

Installationshandbuch

Novell® Identity Manager

3.6.1

15. Mai 2009

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 stimmen zu, alle Gesetze zur Exportkontrolle einzuhalten und alle für den Export, Reexport oder Import von Lieferungen erforderlichen Lizenzen oder Klassifikationen zu erwerben. 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 Website [Novell International Trade Services \(http://www.novell.com/company/policies/trade_services\)](http://www.novell.com/company/policies/trade_services). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Copyright © 2007-2009 Novell, Inc. Alle Rechte vorbehalten. Ohne ausdrückliche schriftliche Genehmigung des Ausstellers darf kein Teil dieser Veröffentlichung reproduziert, fotokopiert, übertragen oder in einem Speichersystem verarbeitet werden.

Novell, Inc. besitzt Rechte auf geistiges Eigentum für die Technologie, die in dem in diesem Dokument beschriebenen Produkt integriert ist. Diese Rechte auf geistiges Eigentum umfassen möglicherweise insbesondere ein oder mehrere Patente in den USA, die auf der [Webseite Novell Legal Patents \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) aufgeführt sind, sowie ein oder mehrere andere Patente oder laufende Patentanträge in den USA und in anderen Ländern.

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	9
Teil I Planung	11
1 Einrichten einer Entwicklungsumgebung	13
2 Erstellen eines Projektplans	15
2.1 Ermittlungsphase	15
2.1.1 Definieren aktueller Geschäftsprozesse	16
2.1.2 Definieren, wie sich die Identity Manager-Lösung auf die aktuellen Geschäftsprozesse auswirkt	17
2.1.3 Identifizieren der wichtigsten Projektbeteiligten auf geschäftlicher und technischer Ebene	17
2.1.4 Gespräche mit allen Projektbeteiligten führen	18
2.1.5 Erstellen einer allgemeinen Strategie und eines konsensfähigen Ausführungsablaufs	18
2.2 Anforderungs- und Entwurfsanalysephase	19
2.2.1 Definieren der Geschäftsanforderungen	20
2.2.2 Analyse der Geschäftsprozesse	21
2.2.3 Entwurf eines Enterprise-Datenmodells	22
2.3 Proof-of-Concept	24
2.4 Validierung und Vorbereitung der Daten	24
2.5 Produktions-Prototyp	25
2.6 Planung des Produktions-Rollout	25
2.7 Produktionsbereitstellung	25
3 Technische Richtlinien	27
3.1 Verwaltungswerkzeuge - Richtlinien	28
3.1.1 Designer-Richtlinien	28
3.1.2 iManager-Richtlinien	29
3.2 Metaverzeichnis-Server-Richtlinien	29
3.3 eDirectory-Richtlinien	30
3.3.1 Identity Manager-Objekte in eDirectory	31
3.3.2 Replizierung der von Identity Manager auf dem Server benötigten Objekte	31
3.3.3 Verwendung der Bereichsfilterung zum Verwalten von Benutzern auf verschiedenen Servern	33
3.4 Benutzeranwendung	35
3.5 Revision und Berichterstellung - Richtlinien	36
Teil II Installation	39
4 Basis-Checkliste für das Identity Manager-System	41
4.1 Voraussetzungen	41
4.2 Planung	42
4.3 Installation	42

4.4	Treiberkonfiguration mit dem Remote Loader	43
4.5	Treiberkonfiguration ohne den Remote Loader	43
4.6	Zusätzliche Konfiguration	44
5	Bezugsquellen für Identity Manager	45
6	Systemanforderungen	47
6.1	eDirectory und iManager	47
6.2	Metaverzeichnis-Server	48
6.2.1	Unterstützte Prozessoren	49
6.2.2	Server-Betriebssysteme	50
6.3	Remote Loader	51
6.4	Benutzeranwendung	52
6.5	Revision und Berichterstellung	52
6.6	Arbeitsstationen	53
6.6.1	Arbeitsstationsplattformen	54
6.6.2	iManager und Webbrowser	55
7	Installation von Identity Manager	57
7.1	Installation von Designer	57
7.2	Installation des Metaverzeichnis-Servers	58
7.2.1	Nicht-root-Installation des Metaverzeichnis-Servers	59
7.2.2	Automatische Installation des Metaverzeichnis-Servers	61
7.3	Installation des Remote Loaders	61
7.3.1	Anforderungen	62
7.3.2	Unterstützte Treiber	62
7.3.3	Installationsvorgang	63
7.3.4	Automatische Installation des Remote Loaders	65
7.3.5	Installation des Java Remote Loader unter UNIX, Linux oder AIX	66
7.4	Installation des rollenbasierten Bereitstellungsmoduls	67
7.5	Installation eines benutzerdefinierten Treibers	67
7.6	Installation von Identity Audit oder Sentinel	67
7.7	Installation von Identity Manager in der Cluster-Umgebung	67
8	Aktivieren von Novell Identity Manager-Produkten	69
8.1	Erwerb einer Produktlizenz für Identity Manager	69
8.2	Installation einer Produktaktivierungsberechtigung	69
8.3	Anzeigen der Produktaktivierungen für Identity Manager und Identity Manager-Treiber	70
9	Fehlerbehebung in Identity Manager	73
	Teil III Upgrades	75
10	Neuheiten	77
10.1	Unterstützung für 64-Bit-Betriebssysteme	77
10.2	Unterstützung für 32-Bit-Remote Loader-Installationen auf 64-Bit-Betriebssystemen	77

11	Unterstützte Versionen für Upgrades und Systemanforderungen	79
11.1	Unterstützte Versionen für Upgrades	79
11.2	Systemanforderungen	79
12	Direktaufrüstung im Vergleich zu Migration	81
12.1	Direktaufrüstung	81
12.2	Migration	82
12.3	Mehrere Server mit einem einzelnen Treibersatz verknüpft	82
13	Durchführung einer Direktaufrüstung	83
13.1	Backup der aktuellen Konfiguration erstellen	85
13.1.1	Sicherstellen, dass Ihr Designer-Projekt aktuell ist	85
13.1.2	Exportieren der Treiberdaten	87
13.2	Anhalten der Treiber	88
13.2.1	Anhalten der Treiber mithilfe von Designer	88
13.2.2	Anhalten der Treiber mithilfe von iManager	88
13.3	Dateien unter Linux/UNIX in den richtigen Speicherorten ablegen	89
13.4	Upgrade von Designer	89
13.5	Upgrade der Metaverzeichnis-Engine und der Treiberkonfigurationsdateien	90
13.6	Upgrade des Remote Loaders	90
13.7	Überlagern der neuen Treiberkonfigurationsdatei über den vorhandenen Treiber	91
13.7.1	Überlagern der neuen Treiberkonfigurationsdatei über den vorhandenen Treiber mithilfe von Designer	91
13.7.2	Überlagern der neuen Treiberkonfigurationsdatei über den vorhandenen Treiber mithilfe von iManager	92
13.8	Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber	92
13.8.1	Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von Designer	93
13.8.2	Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von iManager	94
13.9	Bereitstellen des konvertierten Projekts	94
13.10	Starten der Treiber	95
13.10.1	Starten der Treiber mithilfe von Designer	95
13.10.2	Starten der Treiber mithilfe von iManager	95
14	Durchführen einer Migration	97
14.1	Hinzufügen des neuen Servers zum Treibersatz	98
14.2	Ändern der serverspezifischen Informationen	99
14.2.1	Ändern der serverspezifischen Informationen in Designer	99
14.2.2	Ändern der serverspezifischen Informationen in iManager	100
14.3	Entfernen des alten Servers aus dem Treibersatz	100
14.3.1	Mithilfe von Designer den alten Server aus dem Treibersatz entfernen	100
14.3.2	Mithilfe von iManager den alten Server aus dem Treibersatz entfernen	101
14.3.3	Stilllegen des alten Servers	101

Teil IV Deinstallation von Identity Manager	103
15 Entfernen von Objekten aus eDirectory	105
16 Deinstallation des Metaverzeichnis-Servers und der Treiber	107
16.1 Deinstallation unter Windows	107
16.2 Deinstallation unter Linux/UNIX	107
17 Deinstallation von Designer	109

Informationen zu diesem Handbuch

Novell® Identity Manager 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 Planung, Installation oder zum Aufrüsten eines Identity Manager-Systems, das auf Ihre Umgebung zugeschnitten ist.

- ♦ Teil I, „Planung“, auf Seite 11
 - ♦ Kapitel 2, „Erstellen eines Projektplans“, auf Seite 15
 - ♦ Kapitel 3, „Technische Richtlinien“, auf Seite 27
- ♦ Teil II, „Installation“, auf Seite 39
 - ♦ Kapitel 4, „Basis-Checkliste für das Identity Manager-System“, auf Seite 41
 - ♦ Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 45
 - ♦ Kapitel 6, „Systemanforderungen“, auf Seite 47
 - ♦ Kapitel 7, „Installation von Identity Manager“, auf Seite 57
 - ♦ Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 69
- ♦ Teil III, „Upgrades“, auf Seite 75
 - ♦ Kapitel 10, „Neuheiten“, auf Seite 77
 - ♦ Kapitel 11, „Unterstützte Versionen für Upgrades und Systemanforderungen“, auf Seite 79
 - ♦ Kapitel 12, „Direktaufrüstung im Vergleich zu Migration“, auf Seite 81
 - ♦ Kapitel 13, „Durchführung einer Direktaufrüstung“, auf Seite 83
 - ♦ Kapitel 14, „Durchführen einer Migration“, auf Seite 97
- ♦ Teil IV, „Deinstallation von Identity Manager“, auf Seite 103
 - ♦ Kapitel 15, „Entfernen von Objekten aus eDirectory“, auf Seite 105
 - ♦ Kapitel 16, „Deinstallation des Metaverzeichnis-Servers und der Treiber“, auf Seite 107

Zielgruppe

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

Aktualisierungen für Dokumentationen

Die neueste Version dieses Dokuments finden Sie auf der [Website zur Identity Manager-Dokumentation](http://www.novell.com/documentation/idm361/index.html) (<http://www.novell.com/documentation/idm361/index.html>).

Zusätzliche Dokumentation

Weitere Dokumentation zu Identity Manager finden Sie auf der [Website zur Identity Manager-Dokumentation](http://www.novell.com/documentation/idm361/index.html) (<http://www.novell.com/documentation/idm361/index.html>).

Dokumentation zur Benutzeranwendung finden Sie auf der [Website zur Novell-Dokumentation für das rollenbasierte Bereitstellungsmodul für Identity Manager](http://www.novell.com/documentation/idmrbpm361/index.html) (<http://www.novell.com/documentation/idmrbpm361/index.html>).

Konventionen in der Dokumentation

In dieser Novell-Dokumentation wird ein „Größer als“-Zeichen (>) verwendet, um verschiedene Aktionen innerhalb eines Schritts und Meldungen in einem Querverweispfad voneinander zu trennen.

Ein Markensymbol (® , ™ usw.) kennzeichnet eine Novell-Marke. Ein Sternchen (*) kennzeichnet eine Drittanbieter-Marke.

Wenn ein Pfadname für bestimmte Plattformen mit einem umgekehrten Schrägstrich und für andere Plattformen mit einem Schrägstrich geschrieben werden kann, wird der Pfadname in diesem Handbuch mit einem umgekehrten Schrägstrich dargestellt. Benutzer von Plattformen, die einen Schrägstrich erfordern, wie z. B. Linux* oder UNIX*, sollten die für die Software erforderlichen Schrägstriche verwenden.

Planung

Identity Manager unterstützt Sie bei der Verwaltung von Identitäten und Ressourcen in Ihrem Unternehmen. Darüber hinaus dient es zur Automatisierung vieler Geschäftsprozesse, die zurzeit noch manuell abgewickelt werden.

Weitere Informationen zu den einzelnen Komponenten, aus denen eine Identity Manager-Lösung besteht, finden Sie im Handbuch *Überblick über Identity Manager 3.6.1*.

Zum Erstellen einer effektiven Identity Manager-Lösung für Ihre Umgebung müssen Sie sich zunächst die Zeit nehmen, Ihre Identity Manager-Lösung zu planen und zu erstellen. Die Planung beinhaltet zwei wesentliche Aspekte: die Einrichtung eines Testlabors, um sich mit den Produkten vertraut zu machen, und die Erstellung eines Projektplans, um eine Identity Manager-Lösung zu implementieren. Wenn Sie einen Projektplan erstellen, schließt dies die Definition Ihres Geschäftsprozesses und das Erstellen eines Implementierungsplans ein. In den meisten Unternehmen gibt es viele verschiedene Geschäftsprozesse, die von unterschiedlichen Personen verwaltet werden. Eine vollständige Identity Manager-Lösung wirkt sich auf die meisten dieser Prozesse aus. Es ist sehr wichtig, für die Planung einer Identity Manager-Lösung genügend Zeit einzuplanen, damit diese effektiv in Ihre Umgebung implementiert werden kann.

Es wird empfohlen, dass in jeder Phase der Identity Manager-Implementierung ein Identity Manager-Spezialist hinzugezogen wird. Weitere Informationen zu Partnerschaftsoptionen finden Sie auf der [Partner-Website von Novell®](http://www.novell.com/partners/) (<http://www.novell.com/partners/>). Novell Education bietet auch Kurse für die Identity Manager-Implementierung an.

- ♦ [Kapitel 1, „Einrichten einer Entwicklungsumgebung“](#), auf Seite 13
- ♦ [Kapitel 2, „Erstellen eines Projektplans“](#), auf Seite 15
- ♦ [Kapitel 3, „Technische Richtlinien“](#), auf Seite 27

Einrichten einer Entwicklungsumgebung

1

Bevor Sie die Planungsphase der Identity Manager-Bereitstellung beginnen, müssen Sie mit den Identity Manager-Produkten vertraut sein, damit Sie einen nützlichen Plan erstellen können. Wenn Sie eine Entwicklungsumgebung einrichten, in der Sie Ihre Identity Manager-Lösung entwickeln, analysieren und testen können, lernen Sie jede Komponente des Identity Manager kennen und stoßen dabei möglicherweise auf unerwartete Probleme und Komplikationen.

Wenn Sie beispielsweise Informationen zwischen verschiedenen Systemen synchronisieren, werden dabei die Informationen für jedes System unterschiedlich präsentiert. Wenn Sie die zwischen zwei Systemen zu synchronisierenden Daten ändern, können Sie erkennen, ob sich diese Änderung auf andere Systeme auswirkt, die dieselben Informationen verwenden.

Der andere wichtige Grund, eine Entwicklungsumgebung einzurichten, besteht darin sicherzustellen, dass Ihre Lösungen funktionieren, ohne dabei auf Live-Daten zugreifen zu müssen. Identity Manager verarbeitet Daten. Dazu gehört auch das Löschen von Daten. In einer Testumgebung können Sie Änderungen an Daten vornehmen, ohne dass die „echten“ Daten in Ihrer Produktionsumgebung davon betroffen sind.

Die sollten für jede Bereitstellung des Identity Manager eine Entwicklungsumgebung einrichten. Bereitstellungen unterscheiden sich voneinander. Es gibt unterschiedliche Systeme, Geschäftsrichtlinien und Prozeduren, die in der Identity Manager-Lösung berücksichtigt werden müssen. Eine Entwicklungsumgebung ermöglicht Ihnen, eine auf die jeweilige Situation zugeschnittene Lösung zu erarbeiten.

Das wichtigste Werkzeug beim Entwickeln Ihrer Identity Manager-Lösung ist Designer. Mit ihm können Sie alle Informationen zu Ihrer Umgebung erfassen und diese anschließend zum Erstellen einer individuell zugeschnittenen Identity Manager-Lösung verwenden. Designer können Sie zur Erfassung aller benötigten Informationen für alle Aspekte der Planung einsetzen. Designer vereinfacht das Erstellen eines Projektplans, der sowohl geschäftliche als auch technische Informationen umfasst. Weitere Informationen zu Designer finden Sie im *Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6*.

Verwenden Sie zum Einrichten Ihrer Entwicklungsumgebung die Informationen in **Kapitel 4**, „Basis-Checkliste für das Identity Manager-System“, auf Seite 41. Es handelt sich um eine Installations-Checkliste für alle Identity Manager-Komponenten. Stellen Sie anhand dieser Liste sicher, dass Sie alle Komponenten für Identity Manager, die Sie für die Erstellung eines Projektplans benötigen, installiert und konfiguriert haben. Die Informationen in **Kapitel 3**, „Technische Richtlinien“, auf Seite 27 sind hilfreich beim Einrichten Ihrer Entwicklungsumgebung. Sie erfahren mehr über technische Aspekte, was Ihnen beim Installieren und Konfigurieren der Identity Manager-Komponenten zugute kommt.

Nachdem Sie Ihre Entwicklungsumgebung eingerichtet haben, besteht der nächste Schritt darin, den Projektplan zum Implementieren der Identity Manager-Lösung zu erstellen. Verwenden Sie zum Erstellen des Projektplans die Informationen in **Kapitel 2**, „Erstellen eines Projektplans“, auf Seite 15.

Erstellen eines Projektplans

2

Das Planungsmaterial bietet einen Überblick über die Aktivitätstypen, die normalerweise Teil eines Identity Manager-Projekts sind - von den Anfängen bis zur vollständigen Produktionsbereitstellung. Zur Implementierung einer Identitätsmanagementstrategie müssen Sie Ihre aktuellen Geschäftsprozesse, die Erfordernisse dieser Prozesse sowie die Projektbeteiligten in der Umgebung kennen. Auf dieser Basis können Sie dann eine Lösung entwickeln, die Unterstützung der Projektbeteiligten einholen, die Lösung testen und ein Produktions-Rollout durchführen. In diesem Abschnitt werden die Grundlagen dieses Prozesses erläutert, damit Sie aus Identity Manager den bestmöglichen Nutzen ziehen können.

Dieser Abschnitt erhebt keinen Anspruch auf Vollständigkeit. Es werden weder alle möglichen Konfigurationen erläutert noch müssen die dargestellten Schritte zwingend ausgeführt werden. Jede Umgebung ist anders, sodass die Art der zu verwendenden Aktivitäten flexibel gehandhabt werden muss.

- ♦ [Abschnitt 2.1, „Ermittlungsphase“, auf Seite 15](#)
- ♦ [Abschnitt 2.2, „Anforderungs- und Entwurfsanalysephase“, auf Seite 19](#)
- ♦ [Abschnitt 2.3, „Proof-of-Concept“, auf Seite 24](#)
- ♦ [Abschnitt 2.4, „Validierung und Vorbereitung der Daten“, auf Seite 24](#)
- ♦ [Abschnitt 2.5, „Produktions-Prototyp“, auf Seite 25](#)
- ♦ [Abschnitt 2.6, „Planung des Produktions-Rollout“, auf Seite 25](#)
- ♦ [Abschnitt 2.7, „Produktionsbereitstellung“, auf Seite 25](#)

2.1 Ermittlungsphase

Die Identity Manager-Lösung wirkt sich auf viele Aspekte Ihres Unternehmens aus. Für eine effektive Lösung wird ausreichend Zeit benötigt, um alle aktuellen Geschäftsprozesse zu definieren, um herauszufinden, wie sich eine Implementierung der Identity Manager-Änderungen auf diese Prozesse auswirkt, auf welche Bereiche diese Änderungen Auswirkungen haben und wie die Änderungen implementiert werden.

In der Ermittlungsphase erhalten alle Projektbeteiligten einen allgemeinen Einblick in die Probleme und Lösungen. In dieser Phase wird eine Roadmap mit den wichtigsten Geschäfts- und Systeminformationen erstellt, die von der Identity Manager-Lösung betroffen sind. Zudem haben alle Projektbeteiligten die Möglichkeit, an der Erstellung der Identity Manager-Lösung mitzuwirken, damit sie wissen, wie sich diese auf ihr jeweiliges Geschäftsfeld auswirkt.

In der folgenden Liste werden die Schritte aufgeführt, die für eine erfolgreiche Ermittlungsphase erforderlich sind. Im Laufe der Ermittlungs- und Entwurfsphase werden Sie möglicherweise feststellen, dass Sie zusätzliche Schritte benötigen.

- ♦ [Abschnitt 2.1.1, „Definieren aktueller Geschäftsprozesse“, auf Seite 16](#)
- ♦ [Abschnitt 2.1.2, „Definieren, wie sich die Identity Manager-Lösung auf die aktuellen Geschäftsprozesse auswirkt“, auf Seite 17](#)
- ♦ [Abschnitt 2.1.3, „Identifizieren der wichtigsten Projektbeteiligten auf geschäftlicher und technischer Ebene“, auf Seite 17](#)

- ♦ Abschnitt 2.1.4, „Gespräche mit allen Projektbeteiligten führen“, auf Seite 18
- ♦ Abschnitt 2.1.5, „Erstellen einer allgemeinen Strategie und eines konsensfähigen Ausführungsablaufs“, auf Seite 18

2.1.1 Definieren aktueller Geschäftsprozesse

Identity Manager automatisiert Geschäftsprozesse, damit Identitäten in Ihrer Umgebung einfach verwaltet werden können. Wenn Sie die aktuellen Geschäftsprozesse nicht kennen, können Sie keine Identity Manager-Lösung entwerfen, die diese Prozesse automatisiert. Im Architektenmodus von Designer können Sie Ihre aktuellen Geschäftsprozesse erfassen und diese grafisch darstellen. Weitere Informationen finden Sie unter „Architektenmodus“ im *Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6*.

Hier einige Beispiele für Geschäftsprozesse:

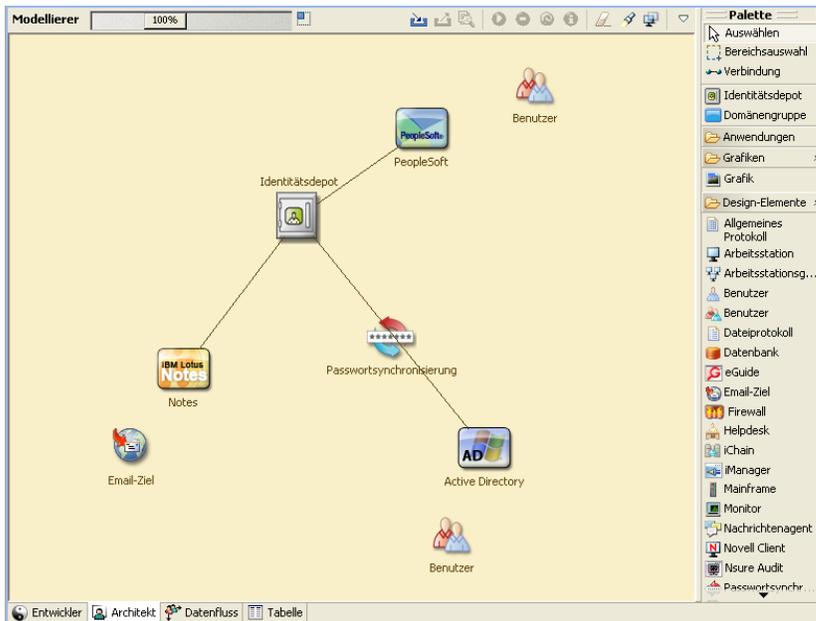
- ♦ Wenn ein Mitarbeiter ausscheidet, wird sein Benutzerkonto im E-Mail-System gelöscht, aber das Benutzerkonto in allen anderen Systemen wird nicht gelöscht, sondern deaktiviert.
- ♦ Das Format einer Email-Adresse eines Benutzers.
- ♦ Systeme oder Ressourcen, auf die Vertriebsmitarbeiter zugreifen können.
- ♦ Systeme oder Ressourcen, auf die Manager zugreifen können.
- ♦ Welche Systeme erzeugen neue Konten? Das Personalsystem oder geschieht dies durch eine Workflow-Anforderung?
- ♦ Eine Passwortrichtlinie für das Unternehmen, anhand der definiert wird, wie oft ein Passwort geändert wird, wie komplex das Passwort ist und welche Systeme das Passwort synchronisieren.

Sie sollten beim Definieren von Geschäftsprozessen wie folgt vorgehen, um alle Prozesse zu verstehen:

- ♦ Definieren Sie die aktuellen Geschäftsaspekte.
- ♦ Legen Sie die Initiativen fest, die zum Angehen dieser Probleme erforderlich sind.
- ♦ Ermitteln Sie, welche Services und Systeme von diesen Initiativen betroffen sind.

Anhand dieser Schritte erhalten Sie einen allgemeinen Überblick über die aktuellen Abläufe bzw. Prozesse in Ihrem Unternehmen und können ermitteln, welche Prozesse verbessert werden müssen. Beispielsweise zeigt **Abbildung 2-1** aus Designer, dass mit dem PeopleSoft*-System neue Benutzerkonten generiert werden. Sie werden in das Identitätsdepot und anschließend in Lotus Notes* und Active Directory* synchronisiert. Passwörter werden zwischen Active Directory und dem Identitätsdepot synchronisiert. Konten werden in das Notes-System synchronisiert, es werden aber keine Konten zurück in das Identitätsdepot synchronisiert.

Abbildung 2-1 Beispiel für Geschäftsprozesse



Der nächste Schritt wird in [Abschnitt 2.1.2, „Definieren, wie sich die Identity Manager-Lösung auf die aktuellen Geschäftsprozesse auswirkt“](#), auf Seite 17 beschrieben.

