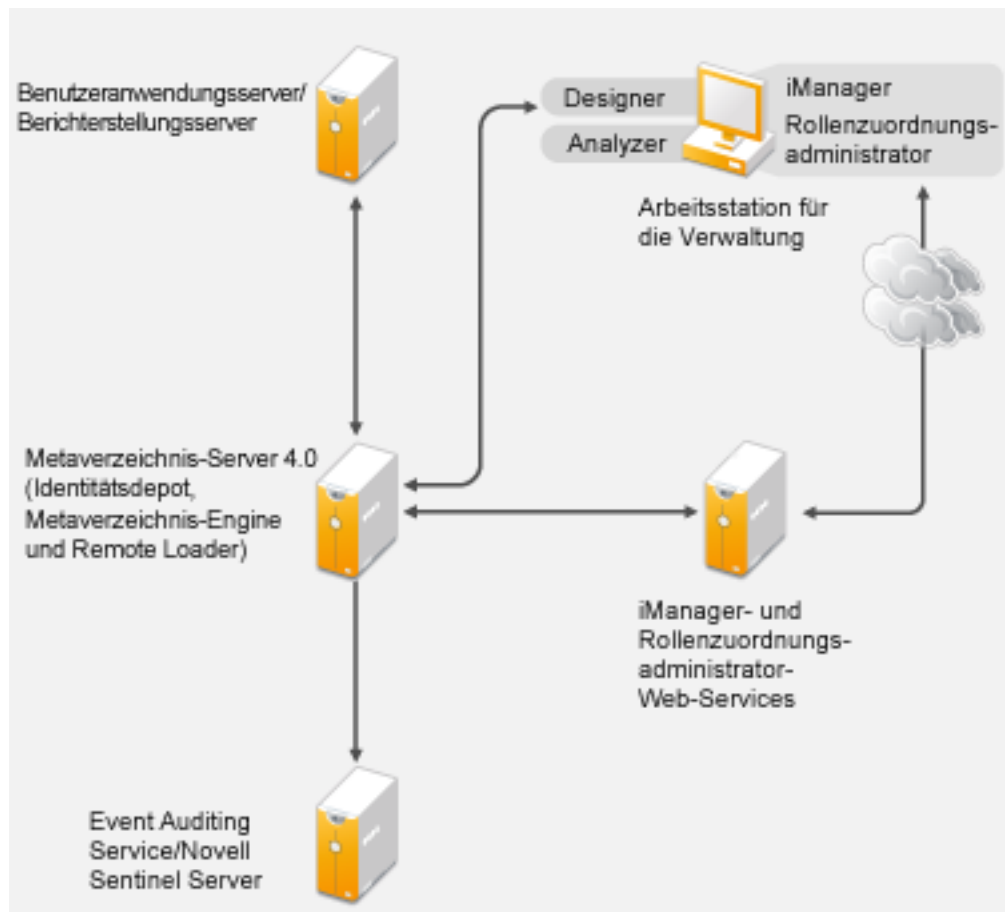
Das integrierte Installationsprogramm konfiguriert die erforderlichen Treiber für das rollenbasierte Bereitstellungsmodul und das Identitätsberichterstellungsmodul. Informationen zum Konfigurieren zusätzlicher Treiber finden Sie auf der [Website zur Identity Manager 4.0 Treiber-Dokumentation](http://www.novell.com/documentation/idm40drivers/) (<http://www.novell.com/documentation/idm40drivers/>).

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 14
- ◆ Abschnitt 2.2, „Revision und Berichterstellung“, auf Seite 16
- ◆ Abschnitt 2.3, „Benutzeranwendung“, auf Seite 16
- ◆ Abschnitt 2.4, „Rollenzuordnungsadministrator“, auf Seite 17
- ◆ Abschnitt 2.5, „iManager, Designer und Analyzer“, auf Seite 17
- ◆ Abschnitt 2.6, „Webbrowser“, auf Seite 18
- ◆ Abschnitt 2.7, „Identitätsdepot-Struktur“, auf Seite 18

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 eDirectory automatisch installiert.

- ♦ [Abschnitt 2.1.1, „Unterstützte Prozessoren“, auf Seite 14](#)
- ♦ [Abschnitt 2.1.2, „Server-Betriebssysteme“, auf Seite 14](#)

2.1.1 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.

2.1.2 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.

Version des Server-Betriebssystems	Hinweise
SUSE Linux Enterprise Server 10 SP3 (32 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 (32 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.
Zonen in Solaris	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.

Der Remote Loader gibt Ihnen mehr Flexibilität bei der Konfiguration Ihrer Identity Manager-Lösung. Er unterstützt sowohl die 32-Bit- als auch die 64-Bit-Version. Standardmäßig erkennt das Installationsprogramm die Betriebssystemversion und installiert anschließend die entsprechende Version des Remote Loaders. In [Tabelle 2-1 auf Seite 14](#) werden die unterstützten Betriebssysteme für den Remote Loader aufgelistet.

Identity Manager 4.0 lässt zu, dass die 32-Bit- und die 64-Bit-Version von Remote Loader auf einem 64-Bit-Betriebssystem gleichzeitig installiert sind. Wenn Sie eine 32-Bit-Version von Remote Loader auf einem 64-Bit-Betriebssystem aufrüsten, rüstet der Prozess den 32-Bit-Remote Loader auf und installiert darüber hinaus den 64-Bit-Remote Loader. Sie können den 32-Bit- und den 64-Bit-Remote Loader auf demselben Computer installieren.

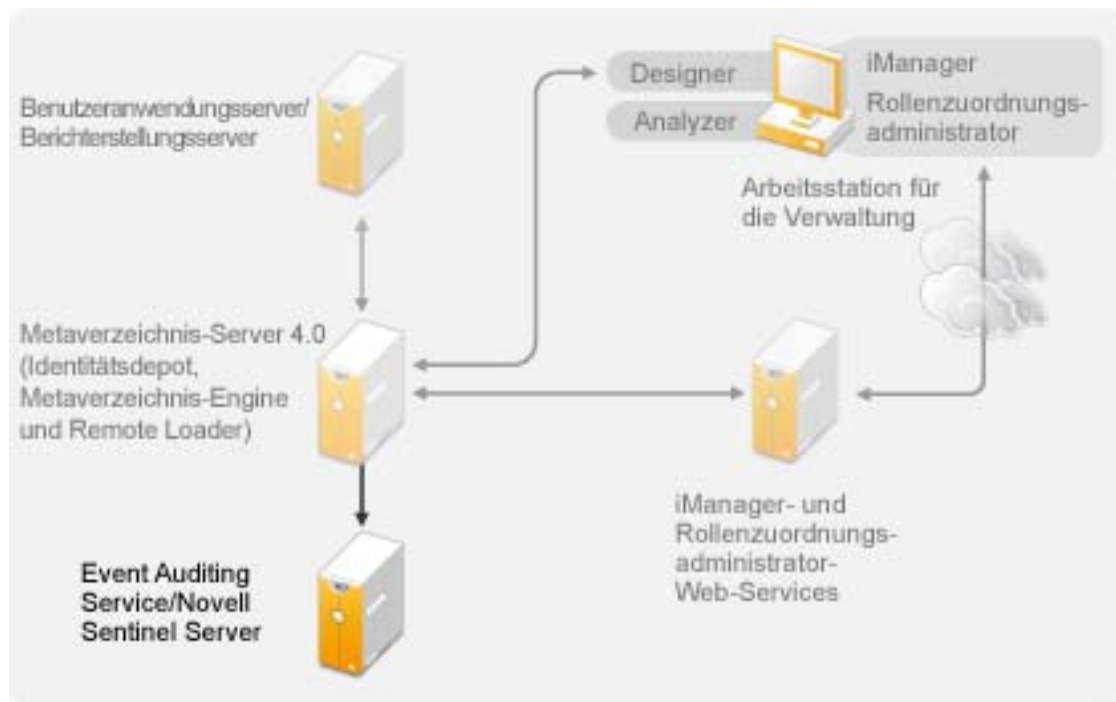
2.2 Revision und Berichterstellung

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 Sammeln von Revisions- und Berichtsdaten über Identity Manager verwendet werden.

Das Identitätsberichterstellungsmodul ist eine Komponente von Identity Manager 4.0. 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 hierzu finden Sie im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul). Informationen zur Konfiguration von Novell Sentinel mit Identity Manager finden Sie im *Identity Manager 4.0 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>) (Novell Sentinel Installationshandbuch).

2.3 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 verwendet JBoss und PostgreSQL als Anwendungsserver bzw. Datenbank.

Eine Liste der Systemanforderungen für die Benutzeranwendung finden Sie im [Identity Manager Roles Based Provisioning Module 4.0 User Application: Installation Guide](#) (Rollenbasiertes Bereitstellungsmodul für Identity Manager 4.0 Benutzeranwendung: Installationshandbuch).

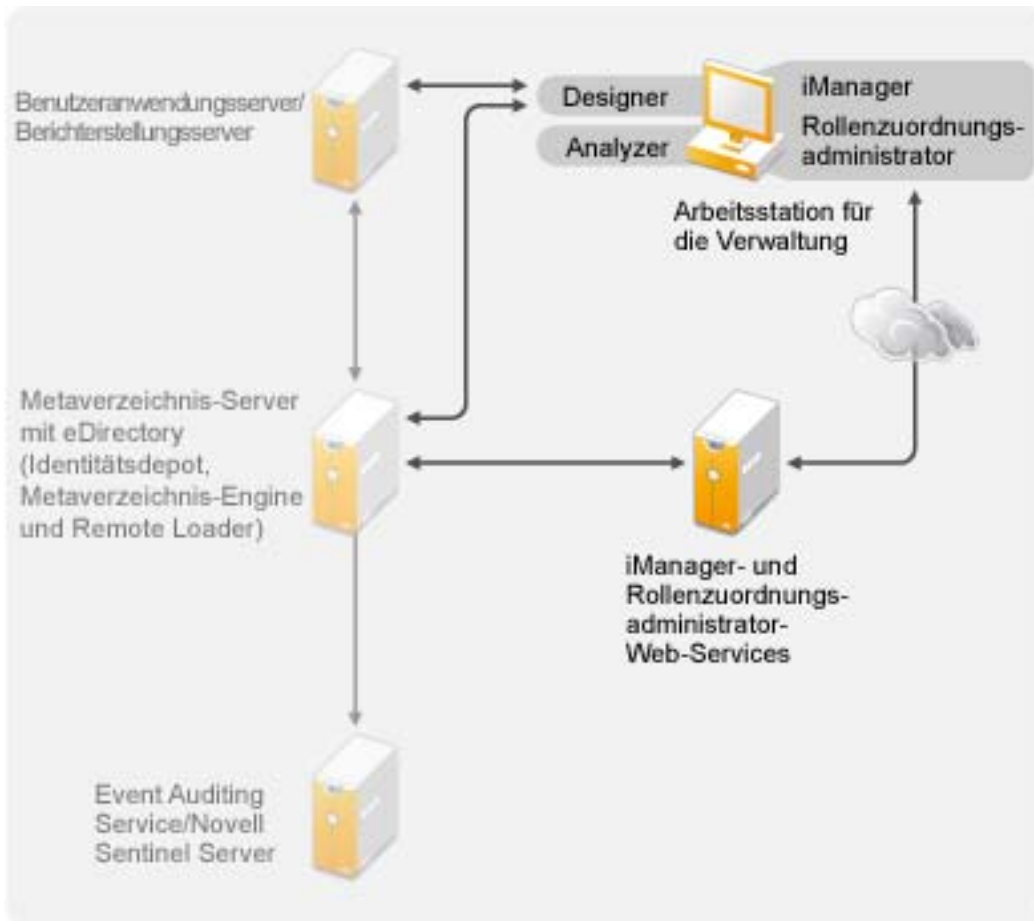
2.4 Rollenzuordnungsadministrator

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. Weitere Informationen finden Sie im [Benutzerhandbuch zum Novell Identity Manager-Rollenzuordnungsadministrator 2.0](#).

2.5 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



2.6 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

2.7 Identitätsdepot-Struktur

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

Abbildung 2-4 Identitätsdepot-Struktur

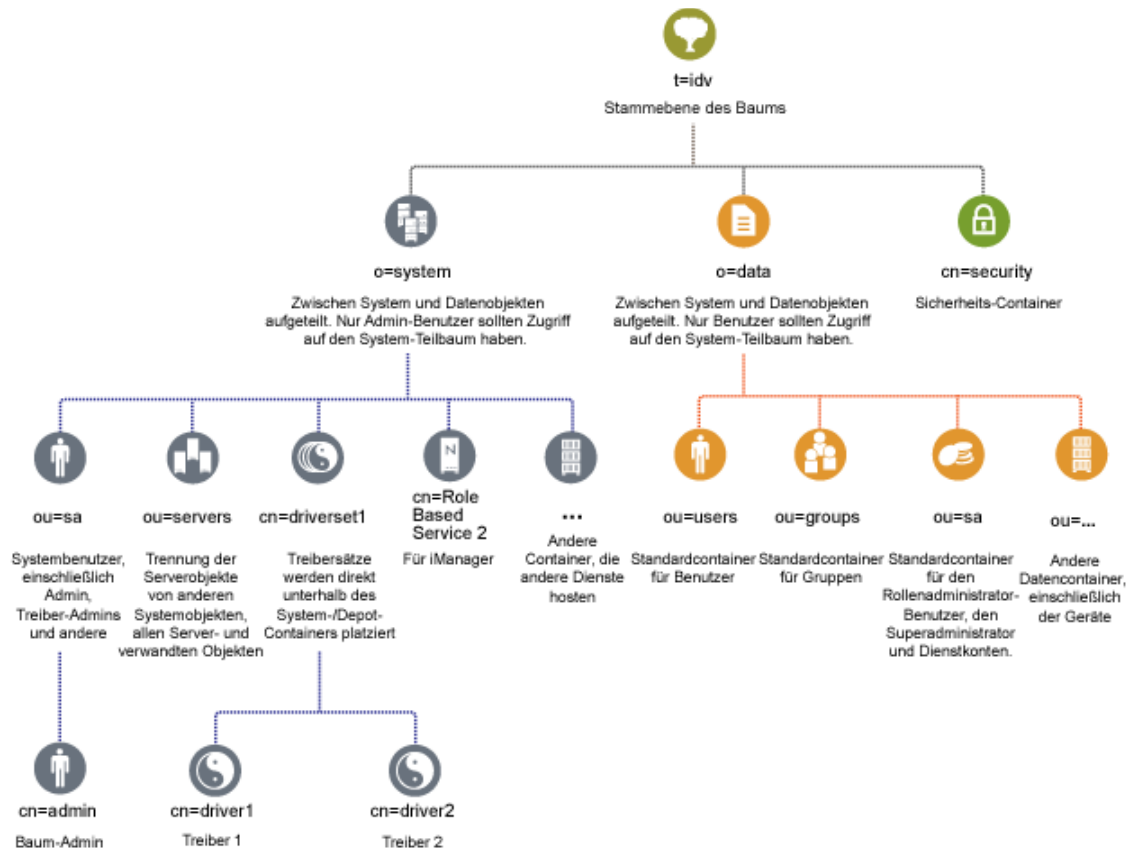


Abbildung 2-4 stellt die Identitätsdepot-Struktur für Identity Manager dar. Diese Struktur ist hauptsächlich für eine Installation in einer einzelnen Umgebung nützlich. Dies ist die Standardstruktur für kleine und mittlere Identity Manager-Bereitstellungen. Multi-Tenant-Umgebungen besitzen möglicherweise 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 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-Struktur ist auf Skalierbarkeit ausgerichtet, da sie drei Hauptkomponenten hat:

- ◆ Abschnitt 2.7.1, „Sicherheit“, auf Seite 20
- ◆ Abschnitt 2.7.2, „Daten“, auf Seite 20
- ◆ Abschnitt 2.7.3, „System“, auf Seite 20

2.7.1 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.

2.7.2 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.

2.7.3 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-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