2.1.2 Definieren, wie sich die Identity Manager-Lösung auf die aktuellen Geschäftsprozesse auswirkt

Nachdem Sie die aktuellen Geschäftsprozesse definiert haben, müssen Sie entscheiden, welche Prozesse in die Identity Manager-Lösung aufgenommen werden sollen.

Am besten betrachten Sie die gesamte Lösung und priorisieren dann die Prozesse, die implementiert werden sollen. Identity Manager umfasst so viele Aspekte Ihrer geschäftlichen Aktivitäten, dass es einfacher ist, eine Gesamtlösung zu planen, anstatt für jeden Geschäftsprozess eine eigene Lösung zu finden.

Erstellen Sie eine Liste der Geschäftsprozesse, die zuerst automatisiert werden sollen, und ermitteln Sie anschließend, auf welche Systeme sich diese Änderungen auswirken. Der nächste Schritt wird in [Abschnitt 2.1.3, „Identifizieren der wichtigsten Projektbeteiligten auf geschäftlicher und technischer Ebene“](#), auf Seite 17 beschrieben.

2.1.3 Identifizieren der wichtigsten Projektbeteiligten auf geschäftlicher und technischer Ebene

Das Identifizieren aller Projektbeteiligten an der Identity Manager-Lösung ist für den Erfolg der Lösung enorm wichtig. In den meisten Firmen gibt es mehrere Kontaktpersonen, die alle geschäftlichen und technischen Aspekte der Geschäftsprozesse kennen. Sie müssen ermitteln, welche Services und Systeme von der Identity Manager-Lösung betroffen sind und wer für diesen Service oder dieses System verantwortlich ist.

Wenn Sie beispielsweise ein E-Mail-System in Ihre Lösung integrieren, müssen Sie das E-Mail-System, den Email-Systemadministrator ist und die verfügbaren Kontaktinformationen aufführen. Sie können all diese Informationen in das Designer-Projekt übernehmen. Jedes Anwendungssymbol bietet einen Ort, an dem Sie Informationen über das System und den Systemadministrator speichern können. Weitere Informationen finden Sie unter „**Eigenschaften dieser Anwendung konfigurieren**“ im *Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6*.

Nachdem Sie alle handelnden Personen eines jeden Geschäftsprozesses identifiziert haben, können Sie mit dem nächsten Schritt in **Abschnitt 2.1.4, „Gespräche mit allen Projektbeteiligten führen“**, auf **Seite 18** fortfahren.

2.1.4 Gespräche mit allen Projektbeteiligten führen

Anhand von Gesprächen mit den wichtigsten Projektbeteiligten auf geschäftlicher und technischer Ebene können Sie Informationen sammeln, die Sie für einen vollständigen Entwurf einer Identity Manager-Lösung benötigen. Sie können die Gespräche auch dazu nutzen, die Projektbeteiligten über die Identity Manager-Lösung zu informieren und ihnen mitzuteilen, wie sich die Lösung auf ihre Bereiche auswirkt. Folgende Aspekte sollten bei Interviews abgedeckt werden:

- ♦ Definieren der Geschäftsprozesse, die von der Identity Manager-Lösung berührt werden. Der Gesprächspartner verfügt möglicherweise über Informationen, die eine Anpassung des aktuellen Plans erforderlich machen.
- ♦ Ermitteln, wie sich die Lösung auf die Projektbeteiligten auswirkt, und Eingehen auf mögliche Bedenken. Fragen Sie außerdem die Projektbeteiligten, wie viel Zeit ihr Beitrag zur Lösung in Anspruch nehmen wird. Die Interviewten können dies evtl. abschätzen und Sie können diese Informationen zur Ermittlung des Arbeitsaufwands für die Lösung heranziehen.
- ♦ Erfassen der wichtigsten Geschäfts- und Systeminformationen von den Projektbeteiligten. Manchmal kann sich ein Vorschlag nachteilig auf einen Geschäftsprozess oder ein System auswirken. Das Erfassen wichtiger Informationen hilft Ihnen, im Rahmen der Identity Manager-Lösung fundierte Entscheidungen zu treffen.

Nachdem Sie die wichtigsten Projektbeteiligten befragt haben, können Sie mit dem nächsten Schritt in **Abschnitt 2.1.5, „Erstellen einer allgemeinen Strategie und eines konsensfähigen Ausführungsablaufs“**, auf **Seite 18** fortfahren.

2.1.5 Erstellen einer allgemeinen Strategie und eines konsensfähigen Ausführungsablaufs

Wenn alle Informationen zusammengestellt wurden, müssen Sie eine allgemeine Strategie bzw. eine Roadmap für die Identity Manager-Lösung entwerfen. Legen Sie alle Funktionen fest, die in der Identity Manager-Lösung berücksichtigt werden sollen. Neue Benutzerkonten werden beispielsweise durch eine Anforderung über einen Workflow generiert, aber der erstellte Benutzertyp hängt von den Ressourcen ab, auf die der Benutzer zugreifen kann.

Stellen Sie diese allgemeine Strategie, falls möglich, in einem einzigen Meeting an alle Projektbeteiligten vor. Dies ermöglicht Ihnen Folgendes:

- ♦ Sie können sich vergewissern, dass die beabsichtigten Initiativen berechtigt sind und welche die höchste Priorität haben.
- ♦ Identifizieren Sie die Planungsaktivitäten in Vorbereitung der Anforderungs- und Entwurfsphase.

- ♦ Legen Sie die Elemente fest, die zum Durchführen einer oder mehrerer dieser Initiativen erforderlich sind.
- ♦ Erstellen Sie einen konsensfähigen Ausführungspfad für die Identity Manager-Lösung.
- ♦ Definieren Sie zusätzliche Schulungen für die Projektbeteiligten.

Mit der Ermittlung erhalten alle Projektbeteiligten einen allgemeinen Einblick in die Probleme und Lösungen. Diese Phase bietet einen hervorragenden Ausgangspunkt für die Analysephase, für die die Projektbeteiligten eine Grundkenntnis von Verzeichnissen sowie von Novell® eDirectory™, Novell Identity Manager und der XML-Integration im Allgemeinen benötigen.

Nachdem Sie die Ermittlungsphase abgeschlossen haben, fahren Sie mit [Abschnitt 2.2](#), „Anforderungs- und Entwurfsanalysephase“, auf Seite 19 fort.

2.2 Anforderungs- und Entwurfsanalysephase

Verwenden Sie die in der Ermittlungsphase erstellte allgemeine Roadmap als Ausgangspunkt für die Analysephase. Sowohl das Dokument als auch das Designer-Projekt benötigen zusätzliche technische und geschäftliche Details. Daraus ergibt sich das Datenmodell und der allgemeine Entwurf der Identity Manager-Architektur, anhand der die Identity Manager-Lösung implementiert wird.

Der Entwurf sollte besonders das Identitätsmanagement umfassen. Es können aber auch viele Elemente, die traditionell einem Ressourcen-Management-Verzeichnis, z. B. Archivierung und Drucken, zugeordnet sind. Identity Manager synchronisiert Benutzerkonten mit Verzeichnissen, die keinen direkten Zugriff auf das Dateisystem des Betriebssystems haben. Beispielsweise können Sie ein Benutzerkonto in Active Directory haben, aber dies gewährt Ihnen keinen Zugriff auf das Dateisystem auf dem Active Directory-Server.

Beantworten Sie anhand der in der Ermittlungsphase gesammelten Informationen die folgenden Beispielfragen, um herauszufinden, ob Sie noch weitere Informationen benötigen. Möglicherweise müssen Sie dazu zusätzliche Interviews mit Projektbeteiligten führen.

- ♦ Welche Versionen der Systemsoftware werden verwendet?
- ♦ Ist der eDirectory-Entwurf zweckdienlich? Enthält der Identity Manager-Server beispielsweise eine Master- oder eine Lese-/Schreibreproduktion der Benutzerobjekte, die synchronisiert werden? Falls nicht, ist der eDirectory-Entwurf nicht zweckdienlich.
- ♦ Ist die Qualität der Daten in allen Systemen sachgemäß? (Wenn die Daten nicht verwendet werden können, wird die Geschäftsrichtlinie möglicherweise nicht wie gewünscht implementiert.) Es gibt beispielsweise doppelte Konten für die Benutzer in den Systemen, die synchronisiert werden, oder das Format der Daten ist innerhalb des Systems nicht konsistent. Die Daten eines jeden Systems müssen vor der Synchronisierung der Informationen evaluiert werden.
- ♦ Ist in Ihrer Umgebung eine Bearbeitung der Daten erforderlich? Beispielsweise ist das Format des Einstellungsdatums eines Benutzers im Personalsystem 23.02.2008 und im Identitätsdepot 23/02/2008. Dies bedeutet, dass das Datum zuerst bearbeitet werden muss, damit eine Synchronisierung erfolgen kann.

Machen Sie sich mit den Informationen in [Kapitel 3](#), „Technische Richtlinien“, auf Seite 27 vertraut, damit Sie für Ihre Umgebung die richtigen Entscheidungen treffen können.

Nach der Analyse der Anforderungen können Sie den Bereich und den Projektplan für die Implementierung erstellen und ermitteln, ob bestimmte Voraussetzungen erfüllt werden müssen. Sie sollten bei der Sammlung von Informationen und der Dokumentation der Anforderungen möglichst sorgfältig vorgehen, um kostspielige Fehler zu vermeiden. Hier ist eine Liste mit den möglichen Anforderungen:

- ♦ Datenmodell, das alle Systeme, autorisierte Datenursprünge, Ereignisse, Informationsfluss, Datenformatstandards sowie Zuordnungsbeziehungen zwischen verbundenen Systemen und Attributen in Identity Manager anzeigt.
- ♦ Geeignete Identity Manager-Architektur für die Lösung.
- ♦ Details für zusätzliche Systemverbindungsanforderungen.
- ♦ Strategien für die Datenvalidierung und das Auffinden übereinstimmender Datensätze.
- ♦ Entwurf der Verzeichnisse zur Unterstützung der Identity Manager-Infrastruktur.

Bei der Bewertung der Anforderungen und des Entwurfs sollten folgende Aufgaben durchgeführt werden:

- ♦ „Definieren der Geschäftsanforderungen“ auf Seite 20
- ♦ „Analyse der Geschäftsprozesse“ auf Seite 21
- ♦ „Entwurf eines Enterprise-Datenmodells“ auf Seite 22

2.2.1 Definieren der Geschäftsanforderungen

In der Ermittlungsphase haben Sie Informationen zu den Geschäftsprozessen und -anforderungen Ihres Unternehmens gesammelt, die diese Geschäftsprozesse definieren. Erstellen Sie eine Liste dieser Geschäftsanforderungen und ordnen Sie anschließend in Designer diese Prozesse zu, indem Sie folgende Aufgaben durchführen:

- ♦ Erstellen Sie eine Liste der Geschäftsanforderungen und ermitteln Sie, welche Systeme von diesem Prozess beeinflusst werden. Beispiel: Eine Geschäftsanforderung bei der Kündigung eines Mitarbeiters könnte sein, dass am Tag der Kündigung der Zugriff des Mitarbeiters auf das Netzwerk und sein Email-Konto gesperrt wird. Dieser Kündigungsprozess wirkt sich auf das Email-System und das Identitätsdepot aus.
- ♦ Erstellen Sie Vorgangsflüsse, Prozessauslöser und Datenzuordnungsbeziehungen.
Wenn beispielsweise in einem bestimmten Prozess etwas geschieht, was geschieht durch diesen Prozess? Welche anderen Prozesse werden ausgelöst?
- ♦ Ordnen Sie Datenflüsse zwischen Anwendungen zu. Diese Informationen werden in Designer angezeigt. Weitere Informationen finden Sie unter „Verwalten des Datenflusses“ im *Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6*.
- ♦ Identifizieren Sie Daten, die von einem Format in ein anderes Format geändert werden müssen, beispielsweise „2/25/2007“ in „25. Februar 2007“.
- ♦ Dokumentieren Sie bestehende Datenabhängigkeiten.
Wenn ein bestimmter Wert geändert wird, ist es wichtig zu wissen, ob für diesen Wert eine Abhängigkeit besteht. Wenn ein bestimmter Prozess geändert wird, ist es wichtig zu wissen, ob für diesen Prozess eine Abhängigkeit besteht.

Wenn Sie z. B. in einem Human-Resources-System für einen Mitarbeiter den Status „Temporär“ auswählen, hat dies möglicherweise zur Folge, dass die IT-Abteilung in eDirectory ein Benutzerobjekt mit eingeschränkten Rechten und einem auf bestimmte Zeiten begrenzten Netzwerkzugang erstellen muss.

- ◆ Listen Sie die Prioritäten auf.

Es können nicht direkt die Anforderungen und Wünsche aller Personen erfüllt werden. Prioritäten für den Entwurf und die Bereitstellung des Bereitstellungssystems vereinfachen die Planung einer Roadmap.

Es kann von Vorteil sein, die Bereitstellung in Phasen zu unterteilen, sodass die Implementierung von Teilen der Bereitstellung zu einem früheren und von anderen Teilen der Bereitstellung zu einem späteren Zeitpunkt erfolgt. Sie können die Bereitstellung auch schrittweise durchführen. Dieser Ansatz sollte auf Gruppen von Personen innerhalb der Organisation basieren.

- ◆ Definieren Sie die Voraussetzungen.

Die für die Implementierung einer bestimmten Phase der Bereitstellung erforderlichen Voraussetzungen sollten dokumentiert werden. Dies umfasst den Zugriff auf die verbundenen Systeme, die mit Identity Manager gekoppelt werden sollen.

- ◆ Identifizieren Sie autorisierte Datenursprünge.

Wenn Sie bereits früh wissen, welche Elemente welchen IT-Administratoren und -Managern zuzuordnen sind, kann dies bei allen beteiligten Parteien zu einer größeren Akzeptanz führen.

Beispiel: Der Kontoadministrator benötigt möglicherweise die Berechtigung, Mitarbeitern Rechte für bestimmte Dateien und Verzeichnisse zu gewähren. Dieser Erfordernis kann Rechnung getragen werden, indem lokale Trustee-Zuweisungen in das Kontosystem implementiert werden.

Nachdem Sie die Geschäftsanforderungen definiert haben, fahren Sie mit [Abschnitt 2.2.2, „Analyse der Geschäftsprozesse“](#), auf Seite 21 fort.

2.2.2 Analyse der Geschäftsprozesse

Nachdem Sie die Analyse der Geschäftsanforderungen abgeschlossen haben, benötigen Sie für die genaue Abstimmung der Identity Manager-Lösung noch weitere Informationen. Sie müssen wichtige Personen wie Manager, Administratoren und Mitarbeiter interviewen, die die Anwendung oder das System einsetzen. Folgende Fragen sollten beantwortet werden:

- ◆ Woher stammen die Daten?
- ◆ Wofür sind die Daten bestimmt?
- ◆ Wer ist für die Daten verantwortlich?
- ◆ Wer ist der Eigentümer der Geschäftsfunktion, zu der die Daten gehören?
- ◆ Wer muss zur Änderung der Daten kontaktiert werden?
- ◆ Welche Folgen hat die Änderung von Daten?
- ◆ Welche Arbeitsmethoden gelten für die Datenbearbeitung (Sammeln und/oder Bearbeitung)?
- ◆ Welche Art von Vorgängen laufen ab?
- ◆ Welche Methoden werden zur Sicherung der Datenqualität und -integrität verwendet?

- ♦ Wo werden die Systeme eingesetzt (auf welchen Servern, in welchen Abteilungen)?
- ♦ Welche Prozesse eignen sich nicht für die automatisierte Bearbeitung?

Dem Administrator eines PeopleSoft-Systems in der Personalabteilung könnten beispielsweise folgende Fragen gestellt werden:

- ♦ Welche Daten werden in der PeopleSoft-Datenbank gespeichert?
- ♦ Welche Elemente werden in den verschiedenen Teilfenstern eines Mitarbeiterkontos angezeigt?
- ♦ Welche Aktionen sind erforderlich, damit sie über das Bereitstellungssystem hinaus wirksam werden (z. B. Aktionen zum Hinzufügen, Modifizieren und Löschen)?
- ♦ Welche dieser Aktionen sind erforderlich? Welche Aktionen sind optional?
- ♦ Welche Aktionen müssen auf Basis der in PeopleSoft durchgeführten Aktionen ausgelöst werden?
- ♦ Welche Operationen/Ereignisse/Aktionen müssen ignoriert werden?
- ♦ Auf welche Weise müssen die Daten transformiert und Identity Manager zugeordnet werden?

Das Befragen wichtiger Personen kann Sie in andere Bereiche der Organisation führen, durch die Sie ein deutlicheres Bild des gesamten Prozesses gewinnen können.

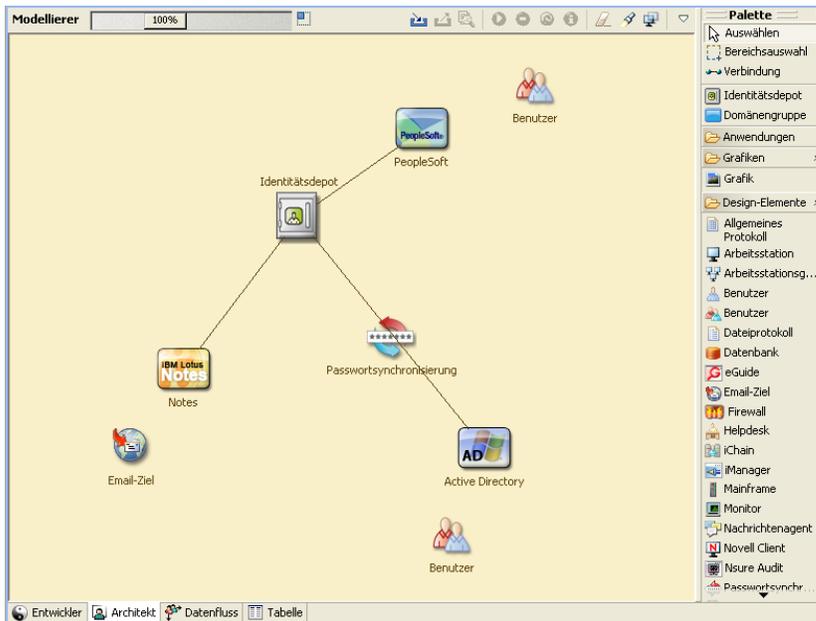
Wenn Sie all diese Informationen gesammelt haben, können Sie ein Enterprise-Datenmodell für Ihre Umgebung entwerfen. Fahren Sie mit [Abschnitt 2.2.3, „Entwurf eines Enterprise-Datenmodells“](#), auf Seite 22 fort, um mit dem Entwurf zu beginnen.

2.2.3 Entwurf eines Enterprise-Datenmodells

Nach der Definition der Geschäftsprozesse können Sie unter Verwendung von Designer mit dem Entwurf eines Datenmodells beginnen, das Ihre aktuellen Geschäftsprozesse widerspiegelt.

Das Modell in Designer gibt den Datenursprung sowie die Richtung des Datenflusses an und zeigt auf, wohin sich die Daten nicht bewegen dürfen. Außerdem wird aufgezeigt, auf welche Weise sich kritische Ereignisse auf den Datenfluss auswirken. Beispielsweise zeigt [Abbildung 2-2](#), dass die Daten aus PeopleSoft abgerufen werden, es aber keinen synchronisierten Datenfluss zurück zu PeopleSoft gibt.

Abbildung 2-2 Datenfluss in Designer



Möglicherweise empfiehlt sich auch die Entwicklung eines Diagramms, das den vorgeschlagenen Geschäftsprozess und die Vorteile veranschaulicht, die durch die Implementierung der automatisierten Bereitstellung erzielt werden.

Am Anfang der Entwicklung dieses Modells steht die Beantwortung folgender Fragen:

- ◆ Welche Objekttypen (z. B. Benutzer oder Gruppen) werden verschoben?
- ◆ Welche Ereignisse sind von Interesse?
- ◆ Welche Attribute müssen synchronisiert werden?
- ◆ Welche Daten werden in Ihrem Unternehmen für die verschiedenen zu verwaltenden Objekttypen gespeichert?
- ◆ Handelt es sich um eine einseitige oder um eine bidirektionale Synchronisierung?
- ◆ Welches System ist für welche Attribute der autorisierte Ursprung?

Außerdem ist es wichtig, die Zusammenhänge verschiedener Werte zwischen den Systemen zu berücksichtigen.

Das Statusfeld eines Mitarbeiters in PeopleSoft kann beispielsweise drei Werte annehmen: „Festangestellter“, „Freiberufler“ und „Praktikant“. Das Active Directory-System hat möglicherweise nur zwei Werte: „Dauerhaft“ und „Temporär“. In diesem Fall müssen die Beziehungen zwischen dem Status „Freiberufler“ in PeopleSoft und den Werten „Dauerhaft“ und „Temporär“ in Active Directory festgelegt werden.

Ziel dieser Tätigkeit ist es, alle Verzeichnissysteme zu verstehen, in welcher Beziehung sie zueinander stehen und welche Objekte und Attribute systemübergreifend synchronisiert werden müssen. Nach der Fertigstellung des Entwurfs besteht der nächste Schritt darin, ein Proof-of-Concept zu erstellen. Fahren Sie mit **Abschnitt 2.3, „Proof-of-Concept“, auf Seite 24** fort.

2.3 Proof-of-Concept

Als Ergebnis dieser Aktivität sollte eine Beispiel-Implementierung in einer Laborumgebung vorliegen, die der Geschäftsrichtlinie und dem Datenfluss in Ihrem Unternehmen entspricht. Sie sollte auf dem Datenmodell basieren, das während der Anforderungsanalyse und der Entwurfsphase entwickelt wurde. Dies ist der letzte Schritt vor dem Produktions-Prototyp.

Hinweis: In dieser Phase bietet es sich an, die Unterstützung des Managements einzuholen und die Finanzierung für die endgültige Umsetzung zu sichern.

Kapitel 3, „Technische Richtlinien“, auf Seite 27 enthält Informationen, die für die Validierung des Proof-of-Concept nützlich sind. Es enthält technische Richtlinien, die Sie bei einer erfolgreichen Identity Manager-Bereitstellung unterstützen.

Neben der Erstellung des Proof-of-Concept müssen Sie auch einen Plan zur Validierung der Daten erstellen, die sich in Ihren Systemen befinden. Mithilfe dieses Schritts stellen Sie sicher, dass keine Konflikte zwischen den Systemen auftreten. Fahren Sie mit **Abschnitt 2.4, „Validierung und Vorbereitung der Daten“, auf Seite 24** fort. Dort finden Sie Informationen darüber, wie Sie diese Konflikte verhindern können.

2.4 Validierung und Vorbereitung der Daten

Die Qualität und Konsistenz der Daten in Produktionssystemen kann variieren und möglicherweise Inkonsistenzen bei der Synchronisierung von Systemen zur Folge haben. In dieser Phase wird eine deutliche Trennung zwischen dem Team, das für die Implementierung der Ressourcen zuständig ist, und den Geschäftseinheiten oder -gruppen vorgenommen, die „Eigentümer“ der Daten in den zu integrierenden Systemen sind oder diese verwalten. Bestehende Risiko- und Kostenfaktoren gehören nicht unbedingt zu einem Bereitstellungsprojekt.

Sie benötigen das Datenmodell, das Sie in den Analyse- und Entwurfsphasen entwickelt haben. Sie sollten auch über eine Strategie zum Datensatz- und Datenformatabgleich verfügen, damit die Daten ordnungsgemäß vorbereitet werden können. Wenn Sie das Datenmodell und -format definiert haben, können Sie wie folgt fortfahren:

- ♦ Erstellen Sie Produktions-Daten-Sets, die in das Identitätsdepot geladen werden können (wie in den Analyse- und Entwurfsaktivitäten definiert). Hierzu gehört auch die Angabe der voraussichtlichen Lademethode (Bulk-Verarbeitung oder über Anschlüsse). Es werden auch Anforderungen für die Daten identifiziert, die validiert oder in bestimmter Weise formatiert werden.
- ♦ Identifizieren Sie Leistungsfaktoren und validieren Sie diese Faktoren auf der Grundlage der verwendeten Geräte und der allgemeinen verteilten Architektur der Identity Manager-Bereitstellung.

Fahren Sie nach der Vorbereitung der Daten mit **Abschnitt 2.5, „Produktions-Prototyp“, auf Seite 25** fort.

2.5 Produktions-Prototyp

Das Ziel dieser Aktivität ist es, die Migration in eine Produktumgebung zu starten. Während dieser Phase ist möglicherweise eine zusätzliche Anpassung erforderlich. In dieser kurzen Einführung können die gewünschten Ergebnisse der vorhergehenden Aktivitäten bestätigt und die Zustimmung für das Produktions-Rollout eingeholt werden. Anhand der Prototyp-Lösung wird der Plan validiert, der bis zu diesem Zeitpunkt im Prozess erstellt wurde.

Hinweis: Diese Phase liefert möglicherweise die Abnahmekriterien für die Lösung und den benötigten Meilenstein auf dem Weg zur vollständigen Produktion.

Die Prototyp-Lösung bietet ein Live-Proof-of-Concept und eine Validierung des Datenmodells sowie der gewünschten Prozessergebnisse. Fahren Sie nach Fertigstellung des Prototyps mit [Abschnitt 2.6, „Planung des Produktions-Rollout“, auf Seite 25](#) fort.