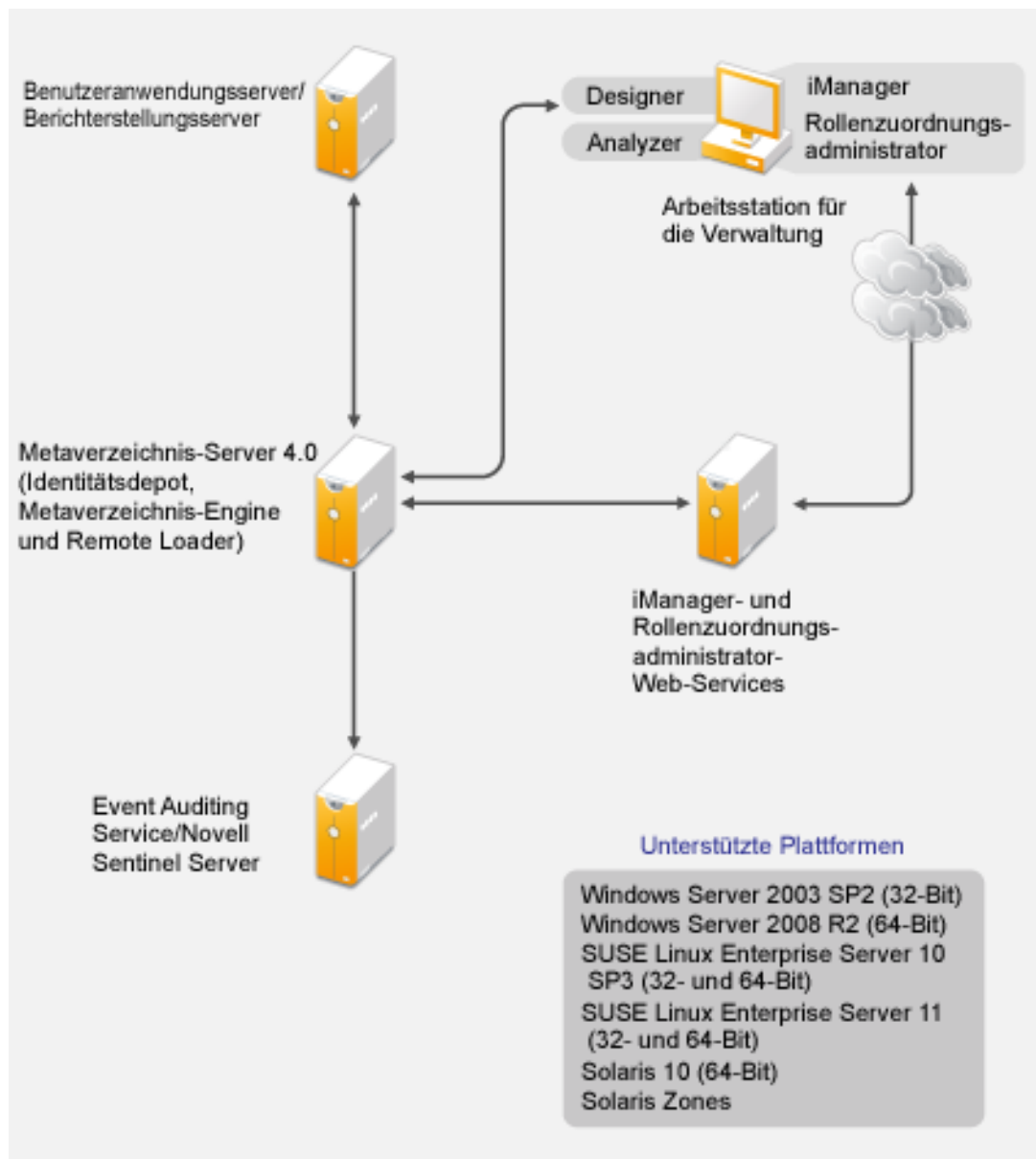
Die Komponenten von Novell Identity Manager können auf mehreren Systemen und Plattformen installiert werden.

- ♦ [Abschnitt 3.1, „Unterstützte Plattformen“, auf Seite 23](#)
- ♦ [Abschnitt 3.2, „Anforderungen“, auf Seite 24](#)

3.1 Unterstützte Plattformen

Abbildung 3-1 zeigt Plattformen, die vom integrierten Installationsprogramm von Novell Identity Manager 4.0 unterstützt werden.

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



- ♦ Das integrierte Installationsprogramm installiert oder konfiguriert Identity Manager-Komponenten nicht auf Red Hat Linux-Plattformen. Informationen zur Installation von Identity Manager-Komponenten auf RedHat Linux und anderen unterstützten Plattformen finden Sie in der jeweiligen Produktdokumentation.
- ♦ Bei Identity Manager 4.0 wird der Event Auditing Service nur auf der Linux-Plattform unterstützt.
- ♦ Bei Identity Manager 4.0 wird auf Solaris nur der Metaverzeichnis-Server unterstützt.
- ♦ Mit dem integrierten Installationsprogramm können das rollenbasierte Bereitstellungsmodul und das Identitätsberichterstellungsmodul nur auf einem Computer mit dem Identitätsdepot installiert werden.
- ♦ Einige Optionen für individuelle Komponenten, bei denen Benutzereingaben erforderlich sind, sind auf jeder Plattform unterschiedlich.

3.2 Anforderungen

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:

- ♦ 2048 MB RAM.
- ♦ 10 GB freier Festplattenspeicher, um alle Komponenten zu installieren.
- ♦ Weiterer Festplattenspeicher für die Konfiguration und Bereitstellung von Daten. Dies kann je nach den verbundenen Systemen 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 Framework Installationshandbuch* angegeben ist. Eine Erklärung der verschiedenen Komponenten finden Sie im Handbuch *Überblick über Identity Manager 4.0*.

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 9. Ausführliche Informationen zu jeder Komponente finden Sie im Handbuch *Überblick über Identity Manager 4.0*.

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 von der Download-Site“](#), auf Seite 25
- ♦ [Abschnitt 4.2, „Neuinstallation mithilfe physischer Medien oder eines ISO-Images“](#), auf Seite 26
- ♦ [Abschnitt 4.3, „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 von der Download-Site

Sie können 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, andernfalls 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 unter [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 *Produkt oder Technologie* den Eintrag *Identity Manager* aus und klicken Sie auf *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. Sie können ein entsprechendes ISO-Image gemäß Ihren Anforderungen auswählen. Jedes ISO-Image enthält die 32-Bit- und 64-Bit-Version des Produkts.
- 4 Befolgen Sie die Bildschirmanweisungen, um die Datei in einen Ordner auf Ihrem Computer herunterzuladen.

- 5 Wiederholen Sie die Schritte ab [Schritt 3](#), bis Sie alle erforderlichen Dateien heruntergeladen haben.
- 6 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.

Tabelle 4-1 Identity Manager-ISO-Images

ISO	Plattform	Beschreibung
<code>windows_identity_manager_enterprise_4.0.iso</code>	Windows	Enthält das DVD-Image für den Metaverzeichnis-Server, Designer, iManager, Rollenzuordnungsadministrator, Analyzer, das Identitätsberichterstellungsmodul und das rollenbasierte Bereitstellungsmodul.
<code>linux_identity_manager_enterprise_4.0.iso</code>	Linux	Enthält das DVD-Image für den Metaverzeichnis-Server, Event Auditing Service, Designer, iManager, Rollenzuordnungsadministrator, Analyzer, das Identitätsberichterstellungsmodul und das rollenbasierte Bereitstellungsmodul.
<code>solaris_identity_manager_enterprise_4.0.iso</code>	Solaris	Enthält das DVD-Image für den Metaverzeichnis-Server. Andere Komponenten werden auf der Solaris-Plattform nicht unterstützt.

4.2 Neuinstallation mithilfe physischer Medien oder eines ISO-Images

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 26
- ♦ [Abschnitt 4.2.2, „Konfiguration“](#), auf Seite 28

4.2.1 Installation

- 1 Greifen Sie auf die Identity Manager 4.0-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 unter [Abschnitt 4.1, „Herunterladen der ISO-Datei von der Download-Site“](#), auf Seite 25.

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

Linux: `./install.bin`

Solaris: `./install.bin`

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

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:

- ◆ Identitätsdepot
- ◆ Rollenbasiertes Bereitstellungsmodul
- ◆ Identitätsberichterstellungsmodul
- ◆ Event Auditing Service
- ◆ Rollenzuordnungsadministrator
- ◆ iManager
- ◆ Designer
- ◆ Analyzer

Hinweis: Wenn Sie das rollenbasierte Bereitstellungsmodul oder das Identitätsberichterstellungsmodul zur Installation auswählen, wird Designer automatisch ebenfalls zur Installation ausgewählt, da das Installationsprogramm Designer intern zum Erstellen der Treiberkonfiguration verwendet. Sie können das rollenbasierte Bereitstellungsmodul und das Identitätsberichterstellungsmodul nicht auf einem anderen System installieren, auf dem das Identitätsdepot nicht vorhanden ist. Sie müssen das rollenbasierte Bereitstellungsmodul und das Identitätsberichterstellungsmodul immer auf demselben Computer installieren. JBoss und PostgreSQL werden als Anwendungsserver bzw. Datenbank verwendet.

Ausgewählte Produkte anpassen: Wählen Sie diese Option aus, wenn Sie den Remote Loader mit dem Metaverzeichnis-Server installieren möchten.

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 Analyzer: `/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 28 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 26 abgeschlossen haben, bevor Sie mit der Konfiguration fortfahren.