2.6 Planung des Produktions-Rollout

In dieser Phase wird die Produktionsumgebung geplant. Dieser Plan sollte Folgendes abdecken:

- ◆ Bestätigung der Serverplattformen, Softwareversionen und Service Packs
- ◆ Bestätigung der allgemeinen Umgebung
- ◆ Bestätigung des Entwurfs des Identitätsdepots in einer gemischten Umgebung
- ◆ Bestätigung, dass die Geschäftslogik korrekt ist
- ◆ Bestätigung, dass die Datensynchronisierung wie geplant ausgeführt wird
- ◆ Planung der Umstellung auf den neuen Prozess
- ◆ Planung einer Rollback-Strategie für den Notfall

Der Plan muss Datumsangaben für die Implementierung und Fertigstellung der einzelnen Schritte des Rollouts enthalten. Jeder Projektbeteiligte liefert Input zu diesen Datumsangaben und stimmt den festgelegten Terminen zu. Dadurch wissen alle am Rollout beteiligten Personen, wann die Änderungen zu erwarten und wann sie abgeschlossen sind.

Wenn der Plan für das Produktions-Rollout fertig ist, fahren Sie mit [Abschnitt 2.7, „Produktionsbereitstellung“, auf Seite 25](#) fort.

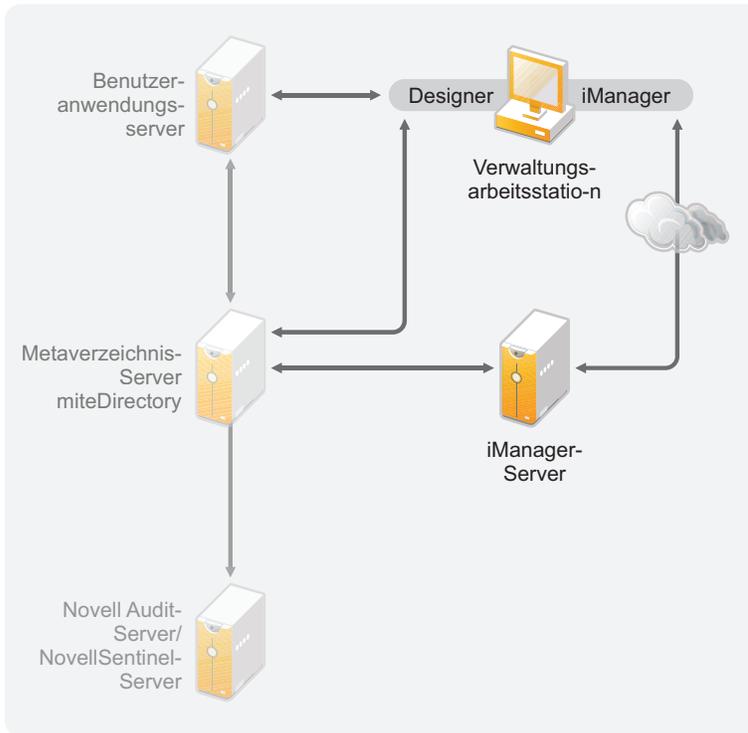
2.7 Produktionsbereitstellung

In der Produktions-Bereitstellungsphase werden alle Pläne umgesetzt und die Identity Manager-Lösung wird in der Live-Umgebung implementiert. Mit dem Plan für das Produktions-Rollout können Sie die verschiedenen Teile der Identity Manager-Lösung in Betrieb nehmen. Dies kann über Nacht geschehen oder sich über einen längeren Zeitraum erstrecken. Dies hängt vom Inhalt Ihres Plans ab.

3.1 Verwaltungswerkzeuge - Richtlinien

Die beiden Verwaltungswerkzeuge für die Identity Manager-Lösung sind Designer und iManager, wie in **Abbildung 3-2** dargestellt. Designer wird für die Planung und Erstellung und iManager für die täglichen Verwaltungsaufgaben der Identity Manager-Lösung verwendet.

Abbildung 3-2 Identity Manager - Verwaltungswerkzeuge



Dieses Dokument enthält ausschließlich Informationen zu Designer und iManager. Die Benutzeranwendung verwendet eine webbasierte Verwaltungsseite, auf die an dieser Stelle nicht weiter eingegangen wird. Weitere Informationen zur Benutzeranwendung finden Sie unter „Administering the User Application“ (<http://www.novell.com/documentation/idmrpbm361/agpro/data/agpropartadminapp.html>) (Verwalten der Benutzeranwendung) im Handbuch zur *Benutzeranwendung: Administration*.

- ♦ **Abschnitt 3.1.1, „Designer-Richtlinien“, auf Seite 28**
- ♦ **Abschnitt 3.1.2, „iManager-Richtlinien“, auf Seite 29**

3.1.1 Designer-Richtlinien

Designer ist ein Thick-Client, der auf einer Arbeitsstation installiert wird. Designer wird zum Entwerfen, Testen, Dokumentieren und Bereitstellen Ihrer Identity Manager-Lösung verwendet. Die Verwendung von Designer über die gesamte Planungsphase hinweg hilft Ihnen bei der zentralen Erfassung von Informationen. Sie erhalten zudem einen Überblick über alle Komponenten der Lösung, wodurch Sie Probleme besser erkennen können.

Bei der Verwendung von Designer gibt es keine weiteren Aspekte zu beachten, sofern nicht mehrere Personen an demselben Projekt arbeiten. Designer ermöglicht die Versionskontrolle des Projekts. Weitere Informationen finden Sie unter „[Versionskontrolle](#)“ im *Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6*.

3.1.2 iManager-Richtlinien

iManager ist das Administrationswerkzeug für Identity Manager. Wenn Sie Identity Manager installieren, wird bei der Installation vorausgesetzt, dass Sie bereits einen iManager-Server in Ihrem eDirectory™-Baum installiert haben.

Wenn mehr als zehn Administratoren dauerhaft gleichzeitig in iManager arbeiten, sollten Sie über einen Server verfügen, der ausschließlich iManager hostet. [Abbildung 3-2](#) stellt diese Konfiguration Ihrer Identity Manager-Lösung dar. Gibt es nur einen Administrator, können Sie iManager ohne Probleme auf Ihrem Metaverzeichnis-Server ausführen.

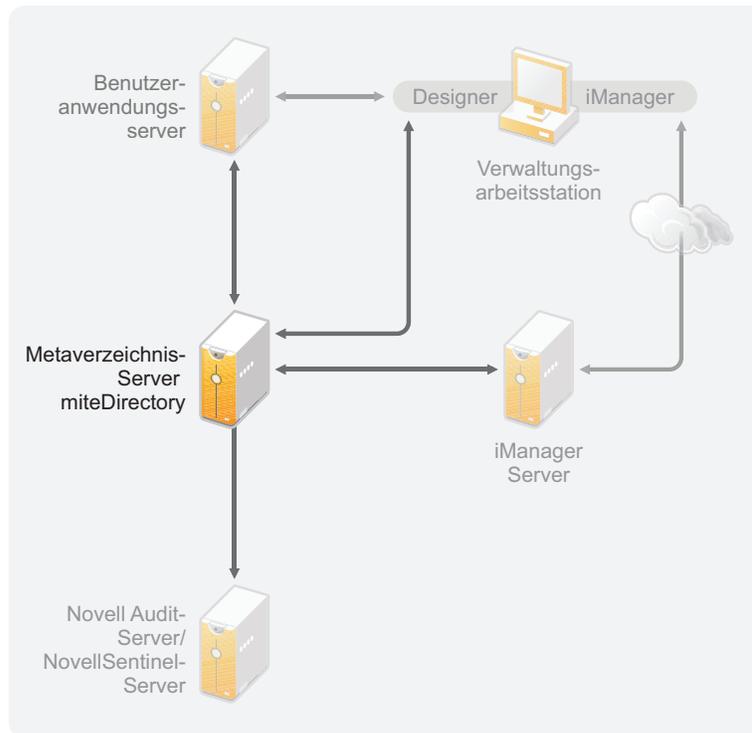
3.2 Metaverzeichnis-Server-Richtlinien

Abhängig von der Arbeitslast des Servers können Sie einen oder mehrere Metaverzeichnis-Server einsetzen. Für den Metaverzeichnis-Server ist es erforderlich, dass eDirectory installiert ist, wie in [Abbildung 3-3](#) dargestellt. Sie können einen Remote Loader-Server hinzufügen (in der Abbildung nicht dargestellt), damit die Arbeitslast bzw. die Konfiguration Ihrer Umgebung besser bewältigt werden kann.

Die Treiber müssen auf demselben Server wie die verbundene Anwendung ausgeführt werden. Achten Sie beispielsweise beim Konfigurieren des Active Directory-Treibers darauf, dass der Server in [Abbildung 3-3](#) ein Mitgliedsserver oder ein Domänencontroller sein muss. Wenn Sie eDirectory und Identity Manager nicht auf einem Mitgliedsserver oder Domänencontroller installieren möchten, können Sie den Remote Loader dort installieren. Der Remote Loader sendet alle Ereignisse von Active Directory an den Metaverzeichnis-Server. Der Remote Loader empfängt Informationen vom Metaverzeichnis-Server und übergibt sie an die verbundene Anwendung.

Der Remote Loader bietet zusätzliche Flexibilität für Ihre Identity Manager-Lösung. Weitere Informationen finden Sie im *Identity Manager 3.6.1 Remote Loader Guide* (Handbuch zu Identity Manager 3.6 Remote Loader).

Abbildung 3-3 Metaverzeichnis-Server



Es gibt viele Variablen, die sich auf die Arbeitsgeschwindigkeit des Servers auswirken. Allgemein wird empfohlen, nicht mehr als zehn Treiber auf einem Metaverzeichnis-Server auszuführen. Wenn allerdings jeder Treiber Millionen von Objekten synchronisiert, ist es u. U. nicht möglich, zehn Treiber auf einem Server auszuführen. Wenn Sie andererseits jedoch nur 100 Objekte pro Treiber synchronisieren, können Sie wahrscheinlich mehr als zehn Treiber auf einem Server ausführen.

Die Einrichtung der Identity Manager-Lösung in einer Testumgebung ermöglicht Ihnen, die Leistungsfähigkeit der Server zu testen. Die Zustandsüberwachungswerkzeuge in iManager liefern Ihnen Basisdaten, anhand derer Sie fundierte Entscheidungen für Ihre Umgebung treffen können. Weitere Informationen über die Werkzeuge zur Überwachung des Treiberzustands finden Sie unter „**Monitoring Driver Health**“ (Überwachen des Treiberzustands) im *Identity Manager 3.6.1 Common Driver Administration Guide* (Identity Manager 3.6 Common Driver Administrationshandbuch).

Zu berücksichtigende Aspekte für die einzelnen Treiber finden Sie auf der [Website zur Identity Manager Treiber-Dokumentation](http://www.novell.com/documentation/idm36drivers/index.html) (<http://www.novell.com/documentation/idm36drivers/index.html>). In jedem Treiberhandbuch finden Sie die für den jeweiligen Treiber spezifischen Informationen.

3.3 eDirectory-Richtlinien

eDirectory ist das Identitätsdepot, in dem die Objekte gespeichert werden, die anhand der Identity Manager-Lösung synchronisiert werden. Die folgenden Abschnitte behandeln die Richtlinien, mit deren Hilfe Sie die Bereitstellung von eDirectory planen können.

- ♦ **Abschnitt 3.3.1, „Identity Manager-Objekte in eDirectory“, auf Seite 31**

- ♦ **Abschnitt 3.3.2, „Replizierung der von Identity Manager auf dem Server benötigten Objekte“, auf Seite 31**
- ♦ **Abschnitt 3.3.3, „Verwendung der Bereichsfilterung zum Verwalten von Benutzern auf verschiedenen Servern“, auf Seite 33**

3.3.1 Identity Manager-Objekte in eDirectory

Die folgende Liste enthält die wesentlichen Identity Manager-Objekte, die in eDirectory gespeichert sind, und deren Verhalten zueinander. Während der Installation von Identity Manager werden keine Objekte erstellt. Die Identity Manager-Objekte werden im Rahmen der Konfiguration der Identity Manager-Lösung erstellt.

- ♦ **Treibersatz:** Ein Treibersatz ist ein Container, der Identity Manager-Treiber und Bibliotheksobjekte enthält. Auf einem Server kann immer nur ein Treibersatz aktiv sein. Sie können einen Treibersatz jedoch mit mehreren Servern verknüpfen. Ein Treiber kann auch mehreren Servern gleichzeitig zugeordnet werden. Er sollte jedoch immer nur auf einem Server gleichzeitig ausgeführt werden. Auf den anderen Servern muss der Treiber deaktiviert sein. Auf jedem mit einem Treibersatz verknüpften Server muss die Metaverzeichnis-Engine installiert sein.
- ♦ **Bibliothek:** Das Bibliotheksobjekt ist ein Repository mit häufig verwendeten Richtlinien, das von mehreren Positionen aus referenziert werden kann. Die Bibliothek wird im Treibersatz gespeichert. In der Bibliothek können Sie eine Richtlinie ablegen, auf die jeder Treiber im Treibersatz zugreifen kann.
- ♦ **Treiber:** Ein Treiber stellt die Verbindung zwischen einer Anwendung und dem Identitätsdepot her. Der Treiber ist das Verbindungsstück, das die Datensynchronisierung und die Freigabe zwischen Systemen ermöglicht. Der Treiber wird im Treibersatz abgelegt.
- ♦ **Auftrag:** Der Zweck eines Auftrags besteht darin, eine Aufgabe zu erledigen, die häufig ausgeführt werden muss. Ein Auftrag kann beispielsweise ein System konfigurieren, um ein Konto an einem bestimmten Tag zu deaktivieren oder um einen Workflow zu starten, mit dem eine Erweiterung der Zugriffsrechte einer Person auf eine Unternehmensressource angefordert wird. Der Auftrag wird im Treibersatz abgelegt.

3.3.2 Replizierung der von Identity Manager auf dem Server benötigten Objekte

Wenn in Ihrer Identity Manager-Umgebung mehrere Server benötigt werden, damit mehrere Identity Manager-Treiber ausgeführt werden können, sollten Sie dies in Ihrem Plan berücksichtigen und sicherstellen, dass bestimmte eDirectory-Objekte auf Servern repliziert werden, auf denen die Identity Manager-Treiber ausgeführt werden sollen.

Sie können gefilterte Reproduktionen verwenden, sofern alle Objekte und Attribute, die der Treiber lesen oder synchronisieren muss, Teil der gefilterten Reproduktion sind.

Denken Sie daran, dem Identity Manager-Treiberobjekt ausreichende eDirectory-Rechte für die zu synchronisierenden Objekte zu erteilen. Gewähren Sie diese Rechte entweder explizit oder definieren Sie das Treiberobjekt als sicherheitsäquivalent mit einem Objekt, das über die gewünschten Rechte verfügt.

Ein eDirectory-Server, auf dem ein Identity Manager-Treiber ausgeführt wird (oder auf den der Treiber verweist, falls Sie den Remote Loader verwenden), muss eine Masterreproduktion oder eine Lese-/Schreibreproduktion der folgenden Elemente enthalten:

- ♦ Das Treibersatzobjekt für den Server.

Für jeden Server, auf dem Identity Manager läuft, muss ein Treibersatzobjekt vorhanden sein. Sofern Sie keine speziellen Anforderungen haben, ordnen Sie nicht mehrere Server demselben Treibersatzobjekt zu.

Hinweis: Beim Erstellen eines Treibersatzobjekts wird standardmäßig eine separate Partition erstellt. Novell® empfiehlt, für das Treibersatzobjekt eine separate Partition zu erstellen. Damit Identity Manager funktioniert, muss der Server eine vollständige Reproduktion des Treibersatzobjekts enthalten. Wenn dem Server eine vollständige Reproduktion des Speicherorts zur Verfügung steht, an dem das Treibersatzobjekt installiert ist, wird keine Partition benötigt.

- ♦ Das Serverobjekt für den Treiber.

Das Serverobjekt wird benötigt, damit der Treiber Schlüsselpaare für Objekte erstellen kann. Außerdem ist es wichtig für die Authentifizierung des Remote Loaders.

- ♦ Die Objekte, die diese Instanz des Treibers synchronisieren soll.

Der Treiber kann nur Objekte synchronisieren, sofern sich eine Reproduktion dieser Objekte auf demselben Server befindet wie der Treiber. Der Identity Manager-Treiber synchronisiert die Objekte in *allen* Containern, die auf dem betreffenden Server repliziert sind, sofern Sie keine anderen Regeln für die Bereichsfilterung festgelegt haben.

Wenn ein Treiber beispielsweise alle Benutzerobjekte synchronisieren soll, geschieht dies am einfachsten durch die Instanz eines Treibers auf dem Server, auf dem sich eine Lese-/Schreibreproduktion aller Benutzer befindet.

In vielen Umgebungen gibt es jedoch keinen Einzelservers, der eine Reproduktion aller Benutzer enthält. Stattdessen sind die Benutzer-Datensätze auf mehrere Server verteilt. In diesem Fall stehen Ihnen drei Möglichkeiten zur Auswahl:

- ♦ **Kumulierung aller Benutzer auf einem Server.** Sie können einen Server erstellen, der alle Benutzer enthält, indem Sie zu einem vorhandenen Server Reproduktionen hinzufügen. Sofern erforderlich können gefilterte Reproduktionen verwendet werden, was die Größe der eDirectory-Datenbank verringert. Die erforderlichen Benutzerobjekte und -attribute müssen jedoch Teil der gefilterten Reproduktion sein.
- ♦ **Verwendung mehrerer Instanzen des Treibers auf mehreren Servern mit Bereichsfilterung.** Wenn Sie die Benutzer nicht auf einem Server kumulieren möchten, müssen Sie festlegen, welche Server alle Benutzer enthalten, und anschließend auf jedem dieser Treiber eine Instanz des Identity Manager-Treibers einrichten.

Damit keine separaten Instanzen eines Treibers versuchen, dieselben Benutzer zu synchronisieren, müssen Sie in der Bereichsfilterung definieren, welche Benutzer von den einzelnen Instanzen des Treibers synchronisiert werden sollen. Mithilfe der Bereichsfilterung können Sie jedem Treiber Regeln hinzufügen, damit die Aktionen des Treibers auf bestimmte Container beschränkt werden. Siehe „[Verwendung der Bereichsfilterung zum Verwalten von Benutzern auf verschiedenen Servern](#)“ auf Seite 33.

- ♦ **Verwendung mehrerer Instanzen des Treibers auf mehreren Servern ohne Bereichsfilterung.** Wenn mehrere Instanzen eines Treibers auf mehreren Servern ohne die Verwendung gefilterter Reproduktionen laufen sollen, müssen Sie für die verschiedenen Treiberinstanzen Richtlinien definieren, auf deren Basis der Treiber im selben Identitätsdepot unterschiedliche Objektsätze verarbeiten kann.
- ♦ Die Schablonenobjekte, die vom Treiber bei der Erstellung von Benutzern verwendet werden sollen, sofern die Verwendung von Schablonen ausgewählt ist.
Identity Manager-Treiber erfordern nicht, dass eDirectory-Schablonenobjekte für die Benutzererstellung festgelegt werden. Wenn Sie jedoch festlegen, dass ein Treiber eine Schablone für die Erstellung von Benutzern in eDirectory verwenden soll, muss das Schablonenobjekt auf dem Server repliziert werden, auf dem der Treiber läuft.
- ♦ Alle Container, die der Identity Manager-Treiber zur Benutzerverwaltung verwenden soll.
Wenn Sie beispielsweise einen Container namens „Inaktive Benutzer“ erstellt haben, der deaktivierte Benutzerkonten enthält, benötigen Sie eine Master- oder eine Lese-/Schreibreproduktion (vorzugsweise eine Masterreproduktion) für diesen Container auf dem Server, auf dem der Treiber läuft.
- ♦ Alle anderen Objekte, auf die sich der Treiber beziehen muss (z. B. Auftragsobjekte für den Avaya* PBX-Treiber).
Wenn die anderen Objekte vom Treiber nur gelesen und nicht geändert werden müssen, ist für diese Objekte auf dem Server eine Lesereproduktion ausreichend.

3.3.3 Verwendung der Bereichsfilterung zum Verwalten von Benutzern auf verschiedenen Servern

Mithilfe der Bereichsfilterung können Sie jedem Treiber Regeln hinzufügen, wodurch die Aktionen des Treibers auf bestimmte Container beschränkt werden. Die Bereichsfilterung sollte beispielsweise in den folgenden Situationen verwendet werden:

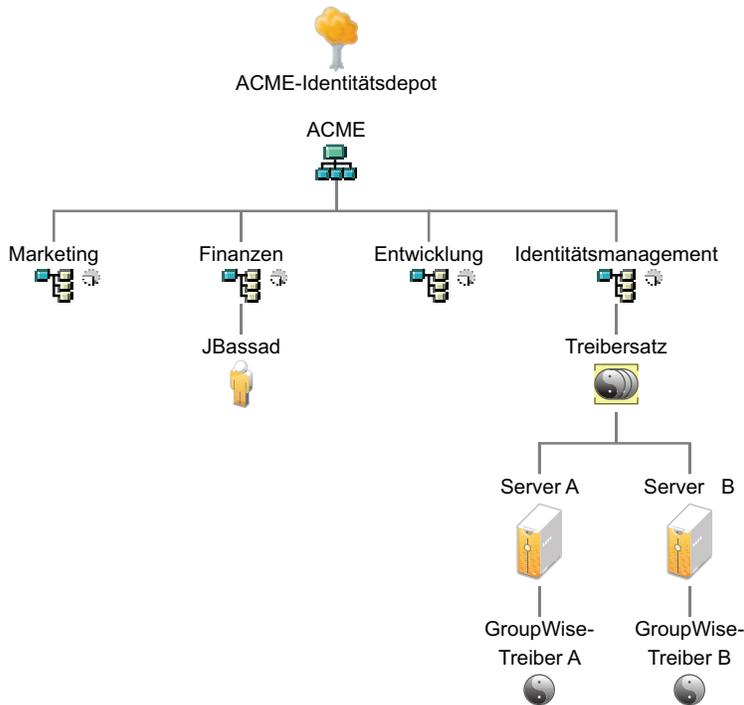
- ♦ Der Treiber soll nur die Benutzer in einem bestimmten Container synchronisieren.
In der Standardeinstellung synchronisiert der Identity Manager-Treiber die Objekte in allen Containern, die auf dem Server repliziert sind, auf denen er läuft. Sie können diesen Bereich einschränken, indem Sie Regeln für die Bereichsfilterung erstellen.
- ♦ Ein Identity Manager-Treiber soll alle Benutzer synchronisieren, aber Sie möchten nicht, dass alle Benutzer auf demselben Server repliziert werden.
Zur Synchronisierung von Benutzern, die nicht auf einem einzelnen Server repliziert sind, müssen Sie die Server festlegen, die alle Benutzer enthalten. Anschließend müssen Sie auf jedem dieser Server eine Instanz des Identity Manager-Treibers erstellen. Damit nicht zwei Instanzen eines Treibers versuchen, dieselben Benutzer zu synchronisieren, müssen Sie in der Bereichsfilterung definieren, welche Benutzer von den einzelnen Instanzen des Treibers synchronisiert werden sollen.

Hinweis: Sie sollten die Bereichsfilterung auch dann verwenden, wenn sich die Reproduktionen der Server gegenwärtig nicht überschneiden. Es könnte sein, dass zu einem späteren Zeitpunkt Reproduktionen auf die Server übertragen werden, sodass eine unbeabsichtigte Überschneidung entsteht. Bei Verwendung der Bereichsfilterung versuchen die Identity Manager-Treiber nicht, dieselben Benutzer zu synchronisieren, selbst wenn zu einem späteren Zeitpunkt Reproduktionen auf die Server übertragen werden.

Im Folgenden finden Sie ein Beispiel für die Verwendung der Bereichsfilterung:

Die folgende Abbildung zeigt ein Identitätsdepot mit drei Containern, in denen folgende Benutzer gespeichert sind: „Marketing“, „Finanzen“ und „Entwicklung“. Sie zeigt auch einen Identitätsmanagement-Container, in dem die Treibersätze gespeichert sind. Jeder dieser Container ist eine separate Partition.

Abbildung 3-4 Beispielbaum für die Bereichsfilterung



In diesem Beispiel verfügt der Identity Manager-Administrator über zwei Identitätsdepot-Server, Server A und Server B (siehe [Abbildung 3-5 auf Seite 35](#)). Keiner der beiden Server enthält eine Kopie aller Benutzer. Jeder Server enthält zwei der drei Partitionen, sodass sich die auf den Servern gespeicherten Bereiche überschneiden.

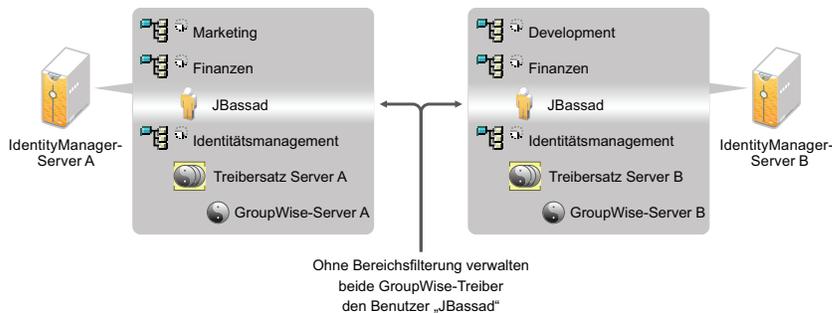
Der Administrator möchte, dass alle Benutzer im Baum vom GroupWise[®]-Treiber synchronisiert werden, aber es sollen keine Reproduktionen der Benutzer auf einem einzelnen Server zusammengefasst werden. Stattdessen verwendet er zwei Instanzen des GroupWise-Treibers, von denen sich eine auf Server A, die andere auf Server B befindet. Er installiert Identity Manager und richtet auf beiden Identity Manager-Servern den GroupWise-Treiber ein.

Server A enthält Reproduktionen der Container „Marketing“ und „Finanzen“. Außerdem befindet sich auf dem Server eine Reproduktion des Identity Management-Containers, der den Treibersatz und das GroupWise-Treiberobjekt für Server A enthält.

Auf Server B befinden sich Reproduktionen der Container „Entwicklung“ und „Finanzen“ sowie der Identity Manager-Container, in dem sich der Treibersatz und das GroupWise-Treiberobjekt für Server B befinden.

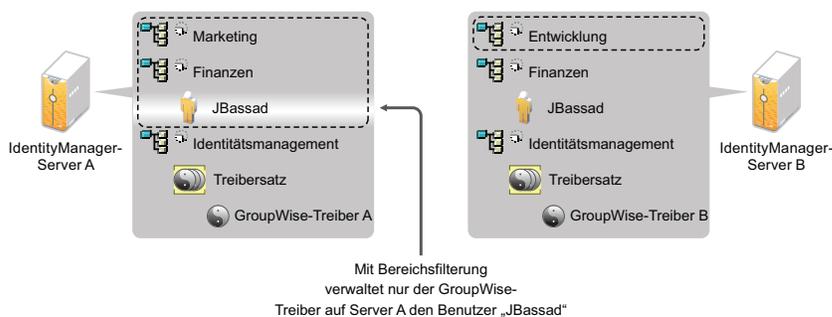
Da sich sowohl auf Server A als auch auf Server B eine Reproduktion des Containers „Finanzen“ befindet, ist auf beiden Servern der Benutzer „JBassad“ gespeichert, der sich im Container „Finanzen“ befindet. Ohne Bereichsfilterung nimmt sowohl GroupWise-Treiber A als auch GroupWise-Treiber B die Synchronisierung von „JBassad“ vor.

Abbildung 3-5 Zwei Server mit sich überschneidenden Reproduktionen, ohne Bereichsfilterung.



Die folgende Abbildung zeigt, dass durch die Bereichsfilterung verhindert wird, dass die zwei Instanzen des Treibers denselben Benutzer verwalten, weil definiert wird, welche Treiber die einzelnen Container synchronisieren.

Abbildung 3-6 Die Bereichsfilterung definiert, welche Treiber die einzelnen Container synchronisieren



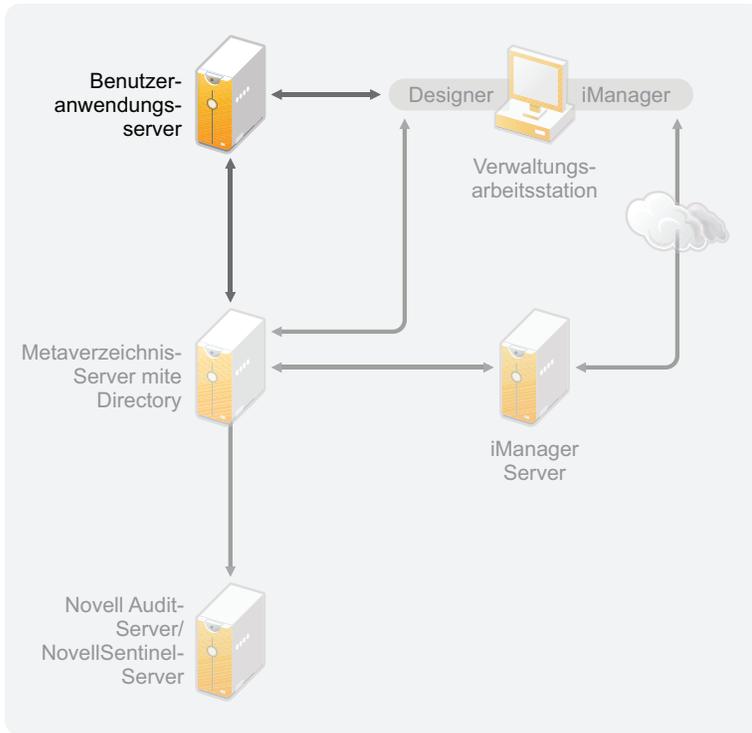
In Identity Manager 3.6.1 sind vordefinierte Regeln enthalten. Zwei dieser Regeln dienen der Bereichsfilterung. Weitere Informationen zu den beiden Regeln „Ereignistransformation - Bereichsfilterung - Teilbäume einbeziehen“ und „Ereignistransformation - Bereichsfilterung - Teilbäume ausschließen“ finden Sie in [Understanding Policies for Identity Manager 3.6](#) (Richtlinien für Identity Manager 3.6).

Für dieses Beispiel sollte die vordefinierte Regel „Teilbäume einbeziehen“ für Server A und Server B verwendet werden. Der Bereich muss für jeden Treiber unterschiedlich definiert sein, sodass sie nur die Benutzer in den angegebenen Containern synchronisieren. Server A würde die Container „Marketing“ und „Finanzen“ synchronisieren und Server B den Container „Entwicklung“.

3.4 Benutzeranwendung

Die Benutzeranwendung sollte auf einem separaten Server ausgeführt werden, wie in [Abbildung 3-7](#) dargestellt. Sie benötigen möglicherweise mehrere Benutzeranwendungs-Server.

Abbildung 3-7 Benutzeranwendung



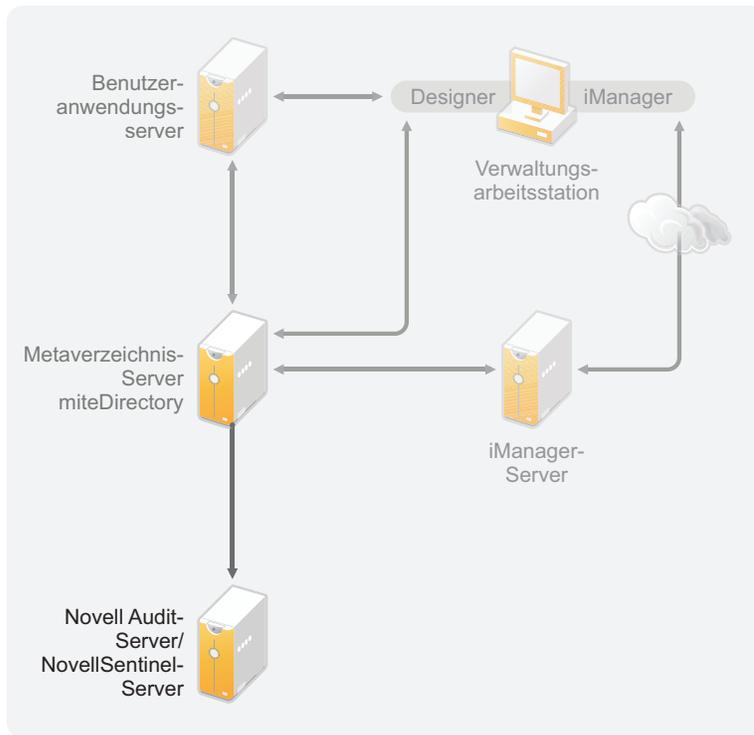
Anhand der Informationen im Abschnitt „Performance Tuning“ (<http://www.novell.com/documentation/idmr361/agpro/data/b2gx735.html>) (Leistungsoptimierung) im *User Application Administration Guide* (Benutzeranwendung: Administrationshandbuch) können Sie ermitteln, wie Sie den Benutzeranwendungs-Server am besten konfigurieren können.

Wenn der Benutzeranwendungs-Server häufig ausgelastet ist, sollten Sie die Verwendung von Clustern in Betracht ziehen. Das Clustering ermöglicht eine hohe Verfügbarkeit, Skalierbarkeit und Lastverteilung. Weitere Informationen finden Sie unter „Clustering“ (<http://www.novell.com/documentation/idmr361/agpro/data/b2gx73a.html>) im *User Application Administration Guide* (Benutzeranwendung: Administrationshandbuch).

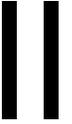
3.5 Revision und Berichterstellung - Richtlinien

Wenn Sie als Teil der Identity Manager-Lösung Revisions- und Berichtsfunktionen benötigen, müssen Sie Identity Audit oder Novell Sentinel™ implementieren. Es wird empfohlen, dass Sie Identity Audit oder Novell Sentinel auf einem separaten Server ausführen, wie in **Abbildung 3-8** dargestellt. Die Anzahl der Server, die für Ihre Lösung erforderlich sind, hängt davon ab, über wie viele Treiber Sie in Ihrer Umgebung verfügen und wie viele Ereignisse Sie für die Revision definiert haben.

Abbildung 3-8 Sentinel



Installation



Die folgenden Abschnitte enthalten die für die Installation eines Identity Manager-Systems erforderlichen Informationen.

- ♦ Kapitel 4, „Basis-Checkliste für das Identity Manager-System“, auf Seite 41
- ♦ Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 45
- ♦ Kapitel 6, „Systemanforderungen“, auf Seite 47
- ♦ Kapitel 7, „Installation von Identity Manager“, auf Seite 57
- ♦ Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 69
- ♦ Kapitel 9, „Fehlerbehebung in Identity Manager“, auf Seite 73

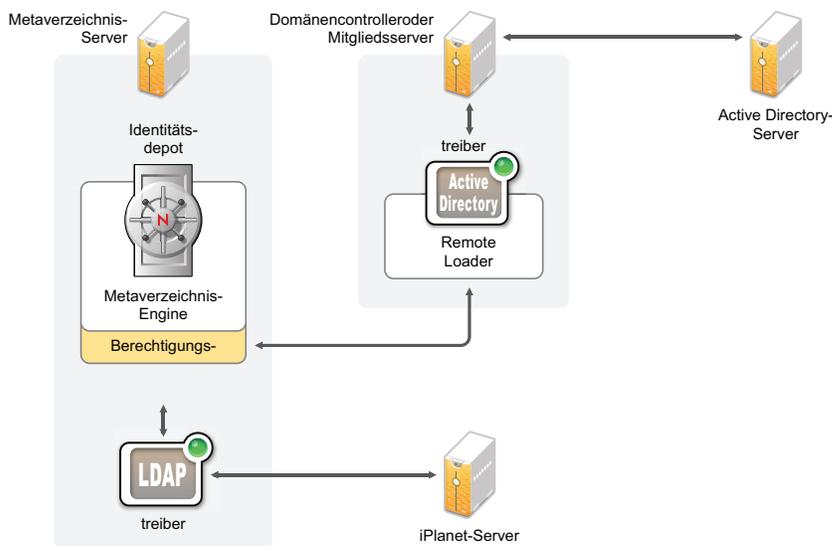
Basis-Checkliste für das Identity Manager-System

4

Es gibt viele unterschiedliche Möglichkeiten, Identity Manager zu konfigurieren und alle Vorteile zu nutzen, die sich aus seinen Funktionen ergeben. **Abbildung 4-1** bietet eine Basiskonfiguration des Identity Manager, der durch die Synchronisierung von Daten Benutzer bereitstellt. Unabhängig von der Identity Manager-Konfiguration beginnen Sie immer mit einem Basissystem.

Anhand dieser Checkliste können Sie Ihr Identity Manager-System konfigurieren und dabei sicherstellen, dass alle Schritte vollständig ausgeführt werden.

Abbildung 4-1 Identity Manager-Basissystem



- ♦ **Abschnitt 4.1**, „Voraussetzungen“, auf Seite 41
- ♦ **Abschnitt 4.2**, „Planung“, auf Seite 42
- ♦ **Abschnitt 4.3**, „Installation“, auf Seite 42
- ♦ **Abschnitt 4.4**, „Treiberkonfiguration mit dem Remote Loader“, auf Seite 43
- ♦ **Abschnitt 4.5**, „Treiberkonfiguration ohne den Remote Loader“, auf Seite 43
- ♦ **Abschnitt 4.6**, „Zusätzliche Konfiguration“, auf Seite 44

4.1 Voraussetzungen

- Installieren Sie Novell® eDirectory™ 8.8.5 oder höher auf dem Server, auf dem Identity Manager ausgeführt werden soll. Stellen Sie sicher, dass NMASTM während der Installation von eDirectory installiert wird. Weitere Informationen hierzu finden Sie auf der [Website zur eDirectory 8.8-Dokumentation \(http://www.novell.com/documentation/edir88/index.html\)](http://www.novell.com/documentation/edir88/index.html).

- ❑ Installieren Sie Novell iManager 2.7.3 auf demselben Server. Weitere Informationen hierzu finden Sie auf der [Website zur iManager-Dokumentation \(http://www.novell.com/documentation/imanager27/index.html\)](http://www.novell.com/documentation/imanager27/index.html).
- ❑ Laden Sie das Identity Manager-Produkt herunter. Anweisungen zum Zugriff auf die Identity Manager-Software finden Sie in **Kapitel 5, „Bezugsquellen für Identity Manager“**, auf Seite 45.
- ❑ Installieren Sie Designer 3.0.1 auf einer Arbeitsstation. Weitere Informationen finden Sie in **Abschnitt 7.1, „Installation von Designer“**, auf Seite 57.

4.2 Planung

Eine sorgfältige Planung ist der Schlüssel für eine erfolgreiche Implementierung und Bereitstellung von Identity Manager.

- ❑ Erstellen Sie eine Entwicklungsumgebung. Es ist wichtig, über Zugriff auf ein Identity Manager-System zu verfügen, damit Sie Ihre Identity Manager-Lösung validieren können. Sie sollten alle Tests und die Entwicklung in der Entwicklungsumgebung durchführen, bevor Sie zur Produktionsumgebung wechseln. Weitere Informationen finden Sie in **Kapitel 1, „Einrichten einer Entwicklungsumgebung“**, auf Seite 13.
- ❑ Erstellen Sie einen Projektplan für die Bereitstellung von Identity Manager. Zu den Aufgaben beim Erstellen eines Projektplans gehören das Definieren der wesentlichen Geschäftsprozesse, das Erstellen einer Identity Manager-Lösung, die diese Prozesse automatisiert, und ein Plan zur technischen Implementierung. Sie benötigen unbedingt einen Projektplan, damit Identity Manager erfolgreich bereitgestellt werden kann. Weitere Informationen finden Sie in **Kapitel 2, „Erstellen eines Projektplans“**, auf Seite 15.

4.3 Installation

- ❑ Installieren Sie den Metaverzeichnis-Server und -Treiber. Weitere Informationen finden Sie in **Kapitel 7, „Installation von Identity Manager“**, auf Seite 57.
- ❑ Aktivieren Sie Identity Manager. Weitere Informationen finden Sie in **Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“**, auf Seite 69.
- ❑ (Optional) Entwerfen und erstellen Sie Berechtigungen für Ihr Identity Manager-System.

Berechtigungen sind definierte Kriterien für eine Person oder Gruppe, die auf mehrere Treiber angewendet werden können. Werden die Kriterien erfüllt, initiieren die Berechtigungen ein Ereignis zum Erteilen oder Entziehen von Zugriffsrechten auf Geschäftsressourcen.

Berechtigungen bieten zusätzliche Steuerungs- und Automatisierungsmöglichkeiten zum Erteilen und Entziehen von Zugriffsrechten auf Ressourcen.

Der wesentliche Vorteil von Berechtigungen besteht darin, dass man Geschäftslogik in den Berechtigungen erstellen bzw. definieren und anschließend diese Logik auf mehrere Treiber verteilen kann. Wenn Sie eine Änderung vornehmen müssen, nehmen Sie diese in der Berechtigung vor und nicht in den einzelnen Treibern.

Berechtigungen werden anhand der folgenden drei Agenten implementiert:

- ◆ Rollenbasierte Berechtigungen mithilfe des Berechtigungsservice-Treibers
- ◆ Workflow
- ◆ Rollenbasiertes Bereitstellungsmodul

Weitere Informationen zu Berechtigungen finden Sie im *Identity Manager 3.6.1 Entitlements Guide* (Handbuch zu Identity Manager 3.6 Berechtigungen).

4.4 Treiberkonfiguration mit dem Remote Loader

Der Remote Loader ermöglicht das Synchronisieren von Informationen zu einem verbundenen System, ohne dass eDirectory auf diesem verbundenen System installiert sein muss. Der Remote Loader synchronisiert die Informationen auf den Metaverzeichnis-Server, der die Daten im Identitätsdepot speichert. Identity Manager verwendet eDirectory als Identitätsdepot.

- ❑ Installieren Sie den Remote Loader auf einem Computer, der mit dem verbundenen System kommuniziert. Der Remote Loader kommuniziert zwischen dem verbundenen System und der Metaverzeichnis-Engine. Er ermöglicht die Kommunikation von Identity Manager mit einem Computer, auf dem eDirectory nicht installiert ist. Weitere Informationen hierzu finden Sie unter „**Installing the Remote Loader**“ (Installation des Remote Loader) im *Identity Manager 3.6.1 Remote Loader Guide* (Handbuch zu Identity Manager 3.6 Remote Loader).
- ❑ Konfigurieren Sie den Remote Loader für einen Treiber. Sie definieren eine bestimmte Instanz von Remote Loader für die Kommunikation mit einem bestimmten Treiber. Weitere Informationen hierzu finden Sie unter „**Configuring the Remote Loader**“ (Konfigurieren des Remote Loader) im *Identity Manager 3.6.1 Remote Loader Guide* (Handbuch zu Identity Manager 3.6 Remote Loader).
- ❑ Konfigurieren Sie den Treiber für die Kommunikation mit dem Remote Loader. Für jeden Treiber steht ein Treiberhandbuch zur Verfügung. Spezielle Informationen zu Ihrem Treiber finden Sie auf der [Website zur Identity Manager 3.6.1 Treiber-Dokumentation \(http://www.novell.com/documentation/idm36drivers/\)](http://www.novell.com/documentation/idm36drivers/).
- ❑ (Optional) Aktivieren Sie die Berechtigungen auf dem Treiber. Vergewissern Sie sich, dass die korrekten Richtlinien zum Ausführen der Berechtigung aktiv sind. Weitere Informationen finden Sie im *Identity Manager 3.6.1 Entitlements Guide* (Handbuch zu Identity Manager 3.6 Berechtigungen).
- ❑ Wiederholen Sie diese Schritte für jeden Treiber in Ihrer Umgebung.

4.5 Treiberkonfiguration ohne den Remote Loader

- ❑ Erstellen und konfigurieren Sie Ihren Treiber. Für jeden Treiber steht ein Treiberhandbuch zur Verfügung. Spezielle Informationen zu Ihrem Treiber finden Sie auf der [Website zur Identity Manager 3.6.1 Treiber-Dokumentation \(http://www.novell.com/documentation/idm36drivers/\)](http://www.novell.com/documentation/idm36drivers/).
- ❑ (Optional) Aktivieren Sie die Berechtigungen auf dem Treiber. Vergewissern Sie sich, dass die korrekten Richtlinien zum Ausführen der Berechtigung aktiv sind. Weitere Informationen finden Sie im *Identity Manager 3.6.1 Entitlements Guide* (Handbuch zu Identity Manager 3.6 Berechtigungen).
- ❑ Wiederholen Sie diese Schritte für jeden Treiber in Ihrer Umgebung.

4.6 Zusätzliche Konfiguration

Wenn das Identity Manager-Basissystem installiert und konfiguriert ist, können Sie die folgenden zusätzlichen Konfigurationsaufgaben durchführen:

- ❑ **Passwortverwaltung:** Wenn Sie mit Identity Manager Passwörter verwalten möchten, müssen Sie zusätzliche Konfigurationen vornehmen. Verwenden Sie die „[Checkliste für die Passwortverwaltung](#)“ im *Identity Manager 3.6.1 Password Management Guide* (Handbuch zur Identity Manager 3.6-Passwortverwaltung), um zu überprüfen, ob alle Konfigurationsschritte vollständig ausgeführt wurden.
- ❑ **Rollenbasierte Bereitstellung:** Wenn Sie im Rahmen Ihrer Identity Manager-Lösung die rollenbasierte Bereitstellung verwenden möchten, überprüfen Sie anhand der Checkliste im *User Application Installation Guide* (<http://www.novell.com/documentation/idmrpbpm361/install/data/bookinfo.html>) (Installationshandbuch zur Benutzeranwendung), ob alle Konfigurationsschritte vollständig ausgeführt wurden.
- ❑ **Revision und Berichterstellung:** Die Verwendung der Revisions- und Berichterstellungsfunktionen in Ihrer Identity Manager-Lösung sind ein Mittel, mit dem Sie zeigen können, dass Ihre Geschäftsrichtlinien mit den Firmenrichtlinien übereinstimmen. Für Revisionen und Berichterstellung können Sie Identity Audit oder Novell Sentinel in Ihre Identity Manager-Lösung integrieren. Weitere Informationen zu Identity Audit finden Sie im *Identity Manager 3.6.1 Integration Guide for Identity Audit* (Identity Manager 3.6 Integrationshandbuch für Identity Audit). Weitere Informationen zu Novell Sentinel finden Sie im *Identity Manager 3.6.1 Reporting Guide for Novell Sentinel* (Identity Manager 3.6 Berichtshandbuch für Novell Sentinel).

Bezugsquellen für Identity Manager

5

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 neben der gewünschten Datei in der Spalte „Download“ auf die Dateigröße.
- 4 Befolgen Sie die Bildschirmanweisungen, um die Datei in einen Ordner auf Ihrem Computer herunterzuladen.
- 5 Wiederholen Sie diesen Vorgang ab Schritt 2, bis Sie alle erforderlichen Dateien heruntergeladen haben. Für die meisten Installationen sind mehrere ISO-Images erforderlich.

Tabelle 5-1 Funktionsweise der ISO-Images

Identity Manager-Komponenten	Plattformen	ISO
Identity Manager-DVD	Identity Manager: Linux, Windows* und UNIX Designer: Linux und Windows	Identity_Manager_3_6_1_DVD.iso
Identity Manager und Treiber-CD	Windows	Identity_Manager_3_6_1_Win.iso
Identity Manager und Treiber-CD	Linux	Identity_Manager_3_6_1_Linux.iso
Identity Manager und Treiber-CD	Solaris	Identity_Manager_3_6_1_Solaris.iso
Identity Manager und -Treiber	AIX	Identity_Manager_3_6_1_AIX.iso
Designer für Identity Manager-CD	Windows	Identity_Manager_3_6_1_Designer_Win.iso
Designer für Identity Manager-CD	Linux	Identity_Manager_3_6_1_Designer_Linux.iso
Benutzeranwendung		Informationen hierzu finden Sie im User Application Installation Guide (http://www.novell.com/documentation/idmrpbm361/index.html) (Installationshandbuch zur Benutzeranwendung).

Mit Identity Manager haben Sie Integrationsmodule für mehrere häufig verwendete Systeme erworben, für die Ihnen möglicherweise bereits Lizenzen vorliegen: Novell® eDirectory™, Microsoft* Active Directory, LDAP v3-Verzeichnisse, Novell GroupWise® und Lotus* Notes* . Alle anderen Identity Manager-Integrationsmodule sind separat erhältlich.

Das ISO-Image der Benutzeranwendung besteht aus der Standardversion, die in Identity Manager 3.6.1 enthalten ist. Das rollenbasierte Bereitstellungsmodul der Benutzeranwendung ist ein Zusatzprodukt mit einem leistungsstarken funktionsbasierten Genehmigungs-Workflow zum Verwalten der Benutzeridentitäten. Das rollenbasierte Bereitstellungsmodul befindet sich auf einem separaten ISO-Image und ist separat erhältlich. Weitere Informationen finden Sie im *User Application Installation Guide* (<http://www.novell.com/documentation/idmrbpm361/index.html>) (Installationshandbuch zur Benutzeranwendung).