So konfigurieren Sie die Identity Manager-Komponenten:

- 1 Wenn Sie von [Schritt 3 auf Seite 26](#) 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 28
 - ♦ [„Zu einem vorhandenen Baum hinzufügen“](#) auf Seite 32

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 29
 - ♦ [„Identitätsdepot > Erweitert“](#) auf Seite 29
 - ♦ [„Rollenbasiertes Bereitstellungsmodul \(RBPM\)“](#) auf Seite 30
 - ♦ [„Rollenbasiertes Bereitstellungsmodul \(RBPM\) > Erweitert“](#) auf Seite 30
 - ♦ [„Identitätsberichterstellungsmodul“](#) auf Seite 30
 - ♦ [„Identitätsberichterstellungsmodul > Erweitert“](#) auf Seite 31
 - ♦ [„Event Auditing Service“](#) auf Seite 32
 - ♦ [„Event Auditing Service > Erweitert“](#) auf Seite 32
 - ♦ [„iManager > Erweitert“](#) auf Seite 32
- 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 unter „[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/a7f08yl.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.

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.

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.

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.

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`

LDAP-Serveradresse: Geben Sie die IP-Adresse und den Port des LDAP-Servers ein.

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

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 33
- ♦ „[Identitätsdepot > Erweitert](#)“ auf Seite 33

- ◆ „Metaverzeichnis-Server“ auf Seite 34
- ◆ „Rollenbasiertes Bereitstellungsmodul (RBPM)“ auf Seite 34
- ◆ „Rollenbasiertes Bereitstellungsmodul (RBPM) > Erweitert“ auf Seite 35
- ◆ „Identitätsberichterstellungsmodul“ auf Seite 35
- ◆ „Event Auditing Service“ auf Seite 35
- ◆ „iManager > Erweitert“ auf Seite 35

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 unter „[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 Administratorname des vorhandenen Servers gleich dem Administratorkontext-DN des vorhandenen Baums und der Admin-Kontext-DN des vorhandenen Servers gleich dem Administrator-Kontext-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-Anschluss: Behalten Sie entweder den Standardwert von 389 für den LDAP-Port bei oder ändern Sie den Wert des Ports.

Sicherer LDAP-Anschluss: 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/a7f08yl.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.

Passwort des idadmin-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.

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

Rollenbasiertes Bereitstellungsmodul (RBPM) > Erweitert

Die erweiterten Konfigurationsoptionen des RBPMs sind für die Konfiguration neuer und vorhandener Bäume gleich. Weitere Informationen finden Sie unter [„Rollenbasiertes Bereitstellungsmodul \(RBPM\) > Erweitert“ auf Seite 30](#).

Identitätsberichterstellungsmodul

Die Konfigurationsoptionen des Identitätsberichterstellungsmoduls sind für die Konfiguration neuer und vorhandener Bäume gleich. Weitere Informationen finden Sie unter [„Identitätsberichterstellungsmodul“ auf Seite 30](#) und [„Identitätsberichterstellungsmodul > Erweitert“ auf Seite 31](#).

Event Auditing Service

Die Konfigurationsoptionen des Event Auditing Services sind für die Konfiguration neuer und vorhandener Bäume gleich. Weitere Informationen finden Sie unter [„Event Auditing Service“ auf Seite 32](#) und [„Event Auditing Service > Erweitert“ auf Seite 32](#).

iManager > Erweitert

Die Konfigurationsoptionen von iManager sind für die Konfiguration neuer und vorhandener Bäume gleich. Weitere Informationen finden Sie unter [„iManager > Erweitert“ auf Seite 32](#).

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	<code><Installationsverzeichnis>\install \logs</code> Der Standard-Speicherort ist <code>C:\Novell\IdentityManager\install\ logs</code>	<code><Installationsverzeichnis>\install\propfiles</code> Der Standard-Speicherort ist <code>C:\Novell\IdentityManager\install\ \logs\propfiles\</code>
Linux/ Solaris	<code>/var/opt/novell/idm/install/logs</code>	<code>/var/opt/novell/idm/install/logs/ propfiles/</code>

4.3 Automatische Installation und Konfiguration

- ◆ [Abschnitt 4.3.1, „Automatische Installation“, auf Seite 36](#)
- ◆ [Abschnitt 4.3.2, „Automatische Konfiguration“, auf Seite 36](#)

4.3.1 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`.

4.3.2 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 diesen 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_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`

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 41
- ♦ [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-----).

- 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-Berechtigungs-nachweis 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 Berechtigungs-nachweis 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 Berechtigungs-nachweises anzeigen oder bei einer Fehlermeldung einen Berechtigungs-nachweis 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 1.2 for Identity Manager Administration Guide](#) (Administrationshandbuch zu Analyzer 1.2 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 das integrierte Installationsprogramm verwenden, um das Identitätsdepot und den Metaverzeichnis-Server aufzurüsten. Wenn Sie das rollenbasierte Bereitstellungsmodul installiert haben oder eine Migration auf neue Hardware durchführen, lesen Sie die Informationen unter „[Aufrüsten oder Migrieren](#)“ im *Identity Manager 4.0 Framework Installationshandbuch*.

- ♦ [Abschnitt 6.1, „Backup der aktuellen Konfiguration erstellen“](#), auf Seite 43
- ♦ [Abschnitt 6.2, „Anhalten der Treiber“](#), auf Seite 46
- ♦ [Abschnitt 6.3, „Aufrüstung von Designer“](#), auf Seite 46
- ♦ [Abschnitt 6.4, „Aufrüsten des Metaverzeichnis-Servers \(Identitätsdepot, Metaverzeichnis-Engine und Remote Loader\)“](#), auf Seite 47
- ♦ [Abschnitt 6.5, „Aufrüsten von Treibern auf Pakete“](#), auf Seite 49
- ♦ [Abschnitt 6.6, „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“](#), auf Seite 50
- ♦ [Abschnitt 6.7, „Bereitstellen des konvertierten Projekts“](#), auf Seite 53
- ♦ [Abschnitt 6.8, „Starten der Treiber“](#), auf Seite 53

6.1 Backup der aktuellen Konfiguration erstellen

Vor der Aufrüstung ist es wichtig, ein Backup der aktuellen Konfiguration Ihres Identity Manager-Systems zu erstellen. Backups können auf zwei verschiedene Weisen erstellt werden:

- ♦ [Abschnitt 6.1.1, „Sicherstellen, dass Ihr Designer-Projekt aktuell ist“](#), auf Seite 43
- ♦ [Abschnitt 6.1.2, „Exportieren der Treiberdaten“](#), auf Seite 45

6.1.1 Sicherstellen, dass Ihr Designer-Projekt aktuell ist

Ein Designer-Projekt enthält das Schema und alle Treiberkonfigurationsinformationen. Wenn Sie ein Projekt Ihrer Identity Manager-Lösung erstellen, können Sie Ihre gesamten Treiber in einem Schritt exportieren, statt einzelne Exportdateien für jeden Treiber zu erstellen.

- ♦ [„Exportieren des aktuellen Projekts“](#) auf Seite 43
- ♦ [„Erstellen eines neuen Projekts aus dem Identitätsdepot“](#) auf Seite 44

Exportieren des aktuellen Projekts

Wenn Sie bereits ein Designer-Projekt haben, vergewissern Sie sich, dass die Informationen in diesem Projekt mit denen im Identitätsdepot synchron sind:

- 1 Öffnen Sie Ihr Projekt in Designer.
- 2 Klicken Sie im Modellierer mit der rechten Maustaste auf das Identitätsdepot und wählen Sie anschließend *Live > Vergleichen*.
- 3 Werten Sie das Projekt aus, gleichen Sie mögliche Unterschiede ab und klicken Sie anschließend auf *OK*.

Weitere Informationen finden Sie unter „[Verwenden der Vergleichsfunktion beim Bereitstellen](#)“ im *Administrationshandbuch zu Designer 4.0 für Identity Manager 4.0*.

- 4 Wählen Sie in der Symbolleiste *Projekt > Exportieren*.
- 5 Klicken Sie auf *Alle markieren*, um alle zu exportierenden Ressourcen auszuwählen.
- 6 Wählen Sie, wo und in welchem Format das Projekt gespeichert werden soll, und klicken Sie anschließend auf *Fertig stellen*.

Speichern Sie das Projekt an einem beliebigen Speicherort, außer im aktuellen Arbeitsbereich. Wenn Sie auf Designer aufrüsten, müssen Sie einen neuen Speicherort für den Arbeitsbereich erstellen. Weitere Informationen finden Sie unter „[Exportieren eines Projekts](#)“ im *Administrationshandbuch zu Designer 4.0 für Identity Manager 4.0*.

Erstellen eines neuen Projekts aus dem Identitätsdepot

Wenn Sie kein Designer-Projekt Ihrer aktuellen Identity Manager-Lösung haben, müssen Sie ein Projekt als Sicherung Ihrer aktuellen Lösung erstellen.

- 1 Installieren Sie Designer 4.0.
Sie können ein Identity Manager 3.6.x-Projekt mit Designer 4.0 erstellen. Weitere Informationen finden Sie unter „[Installation von Designer](#)“ im *Identity Manager 4.0 Framework Installationshandbuch*.
- 2 Starten Sie Designer und geben Sie einen Speicherort für Ihren Arbeitsbereich an.
- 3 Wählen Sie aus, ob Sie auf Online-Updates prüfen möchten, und klicken Sie anschließend auf *OK*.
- 4 Klicken Sie in der Begrüßungsseite auf *Designer ausführen*.
- 5 Wählen Sie in der Symbolleiste *Projekt > Projekt importieren > Identitätsdepot*.
- 6 Geben Sie einen Namen für das Projekt an und verwenden Sie anschließend entweder den Standardspeicherort für Ihr Projekt oder wählen Sie einen anderen Speicherort aus.
- 7 Klicken Sie auf *Weiter*.
- 8 Geben Sie die Verbindungsinformationen für das Identitätsdepot an:
Hostname: Geben Sie die IP-Adresse oder den DNS-Namen des Identitätsdepot-Servers an.
Benutzername: Geben Sie den DN des Benutzers an, der zum Authentifizieren beim Identitätsdepot verwendet wird.
Passwort: Geben Sie das Passwort für den Authentifizierungsbenuer an.
- 9 Klicken Sie auf *Weiter*.
- 10 Lassen Sie die Optionen „Identitätsdepot - Schema“ und „Standard-Benachrichtigungssammlung“ ausgewählt.
- 11 Erweitern Sie die Standard-Benachrichtigungssammlung und heben Sie die Auswahl der Sprachen auf, die Sie nicht benötigen.
Die Standard-Benachrichtigungssammlungen sind in viele unterschiedliche Sprachen übersetzt. Sie können alle Sprachen importieren oder nur die Sprachen auswählen, die Sie verwenden.
- 12 Klicken Sie auf *Durchsuchen*, suchen Sie das Verzeichnis und wählen Sie einen Treibersatz aus, den Sie importieren möchten.

- 13 Wiederholen Sie [Schritt 12](#) für jeden Treibersatz in diesem Identitätsdepot und klicken Sie anschließend auf *Fertig stellen*.
- 14 Klicken Sie auf *OK*, nachdem das Projekt importiert wurde.
- 15 Wenn Sie nur ein Identitätsdepot haben, sind Sie fertig. Wenn Sie mehrere Identitätsdepots haben, fahren Sie mit [Schritt 16](#) fort.
- 16 Klicken Sie in der Symbolleiste auf *Live > Importieren*.
- 17 Wiederholen Sie [Schritt 8](#) bis [Schritt 14](#) für jedes weitere Identitätsdepot.

6.1.2 Exportieren der Treiberdaten


Beim Exportieren der Treiberdaten wird ein Backup Ihrer aktuellen Konfiguration erstellt. Designer unterstützt jedoch momentan nicht die Erstellung von Backups der Treiber und Richtlinien der rollenbasierten Berechtigungen. Verwenden Sie iManager, um zu überprüfen, ob Sie über einen Export der Treiber der rollenbasierten Berechtigungen verfügen.

- ♦ „Exportieren der Treiberdaten mithilfe von Designer“ auf Seite 45
- ♦ „Exportieren der Treiberdaten mithilfe von iManager“ auf Seite 45

Exportieren der Treiberdaten mithilfe von Designer

- 1 Stellen Sie sicher, dass Ihr Projekt in Designer über die aktuellste Treiberversion verfügt.
Eine Anleitung dazu finden Sie unter „[Importieren einer Bibliothek, eines Treibersatzes oder eines Treibers vom Identitätsdepot](#)“ im *Administrationshandbuch zu Designer 4.0 für Identity Manager 4.0*.
- 2 Klicken Sie im Modellierer mit der rechten Maustaste auf die Treiberlinie des aufzurüstenden Treibers.
- 3 Wählen Sie *In Konfigurationsdatei exportieren*.
- 4 Wählen Sie den Speicherort für die Konfigurationsdatei und klicken Sie anschließend auf *Speichern*.
- 5 Klicken Sie auf der Ergebnisseite auf *OK*.
- 6 Führen Sie [Schritt 1](#) bis [Schritt 5](#) für alle Treiber aus.

Exportieren der Treiberdaten mithilfe von iManager

- 1 Klicken Sie in iManager auf *Identity Manager > Identity Manager-Überblick*.
- 2 Wählen Sie in der Baumstruktur den Speicherort aus, in dem nach Treibersatzobjekten gesucht werden soll, und klicken Sie dann auf das Suchsymbol .
- 3 Klicken Sie auf das Treibersatzobjekt, das den aufzurüstenden Treiber enthält.
- 4 Klicken Sie auf den aufzurüstenden Treiber und anschließend auf *Exportieren*.
- 5 Klicken Sie auf *Weiter* und dann auf *Alle enthaltenen Richtlinien exportieren, egal ob sie mit der Konfiguration verknüpft sind oder nicht*.
- 6 Klicken Sie auf *Weiter* und dann auf *Speichern unter*.
- 7 Wählen Sie *Auf Festplatte speichern* und klicken Sie dann auf *OK*.
- 8 Klicken Sie auf *Fertig stellen*.
- 9 Führen Sie [Schritt 1](#) bis [Schritt 8](#) für alle Treiber aus.

6.2 Anhalten der Treiber



Vor der Aufrüstung der Dateien müssen die Treiber angehalten werden.

- [Abschnitt 6.2.1, „Anhalten der Treiber mithilfe von Designer“](#), auf Seite 46
- [Abschnitt 6.2.2, „Anhalten der Treiber mithilfe von iManager“](#), auf Seite 46

6.2.1 Anhalten der Treiber mithilfe von Designer

- 1 Wählen Sie das Objekt „Identitätsdepot“  auf der Registerkarte *Gliederung* aus.
- 2 Klicken Sie in der Symbolleiste „Modellierer“ auf das Symbol *Alle Treiber anhalten* .
Alle im Projekt verwendeten Treiber werden angehalten.
- 3 Wählen Sie für die Treiber die manuelle Startoption aus, um zu vermeiden, dass die Treiber vor Abschluss der Aufrüstung starten:
 - 3a Doppelklicken Sie auf das Treibersymbol  in der Registerkarte *Gliederung*.
 - 3b Wählen Sie *Treiberkonfiguration* > *Startoption*.
 - 3c Wählen Sie *Manuell* und klicken Sie dann auf *OK*.
 - 3d Führen Sie [Schritt 3a](#) bis [Schritt 3c](#) für alle Treiber aus.

6.2.2 Anhalten der Treiber mithilfe von iManager

- 1 Klicken Sie in iManager auf *Identity Manager* > *Identity Manager-Überblick*.
- 2 Wählen Sie in der Baumstruktur den Speicherort aus, in dem nach Treibersatzobjekten gesucht werden soll, und klicken Sie dann auf das Suchsymbol .
- 3 Klicken Sie auf das Treibersatzobjekt.
- 4 Klicken Sie auf *Treiber* > *Alle Treiber anhalten*.
- 5 Führen Sie [Schritt 2](#) bis [Schritt 4](#) für alle Treibersatzobjekte aus.
- 6 Wählen Sie für die Treiber die manuelle Startoption aus, um zu vermeiden, dass die Treiber vor Abschluss der Aufrüstung starten:
 - 6a Klicken Sie in iManager auf *Identity Manager* > *Identity Manager-Überblick*.
 - 6b Wählen Sie in der Baumstruktur den Speicherort aus, in dem nach Treibersatzobjekten gesucht werden soll, und klicken Sie dann auf das Suchsymbol .
 - 6c Klicken Sie auf das Treibersatzobjekt.
 - 6d Klicken Sie in der oberen rechten Ecke des Treibersymbols auf *Eigenschaften bearbeiten*.
 - 6e Wählen Sie auf der Seite „Treiberkonfiguration“ unter *Startoption* die Option *Manuell* aus und klicken Sie anschließend auf *OK*.
 - 6f Führen Sie [Schritt 6a](#) bis [Schritt 6e](#) für alle Treiber in Ihrer Baumstruktur aus.

6.3 Aufrüstung von Designer

Exportieren Sie vor der Aufrüstung von Designer Ihre Projekte, um diese zu sichern. Eine Anleitung zum Exportieren Ihres Projekts finden Sie unter [„Exporting a Project“](#) (Exportieren eines Projekts) im [Administrationshandbuch zu Designer 4.0 für Identity Manager 4.0](#).

Designer kann nur unter Windows oder Linux installiert werden. Wenn Ihre Metaverzeichnis-Engine auf einem Solaris-System installiert ist, muss die Installation von Designer auf einem separaten Server erfolgen.