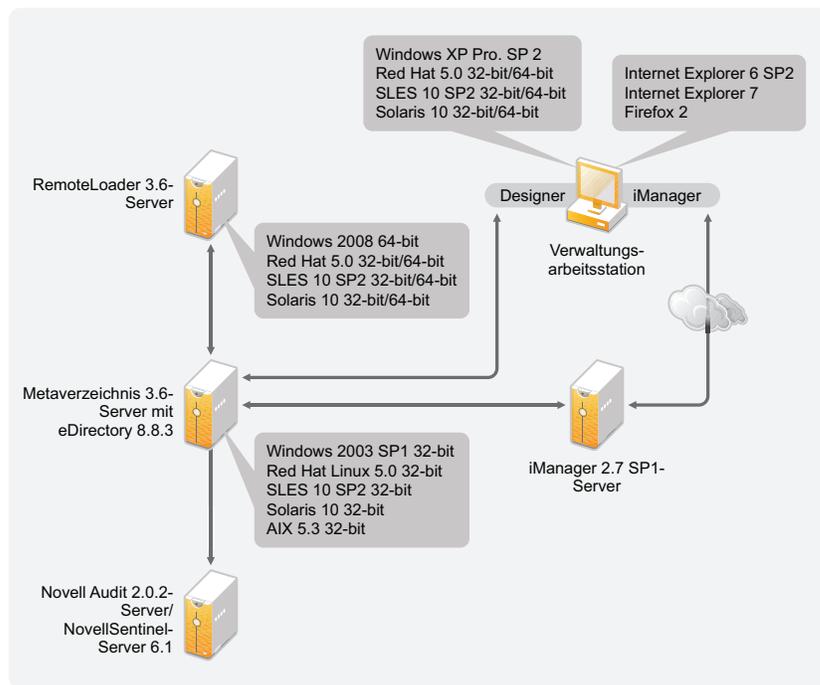
Beim Kauf von Identity Manager erhalten Sie auch Designer für Identity Manager. Designer ist ein leistungsfähiges, flexibles Verwaltungswerkzeug, das die Konfiguration und die Bereitstellung erheblich vereinfacht.

Systemanforderungen

6

Die Komponenten von Novell® Identity Manager können auf mehreren Systemen und Plattformen installiert werden. **Abbildung 6-1** zeigt, welche Plattformen und Systeme unterstützt werden.

Abbildung 6-1 Systemanforderungen für die Identity Manager-Komponenten



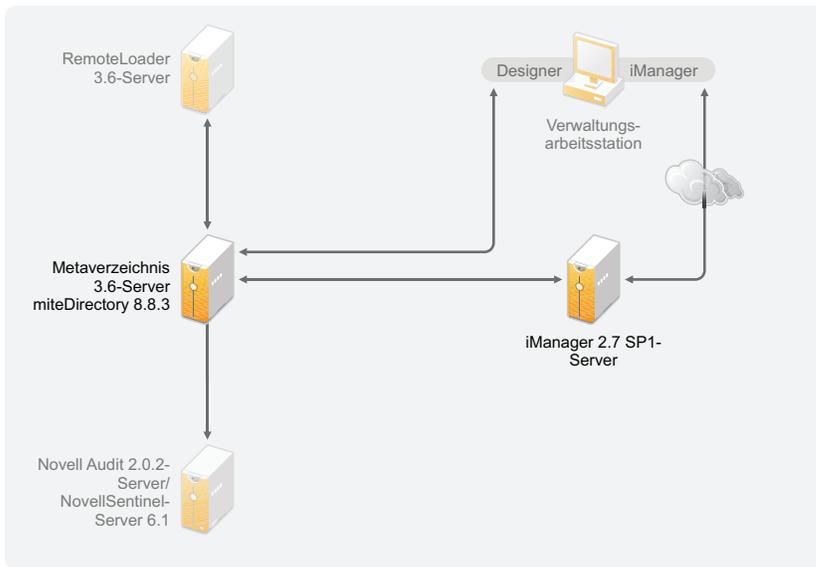
Je nach Systemkonfiguration müssen Sie das Identity Manager-Installationsprogramm möglicherweise mehrmals ausführen, um die Komponenten von Identity Manager auf den entsprechenden Systemen zu installieren.

- ♦ **Abschnitt 6.1, „eDirectory und iManager“, auf Seite 47**
- ♦ **Abschnitt 6.2, „Metaverzeichnis-Server“, auf Seite 48**
- ♦ **Abschnitt 6.3, „Remote Loader“, auf Seite 51**
- ♦ **Abschnitt 6.4, „Benutzeranwendung“, auf Seite 52**
- ♦ **Abschnitt 6.5, „Revision und Berichterstellung“, auf Seite 52**
- ♦ **Abschnitt 6.6, „Arbeitsstationen“, auf Seite 53**

6.1 eDirectory und iManager

Für Identity Manager wird vorausgesetzt, dass eDirectory™ und iManager installiert sind. Auf diesen Produkten basiert Identity Manager. **Abbildung 6-2** veranschaulicht diese Komponenten.

Abbildung 6-2 Basisprodukte für Identity Manager



Die folgende Liste enthält die erforderlichen Versionen dieser Produkte:

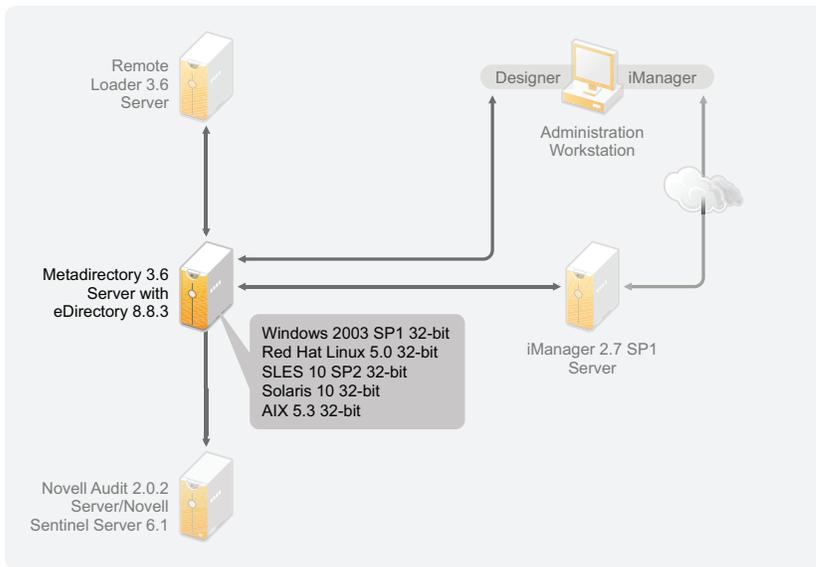
- ♦ eDirectory 8.8.5 oder höher (32- oder 64-Bit)
- ♦ iManager 2.7.3

Informationen zu den Systemanforderungen für eDirectory finden Sie im *Novell eDirectory 8.8 SP5 Installation Guide* (<http://www.novell.com/documentation/edir88/index.html>) (Installationshandbuch zu Novell eDirectory 8.8 SP3). Informationen zu den Systemanforderungen für iManager finden Sie im *iManager 2.7-Installationshandbuch* (<http://www.novell.com/documentation/imanager27/index.html>).

6.2 Metaverzeichnis-Server

Der Metaverzeichnis-Server verarbeitet die Treiberereignisse - und zwar unabhängig davon, ob sie mit dem Remote Loader konfiguriert wurden oder nicht. Eine Liste der unterstützten Betriebssysteme finden Sie in [Abbildung 6-3](#).

Abbildung 6-3 Unterstützte Betriebssysteme für den Metaverzeichnis-Server



Während der Installation des Metaverzeichnis-Servers erkennt das Installationsprogramm, welche eDirectory-Version installiert ist.

Hinweis: Auf dem Computer muss eDirectory 8.8.5 oder höher (32- oder 64-Bit) installiert sein. Ist dies nicht der Fall, wird die Installation abgebrochen.

- ♦ [Abschnitt 6.2.1, „Unterstützte Prozessoren“, auf Seite 49](#)
- ♦ [Abschnitt 6.2.2, „Server-Betriebssysteme“, auf Seite 50](#)

6.2.1 Unterstützte Prozessoren

Die hier aufgelisteten Prozessoren werden zum Testen von Identity Manager verwendet. Der SPARC^{*}-Prozessor wird für Solaris^{*}-Tests verwendet.

Folgende 32-Bit-Prozessoren werden für Linux- (Red Hat^{*} und SUSE[®] Linux Enterprise Server) und Windows-Betriebssysteme unterstützt:

- ♦ Intel^{*} x86-32
- ♦ AMD^{*} x86-32

Folgende 64-Bit-Prozessoren werden für Linux- (Red Hat und SUSE Linux Enterprise Server) und Windows-Betriebssysteme unterstützt:

- ♦ Intel EM64T
- ♦ AMD Athlon64
- ♦ AMD Opteron^{*}

6.2.2 Server-Betriebssysteme

Sie können die Metaverzeichnis-Engine als 32-Bit-Anwendung auf einem 64-Bit-Betriebssystem installieren. **Tabelle 6-1** enthält eine Liste der unterstützten Server-Betriebssysteme, auf denen der Metaverzeichnis-Server ausgeführt werden kann.

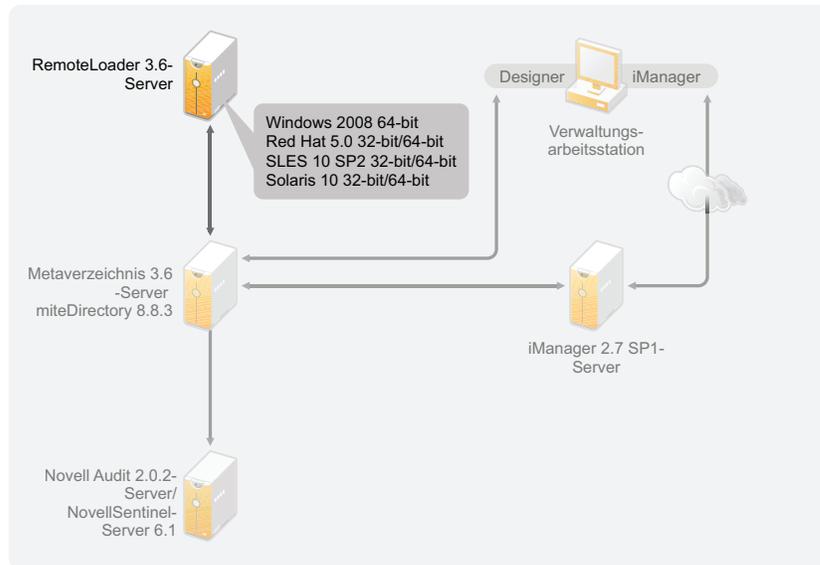
Tabelle 6-1 *Unterstützte Serverbetriebssysteme*

Version des Server-Betriebssystems	Hinweise
Windows Server* 2003 SP2 (32-Bit)	Der Metaverzeichnis-Server läuft nur im 32-Bit-Modus.
Windows Server 2008 (32- und 64-Bit)	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus.
Red Hat 5.0 oder höher (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 10 SP1 oder höher (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 (32- und 64-Bit)	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus.
Solaris Zones (32- und 64-Bit)	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus.
AIX* 5L v5.3 (64-Bit)	Der Metaverzeichnis-Server läuft nur im 32-Bit-Modus.
Xen*	Xen wird unterstützt, wenn die Xen Virtual Machine als Gastbetriebssystem entweder SLES 10, OES 2 oder OES 2 SP1 im paravirtualisierten Modus ausführt.
VMware*	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus.
Open Enterprise Server 2 SP1 (32- und 64-Bit)	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus.

6.3 Remote Loader

Der Remote Loader gibt Ihnen mehr Flexibilität bei der Konfiguration Ihrer Identity Manager-Lösung. Er bietet 32- sowie 64-Bit-Unterstützung. Standardmäßig erkennt das Installationsprogramm die Betriebssystemversion und installiert anschließend die entsprechende Version des Remote Loaders. Informationen zur Installation des Remote Loaders als 32-Bit-Anwendung auf einem 64-Bit-Betriebssystem finden Sie unter „[Installation des Remote Loaders als 32-Bit-Anwendung auf einem 64-Bit-Betriebssystem](#)“ auf Seite 64. In [Abbildung 6-4](#) werden die unterstützten Betriebssysteme für den Remote Loader aufgelistet.

Abbildung 6-4 Unterstützte Betriebssysteme für den Remote Loader



Wenn Sie die Metaverzeichnis-Engine als 32-Bit-Anwendung auf einem 64-Bit-Betriebssystem installiert haben, können Sie den 64-Bit-Remote Loader nicht auf demselben Computer installieren. Die Bibliotheken für die 32-Bit-Metaverzeichnis-Engine und den 64-Bit-Remote Loader haben dieselben Namen. Wenn sie auf demselben Computer installiert sind, verursacht dies Konflikte.

In [Tabelle 6-2](#) werden die unterstützten Betriebssysteme für den Remote Loader aufgelistet.

Tabelle 6-2 Unterstützte Betriebssysteme für den Remote Loader

Version des Server-Betriebssystems	Hinweise
Windows Server* 2003 SP2 (32- und 64-Bit)	Der Remote Loader läuft entweder im 32-Bit- oder im 64-Bit-Modus.
Windows Server 2008 (32- und 64-Bit)	Der Remote Loader läuft entweder im 32-Bit- oder im 64-Bit-Modus.
Windows Server 2008 Server Core (32- und 64-Bit)	Der Remote Loader läuft entweder im 32-Bit- oder im 64-Bit-Modus.

Version des Server-Betriebssystems	Hinweise
Red Hat 5.0 oder höher (32- und 64-Bit)	Der Remote Loader 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 10 SP1 oder höher (32- und 64-Bit)	Der Remote Loader 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 Remote Loader 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 (32- und 64-Bit)	Der Remote Loader läuft entweder im 32-Bit- oder im 64-Bit-Modus.
Solaris Zones (32- und 64-Bit)	Der Remote Loader läuft entweder im 32-Bit- oder im 64-Bit-Modus.
AIX* 5L v5.3 (64-Bit)	Der Remote Loader läuft nur im 32-Bit-Modus. Der 64-Bit-Remote Loader wird nicht unterstützt.
Open Enterprise Server 2 SP1 (32- und 64-Bit)	Der Remote Loader läuft entweder im 32-Bit- oder im 64-Bit-Modus.

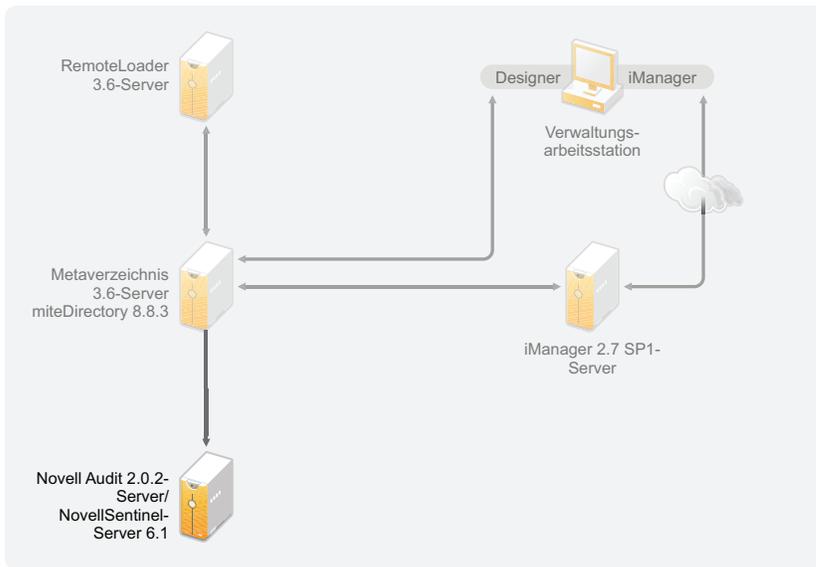
6.4 Benutzeranwendung

Im *User Application Installation Guide* (<http://www.novell.com/documentation/idmrpbm361/index.html>) (Installationshandbuch zur Benutzeranwendung) finden Sie eine Liste der Systemanforderungen für die Benutzeranwendung.

6.5 Revision und Berichterstellung

Identity Audit und Novell Sentinel™ sind zwei unterschiedliche Werkzeuge, die zum Sammeln von Revisions- und Berichtsdaten über Identity Manager verwendet werden. In **Abbildung 6-5** werden die Sentinel-Versionen aufgeführt, die von Identity Manager 3.6.1 unterstützt werden.

Abbildung 6-5 Sentinel



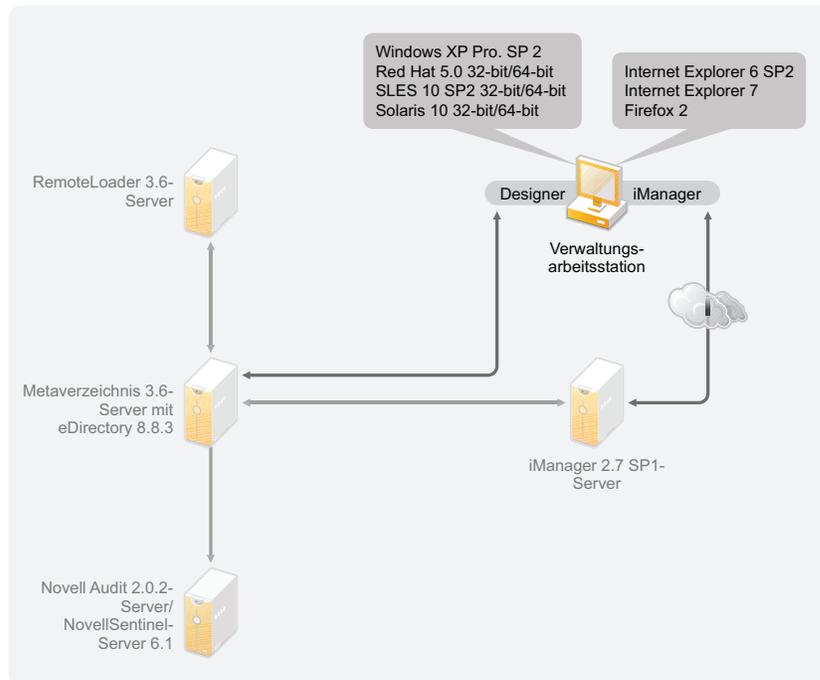
Dies ist eine optionale Erweiterung für die Identity Manager-Lösung. Durch die Erweiterung um die Funktionen für die Revision und die Berichterstellung können Sie die Konformitätsstandards erfüllen, die von vielen Unternehmen eingehalten werden müssen. Die Software erstellt Revisionsprotokolle für alle zu protokollierenden Ereignisse und kann Berichte erzeugen, um sicherzustellen, dass Sie alle für Ihr Unternehmen geltenden Revisionsstandards erfüllen.

Informationen zur Konfiguration von Identity Audit mit Identity Manager finden Sie im *Identity Manager 3.6.1-Integrationshandbuch für Identity Audit*. Informationen zur Konfiguration von Novell Sentinel mit Identity Manager finden Sie im *Identity Manager 3.6.1 Reporting Guide for Novell Sentinel* (Identity Manager 3.6-Berichtshandbuch für Novell Sentinel). Informationen zu den Systemanforderungen für Identity Audit finden Sie im Handbuch zu *Identity Audit* (<http://www.novell.com/documentation/identityaudit/index.html>). Informationen zu den Systemanforderungen für Novell Sentinel finden Sie im *Novell Sentinel Installationshandbuch* (<http://www.novell.com/documentation/sentinel6/index.html>).

6.6 Arbeitsstationen

Die Arbeitsstationen werden für Designer, iManager oder die webbasierte Verwaltungsseite der Benutzeranwendung verwendet. In **Abbildung 6-6** werden die unterschiedlichen Komponenten für Arbeitsstationen aufgelistet, die von Identity Manager 3.6.1 unterstützt werden.

Abbildung 6-6 Unterstützte Komponenten für Arbeitsstationen



Es gibt drei unterschiedliche Elemente, die Arbeitsstationen betreffen:

- ◆ [Abschnitt 6.6.1, „Arbeitsstationsplattformen“, auf Seite 54](#)
- ◆ [Abschnitt 6.6.2, „iManager und Webbrowser“, auf Seite 55](#)

6.6.1 Arbeitsstationsplattformen

Tabelle 6-3 enthält eine Liste der unterstützten Arbeitsstationsplattformen für Designer und iManager.

Tabelle 6-3 Unterstützte Arbeitsstationsplattformen

Plattformen	Details
Windows Vista*	Die Ultimate Edition und die Business Edition werden unterstützt.
Windows XP Professional SP2	
openSUSE® 10.3	Wenden Sie die neuesten Patches über die automatische Aktualisierungsfunktion an.
SUSE Linux Enterprise Desktop 10 SP1/SP2	Wenden Sie die neuesten Patches über die automatische Aktualisierungsfunktion an.
SUSE Linux Enterprise Server 10 SP1/SP2	Wenden Sie die neuesten Patches über die automatische Aktualisierungsfunktion an.

6.6.2 iManager und Webbrowser

Identity Manager 3.6.1 unterstützt die iManager-Version 2.7.3. Mit dieser Version können alle Plugins ausgeführt werden, die zur Konfiguration und Verwaltung von Identity Manager benötigt werden.

Zur Verwaltung von Identity Manager werden die folgenden Webbrowser unterstützt:

- ◆ Internet Explorer* 6 mit SP2
- ◆ Internet Explorer 7
- ◆ Firefox* 2

Installation von Identity Manager

7

Identity Manager verfügt über separate Installationsvorgänge für die unterschiedlichen Komponenten. Es ist wichtig, in der Planungsphase der Identity Manager-Implementierung Designer zu installieren und zu verwenden. Weitere Informationen finden Sie in [Kapitel 2, „Erstellen eines Projektplans“](#), auf Seite 15.

Als Nächstes können Sie den Metaverzeichnis-Server und den Remote Loader in beliebiger Reihenfolge installieren. Die verbleibenden Komponenten müssen in der genannten Reihenfolge installiert werden. Eine Erklärung der verschiedenen Komponenten finden Sie im Handbuch [Überblick über Identity Manager 3.6.1](#).

- ♦ [Abschnitt 7.1, „Installation von Designer“](#), auf Seite 57
- ♦ [Abschnitt 7.2, „Installation des Metaverzeichnis-Servers“](#), auf Seite 58
- ♦ [Abschnitt 7.3, „Installation des Remote Loaders“](#), auf Seite 61
- ♦ [Abschnitt 7.4, „Installation des rollenbasierten Bereitstellungsmoduls“](#), auf Seite 67
- ♦ [Abschnitt 7.5, „Installation eines benutzerdefinierten Treibers“](#), auf Seite 67
- ♦ [Abschnitt 7.6, „Installation von Identity Audit oder Sentinel“](#), auf Seite 67
- ♦ [Abschnitt 7.7, „Installation von Identity Manager in der Cluster-Umgebung“](#), auf Seite 67

7.1 Installation von Designer

Designer 3.0.1 ist ein Werkzeug für Arbeitsstationen, mit dem Sie Ihre Identity Manager-Lösung entwerfen können. Installieren Sie zunächst Designer und verwenden Sie ihn bei der Planung der Identity Manager-Implementierung. Weitere Informationen zur Planung finden Sie in [Teil I, „Planung“](#), auf Seite 11.

- 1 Stellen Sie sicher, dass das Betriebssystem Ihrer Arbeitsstation unterstützt wird. Weitere Informationen finden Sie in [Abschnitt 6.6, „Arbeitsstationen“](#), auf Seite 53.
- 2 Starten Sie die Installation, indem Sie das entsprechende Programm für die Plattform Ihrer Arbeitsstation ausführen.
 - ♦ **Windows:** IDM3.6.1_Designer_Win:/windows/designer/install.exe
 - ♦ **Linux:** IDM3.6.1_Designer_Linux:/linux/designer/installFühren Sie die Binärdatei aus, indem Sie `eingeben./install`.
- 3 Mithilfe der folgenden Informationen wird die Installation ausgeführt:
 - ♦ **Installationsordner:** Geben Sie einen Speicherort auf der Arbeitsstation an, in dem Designer installiert ist.
 - ♦ **Verknüpfungen erstellen:** Wählen Sie aus, ob auf Ihrem Desktop und/oder in Ihrem Desktop-Menü eine Verknüpfung erstellt werden soll.
- 4 Weitere Informationen hierzu finden Sie im [Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6](#).

7.2 Installation des Metaverzeichnis-Servers

Auf Linux\UNIX-Plattformen können Sie den Metaverzeichnis-Server als `root`- oder Nicht-root-Benutzer installieren. Die Installation von Identity Manager als Nicht-root-Benutzer erhöht die Sicherheit auf dem Server. eDirectory muss von einem Nicht-root-Benutzer installiert werden, damit die Nicht-root-Installation funktioniert. Bei einer Nicht-root-Installation verläuft der Installationsvorgang anders. Die Vorgehensweise für diese Art der Installation wird in [Abschnitt 7.2.1, „Nicht-root-Installation des Metaverzeichnis-Servers“](#), auf Seite 59 beschrieben.

Die folgende Vorgehensweise beinhaltet die Installation des Metaverzeichnis-Servers, der Webkomponenten und der Dienstprogramme für die von Identity Manager unterstützten Plattformen.

- 1 Stellen Sie sicher, dass Ihr System den in [Kapitel 6, „Systemanforderungen“](#), auf Seite 47 aufgeführten Systemanforderungen entspricht.
- 2 (Nur Linux\UNIX) Wenn Sie sicherstellen möchten, dass die Umgebungsvariablen für eDirectory exportiert werden, bevor die Installation unter Linux/UNIX gestartet wird, geben Sie an der Eingabeaufforderung folgenden Befehl ein:

```
set | grep PATH
```

Die Umgebungsvariablen legen den Pfad für die Installation von eDirectory fest. Wenn die Umgebungsvariablen festgelegt sind, wird der eDirectory-Installationspfad aufgeführt. Wenn keine Umgebungsvariablen festgelegt sind, tritt bei der Installation von Identity Manager ein Fehler auf.