So rüsten Sie Designer auf:

- 1 Starten Sie das Designer-Installationsprogramm vom Identity Manager-Datenträger:
Linux: `./products/Designer/install`
Führen Sie die Binärdatei aus, indem Sie eingeben `./install`.
Windows: `\products\Designer\install.exe`
- 2 Wählen Sie die Sprache aus, in der Sie Designer installieren möchten, und lesen und akzeptieren Sie dann die Lizenzvereinbarung.
- 3 Geben Sie das Verzeichnis an, in dem Designer installiert ist, und klicken Sie anschließend auf *Ja* in der Meldung, die besagt, dass Designer bereits installiert ist.
- 4 Wählen Sie aus, ob auf Ihrem Desktop und/oder in Ihrem Desktop-Menü eine Verknüpfung erstellt werden soll.
- 5 Prüfen Sie die Zusammenfassung und klicken Sie auf *Installieren*.
- 6 Lesen Sie die Readme-Datei und klicken Sie dann auf *Weiter*.
- 7 Wählen Sie, dass Designer gestartet werden soll, und klicken Sie dann auf *Fertig*.
- 8 Geben Sie einen Speicherort für Ihren Designer-Arbeitsbereich an und klicken Sie auf *OK*.
- 9 Klicken Sie in der Warnmeldung, die angibt, dass Ihr Projekt geschlossen und konvertiert werden muss, auf *OK*.
- 10 Erweitern Sie in der Projektansicht das Projekt und doppelklicken Sie auf *Projekt muss konvertiert werden*.
- 11 Prüfen Sie die Schritte, die der Assistent zum Konvertieren des Projekts durchführt, und klicken Sie auf *Weiter*.
- 12 Geben Sie einen Namen für die Sicherung Ihres Projekts an und klicken Sie auf *Weiter*.
- 13 Lesen Sie die Zusammenfassung der Aktionen, die bei der Konvertierung durchgeführt werden, und klicken Sie anschließend auf *Konvertieren*.
- 14 Lesen Sie die Zusammenfassung nach der Konvertierung und klicken Sie auf *Öffnen*.

Designer wurde aktualisiert und das Projekt wurde in das aktuelle Format konvertiert.

6.4 Aufrüsten des Metaverzeichnis-Servers (Identitätsdepot, Metaverzeichnis-Engine und Remote Loader)

Nach dem Aufrüsten der unterstützenden Komponenten wird der Metaverzeichnis-Server aufgerüstet. Während der Aufrüstung werden die im Dateisystem gespeicherten Dateien des Treiberschnittstellenmoduls aktualisiert.

- 1 Stellen Sie sicher, dass alle Treiber angehalten wurden. Eine Anleitung dazu finden Sie in [Abschnitt 6.2, „Anhalten der Treiber“](#), auf Seite 46.
- 2 Halten Sie den lcache-Prozess manuell an.

- 3 Wenn Sie von Identity Manager 3.6 oder höher aufrüsten, führen Sie das Dienstprogramm „NrfCaseUpdate“ aus, damit Suchvorgänge nach Rollen und Ressourcen mit Beachtung der Groß-/Kleinschreibung unterstützt werden.

Wenn Sie das Dienstprogramm „NrfCaseUpdate“ nicht ausführen, schlägt die Aufrüstung 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 Benutzeranwendung: Installationshandbuch](#).

Hinweis: Wenn Sie nur den Remote Loader aufrüsten, müssen Sie das Dienstprogramm „NrfCaseUpdate“ nicht ausführen.

- 4 Starten Sie das integrierte Installationsprogramm vom Identity Manager-Datenträger:
 - ♦ **Linux:** `./install.bin`
 - ♦ **Solaris:** `./install.bin`
Führen Sie die Binärdatei aus, indem Sie eingeben `./install.bin`.
 - ♦ **Windows:** `install.exe`
- 5 Wählen Sie die Sprache aus, in der die Aufrüstung durchgeführt werden soll, und klicken Sie anschließend auf *OK*.
- 6 Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf *Weiter*.
- 7 Klicken Sie auf *Aufrüsten*, um das Identitätsdepot und den Metaverzeichnis-Server aufzurüsten, und klicken Sie anschließend auf *Weiter*.
- 8 Wählen Sie *Metaverzeichnis-Server* und klicken Sie anschließend auf *Weiter*.
Das Identitätsdepot wird automatisch aktualisiert.
- 9 Geben Sie den Namen eines Benutzers mit vollständigen Verwaltungsrechten für das Identitätsdepot im LDAP-Format an.
 - ♦ **Linux/UNIX:** Geben Sie die Parameter *Admin-DN* und *Admin-Passwort* an.
 - ♦ **Windows:** Geben Sie die Parameter *Admin-DN*, *Containername* und *Admin-Passwort* an.
- 10 Geben Sie das Passwort für den Benutzer mit Verwaltungsrechten für das Identitätsdepot an und klicken Sie anschließend auf *Weiter*.

Hinweis: [Schritt 9](#) und [Schritt 10](#) gelten nicht für das Aufrüsten des Remote Loaders.

- 11 Lesen Sie die Zusammenfassung vor der Aufrüstung und klicken Sie auf *Installieren*.
- 12 Lesen Sie die Zusammenfassung der Aufrüstung und klicken Sie auf *Fertig*.

Sie können die Aufrüstungs-Protokolldatei (`ii_upgrade.log`) überprüfen, die sich am folgenden Speicherort befindet:

- ♦ **Linux/UNIX:** `/var/opt/novell/idm/install/logs`
- ♦ **Windows:** `C:\Novell\IdentityManager\install\logs`

Die aufgelisteten Pfade sind die Standardinstallationspfade.

6.5 Aufrüsten von Treibern auf Pakete

Pakete sind die neue Content Management-Funktion in Identity Manager 4.0. Pakete enthalten die Bausteine von Richtlinien zum Erstellen von Treibern. Alle neuen Treiberinhalte werden statt über Treiberkonfigurationsdateien über Pakete bereitgestellt.

Pakete werden über Designer verwaltet, gepflegt und erstellt. iManager kann Pakete erkennen, in iManager vorgenommene Änderungen an Treiberinhalten werden jedoch nicht von Designer übernommen. Weitere Informationen zum Verwalten von Paketen finden Sie unter „[Verwalten der Identity Manager-Inhalte](#)“ im *Administrationshandbuch zu Designer 4.0 für Identity Manager 4.0*.

Es gibt drei unterschiedliche Methoden, Treiber zu Paketen aufzurüsten:

- ♦ [Abschnitt 6.5.1, „Einen neuen Treiber erstellen“](#), auf Seite 49
- ♦ [Abschnitt 6.5.2, „Vorhandene Inhalte durch Inhalte aus Paketen ersetzen“](#), auf Seite 49
- ♦ [Abschnitt 6.5.3, „Aktuelle Inhalte beibehalten und neue Inhalte über Pakete hinzufügen“](#), auf Seite 50

6.5.1 Einen neuen Treiber erstellen

Die einfachste und sauberste Methode, um Pakete zu Treibern aufzurüsten, besteht darin, den vorhandenen Treiber zu löschen und einen neuen Treiber mithilfe von Paketen zu erstellen. Fügen Sie alle gewünschten Treiberfunktionen mit Paketen hinzu. Die Schritte zum Erstellen eines neuen Treibers mit Paketen finden Sie im jeweiligen Treiberhandbuch. Die Schritte hierfür sind bei jedem Treiber unterschiedlich. Anweisungen hierzu finden Sie auf der [Website zur Identity Manager-Treiberdokumentation \(http://www.novell.com/documentation/idm40drivers/\)](#).

6.5.2 Vorhandene Inhalte durch Inhalte aus Paketen ersetzen

Wenn die vom Treiber erstellten Verknüpfungen beibehalten werden müssen, sollten Sie den Treiber nicht löschen und neu erstellen. Sie können den vorhandenen Treiberinhalt durch Pakete ersetzen.

- 1 Erstellen Sie eine Sicherung des Treibers und aller seiner angepassten Inhalte.

Eine Anleitung dazu finden Sie in [Abschnitt 6.1.2, „Exportieren der Treiberdaten“](#), auf Seite 45.

- 2 Löschen Sie in Designer alle im Treiber gespeicherten Objekte. Löschen Sie die Richtlinien, Filter, Berechtigungen und alle anderen im Treiber gespeicherten Elemente.

- 3 Importieren Sie die Treiberpakete in den Paketkatalog.

Anweisungen finden Sie unter „[Importieren von Paketen in den Paketkatalog](#)“ im *Administrationshandbuch zu Designer 4.0 für Identity Manager 4.0*.

- 4 Installieren Sie die Pakete im Treiber.

Anweisungen finden Sie im jeweiligen Treiberhandbuch auf der [Website zur Identity Manager-Treiberdokumentation \(http://www.novell.com/documentation/idm40drivers/\)](#).

- 5 Fügen Sie die Basis-, obligatorischen und optionalen Pakete zum Treiber hinzu, um die gewünschte Funktionalität zu erhalten. Diese Schritte sind bei jedem Treiber unterschiedlich.

Anweisungen finden Sie im jeweiligen Treiberhandbuch auf der [Website zur Identity Manager-Treiberdokumentation \(http://www.novell.com/documentation/idm40drivers/\)](#).

6 Stellen Sie alle benutzerdefinierten Richtlinien und Regeln für den Treiber wieder her.

Eine Anleitung dazu finden Sie in [Abschnitt 6.6, „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“](#), auf Seite 50.

Der Treiber funktioniert nun wie vorher, seine Inhalte stammen aber aus Paketen und nicht aus einer Treiberkonfigurationsdatei.

6.5.3 Aktuelle Inhalte beibehalten und neue Inhalte über Pakete hinzufügen

Sie können den Treiber im aktuellen Zustand belassen und mithilfe der Pakete um neue Funktionen erweitern, solange keine Überschneidung zwischen den Funktionen in den Paketen und den aktuellen Funktionen des Treibers besteht. Wenn Sie ein Paket installieren, kann es vorhandene Richtlinien überschreiben, sodass der Treiber nicht mehr funktioniert.

So fügen Sie mithilfe von Paketen neue Inhalte zum Treiber hinzu:

1 Erstellen Sie eine Sicherung des Treibers und aller seiner angepassten Inhalte.

Eine Anleitung dazu finden Sie in [Abschnitt 6.1.2, „Exportieren der Treiberdaten“](#), auf Seite 45.

2 Importieren Sie die Treiberpakete in den Paketkatalog.

Anweisungen finden Sie unter [„Importieren von Paketen in den Paketkatalog“](#) im *Administrationshandbuch zu Designer 4.0 für Identity Manager 4.0*.

3 Installieren Sie die Pakete im Treiber.

Anweisungen finden Sie im jeweiligen Treiberhandbuch auf der [Website zur Identity Manager-Treiberdokumentation \(http://www.novell.com/documentation/idm40drivers/\)](#).

4 Fügen Sie die gewünschten Pakete zum Treiber hinzu. Diese Schritte sind bei jedem Treiber unterschiedlich.

Anweisungen hierzu finden Sie auf der [Website zur Identity Manager-Treiberdokumentation \(http://www.novell.com/documentation/idm40drivers/\)](#).

Der Treiber enthält nun die über die Pakete hinzugefügten neuen Funktionen.

6.6 Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber

Wenn Sie benutzerdefinierte Richtlinien oder Regeln verwenden, müssen diese nach der Überlagerung mit der neuen Treiberkonfigurationsdatei für den Treiber wiederhergestellt werden. Wenn diese Richtlinien andere Namen haben, sind sie noch im Treiber gespeichert, aber die Links sind kaputt und müssen erneuert werden.

- ♦ [Abschnitt 6.6.1, „Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von Designer“](#), auf Seite 51
- ♦ [Abschnitt 6.6.2, „Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von iManager“](#), auf Seite 52


6.6.1 Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von Designer

Es gibt zwei Möglichkeiten, Richtlinien zum Richtlinienatz hinzuzufügen:


- ♦ „Hinzufügen einer benutzerdefinierten Richtlinie über die Gliederungsansicht“ auf Seite 51
- ♦ „Hinzufügen einer benutzerdefinierten Richtlinie über die Ansicht „Richtlinienfluss anzeigen““ auf Seite 51

Führen Sie die Verfahren in einer Testumgebung durch, bevor Sie den Treiber in Ihrer Produktionsumgebung einsetzen.

Hinzufügen einer benutzerdefinierten Richtlinie über die Gliederungsansicht

- 1 Wählen Sie zum Anzeigen der Ansicht *Richtliniensatz* in der *Gliederungsansicht* den aufgerüsteten Treiber aus.
- 2 Klicken Sie mit der rechten Maustaste auf das Symbol für den Richtlinienatz , dessen benutzerdefinierte Richtlinie Sie wiederherstellen möchten, und wählen Sie anschließend *Neu > Von Kopie*.
- 3 Wechseln Sie zur benutzerdefinierten Richtlinie und markieren Sie sie. Klicken Sie anschließend auf *OK*.
- 4 Geben Sie den Namen für die neue benutzerdefinierte Richtlinie an und klicken Sie dann auf *OK*.
- 5 Klicken Sie zum Speichern des Projekts in der Dateikonfliktmeldung auf *Ja*.
- 6 Wenn der Richtlinien-Builder die Richtlinie geöffnet hat, stellen Sie sicher, dass die Informationen in der kopierten Richtlinie richtig sind.
- 7 Wiederholen Sie [Schritt 2](#) bis [Schritt 6](#) für alle benutzerdefinierten Richtlinien, die für den Treiber wiederhergestellt werden sollen.
- 8 Starten Sie den Treiber und testen Sie ihn.
Weitere Informationen zum Starten des Treibers finden Sie in [Abschnitt 6.8, „Starten der Treiber“](#), auf Seite 53. Weitere Informationen zum Testen des Treibers finden Sie unter [„Testing Policies with Policy Simulator“](#) (Testen von Richtlinien mit dem Richtlinien Simulator) im Handbuch *Policies in Designer 4.0* (Richtlinien in Designer 3.0).
- 9 Wenn Sie überprüft haben, dass die Richtlinien funktionieren, können Sie den Treiber in der Produktionsumgebung einsetzen.


Hinzufügen einer benutzerdefinierten Richtlinie über die Ansicht „Richtlinienfluss anzeigen“

- 1 Wählen Sie in der *Gliederungsansicht* den aufgerüsteten Treiber aus und klicken Sie anschließend auf das Symbol *Richtlinienfluss anzeigen* .
- 2 Klicken Sie mit der rechten Maustaste auf den Richtlinienatz, dessen benutzerdefinierte Richtlinie Sie wiederherstellen möchten, und wählen Sie anschließend *Richtlinie hinzufügen > Vorhandene kopieren*.
- 3 Wechseln Sie zur benutzerdefinierten Richtlinie und markieren Sie sie. Klicken Sie anschließend auf *OK*.

- 4 Geben Sie den Namen für die neue benutzerdefinierte Richtlinie an und klicken Sie dann auf *OK*.
- 5 Klicken Sie zum Speichern des Projekts in der Dateikonfliktmeldung auf *Ja*.
- 6 Wenn der Richtlinien-Builder die Richtlinie geöffnet hat, stellen Sie sicher, dass die Informationen in der kopierten Richtlinie richtig sind.
- 7 Wiederholen Sie [Schritt 2](#) bis [Schritt 6](#) für alle benutzerdefinierten Richtlinien, die für den Treiber wiederhergestellt werden sollen.
- 8 Starten Sie den Treiber und testen Sie ihn.
 Weitere Informationen zum Starten des Treibers finden Sie in [Abschnitt 6.8, „Starten der Treiber“](#), auf Seite 53. Weitere Informationen zum Testen des Treibers finden Sie unter [„Testing Policies with Policy Simulator“](#) (Testen von Richtlinien mit den Richtlinien Simulator) im Handbuch *Policies in Designer 4.0* (Richtlinien in Designer 3.0).
- 9 Wenn Sie überprüft haben, dass die Richtlinien funktionieren, können Sie den Treiber in der Produktionsumgebung einsetzen.

6.6.2 Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von iManager

Führen Sie dieses Verfahren in einer Testumgebung durch, bevor Sie den Treiber in Ihrer Produktionsumgebung einsetzen.

- 1 Klicken Sie in iManager auf *Identity Manager > Identity Manager-Überblick*.
- 2 Wählen Sie in der Baumstruktur den Speicherort aus, in dem nach Treibersatzobjekten gesucht werden soll, und klicken Sie dann auf das Suchsymbol .
- 3 Klicken Sie auf das Treibersatzobjekt, das den aufgerüsteten Treiber enthält.
- 4 Klicken Sie auf das Treibersymbol und wählen Sie dann den Richtlinienatz, dessen benutzerdefinierte Richtlinie wiederhergestellt werden soll.
- 5 Klicken Sie auf *Einfügen*.
- 6 Wählen Sie *Vorhandene Richtlinie verwenden*. Wechseln Sie anschließend zur benutzerdefinierten Richtlinie und wählen Sie sie aus.
- 7 Klicken Sie auf *OK* und anschließend auf *Schließen*.
- 8 Wiederholen Sie [Schritt 3](#) bis [Schritt 7](#) für alle benutzerdefinierten Richtlinien, die für den Treiber wiederhergestellt werden sollen.
- 9 Starten Sie den Treiber und testen Sie ihn.
 Weitere Informationen zum Starten des Treibers finden Sie in [Abschnitt 6.8, „Starten der Treiber“](#), auf Seite 53. In iManager gibt es keinen Richtlinien Simulator. Lösen Sie zum Testen der Richtlinien Ereignisse aus, durch die die Richtlinien ausgeführt werden. Sie können z. B. einen Benutzer erstellen, ändern oder löschen.
- 10 Wenn Sie überprüft haben, dass die Richtlinien funktionieren, können Sie den Treiber in der Produktionsumgebung einsetzen.