Geben Sie folgenden Befehl ein, um die Umgebungsvariablen für Ihre aktuelle Shell festzulegen:

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

Achten Sie auf das Leerzeichen zwischen dem Punkt (.) und dem Schrägstrich (/), damit der Befehl funktioniert. Weitere Informationen hierzu finden Sie unter [„Using the nds-install Utility to Install eDirectory Components“](#) (<http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#ai39feq>) (Installation von eDirectory-Komponenten mithilfe des nds-install-Dienstprogramms).

- 3 Starten Sie die Installation, indem Sie das entsprechende Programm für Ihre Plattform ausführen.
 - ♦ **Windows:** `IDM3.6.1_Win:windows\setup\idm_install.exe`
 - ♦ **Linux - GUI-Installation:** `IDM3_6_1_Lin/install.bin [-i gui]`
 - ♦ **Linux - Installation über die Befehlszeile:** `IDM3_6_1_Lin/install.bin -i console`
 - ♦ **Solaris - GUI-Installation:** `IDM3_6_1_Solaris/install.bin [-i gui]`
 - ♦ **Solaris - Installation über die Befehlszeile:** `IDM3_6_1_Solaris/install.bin -i console`
 - ♦ **AIX - GUI-Installation:** `IDM3_6_1_AIX/install.bin [-i gui]`
 - ♦ **AIX - Installation über die Befehlszeile:** `IDM3_6_1_AIX/install.bin -i console`

Geben Sie ein, um die Binärdateien unter Linux\Solaris\AIX auszuführen./
`install.bin [-i {gui | console}]`.

4 Mithilfe der folgenden Informationen wird die Installation ausgeführt:

- ♦ **Komponenten auswählen:** Wählen Sie den Metaverzeichnis-Server, iManager-Plugins und Dienstprogramme für die Installation des Metaverzeichnis-Servers aus.
 - ♦ **Novell Identity Manager Metadirectory Server:** Diese Option setzt voraus, dass das Identitätsdepot auf diesem Server installiert ist. Sie erweitert das Identity Manager-Schema und installiert die Metaverzeichnis-Engine, die Identity Manager-Treiber und den Novell® Audit Agent.
 - ♦ **Novell Identity Manager - Server für verbundene Systeme:** Diese Option setzt nicht voraus, dass das Identitätsdepot auf diesem Server installiert ist. Wählen Sie diese Option nur, wenn Sie den Remote Loader installieren. Weitere Informationen finden Sie in [Abschnitt 7.3, „Installation des Remote Loaders“](#), auf Seite 61.
 - ♦ **None:** Wählen Sie diese Option, wenn Sie die iManager-Plugins oder die Dienstprogramme installieren möchten, ohne den Metaverzeichnis-Server oder den Server des verbundenen Systems auf diesem Server zu installieren.
 - ♦ **Novell Identity Manager - Webbasierter Administrationsserver:** Wählen Sie diese Option, wenn iManager auf diesem Server installiert ist. Mit dieser Option werden die iManager-Plugins für Identity Manager installiert.
 - ♦ **Dienstprogramme:** Mit dieser Option werden Dienstprogramme installiert, die Sie bei der Konfiguration der Treiber für die verbundenen Systeme unterstützen. Nicht für alle Treiber sind Dienstprogramme verfügbar. Wenn Sie nicht sicher sind, ob Sie diese Funktion installieren möchten, sollten Sie sie auswählen, da sie nur wenig Festplattenspeicher benötigt.
 - ♦ **Ausgewählte Komponenten anpassen:** Mit dieser Option können Sie die Komponenten anpassen, die Sie für die Installation ausgewählt haben. Bevor Sie diese Option wählen, müssen Sie zunächst die zu installierenden Komponenten auswählen.
 - ♦ **Authentifizierung:** Geben Sie einen Benutzer und das zugehörige Passwort an, der über genügend Berechtigungen zum Erweitern des Schemas in eDirectory verfügt. Geben Sie den Benutzernamen im LDAP-Format an. Beispiel: cn=IDM-Admin,o=Firma.
- 5 Aktivieren Sie Identity Manager. Weitere Informationen finden Sie in [Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“](#), auf Seite 69.
- 6 Erstellen und konfigurieren Sie Ihre Treiberobjekte. Diese Informationen sind in jedem Treiberhandbuch enthalten. Weitere Informationen hierzu finden Sie in der [Identity Manager-Treiberdokumentation \(http://www.novell.com/documentation/idm36drivers/\)](http://www.novell.com/documentation/idm36drivers/).

7.2.1 Nicht-root-Installation des Metaverzeichnis-Servers

Die Installation von Identity Manager als Nicht-root-Benutzer erhöht die Sicherheit des UNIX/Linux-Servers. Identity Manager kann nicht als Nicht-root-Benutzer installiert werden, falls eDirectory von einem root-Benutzer installiert wurde.

Bei der Nicht-root-Installation werden die folgenden Komponenten nicht installiert:

- ♦ **Remote Loader:** Wenn Sie den Remote Loader als Nicht-root-Benutzer installieren müssen, verwenden Sie den Java Remote Loader. Weitere Informationen finden Sie in [Abschnitt 7.3.5, „Installation des Java Remote Loader unter UNIX, Linux oder AIX“](#), auf Seite 66.
- ♦ **UNIX/Linux-Kontentreiber:** Erfordert root-Berechtigungen.

- ♦ **Novell Sentinel-Plattformagent:** Installieren Sie den Novell Sentinel-Plattformagenten als root-Benutzer. Erstellen Sie die Datei `Dirxml.properties` im Verzeichnis `/etc/opt/novell/sentinelpa/conf`. Nicht-root-Benutzer müssen Schreibzugriff auf das Verzeichnis haben, in dem das Ereignisprotokoll generiert wird (das Standardverzeichnis ist `/var/opt/novell/sentinelpa/data/AuditEvents.log`).

Gehen Sie wie folgt vor, um den Metaverzeichnis-Server als Nicht-root-Version zu installieren:

- 1 Installieren Sie eDirectory 8.8.5 oder höher als Nicht-root-Benutzer. Weitere Informationen hierzu finden Sie unter „Nonroot User Installing eDirectory 8.8“ (<http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#bs6a3gs>) (Installation von eDirectory 8.8 durch einen Nicht-root-Benutzer).
- 2 Melden Sie sich mit den Anmeldedaten an, die für die Nicht-root-Installation von eDirectory verwendet wurden.

Identity Manager muss vom selben Benutzer installiert werden, der auch die Nicht-root-Installation von eDirectory ausgeführt hat. Der Benutzer, der Identity Manager installiert, muss über Schreibzugriff für die Verzeichnisse und Dateien der Nicht-root-Installation von eDirectory verfügen.

- 3 Führen Sie das Installationsprogramm für Ihre Plattform aus.

- ♦ **Linux:** `IDM3.6.1_Lin/linux/setup/idm-nonroot-install`
- ♦ **AIX:** `IDM3.6.1_Unix/aix/setup/idm-nonroot-install`

Wichtig: Nur das AIX-Maintenance-Level 5300-09 wird unterstützt. Neuere oder ältere Maintenance-Levels werden nicht unterstützt.

- ♦ **Solaris:** `IDM3.6.1_solaris/setup/idm-nonroot-install`

Führen Sie die Skriptdateien aus, indem Sie `eingeben./idm-nonroot-install`

- 4 Mithilfe der folgenden Informationen wird die Installation ausgeführt:

- ♦ **Basisverzeichnis für die Nicht-root-Installation von eDirectory:** Geben Sie das Verzeichnis an, in dem die Nicht-root-Version von eDirectory installiert ist. Beispiel: `/home/user/install/eDirectory`.
- ♦ **NDS-Schema erweitern:** Wenn dies der erste Identity Manager-Server ist, der in dieser eDirectory-Instanz gespeichert wird, geben Sie zum Erweitern des Schemas `y` ein. Wenn das Schema nicht erweitert ist, funktioniert Identity Manager nicht.

Sie werden aufgefordert, das Schema für jede eDirectory-Instanz zu erweitern, die dem Nicht-root-Benutzer gehören, der von der Nicht-root-Installation von eDirectory gehostet wird.

Wenn Sie die Schemaerweiterung auswählen, geben Sie den vollständigen eindeutigen Name (Distinguished Name, DN) des eDirectory-Benutzers an, der über Berechtigungen zum Erweitern des Schemas verfügt. Der Benutzer kann das Schema nur erweitern, wenn er über Supervisor-Berechtigungen für die gesamte Baumstruktur verfügt. Weitere Informationen zur Erweiterung des Schemas als Nicht-root-Benutzer finden Sie in der Datei `schema.log`, die im `data`-Verzeichnis jeder eDirectory-Instanz gespeichert ist.

Führen Sie das Programm `/opt/novell/eDirectory/idm-install-schema` aus, um das Schema nach abgeschlossener Installation auf weiteren eDirectory-Instanzen zu installieren.

- ♦ **Dienstprogramme:** (Optional) Wenn Sie ein Identity Manager-Treiberdienstprogramm benötigen, müssen Sie die Dienstprogramme von den Datenträgern für die Identity Manager-Installation auf den Identity Manager-Server kopieren. Alle Dienstprogramme befinden sich im Verzeichnis `IDM3.6.1_Plattform/setup/utilities`.
- 5 Aktivieren Sie Identity Manager. Weitere Informationen finden Sie in **Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 69.**
 - 6 Erstellen und konfigurieren Sie die Treiberobjekte. Diese Informationen sind in jedem Treiberhandbuch enthalten. Weitere Informationen hierzu finden Sie in der **Identity Manager-Treiberdokumentation** (<http://www.novell.com/documentation/idm36drivers/>).

7.2.2 Automatische Installation des Metaverzeichnis-Servers

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

- ♦ **Linux:** `IDM3_6_1_Lin/install.bin -i silent -f <Dateiname>.properties`
- ♦ **Solaris:** `IDM3_6_1_Solaris/install.bin -i silent -f <Dateiname>.properties`
- ♦ **AIX:** `IDM3_6_1_AIX/install.bin -i silent -f <Dateiname>.properties`

Erstellen Sie im Verzeichnis, in dem sich das Installationsprogramm von Identity Manager befindet, die Eigenschaftsdatei `<Dateiname>.properties` mit den folgenden Attributen:

```
EDIR_USER_NAME=cn=admin,o=test
EDIR_USER_PASSWORD=test
METADIRECTORY_SERVER_SELECTED=true
CONNECTED_SYSTEM_SELECTED=false
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

Die Standardinstallationsverzeichnisse sind in der Datei `/tmp/idmInstall.log` aufgeführt.

Hinweis: Wenn Sie iManager installiert haben und später iManager-Plugins installieren möchten, müssen Sie den Wert `WEB_ADMIN_SELECTED` auf `true` setzen.

Hinweis: Wenn Sie Identity Manager auf mehreren Instanzen installieren möchten (automatische Installation), müssen Sie sicherstellen, dass die Datei `<Dateiname>.properties` folgenden Eintrag enthält:

```
EDIR_NCP_PORT=1524
EDIR_NDS_CONF=/etc/opt/novell/eDirectory/conf
EDIR_IP_ADDRESS=<xxx.xx.xx.xx>
```

7.3 Installation des Remote Loaders

Der Remote Loader erweitert die Funktionalität von Identity Manager, indem er dem Treiber ermöglicht, auf das verbundene System zuzugreifen, ohne dass das Identitätsdepot und die Metaverzeichnis-Engine auf demselben Server wie das verbundene System installiert sein müssen.

Im Rahmen des Planungsprozesses müssen Sie sich für oder gegen die Verwendung des Remote Loader entscheiden. Weitere Informationen zum Planungsprozess finden Sie in **Kapitel 3**, „Technische Richtlinien“, auf Seite 27.

- ♦ **Abschnitt 7.3.1**, „Anforderungen“, auf Seite 62
- ♦ **Abschnitt 7.3.2**, „Unterstützte Treiber“, auf Seite 62
- ♦ **Abschnitt 7.3.3**, „Installationsvorgang“, auf Seite 63

Wenn Sie den Remote Loader von einem Nicht-root-Benutzer installieren lassen möchten, verwenden Sie den Java Remote Loader. Er kann auch für die Anpassung Ihrer Umgebung und deren Installation auf einer nicht unterstützten Plattform wie beispielsweise HP-UX* verwendet werden. Weitere Informationen finden Sie in **Abschnitt 7.3.5**, „Installation des Java Remote Loader unter UNIX, Linux oder AIX“, auf Seite 66.

7.3.1 Anforderungen

Der Remote Loader erfordert, dass alle verbundenen Systeme des Treibers verfügbar sind und die jeweiligen APIs zur Verfügung gestellt werden. Informationen zu den treiberspezifischen Anforderungen für das Betriebssystem und das verbundene System finden Sie in der **Treiberdokumentation zu Identity Manager** (<http://www.novell.com/documentation/idm36drivers>).

7.3.2 Unterstützte Treiber

Nicht alle Identity Manager-Treiber werden vom Remote Loader unterstützt. In **Tabelle 7-1** sind die Treiber aufgeführt, die mit Remote Loader kompatibel sind.

Tabelle 7-1 Mit dem Remote Loader kompatible Treiber

Active Directory	Avaya* PBX
Text mit Begrenzungszeichen	GroupWise®
JDBC*	JMS
LDAP	Linux- und UNIX-Treiber
Lotus Notes*	PeopleSoft* 5.2
Remedy* ARS	SAP* HR
SAP-Benutzerverwaltung	Skripts
SOAP	Auftrag
„Manuelle Aufgabe“-Services	Null Services
LoopBack	

Die in **Tabelle 7-2** aufgeführten Treiber sind nicht mit dem Remote Loader kompatibel.

Tabelle 7-2 Nicht mit dem Remote Loader kompatibel

eDirectory	Berechtigungsservice
Rollenservice	Benutzeranwendung

7.3.3 Installationsvorgang

Der Remote Loader verfügt über unterschiedliche Programme für die verschiedenen Plattformen, die die Kommunikation mit der Metaverzeichnis-Engine ermöglichen.

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

So installieren Sie den Remote Loader:

1 Stellen Sie sicher, dass Ihr System den in [Kapitel 6, „Systemanforderungen“](#), auf Seite 47 aufgeführten Systemanforderungen entspricht.

2 Starten Sie die Installation, indem Sie das entsprechende Programm für Ihre Plattform ausführen.

- ♦ **Windows:** `IDM3.6.1_Win:windows\setup\idm_install.exe`
- ♦ **Linux - GUI-Installation:** `IDM3_6_1_Lin/install.bin [-i gui]`
- ♦ **Linux - Installation über die Befehlszeile:** `IDM3_6_1_Lin/install.bin -i console`
- ♦ **Solaris - GUI-Installation:** `IDM3_6_1_Solaris/install.bin [-i gui]`
- ♦ **Solaris - Installation über die Befehlszeile:** `IDM3_6_1_Solaris/install.bin -i console`
- ♦ **AIX - GUI-Installation:** `IDM3_6_1_AIX/install.bin [-i gui]`
- ♦ **AIX - Installation über die Befehlszeile:** `IDM3_6_1_AIX/install.bin -i console`

Geben Sie ein, um die Binärdateien unter Linux\Solaris\AIX auszuführen./
`install.bin [-i {gui | console}]`.

Wichtig: Nur das AIX-Maintenance-Level 5300-09 wird unterstützt. Neuere oder ältere Maintenance-Levels werden nicht unterstützt.

3 Mithilfe der folgenden Informationen wird die Installation ausgeführt:

- ♦ **Komponenten auswählen:** Wählen Sie den Server und die Dienstprogramme des verbundenen Systems aus, um den Remote Loader zu installieren.
 - ♦ **Novell Identity Manager Metadirectory Server:** Wählen Sie diese Option nur, wenn Sie den Metaverzeichnis-Server installieren. Diese Option setzt voraus, dass das Identitätsdepot auf diesem Server installiert ist. Weitere Informationen finden Sie in [Abschnitt 7.2, „Installation des Metaverzeichnis-Servers“](#), auf Seite 58.
 - ♦ **Novell Identity Manager - Server für verbundene Systeme:** Diese Option setzt nicht voraus, dass das Identitätsdepot auf diesem Server installiert ist. Sie installiert den Remote Loader-Service auf Ihrem Anwendungsserver.
 - ♦ **Keine:** Wählen Sie diese Option, wenn Sie die iManager-Plugins oder die Dienstprogramme installieren möchten, ohne den Metaverzeichnis-Server oder den Server des verbundenen Systems auf diesem Server zu installieren.

- ♦ **Novell Identity Manager - Webbasierter Administrationsserver:** Wählen Sie diese Option, wenn iManager auf diesem Server installiert ist. Mit dieser Option werden die iManager-Plugins für Identity Manager installiert.
- ♦ **Dienstprogramme:** Mit dieser Option werden Dienstprogramme installiert, die Sie bei der Konfiguration der Treiber für die verbundenen Systeme unterstützen. Nicht für alle Treiber sind Dienstprogramme verfügbar. Wenn Sie nicht sicher sind, ob Sie diese Funktion installieren möchten, sollten Sie sie auswählen, da sie nur wenig Festplattenspeicher benötigt.

Warnung: Wählen Sie für die Installation von Identity Manager 3.6.1 nicht die Komponente "Dienstprogramme" aus. Bei Auswahl der Komponente "Dienstprogramme" wird die Installation nicht fortgesetzt.

- ♦ **Benutzerdefiniert:** Wählen Sie diese Option, wenn Sie die installierten Funktionen anpassen möchten. Die folgenden Optionen stehen zur Auswahl:
 - ♦ **Remote Loader-Service:** Der Service, der mit der Metaverzeichnis-Engine kommuniziert.
 - ♦ **Treiber:** Wählen Sie aus, welche Treiberdateien installiert werden sollen. Es wird empfohlen, alle Treiberdateien zu installieren. So müssen Sie die Installation nicht erneut ausführen, wenn Sie eine weitere Remote Loader-Instanz hinzufügen.
 - ♦ **Identity Audit-Systemkomponenten für Identity Manager registrieren:** Wählen Sie diese Option, wenn Identity Audit oder Novell Sentinel installiert ist.

Wenn Sie keine der oben aufgeführten Optionen auswählen, kann die benutzerdefinierte Installation nicht fortgesetzt werden.

- ♦ **(Nur Windows) Installationsverzeichnis des Servers für verbundene Systeme:** Geben Sie das Verzeichnis an, in dem der Server des verbundenen Systems installiert ist.
 - ♦ **(Nur Windows) Installationsverzeichnis für Dienstprogramme:** Geben Sie das Verzeichnis an, in dem die Dienstprogramme installiert sind.
- 4 Erstellen und konfigurieren Sie Ihre Treiberobjekte so, dass sie den Remote Loader verwenden. Diese Informationen sind in jedem Treiberhandbuch enthalten. Weitere Informationen hierzu finden Sie in der [Identity Manager-Treiberdokumentation \(http://www.novell.com/documentation/idm36drivers/\)](http://www.novell.com/documentation/idm36drivers/).
 - 5 Erstellen Sie eine Konfigurationsdatei, damit Remote Loader zusammen mit dem verbundenen System verwendet werden kann. Weitere Informationen hierzu finden Sie unter „[Configuring the Remote Loader for Linux/UNIX by Creating a Configuration File](#)“ (Konfiguration des Remote Loader für Linux/UNIX durch Erstellung einer Konfigurationsdatei) im Handbuch zu *Identity Manager 3.6.1 Remote Loader*.

Installation des Remote Loaders als 32-Bit-Anwendung auf einem 64-Bit-Betriebssystem

Unter Windows:

- 1 Wählen Sie die Datei `32bit_RL_Install.properties` im Verzeichnis `..\Windows\setup\` aus und setzen Sie die Eigenschaftswerte für `RL_32BIT_INSTALL_ON_64BIT` wie folgt auf `true`:

```
RL_32BIT_INSTALL_ON_64BIT=true
```

- 2 Wechseln Sie an der Eingabeaufforderung zum Installationsverzeichnis von IDM 3.6.1 (C:\IDM3.6.1\windows\setup) und geben Sie den folgenden Befehl ein:

```
idm_install.exe - i gui[console] -f 32bit_RL_Install.properties
```

- 3 Führen Sie die Anweisungen ab **Schritt 3** unter **Abschnitt 7.3.3, „Installationsvorgang“**, auf **Seite 63** aus, um die Installation abzuschließen.

Unter Linux:

- 1 Wählen Sie die Datei 32bit_RL_Install.properties im Verzeichnis ../linux/setup aus und setzen Sie die Eigenschaftswerte für `RL_32BIT_INSTALL_ON_64BIT` wie folgt auf `true`:

```
RL_32BIT_INSTALL_ON_64BIT=true
```

- 2 Wechseln Sie im Terminal zum Installationsverzeichnis von IDM 3.6.1 (../linux/setup) und geben Sie den folgenden Befehl ein:

```
idm_linux.bin - i gui[console] -f 32bit_RL_Install.properties
```

- 3 Führen Sie die Anweisungen ab **Schritt 3** unter **Abschnitt 7.3.3, „Installationsvorgang“**, auf **Seite 63** aus, um die Installation abzuschließen.

7.3.4 Automatische Installation des Remote Loaders

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

- ♦ **Linux:** `IDM3_6_1_Lin/install.bin -i silent -f <Dateiname>.properties`
- ♦ **Solaris:** `IDM3_6_1_Solaris/install.bin -i silent -f <Dateiname>.properties`
- ♦ **AIX:** `IDM3_6_1_AIX/install.bin -i silent -f <Dateiname>.properties`

Erstellen Sie im Verzeichnis, in dem sich das Installationsprogramm von Identity Manager befindet, die Eigenschaftsdatei `<Dateiname>.properties` mit den folgenden Attributen:

```
EDIR_USER_NAME=cn=admin,o=test
EDIR_USER_PASSWORD=test
METADIRECTORY_SERVER_SELECTED=false
CONNECTED_SYSTEM_SELECTED=true
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

Die Standardinstallationsverzeichnisse sind in der Datei `/tmp/idmInstall.log` aufgeführt.

Hinweis: Wenn Sie iManager installiert haben und später iManager-Plugins installieren möchten, müssen Sie den Wert `WEB_ADMIN_SELECTED` auf `true` setzen.

7.3.5 Installation des Java Remote Loader unter UNIX, Linux oder AIX

`dirxml_jremote` ist ein reiner Java-Remote-Loader. Er wird zum Datenaustausch zwischen der auf dem Server aktiven Metaverzeichnis-Engine und den Identity Manager-Treibern verwendet, die an einem anderen Standort ausgeführt werden, auf dem `rdxml` nicht aktiviert ist. Er sollte auf jedem System mit einer kompatiblen JRE (ab 1.5.0) und Java Sockets ausgeführt werden können. Er wird von allen Linux-/UNIX-Plattformen unterstützt, die von Identity Manager unterstützt werden.

- 1 Stellen Sie sicher, dass Java 1.5.x JDK*/JRE auf dem Host-System verfügbar ist.
- 2 Kopieren Sie die Datei `dirxml_jremote_dev.tar.gz` an den gewünschten Speicherort auf dem Remote-Server.
- 3 Kopieren Sie die Datei `dirxml_jremote.tar.gz` oder `dirxml_jremote_mvs.tar` an den gewünschten Speicherort auf dem Remote-Server.

Beispiel: `/usr/idm`

Die Datei befindet sich unter den Linux- bzw. UNIX-ISO-Images am selben Speicherort. Die Dateien befinden sich im Ordner `java_remoteloader` unterhalb des Stammordners des ISO-Image. Wenn Sie Informationen zu `mvs` benötigen, dekomprimieren Sie die Datei `dirxml_jremote_mvs.tar` und öffnen Sie das Dokument `usage.html`.

- 4 Entpacken und extrahieren Sie die Dateien `dirxml_jremote.tar.gz` und `dirxml_jremote_dev.tar.gz`.

Beispiel: `gunzip dirxml_jremote.tar.gz` bzw. `tar -xvf dirxml_jremote_dev.tar`

- 5 Kopieren Sie die `.jar`-Dateien des Anwendungsschnittstellenmoduls in das Unterverzeichnis `lib`, das beim Extrahieren der `dirxml_jremote.tar`-Datei erstellt wurde.

Da die `tar`-Datei keine Treiber enthält, müssen Sie die Treiber manuell in das `lib`-Verzeichnis kopieren. Das `lib`-Verzeichnis befindet sich in dem von Ihnen zuvor dekomprimierten Verzeichnis.

- 6 Passen Sie das `dirxml_jremote`-Skript an, indem Sie einen der folgenden Schritte ausführen:
 - ♦ Stellen Sie sicher, dass die Java-Programmdatei durch die Umgebungsvariable `PATH` erreichbar ist, indem Sie die Umgebungsvariable `RDXML_PATH` festlegen. Legen Sie die Umgebungsvariable mithilfe der folgenden Befehle fest:
 1. `set RDXML_PATH=path`
 2. `export RDXML_PATH`
 - ♦ Bearbeiten Sie das `dirxml_jremote`-Skript und fügen Sie den Pfad der Java-Programmdatei am Anfang der Skriptzeile ein, die Java ausführt.
- 7 Konfigurieren Sie die Beispieldatei `config8000.txt` zur Verwendung mit dem Anwendungsschnittstellenmodul. Weitere Informationen hierzu finden Sie unter „[Configuring the Remote Loader for Linux/UNIX by Creating a Configuration File](#)“ (Konfiguration des Remote Loader für Linux/UNIX durch Erstellung einer Konfigurationsdatei) im Handbuch zu *Identity Manager 3.6.1 Remote Loader Identity Manager 3.6.1 Remote Loader Guide*.