6.7 Bereitstellen des konvertierten Projekts




Stellen Sie das konvertierte Designer-Projekt im Identitätsdepot bereit. Weitere Informationen finden Sie unter „[Bereitstellen und Exportieren](#)“ im *Administrationshandbuch zu Designer 4.0 für Identity Manager 4.0*.

6.8 Starten der Treiber


Nach der Aufrüstung aller Identity Manager-Komponenten müssen die Treiber neu gestartet werden. Es ist außerdem wichtig, die gestarteten Treiber zu testen, um zu überprüfen, ob noch alle Richtlinien funktionieren.


- ♦ [Abschnitt 6.8.1, „Starten der Treiber mithilfe von Designer“](#), auf Seite 53
- ♦ [Abschnitt 6.8.2, „Starten der Treiber mithilfe von iManager“](#), auf Seite 53

6.8.1 Starten der Treiber mithilfe von Designer

- 1 Wählen Sie das Objekt „Identitätsdepot“  in der Registerkarte *Gliederung*.
- 2 Klicken Sie in der „Modellierer“-Symbolleiste auf das Symbol *Alle Treiber starten* . Alle Treiber im Projekt werden gestartet.
- 3 Legen Sie die Treiber-Startoptionen fest:
 - 3a Doppelklicken Sie auf das Treibersymbol  in der Registerkarte *Gliederung*.
 - 3b Wählen Sie *Treiberkonfiguration > Startoption*.
 - 3c Wählen Sie *Autom. starten* bzw. die gewünschte Methode für den Start des Treibers aus. Klicken Sie anschließend auf *OK*.
 - 3d Führen Sie [Schritt 3a](#) bis [Schritt 3c](#) für alle Treiber aus.
- 4 Testen Sie die Treiber, um sicherzustellen, dass die Richtlinien wie gewünscht funktionieren. Weitere Informationen zum Testen Ihrer Richtlinien finden Sie unter „[Testing Policies with Policy Simulator](#)“ (Testen von Richtlinien mit dem Richtlinien Simulator) im Handbuch *Policies in Designer 4.0* (Richtlinien in Designer 3.0).

6.8.2 Starten der Treiber mithilfe von iManager

- 1 Klicken Sie in iManager auf *Identity Manager > Identity Manager-Überblick*.
- 2 Wählen Sie in der Baumstruktur den Speicherort aus, in dem nach Treibersatzobjekten gesucht werden soll, und klicken Sie dann auf das Suchsymbol .
- 3 Klicken Sie auf das Treibersatzobjekt.
- 4 Wählen Sie *Treiber > Alle Treiber starten*, um alle Treiber gleichzeitig zu starten.
oder
Klicken Sie in der oberen rechten Ecke des Treibersymbols auf *Treiber starten*, um jeden Treiber einzeln zu starten.
- 5 Wenn Sie mehrere Treiber verwenden, wiederholen Sie [Schritt 2](#) bis [Schritt 4](#).
- 6 Legen Sie die Treiber-Startoptionen fest:
 - 6a Klicken Sie in iManager auf *Identity Manager > Identity Manager-Überblick*.

- 6b** Wählen Sie in der Baumstruktur den Speicherort aus, in dem nach Treibersatzobjekten gesucht werden soll, und klicken Sie dann auf das Suchsymbol .
 - 6c** Klicken Sie auf das Treibersatzobjekt.
 - 6d** Klicken Sie in der oberen rechten Ecke des Treibersymbols auf *Eigenschaften bearbeiten*.
 - 6e** Wählen Sie auf der Seite „Treiberkonfiguration“ unter *Startoption* die Option *Autom. starten* bzw. die gewünschte Methode für den Start des Treibers aus. Klicken Sie anschließend auf *OK*.
 - 6f** Führen Sie [Schritt 6b](#) bis [Schritt 6e](#) für alle Treiber aus.
- 7** Testen Sie die Treiber, um sicherzustellen, dass die Richtlinien wie gewünscht funktionieren. In iManager gibt es keinen Richtlinienimulator. Lösen Sie zum Testen der Richtlinien Ereignisse aus, durch die die Richtlinien ausgeführt werden. Sie können z. B. einen Benutzer erstellen, ändern oder löschen.

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 55
- ♦ „Übergeben obligatorischer Parameter während der Konfiguration“ auf Seite 56
- ♦ „Die Konfiguration schlägt fehl, wenn die Datei „hosts“ den Eintrag „127.0.0.2“ enthält“ auf Seite 56
- ♦ „Das Installationsprogramm gibt „java.io.FileNotFoundException“ aus“ auf Seite 57
- ♦ „Der Baumname wird automatisch generiert, wenn der Baumname bereits vorhanden ist“ auf Seite 57
- ♦ „Sekundärserver-Installation“ auf Seite 57
- ♦ „Dienste werden nicht ausgeführt“ auf Seite 57
- ♦ „Erkennung des aktuellen Systemstatus“ auf Seite 57
- ♦ „Das integrierte Installationsprogramm hängt sich möglicherweise während der Identity Manager-Aufrüstung auf“ auf Seite 58
- ♦ „Beim Installieren der Windows-Laufzeit-Distribution wird möglicherweise aufgrund eines Installationsfehlers ein Neustart erzwungen“ auf Seite 58
- ♦ „lcache-Problem während der Identity Manager-Aufrüstung“ auf Seite 58
- ♦ „Die Aufrüstung schlägt unter Windows Server 2003 fehl“ auf Seite 58
- ♦ „Konfiguration der ISO, die unter UNIX über Drittanbieter-ISO-Extraktionswerkzeuge extrahiert wurde“ auf Seite 59
- ♦ „Das Aktivieren von XDAS beeinträchtigt die Leistung“ auf Seite 59
- ♦ „Deinstallationsprobleme bei Identity Manager-Komponenten“ auf Seite 59

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: Zum Ermitteln typischer Fehler finden Sie in der Datei `ii_install.log` Informationen zu Installationsproblemen, die Datei `ii_configure.log` enthält Informationen zu Konfigurationsproblemen und die Datei `ii_uninstall.log` Informationen zu Deinstallationsproblemen. Suchen Sie in den Protokolldateien nach dem Text „exitValue = 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 Ausweidlösungen:

- ♦ 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 möglicherweise während der Identity Manager-Aufrüstung auf

Mögliche Ursache: Vor dem Aufrüsten von Identity Manager unter Windows versucht das integrierte Installationsprogramm, alle abhängigen Dienste anzuhalten. Manchmal kann sich das Installationsprogramm beim Anhalten des DHost-Dienstes aufhängen.

Aktion: Halten Sie den DHost-Dienst manuell über den Aufgabenmanager an, um mit der Aufrüstung fortzufahren.

Beim Installieren der Windows-Laufzeit-Distribution wird möglicherweise aufgrund eines Installationsfehlers einen 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.

lcache-Problem während der Identity Manager-Aufrüstung

Ursprung: Nach dem Aufrüsten von Identity Manager protokolliert der Plattformagent Ereignisse möglicherweise nicht wie gewünscht. Dieses Problem tritt auf, weil der Plattformagent während der Identity Manager-Aufrüstung unter Linux nicht aufgerüstet wird. Unter Windows und Solaris wird der Plattformagent auf die neueste Version aufgerüstet, der neue Plattformagent hat jedoch andere Standardports, sodass ein Neustart von lcache erforderlich ist.

Aktion: Sie müssen lcache manuell anhalten, bevor Sie die Aufrüstung starten.

Die Aufrüstung schlägt unter Windows Server 2003 fehl

Erklärung: Das Aufrüsten von Identity Manager 3.6.1 auf eDirectory 8.8 SP5 schlägt auf einem 32-Bit-Windows 2003-Computer fehl, wenn Folgendes zutrifft:

- ♦ Symantec Antivirus ist installiert und aktiviert
- ♦ Das Setup befindet sich auf einem zugeordneten Laufwerk

Aktion: Kopieren Sie die Installationsdateien auf einen lokalen Computer und führen Sie die Installation durch.

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

Erklärung: Die Konfiguration des integrierten Installationsprogramms von Identity Manager 4.0 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: Die Deinstallationsoption ist deaktiviert, während ein erneuter Deinstallationsversuch mit der Datei `uninstall.bin` unternommen wird.

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 Framework Installationshandbuch*.

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:** `./Uninstall_Identity Manager Components.bin`

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

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

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

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

Das Deinstallationsprogramm befindet sich unter

`<Installationsverzeichnis>\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.