7.4 Installation des rollensbasierten Bereitstellungsmoduls

Weitere Informationen zur Installation des rollensbasierten Bereitstellungsmoduls finden Sie im *Installationshandbuch* (<http://www.novell.com/documentation/idmrbpm361/index.html>) des rollensbasierten Bereitstellungsmoduls.

7.5 Installation eines benutzerdefinierten Treibers

Sie können einen benutzerdefinierten Treiber erstellen, der in Ihrer Umgebung verwendet werden soll. Weitere Informationen zur Erstellung oder Installation eines benutzerdefinierten Treibers finden Sie im *Novell Developer Kit* (<http://developer.novell.com/wiki/index.php/Dirxml>).

7.6 Installation von Identity Audit oder Sentinel

Dies ist eine optionale Erweiterung für die Identity Manager-Lösung. Durch die Erweiterung um die Funktionen für die Revision und die Berichterstellung können Sie die Konformitätsstandards erfüllen, die von vielen Unternehmen eingehalten werden müssen. Die Software erstellt Revisionsprotokolle für alle zu protokollierenden Ereignisse und kann Berichte erzeugen, um sicherzustellen, dass Sie alle für Ihr Unternehmen geltenden Revisionsstandards erfüllen.

Informationen zur Konfiguration von Identity Audit mit Identity Manager finden Sie im *Identity Manager 3.6.1-Integrationshandbuch für Identity Audit*. Informationen zur Konfiguration von Novell Sentinel mit Identity Manager finden Sie im *Identity Manager 3.6.1 Reporting Guide for Novell Sentinel* (Identity Manager 3.6-Berichtshandbuch für Novell Sentinel). Informationen zu den Systemanforderungen für Identity Audit finden Sie im Handbuch zu *Identity Audit* (<http://www.novell.com/documentation/identityaudit/index.html>). Informationen zu den Systemanforderungen für Sentinel finden Sie im *Novell Sentinel-Installationshandbuch* (<http://www.novell.com/documentation/sentinel6/index.html>).

7.7 Installation von Identity Manager in der Cluster-Umgebung

Wenn Sie Identity Manager in einer Cluster-Umgebung bereitstellen, unterstützt Novell die Ausführung von Identity Manager im Cluster, obwohl das Cluster selbst in den meisten Fällen nicht unterstützt wird. Im Folgenden werden zwei Szenarios und der Umfang der geleisteten Unterstützung beschrieben:

- ♦ Wenn Sie die Identity Manager-Engine oder den Remote Loader auf dem SUSE Linux Enterprise Server (SLES) ausführen und die Hochverfügbarkeit mithilfe des Heartbeat verwalten, werden alle Funktionen unterstützt.
- ♦ Wenn Sie die Identity Manager-Engine oder den Remote Loader in einer Cluster-Umgebung oder auf einer anderen unterstützten Plattform ausführen, wird die Unterstützung auf alle Funktionen mit Ausnahme des Cluster-Verwaltungssystems erweitert.

Hinweis: SLES ist die einzige Plattform, die vollständig in einer Cluster-Umgebung unterstützt wird.

Weitere Informationen zur Konfiguration eines Clusters mit Identity Manager finden Sie in folgenden Ressourcen:

- ♦ AppNote „Configuring a Linux High Availability Cluster for IDM 3 and eDirectory 8.8“ (Konfiguration eines Hochverfügbarkeits-Clusters unter Linux für IDM 3 und eDirectory 8.8) auf der [Cool Solutions Website von Novell \(http://www.novell.com/coolsolutions/appnote/18591.html\)](http://www.novell.com/coolsolutions/appnote/18591.html).
- ♦ AppNote „Clustering eDirectory and IDM on Windows 2003“ (Cluster-Gruppierung von eDirectory und IDM unter Windows 2003) auf der [Cool Solutions Website von Novell \(http://www.novell.com/coolsolutions/appnote/14856.html\)](http://www.novell.com/coolsolutions/appnote/14856.html).
- ♦ AppNote „High Availability on PolyServe Clusters“ (Hochverfügbarkeit auf PolyServe-Clustern) auf der [Cool Solutions Website von Novell \(http://www.novell.com/coolsolutions/appnote/16131.html\)](http://www.novell.com/coolsolutions/appnote/16131.html).
- ♦ „Setting Up an Identity Manager Cluster on Windows“ auf der [Support-Website von Novell \(http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3575742&sliceId=SAL_Public&dialogID=310596&stateId=1%20%20308676\)](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3575742&sliceId=SAL_Public&dialogID=310596&stateId=1%20%20308676). Die Dokumentnummer ist 3575742.

Aktivieren von Novell Identity Manager-Produkten

8

Im Folgenden wird erläutert, wie die Aktivierung von Produkten erfolgt, die auf Novell® Identity Manager basieren. Identity Manager, die Integrationsmodule und das Bereitstellungsmodul müssen innerhalb von 90 Tagen nach der Installation aktiviert werden, anderenfalls werden sie außer Betrieb gesetzt. Sie können Identity Manager-Produkte zu einem beliebigen Zeitpunkt während oder nach Ablauf der 90 Tage aktivieren.

Führen Sie zur Aktivierung von Identity Manager und den Treibern folgende Schritte aus:

- ♦ **Abschnitt 8.1, „Erwerb einer Produktlizenz für Identity Manager“, auf Seite 69**
- ♦ **Abschnitt 8.2, „Installation einer Produktaktivierungsberechtigung“, auf Seite 69**
- ♦ **Abschnitt 8.3, „Anzeigen der Produktaktivierungen für Identity Manager und Identity Manager-Treiber“, auf Seite 70**

8.1 Erwerb einer Produktlizenz für Identity Manager

Sie können über die Novell Identity Manager-Bestell-Website (<http://www.novell.com/products/identitymanager/howtobuy.html>) eine Identity Manager-Produktlizenz erwerben.

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 einen Berechtigungsnachweis 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.

8.2 Installation einer Produktaktivierungsberechtigung

Die Produktaktivierungsberechtigung sollte über iManager installiert werden.

- 1 Nach dem Erwerb einer Lizenz erhalten Sie von Novell eine Email mit Ihrer Kunden-ID. Die Email enthält außerdem unter „Auftragsdetails“ einen Link zur Website, auf der Sie einen Berechtigungsnachweis erhalten. Rufen Sie die Website auf, indem Sie auf den Link klicken.
- 2 Klicken Sie auf den Link zum Herunterladen der Lizenz und führen Sie einen der folgenden Schritte aus:
 - ♦ Speichern Sie die Datei mit der Produktaktivierungsberechtigung.
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.

8.3 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 die Suche 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.

Fehlerbehebung in Identity Manager

9

Bei der Installation von Identity Manager sollten Sie Folgendes beachten:

- ♦ Wenn unter AIX 5.3 NFS-Mounts deaktiviert sind, reagiert die IDM 3.6.1-Installation nicht. Dieses Verhalten tritt auch auf, wenn sich das ISO-Image des IDM-Installationsprogramms und AIX auf demselben Computer befinden und gemountete Partitionen nicht verfügbar sind.

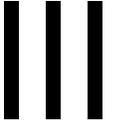
Lösung: Hängen Sie die Mounts, die nicht mehr reagieren, aus bzw. mounten Sie sie erneut und fahren Sie mit der Installation fort.

- ♦ Wenn Sie als Nicht-root-Benutzer IDM 3.6.1 unter Solaris 10 installieren, wird möglicherweise der folgende Fehler für den Lotus Notes-Treiber angezeigt:

```
ln: cannot create /usr/lib/locale/ja/wnn//ndsrep: File exists
ln: cannot create
cp: cannot create /usr/lib/locale/ja/wnn//libnotesdrvjni.so.1.0.0:
Permission
denied
ln: cannot create /usr/lib/locale/ja/wnn//libnotesdrvjni.so.1: File exists
ln: cannot create /usr/lib/locale/ja/wnn//libnotesdrvjni.so: File exists
```

Lösung: Erstellen Sie die symbolischen Links manuell. Weitere Informationen zum Prüfen und Neuerstellen von symbolischen Links finden Sie unter „[Troubleshooting Installation Problems](#)“ (Beheben von Installationsproblemen) im *Identity Manager 3.6.1 Driver for Lotus Notes Implementation Guide* (Handbuch für die Implementierung des Identity Manager 3.6.1-Treibers für Lotus Notes).

Upgrades



Die folgenden Abschnitte enthalten Informationen zur Aktualisierung Ihrer vorhandenen Identity Manager-Lösung:

- ♦ [Kapitel 10, „Neuheiten“, auf Seite 77](#)
- ♦ [Kapitel 11, „Unterstützte Versionen für Upgrades und Systemanforderungen“, auf Seite 79](#)
- ♦ [Kapitel 12, „Direktaufrüstung im Vergleich zu Migration“, auf Seite 81](#)
- ♦ [Kapitel 13, „Durchführung einer Direktaufrüstung“, auf Seite 83](#)
- ♦ [Kapitel 14, „Durchführen einer Migration“, auf Seite 97](#)

- [Abschnitt 10.1, „Unterstützung für 64-Bit-Betriebssysteme“](#), auf Seite 77
- [Abschnitt 10.2, „Unterstützung für 32-Bit-Remote Loader-Installationen auf 64-Bit-Betriebssystemen“](#), auf Seite 77

10.1 Unterstützung für 64-Bit-Betriebssysteme

Identity Manager wird jetzt auf 64-Bit-Betriebssystemen unterstützt. Eine Liste der unterstützten Betriebssysteme finden Sie in [Abschnitt 6.2.2, „Server-Betriebssysteme“](#), auf Seite 50.

10.2 Unterstützung für 32-Bit-Remote Loader-Installationen auf 64-Bit-Betriebssystemen

Identity Manager unterstützt die Installation von Remote Loader als 32-Bit-Anwendung auf 64-Bit-Betriebssystemen. Eine Liste der unterstützten Betriebssysteme finden Sie in [Abschnitt 6.3, „Remote Loader“](#), auf Seite 51.

Unterstützte Versionen für Upgrades und Systemanforderungen

- [Abschnitt 11.1, „Unterstützte Versionen für Upgrades“](#), auf Seite 79
- [Abschnitt 11.2, „Systemanforderungen“](#), auf Seite 79

11.1 Unterstützte Versionen für Upgrades

Die Tabelle zeigt die unterstützten Upgrades für die vorherigen Versionen von Identity Manager an.

Tabelle 11-1 *Unterstützte Versionen für Upgrades*

Installierte Versionen	Neueste Version	Wird ein Upgrade unterstützt
DirXML® 1.1a	Identity Manager 3.6.1	Nein
Identity Manager 2.x	Identity Manager 3.6.1	Nein
Identity Manager 3.0.x	Identity Manager 3.6.1	Nein
Identity Manager 3.5.x	Identity Manager 3.6.1	Ja

Hinweis: Identity Manager 3.5.x funktioniert auf allen Plattformen, die Unterstützung für Remote Loader 3.6 und 3.6.1 bieten.

11.2 Systemanforderungen

Für das Aufrüsten auf Identity Manager 3.6.1 müssen die Server, die die Identity Manager-Services ausführen, die Mindestanforderungen erfüllen. In [Kapitel 6, „Systemanforderungen“](#), auf Seite 47 finden Sie eine Liste der Mindestanforderungen für jede Plattform.

Direktaufrüstung im Vergleich zu Migration

12

Es gibt zwei verschiedene Möglichkeiten, um aufzurüsten: Direktaufrüstung oder Migration. Jede Methode hat Vor- und Nachteile und es gibt Szenarien, in denen nur eine Methode verwendet werden kann.

- ♦ [Abschnitt 12.1, „Direktaufrüstung“, auf Seite 81](#)
- ♦ [Abschnitt 12.2, „Migration“, auf Seite 82](#)
- ♦ [Abschnitt 12.3, „Mehrere Server mit einem einzelnen Treibersatz verknüpft“, auf Seite 82](#)

12.1 Direktaufrüstung

Bei der Direktaufrüstung wird die neue Version von Identity Manager auf dem vorhandenen Server installiert. Zur Installation von Identity Manager müssen Sie die aktuellen Versionen des Betriebssystems und von eDirectory™ auf die unterstützten Versionen für Identity Manager 3.6.1 aufrüsten. Eine Liste der unterstützten Plattformen finden Sie unter [Kapitel 6, „Systemanforderungen“, auf Seite 47](#).

Die Vorteile sind:

- ♦ Keine neue Hardware
- ♦ Keine Migration von Daten

Die Nachteile sind:

- ♦ Ausfallzeit, wenn das Betriebssystem aktualisiert und der Server neu gestartet wird
- ♦ Ausfallzeit, wenn eDirectory aktualisiert und neu gestartet wird

Es gibt bestimmte Szenarien, bei denen eine Direktaufrüstung nicht sinnvoll ist oder mehrere Direktaufrüstungen durchgeführt werden müssen. Da Identity Manager 3.5.x und höher die einzigen unterstützten Migrationspfade sind, sind sie die einzigen Versionen, die in den folgenden Szenarien enthalten sind:

Eine Direktaufrüstung ist nur möglich, wenn Identity Manager 3.5.x auf einem unterstützten Betriebssystem installiert ist. Es gibt jedoch bestimmte Szenarien, bei denen eine Direktaufrüstung nicht sinnvoll ist. Die folgenden Beispiele zeigen, in welchen Situationen, eine Direktaufrüstung nicht sinnvoll ist:

- ♦ **Nicht unterstütztes Betriebssystem:** Wenn die aktuelle Version des Betriebssystems von Identity Manager 3.6.1 nicht unterstützt wird, besteht der einzige unterstützte Upgrade-Pfad in der Durchführung einer Migration auf einen neuen Server.

- ♦ **Identity Manager 3.0.x:** Wenn es sich bei der aktuellen Version von Identity Manager um 3.0.x handelt, können Sie keine Direktaufrüstung durchführen. Es stehen zwei Optionen zur Verfügung:
 - ♦ Führen Sie eine Direktaufrüstung auf Identity Manager 3.5.1 durch, rüsten Sie auf eDirectory 8.8.5 auf und führen Sie anschließend eine Direktaufrüstung auf Identity Manager 3.6.1 durch.
 - ♦ Führen Sie eine Migration auf einen neuen Server durch.

Wenn Sie eine Direktaufrüstung durchführen, fahren Sie mit [Kapitel 13, „Durchführung einer Direktaufrüstung“](#), auf Seite 83 fort.

12.2 Migration

Bei einer Migration wird Identity Manager 3.6.1 auf einem neuen Server installiert und anschließend werden die vorhandenen Daten auf diesen neuen Server migriert. Befolgen Sie [Kapitel 4, „Basis-Checkliste für das Identity Manager-System“](#), auf Seite 41, um zu überprüfen, ob die Installation abgeschlossen ist.

Die Vorteile sind:

- ♦ Es gibt eine minimale Ausfallzeit für die Treiber

Die Nachteile sind:

- ♦ Erfordert neue Hardware

Wenn Sie eine Migration durchführen, fahren Sie mit [Kapitel 14, „Durchführen einer Migration“](#), auf Seite 97 fort.

12.3 Mehrere Server mit einem einzelnen Treibersatz verknüpft

Wenn Sie mehrere Server mit einem Treibersatz verknüpft haben, können Sie eine Direktaufrüstung oder eine Migration nur auf einem Server gleichzeitig durchführen. Wenn Sie nicht genügend Zeit haben, um die Server zum gleichen Zeitpunkt aufzurüsten, arbeiten die Treiber weiterhin mit den verschiedenen Versionen von Identity Manager, bis die Upgrades für jeden Server abgeschlossen werden können.

Die Identity Manager-Engine ist abwärtskompatibel, sodass die Identity Manager 3.6.1-Engine die Treiber von Identity Manager 3.5.x und Identity Manager x ohne Probleme ausführen kann.

Warnung: Wenn Sie Funktionen für Treiber aktivieren, die nur unter Identity Manager 3.6.1 unterstützt werden, arbeiten die Treiber nicht mehr auf den Servern mit gemischten Versionen. Die älteren Engines können die neue Funktionalität nicht verarbeiten. Dies deaktiviert die Treiber, bis alle Server auf Identity Manager 3.6.1 aufgerüstet wurden.

Durchführung einer Direktaufrüstung

13

Informieren Sie sich vor dem Beginn über die Unterschiede zwischen der Direktaufrüstung und der Migration. Weitere Informationen hierzu finden Sie unter **Kapitel 12, „Direktaufrüstung im Vergleich zu Migration“**, auf Seite 81.

Verwenden Sie die folgende Checkliste, um zu überprüfen, ob alle Schritte in der richtigen Reihenfolge abgeschlossen wurden, damit eine erfolgreiche Direktaufrüstung des Identity Manager-Systems sichergestellt werden kann. Führen Sie folgende Schritte für jeden Identity Manager-Server in Ihrer Umgebung aus.

- Erstellen Sie ein Backup der aktuellen Konfiguration Ihrer Identity Manager-Lösung. Exportieren Sie hierzu Ihre Treiber oder erstellen Sie ein Designer-Projekt Ihrer Identity Manager-Lösung. Weitere Informationen finden Sie in **Abschnitt 13.1, „Backup der aktuellen Konfiguration erstellen“**, auf Seite 85.
- Vergewissern Sie sich, dass die Betriebssystemversionen der Server, auf denen Identity Manager ausgeführt wird, unterstützt werden. Eine Liste der unterstützten Betriebssysteme finden Sie in **Kapitel 6, „Systemanforderungen“**, auf Seite 47. Wenn das Betriebssystem nur einen Service-Pack benötigt, um die Systemanforderungen zu erfüllen, fahren Sie mit der Direktaufrüstung fort. Wenn mehr erforderlich ist, müssen Sie statt der Direktaufrüstung eine Migration durchführen. Fahren Sie mit **Kapitel 14, „Durchführen einer Migration“**, auf Seite 97 fort, wenn Sie eines der folgenden Betriebssysteme haben:
 - ◆ NetWare®
 - ◆ Windows NT
 - ◆ Windows 2000
 - ◆ Red Hat Linux 3
 - ◆ SLES 8
 - ◆ Solaris 8 oder 9
- Führen Sie auf Ihrem iManager-Server ein Upgrade auf iManager 2.7.3 durch. Weitere Informationen hierzu finden Sie im Installationshandbuch zu *iManager* (http://www.novell.com/documentation/imanager27/imanager_install_27/data/hk42s9ot.html).
- Beenden Sie die Treiber, die mit dem Server verknüpft sind, den Sie aufrüsten. Weitere Informationen finden Sie in **Abschnitt 13.2, „Anhalten der Treiber“**, auf Seite 88.
- Rüsten Sie auf dem Server, auf dem Identity Manager ausgeführt wird, eDirectory™ auf 8.8.5 oder höher auf. Weitere Informationen finden Sie im **eDirectory Installationshandbuch** (<http://www.novell.com/documentation/edir88/index.html>).
- (Bedingt) Wenn Ihre Plattform Linux-, UNIX- oder Solaris ist, müssen Sie zusätzliche Schritte unternehmen, damit die Dateien an den richtigen Speicherorten abgelegt werden. Weitere Informationen finden Sie in **Abschnitt 13.3, „Dateien unter Linux/UNIX in den richtigen Speicherorten ablegen“**, auf Seite 89.
- Starten Sie die Treiber und vergewissern Sie sich, dass die Treiber starten. Dadurch wird auch überprüft, ob das Upgrade auf eDirectory 8.8.5 erfolgreich war. Weitere Informationen finden Sie in **Abschnitt 13.10, „Starten der Treiber“**, auf Seite 95.

- ❑ Upgrade auf Designer 3.0.1. Weitere Informationen finden Sie unter „**Designer aktualisieren**“ im *Administrationshandbuch zu Designer 3.0 für Identity Manager 3.6*.
- ❑ Konvertieren Sie das Designer-Projekt. Weitere Upgrade-Informationen finden Sie unter „**Converting Earlier Projects**“ (Konvertieren früherer Projekte) im *Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6*.
- ❑ Beenden Sie die Treiber, die mit dem Server verknüpft sind, den Sie aufrüsten. Weitere Informationen finden Sie in **Abschnitt 13.2, „Anhalten der Treiber“**, auf Seite 88.
- ❑ Rüsten Sie den Metaverzeichnis-Server auf. Weitere Informationen finden Sie in **Abschnitt 13.5, „Upgrade der Metaverzeichnis-Engine und der Treiberkonfigurationsdateien“**, auf Seite 90.
- ❑ (Bedingt) Wenn es sich bei einem der Treiber im Treibersatz dieses Servers um Remote Loader-Treiber handelt, rüsten Sie die Remote Loader-Server für jeden Treiber auf. Weitere Informationen finden Sie unter **Abschnitt 13.6, „Upgrade des Remote Loaders“**, auf Seite 90.
- ❑ (Bedingt) Wenn es sich bei diesem Server um Ihren Benutzeranwendungs-Server handelt, führen Sie die folgenden zusätzlichen Schritte aus:
 - ❑ Der Benutzeranwendungstreiber muss in Designer migriert werden. Weitere Informationen finden Sie im *Migrationshandbuch des rollenbasierten Bereitstellungsmoduls* (<http://www.novell.com/documentation/idmrpbpm361/index.html>).
 - ❑ Erstellen Sie einen neuen Rollenservice-Treiber. Die Rollenservice-Treiber werden nicht migriert. Wenn Sie einen vorhandenen Rollenservice-Treiber für Version 3.6.1 haben, müssen Sie einen neuen Treiber für Version 3.6.1 erstellen. Weitere Informationen finden Sie im *Migrationshandbuch des rollenbasierten Bereitstellungsmoduls* (<http://www.novell.com/documentation/idmrpbpm361/index.html>).
 - ❑ Stellen Sie den migrierten Benutzeranwendungstreiber im Identitätsdepot bereit. Weitere Informationen finden Sie im *Migrationshandbuch des rollenbasierten Bereitstellungsmoduls* (<http://www.novell.com/documentation/idmrpbpm361/index.html>).
 - ❑ Rüsten Sie die Benutzeranwendung auf. Weitere Informationen finden Sie im *Migrationshandbuch des rollenbasierten Bereitstellungsmoduls* (<http://www.novell.com/documentation/idmrpbpm361/index.html>).
- ❑ (Optional) Überlagern Sie die neuen Treiberkonfigurationsdateien über die vorhandenen Treiber, um neue Richtlinien zu erhalten. Dies ist nur dann erforderlich, wenn in den Richtlinien eines Treibers neue Funktionalität enthalten ist, die Sie zu Ihrem vorhandenen Treiber hinzufügen möchten. Weitere Informationen finden Sie in **Abschnitt 13.7, „Überlagern der neuen Treiberkonfigurationsdatei über den vorhandenen Treiber“**, auf Seite 91.
- ❑ (Optional) Stellen Sie die benutzerdefinierten Richtlinien und Regeln auf den Treibern wieder her. Wenn Sie die neuen Treiberkonfigurationsdateien überlagern, werden die Richtlinien überschrieben, sodass eine Wiederherstellung der Richtlinien nur erforderlich ist, wenn Sie eine Überlagerung der neuen Treiberkonfigurationsdatei durchgeführt haben. Weitere Informationen finden Sie in **Abschnitt 13.8, „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“**, auf Seite 92.
- ❑ Stellen Sie das konvertierte Designer-Projekt im Identitätsdepot bereit. Weitere Informationen finden Sie unter „**Bereitstellen und Exportieren**“ im *Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6*.
- ❑ Starten Sie die mit diesem Server verknüpften Treiber. Weitere Informationen finden Sie unter **Abschnitt 13.10, „Starten der Treiber“**, auf Seite 95.

- ❑ Bei Verwendung von Novell Sentinel™ müssen Sie eine Aktualisierung auf Novell Sentinel 6.1 vornehmen. Weitere Informationen zur Aktualisierung von Sentinel finden Sie im Installationshandbuch zu *Sentinel* (http://www.novell.com/documentation/sentinel6/pdfdoc/sentinel60_installationguide.pdf).
- ❑ Aktivieren Sie die Metaverzeichnis-Engine und die aufgerüsteten Treiber. Weitere Informationen finden Sie in **Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“**, auf Seite 69.

13.1 Backup der aktuellen Konfiguration erstellen

Vor der Aufrüstung ist es wichtig, ein Backup der aktuellen Konfiguration Ihres Identity Manager-Systems zu erstellen. Wenn Sie die Benutzeranwendung verwenden, sind keine weiteren Schritte erforderlich. Die gesamte Konfiguration der Benutzeranwendung wird im Benutzeranwendungstreiber gespeichert. Backups können auf zwei verschiedene Weisen erstellt werden:

- ♦ **Abschnitt 13.1.1, „Sicherstellen, dass Ihr Designer-Projekt aktuell ist“**, auf Seite 85
- ♦ **Abschnitt 13.1.2, „Exportieren der Treiberdaten“**, auf Seite 87

13.1.1 Sicherstellen, dass Ihr Designer-Projekt aktuell ist

Ein Designer-Projekt enthält das Schema und alle Treiberkonfigurationsinformationen, außer für den Treiber für rollenbasierte Berechtigungen. 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 85
- ♦ **„Erstellen eines neuen Projekts aus dem Identitätsdepot“** auf Seite 86

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 3.0.1 für Identity Manager 3.6*.

- 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 3.0.1 aufrüsten, müssen Sie einen neuen Speicherort für den Arbeitsbereich erstellen. Weitere Informationen finden Sie unter „Exportieren eines Projekts“ im *Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6*.

Erstellen eines neuen Projekts aus dem Identitätsdepot

Wenn Sie kein Designer-Projekt Ihrer Identity Manager-Lösung haben, gehen Sie folgendermaßen vor:

- 1 Laden Sie Designer 3.0.1 herunter und installieren Sie es.
Sie können ein Identity Manager 3.6.x-Projekt mit Designer 3.0.1 erstellen. Weitere Informationen finden Sie unter **Abschnitt 7.1, „Installation von Designer“**, auf Seite 57.
- 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 des Authentifizierungsbenedutzers 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.

13.1.2 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 87
- ♦ „Exportieren der Treiberdaten mithilfe von iManager“ auf Seite 87

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 „**Importing a Library, a Driver Set, or Driver from the Identity Vault**“ (Importieren einer Bibliothek, eines Treibersatzes oder eines Treibers vom Identitätsdepot) im *Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6*.
- 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.

13.2 Anhalten der Treiber

Vor dem Upgrade der Dateien müssen die Treiber angehalten werden.

- [Abschnitt 13.2.1](#), „Anhalten der Treiber mithilfe von Designer“, auf Seite 88
- [Abschnitt 13.2.2](#), „Anhalten der Treiber mithilfe von iManager“, auf Seite 88

13.2.1 Anhalten der Treiber mithilfe von Designer

- 1 Wählen Sie das Objekt „Identitätsdepot“  in der Registerkarte *Gliederung*.
- 2 Klicken Sie in der Symbolleiste „Modellierer“ auf das Symbol *Alle Treiber anhalten* .
Alle im Projekt verwendeten Treiber werden angehalten.
- 3 Wählen Sie für die Treiber die manuelle Startoption aus, um zu vermeiden, dass die Treiber vor Abschluss des Upgrades 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.

13.2.2 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 des Upgrades 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.

13.3 Dateien unter Linux/UNIX in den richtigen Speicherorten ablegen

Bei einer Direktaufrüstung von eDirectory 8.7.3 auf eDirectory 8.8.5 werden die eDirectory-Dateien in unterschiedlichen Verzeichnissen gespeichert. Da Identity Manager installiert ist, kann eDirectory erst gestartet werden, wenn sich die erforderlichen Identity Manager-Dateien im entsprechenden Verzeichnis befinden. Führen Sie die folgenden Schritte aus, um die Dateien an den richtigen Speicherorten abzulegen:

- 1 Führen Sie nach der Aufrüstung von eDirectory auf 8.8.5 die Identity Manager-Installation mit dem folgenden Befehl aus:

```
./install.bin -i console -DCLUSTER_INSTALL=true
```

Dadurch werden die richtigen Dateien ohne Authentifizierung bei eDirectory hinzugefügt.

- 2 Geben Sie `ndsconfig upgrade` ein, um die eDirectory-Dateien aufzurüsten.

- 3 Überprüfen Sie, ob der folgende Eintrag in der Datei `nds.conf` vorhanden ist:

```
n4u.server.interfaces=<IP-Adresse>@<Port>
```

Beispiel:`n4u.server.interfaces=<IP-Adresse>@524`

Falls der Eintrag `n4u.server.interfaces` nicht vorhanden ist, müssen Sie ihn manuell festlegen. Führen Sie die folgenden Schritte aus, um „`n4u.server.interfaces`“ festzulegen:

1. Führen Sie zum Abrufen des `ncp`-Ports den folgenden Befehl aus:

```
ndsconfig get "n4u.server.interfaces"
```

Dieser Befehl gibt die `ncp`-Portnummer, z. B. `n4u.server.interfaces=@524`, zurück.

2. Führen Sie den folgenden Befehl aus, um `ndsconfig` für `n4u.server.interfaces` zu konfigurieren:

```
ndsconfig set n4u.server.interfaces=<IP-Adresse>@<Port>
```

Hierbei gilt:

<IP-Adresse> ist die IP-Adresse des Computers, auf dem eDirectory installiert ist.

<Port> ist die in Schritt 1 abgerufene `ncp`-Portnummer.

Beispiel:

```
ndsconfig set n4u.server.interfaces=<IP-Adresse>@524
```

- 4 Fahren Sie mit [Abschnitt 13.5, „Upgrade der Metaverzeichnis-Engine und der Treiberkonfigurationsdateien“](#), auf Seite 90 fort.

13.4 Upgrade von Designer

Exportieren Sie vor dem Upgrade 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 3.0.1 für Identity Manager 3.6*. Weitere Upgrade-Informationen finden Sie unter „[Converting Earlier Projects](#)“ (Konvertieren früherer Projekte) im *Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6*.

13.5 Upgrade der Metaverzeichnis-Engine und der Treiberkonfigurationsdateien

Nach dem Upgrade der unterstützenden Komponenten wird die Metaverzeichnis-Engine aufgerüstet. Während des Upgrades werden die im Dateisystem gespeicherten Treiberkonfigurationsdateien aktualisiert.

- 1 Stellen Sie sicher, dass alle Treiber angehalten wurden. Eine Anleitung dazu finden Sie in [Abschnitt 13.2, „Anhalten der Treiber“](#), auf Seite 88.
- 2 Installieren Sie Identity Manager 3.6.1.
Die Schritte für das Upgrade auf Identity Manager 3.6.1 sind identisch mit den Schritten für die Installation von Identity Manager 3.6.1. Eine Anleitung für die Installation von Identity Manager finden Sie in [Kapitel 7, „Installation von Identity Manager“](#), auf Seite 57.
Bei der Installation von Identity Manager 3.6.1 werden die vorherigen Identity Manager-Versionen überschrieben. Hierbei werden die Binärdateien aktualisiert, das Schema erweitert und die Treiberkonfigurationsdateien aktualisiert.

Hinweis: Wenn Sie Identity Manager von 32-Bit auf 64-Bit aufrüsten, funktionieren der Groupwise-Treiber und die nativen benutzerdefinierten Treiber nicht.

13.6 Upgrade des Remote Loaders

Wenn Sie den Remote Loader ausführen, müssen auch die Remote Loader-Dateien aufgerüstet werden.

- 1 Erstellen Sie eine Sicherung der Remote Loader-Konfigurationsdateien. Der Standard-Speicherort lautet:
 - ♦ **Windows:** `C:\Novell\RemoteLoader\Remote Loader-Name-config.txt`
 - ♦ **Linux:** Erstellen Sie im „rdxml“-Pfad Ihre eigene Konfigurationsdatei.
- 2 Stellen Sie sicher, dass alle Treiber angehalten wurden. Eine Anleitung dazu finden Sie in [Abschnitt 13.2, „Anhalten der Treiber“](#), auf Seite 88.
- 3 Halten Sie den Remote Loader-Service bzw. den Daemon für jeden Treiber an.
 - ♦ **Windows:** Wählen Sie in der Remote Loader-Konsole die Remote Loader-Instanz aus und klicken Sie anschließend auf *Anhalten*.
 - ♦ **Linux:** `rdxml -config Pfad_zur_Konfigurationsdatei -u`
 - ♦ **Java Remote Loader:** `dirxml_jremote -config Pfad_zur_Konfigurationsdatei -u`
- 4 Führen Sie die Installationsprogramme für den Remote Loader aus.
Durch den Installationsvorgang werden die Dateien und Binärdateien auf die aktuelle Version aufgerüstet. Weitere Informationen finden Sie in [Abschnitt 7.3, „Installation des Remote Loaders“](#), auf Seite 61.
- 5 Sobald die Installation abgeschlossen ist, stellen Sie sicher, dass Ihre Konfigurationsdateien die Informationen Ihrer Umgebung enthalten.
- 6 (Bedingt) Falls Sie Probleme mit der Konfigurationsdatei haben, kopieren Sie die in [Schritt 1](#) erstellte Sicherungsdatei. Fahren Sie anderenfalls fort mit [Schritt 7](#).

7 Starten Sie den Remote Loader-Service bzw. den Daemon für jeden Treiber.

- ♦ **Windows:** Wählen Sie in der Remote Loader-Konsole die Remote Loader-Instanz aus und klicken Sie anschließend auf *Starten*.
- ♦ **Linux:** `rdxml -config Pfad_zu_Konfigurationsdatei -sp Passwort Passwort`
- ♦ **Java Remote Loader:** `dirxml_jremote -config Pfad_zu_Konfigurationsdatei -sp Passwort Passwort`

Hinweis: Wenn Sie Remote Loader von 32-Bit auf 64-Bit aufrüsten, funktionieren der Groupwise-Treiber und die nativen benutzerdefinierten Treiber nicht.

13.7 Überlagern der neuen Treiberkonfigurationsdatei über den vorhandenen Treiber

Stellen Sie zunächst sicher, dass die Namen der benutzerdefinierten Richtlinien nicht mit denen der Standardrichtlinien übereinstimmen. Wenn eine Treiberkonfiguration mit einer neuen Treiberdatei überlagert wird, werden die vorhandenen Richtlinien jeweils überschrieben. Benutzerdefinierte Richtlinien ohne eindeutigen Namen werden verworfen.

Überlagern Sie die neue Treiberkonfigurationsdatei über Ihren vorhandenen Treiber, um ihn mit den neuen Richtlinien oder Funktionen in der Treiberkonfigurationsdatei zu aktualisieren.

- ♦ [Abschnitt 13.7.1, „Überlagern der neuen Treiberkonfigurationsdatei über den vorhandenen Treiber mithilfe von Designer“, auf Seite 91](#)
- ♦ [Abschnitt 13.7.2, „Überlagern der neuen Treiberkonfigurationsdatei über den vorhandenen Treiber mithilfe von iManager“, auf Seite 92](#)

13.7.1 Überlagern der neuen Treiberkonfigurationsdatei über den vorhandenen Treiber mithilfe von Designer

- 1 Klicken Sie im Modellierer mit der rechten Maustaste auf die Treiberlinie des aufzurüstenden Treibers.
- 2 Wählen Sie *Konfigurationsassistenten starten*.
- 3 Klicken Sie auf der Warnungsseite auf *Ja*.

Mit dieser Warnung werden Sie darüber informiert, dass alle Treibereinstellungen und -richtlinien zurückgesetzt werden.

Wichtig: Stellen Sie sicher, dass die Namen der benutzerdefinierten Richtlinien nicht mit denen der Standardrichtlinien übereinstimmen, damit keine Daten verloren gehen.

- 4 Wählen Sie die Treiberkonfiguration für den aufzurüstenden Treiber aus und klicken Sie anschließend auf *Ausführen*.
- 5 Geben Sie die Treiberinformationen ein und klicken Sie anschließend auf *Weiter*.
Möglicherweise müssen mehrere Seiten mit Informationen angegeben werden.
- 6 Klicken Sie auf der Ergebnisseite auf *OK*.

- 7 Überprüfen Sie, ob die Treiberparameter und -richtlinien wie gewünscht eingerichtet sind.
- 8 Wenn Sie benutzerdefinierte Richtlinien verwenden, fahren Sie mit [Abschnitt 13.8, „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“](#), auf [Seite 92](#) fort. Fahren Sie anderenfalls mit [Abschnitt 13.10, „Starten der Treiber“](#), auf [Seite 95](#) fort.

13.7.2 Überlagern der neuen Treiberkonfigurationsdatei über den vorhandenen 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 > Treiber hinzufügen* und dann auf *Weiter* auf der Seite des Assistenten für neue Treiber.
- 5 Wählen Sie die zu überlagernde Treiberkonfiguration aus und klicken Sie anschließend auf *Weiter*.
- 6 Wählen Sie im Feld *Vorhandene Treiber* den aufzurüstenden Treiber aus und markieren Sie ihn.
- 7 Geben Sie die Treiberinformationen ein und klicken Sie anschließend auf *Weiter*.
- 8 Wählen Sie auf der Zusammenfassungsseite *Diesen Treiber und die Richtlinienbibliotheken insgesamt aktualisieren*.

Wichtig: Stellen Sie sicher, dass alle benutzerdefinierten Richtlinien einen anderen Namen haben als die Standardrichtlinien, damit keine Daten verloren gehen.

- 9 Klicken Sie auf *Weiter* und dann auf *Fertig stellen* auf der Zusammenfassungsseite.
- 10 Überprüfen Sie, ob die Treiberparameter und -richtlinien wie gewünscht eingerichtet sind.
- 11 Wenn Sie benutzerdefinierte Richtlinien verwenden, fahren Sie mit [Abschnitt 13.8, „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“](#), auf [Seite 92](#) fort. Fahren Sie anderenfalls mit [Abschnitt 13.10, „Starten der Treiber“](#), auf [Seite 95](#) fort.

13.8 Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber

Wenn Sie benutzerdefinierte Richtlinien oder Regeln verwenden, müssen Sie 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 13.8.1, „Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von Designer“](#), auf [Seite 93](#)
- ♦ [Abschnitt 13.8.2, „Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von iManager“](#), auf [Seite 94](#)

13.8.1 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 93
- ♦ „Hinzufügen einer benutzerdefinierten Richtlinie über die Ansicht „Richtlinienfluss anzeigen““ auf Seite 93

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 13.10, „Starten der Treiber“**, auf Seite 95. 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 3.0* (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 13.10, „Starten der Treiber“**, auf Seite 95. 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 3.0* (Richtlinien in Designer 3.0).
- 9 Wenn Sie überprüft haben, dass die Richtlinien funktionieren, können Sie den Treiber in der Produktionsumgebung einsetzen.

13.8.2 Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den 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, 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 13.10, „Starten der Treiber“**, auf Seite 95. 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.

13.9 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 3.0.1 für Identity Manager 3.6*.

13.10 Starten der Treiber

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

- ♦ [Abschnitt 13.10.1, „Starten der Treiber mithilfe von Designer“, auf Seite 95](#)
- ♦ [Abschnitt 13.10.2, „Starten der Treiber mithilfe von iManager“, auf Seite 95](#)

13.10.1 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 3.0* (Richtlinien in Designer 3.0).

13.10.2 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 Richtliniensimulator. Lösen Sie zum Testen der Richtlinien Ereignisse aus, durch die die Richtlinien ausgeführt werden. Sie können z. B. einen Benutzer erstellen, ändern oder löschen.

Durchführen einer Migration

14

Informieren Sie sich vor dem Beginn über die Unterschiede zwischen der Direktaufrüstung und der Migration. Weitere Informationen hierzu finden Sie unter **Kapitel 12, „Direktaufrüstung im Vergleich zu Migration“**, auf Seite 81.

Verwenden Sie die folgende Checkliste, um zu überprüfen, ob alle Schritte in der richtigen Reihenfolge abgeschlossen wurden, damit eine erfolgreiche Migration des Identity Manager-Systems sichergestellt werden kann. Führen Sie folgende Schritte für jeden Identity Manager-Server in Ihrer Umgebung aus.

- Erstellen Sie ein Backup der aktuellen Konfiguration Ihrer Identity Manager-Lösung. Exportieren Sie hierzu Ihre Treiber oder erstellen Sie ein Designer-Projekt Ihrer Identity Manager-Lösung. Weitere Informationen finden Sie in **Abschnitt 13.1, „Backup der aktuellen Konfiguration erstellen“**, auf Seite 85.
- Installieren Sie die gewünschten Betriebssysteme. Eine Liste der unterstützten Plattformen finden Sie unter **Kapitel 6, „Systemanforderungen“**, auf Seite 47.
- Installieren Sie eDirectory™ 8.8.5 auf dem Server. Weitere Informationen finden Sie im *eDirectory/Installationshandbuch* (<http://www.novell.com/documentation/edir88/index.html>).
- Fügen Sie diesem neuen Server die gleichen eDirectory-Reproduktionen hinzu, die sich auf dem aktuellen Identity Manager-Server befinden. Weitere Informationen finden Sie unter **„Administering Replicas“** (<http://www.novell.com/documentation/edir88/edir88/data/fbgciad.html>) (Verwalten von Reproduktionen) im *eDirectory Administrationshandbuch* (<http://www.novell.com/documentation/edir88/pdfdoc/edir88/edir88.pdf>).
- Installieren Sie Identity Manager 3.6.1. Verwenden Sie **Kapitel 4, „Basis-Checkliste für das Identity Manager-System“**, auf Seite 41, um zu überprüfen, ob alle Schritte durchgeführt wurden.
- Wenn es sich bei einem der Treiber im Treibersatz um Remote Loader-Treiber handelt, rüsten Sie den Remote Loader-Server für jeden Treiber auf. Weitere Informationen finden Sie in **Abschnitt 13.6, „Upgrade des Remote Loaders“**, auf Seite 90.
- (Bedingt) Wenn es sich bei dem alten Server um Ihren Benutzeranwendungs-Server handelt, führen Sie die folgenden zusätzlichen Schritte aus:
 - Der Benutzeranwendungstreiber muss in Designer migriert werden. Weitere Informationen finden Sie im *Migrationshandbuch des rollenbasierten Bereitstellungsmoduls* (<http://www.novell.com/documentation/idmrpbpm361/index.html>).
 - Erstellen Sie einen neuen Rollenservice-Treiber. Der Rollenservice-Treiber wird nicht migriert. Wenn Sie einen vorhandenen Rollenservice-Treiber für Version 3.6.1 haben, müssen Sie einen neuen Treiber für Version 3.6.1 erstellen. Weitere Informationen finden Sie im *Migrationshandbuch des rollenbasierten Bereitstellungsmoduls* (<http://www.novell.com/documentation/idmrpbpm361/index.html>).
 - Stellen Sie den migrierten Benutzeranwendungstreiber im Identitätsdepot bereit. Weitere Informationen finden Sie im *Migrationshandbuch des rollenbasierten Bereitstellungsmoduls* (<http://www.novell.com/documentation/idmrpbpm361/index.html>).
 - Installieren Sie die Benutzeranwendung auf diesem neuen Server. Weitere Informationen finden Sie im *Installationshandbuch des rollenbasierten Bereitstellungsmoduls* (<http://www.novell.com/documentation/idmrpbpm361/install/data/bookinfo.html>).

- ❑ Fügen Sie den neuen Server zum Treibersatz hinzu. Weitere Informationen finden Sie in [Abschnitt 14.1, „Hinzufügen des neuen Servers zum Treibersatz“](#), auf Seite 98.
- ❑ Ändern Sie die serverspezifischen Informationen für jeden Treiber. Weitere Informationen finden Sie in [Abschnitt 14.2, „Ändern der serverspezifischen Informationen“](#), auf Seite 99.
- ❑ (Bedingt) Führen Sie `configupdate.sh` oder `configupdate.bat` aus, um für die Konfiguration der Benutzeranwendung die serverspezifischen Informationen des alten Servers auf den neuen Server zu ändern. Weitere Informationen finden Sie unter „[Benutzeranwendung - Konfigurationsreferenz](#)“ (<http://www.novell.com/documentation/idmrpbm361/install/data/bb1zmw0.html>) im *Installationshandbuch des rollenbasierten Bereitstellungsmoduls* (<http://www.novell.com/documentation/idmrpbm361/install/data/bookinfo.html>).
- ❑ (Optional) Überlagern Sie die neuen Treiberkonfigurationsdateien über die vorhandenen Treiber, um neue Richtlinien zu erhalten. Dies ist nur dann erforderlich, wenn in den Richtlinien eines Treibers neue Funktionalität enthalten ist, die Sie zu Ihrem vorhandenen Treiber hinzufügen möchten. Weitere Informationen finden Sie in [Abschnitt 13.7, „Überlagern der neuen Treiberkonfigurationsdatei über den vorhandenen Treiber“](#), auf Seite 91.
- ❑ (Optional) Stellen Sie die benutzerdefinierten Richtlinien und Regeln auf den Treibern wieder her. Wenn Sie die neuen Treiberkonfigurationsdateien überlagern, werden die Richtlinien überschrieben, sodass eine Wiederherstellung der Richtlinien nur erforderlich ist, wenn Sie eine Überlagerung der neuen Treiberkonfigurationsdatei durchgeführt haben. Weitere Informationen finden Sie in [Abschnitt 13.8, „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“](#), auf Seite 92.
- ❑ Entfernen Sie den alten Server aus dem Treibersatz. Weitere Informationen finden Sie in [Abschnitt 14.3, „Entfernen des alten Servers aus dem Treibersatz“](#), auf Seite 100.
- ❑ Bei Verwendung von Novell Sentinel™ müssen Sie eine Aktualisierung auf Novell Sentinel 6.1 vornehmen. Weitere Informationen zur Aktualisierung von Sentinel finden Sie im Installationshandbuch zu *Sentinel* (http://www.novell.com/documentation/sentinel6/pdfdoc/sentinel6_installationguide.pdf).
- ❑ Aktivieren Sie die Metaverzeichnis-Engine und die aufgerüsteten Treiber. Weitere Informationen finden Sie in [Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“](#), auf Seite 69.

14.1 Hinzufügen des neuen Servers zum Treibersatz

Wenn Sie iManager verwenden, müssen Sie den neuen Server zum Treibersatz hinzufügen. Designer enthält einen Migrationsassistenten für den Server, der diesen Schritt für Sie durchführt. Wenn Sie Designer verwenden, fahren Sie mit [Abschnitt 14.2, „Ändern der serverspezifischen Informationen“](#), auf Seite 99 fort. Wenn Sie iManager verwenden, führen Sie die folgenden Schritte durch:

- 1 Klicken Sie in iManager auf , um die Identity Manager-Verwaltungsseite anzuzeigen.
- 2 Klicken Sie auf *Identity Manager-Überblick*.
- 3 Suchen Sie den Container, der den Treibersatz enthält und wählen Sie ihn aus.
- 4 Klicken Sie auf den Treibersatznamen, um auf die Seite „Treibersatz-Überblick“ zuzugreifen.
- 5 Klicken Sie auf *Server > Server hinzufügen*.
- 6 Suchen Sie den neuen Identity Manager 3.6.1-Server, wählen Sie ihn aus und klicken Sie anschließend auf *OK*.

14.2 Ändern der serverspezifischen Informationen

Sie müssen alle serverspezifischen Informationen, die in jedem Treiber gespeichert sind, auf die Informationen des neuen Servers ändern. Die serverspezifischen Informationen sind enthalten in:

- ♦ Globalkonfigurationswerte
- ♦ Engine-Steuerungswerte
- ♦ Benannte Passwörter
- ♦ Treiberauthentifizierungsinformationen
- ♦ Treiber-Startoptionen
- ♦ Treiberparameter

Dies erfolgt in Designer oder in iManager. Wenn Sie Designer verwenden, ist es ein automatisierter Prozess. Wenn Sie iManager verwenden, ist es ein manueller Prozess.

- ♦ [Abschnitt 14.2.1, „Ändern der serverspezifischen Informationen in Designer“](#), auf Seite 99
- ♦ [Abschnitt 14.2.2, „Ändern der serverspezifischen Informationen in iManager“](#), auf Seite 100

14.2.1 Ändern der serverspezifischen Informationen in Designer

Das Verfahren betrifft alle Treiber, die im Treibersatz gespeichert sind.

- 1 Öffnen Sie Ihr Projekt in Designer.
- 2 Klicken Sie in der Registerkarte *Gliederung* mit der rechten Maustaste auf den Server und wählen Sie anschließend *Migrieren*.
- 3 Lesen Sie den Überblick, damit Sie sehen, welche Elemente auf den neuen Server migriert werden, und klicken Sie anschließend auf *Weiter*.
- 4 Wählen Sie den Zielserver aus der Liste der verfügbaren Server aus und klicken Sie anschließend auf *Weiter*.

Es werden nur die Server aufgelistet, die momentan nicht mit einem Treibersatz verknüpft sind und deren Version gleich der oder neuer als die Version des Identity Manager-Ursprungsservers ist.

- 5 Wählen Sie *Zielserver aktiv machen*.

Es stehen drei Optionen zur Verfügung, aber *Zielserver aktiv machen* wird empfohlen.

- ♦ **Zielserver aktiv machen:** Kopiert die Einstellungen vom Ursprungsserver auf den Zielserver und deaktiviert die Treiber auf dem Ursprungsserver.
- ♦ **Ursprungsserver aktiv lassen:** Kopiert die Einstellungen nicht und deaktiviert alle Treiber auf dem Zielserver.
- ♦ **Ziel- und Ursprungsserver aktiv machen:** Kopiert die Einstellungen vom Ursprungsserver auf den Zielserver, ohne die Treiber auf dem Ursprungs- oder Zielserver zu deaktivieren. Diese Option wird nicht empfohlen. Wenn beide Treiber gestartet wurden, werden die gleichen Informationen in zwei verschiedene Warteschlangen geschrieben, was zu Beschädigungen führen kann.

- 6 Klicken Sie auf *Migrieren*.

Nachdem die serverspezifischen Informationen migriert wurden, müssen Sie die geänderten Treiber im Identitätsdepot bereitstellen. Weitere Informationen finden Sie unter „[Bereitstellen eines Treibers in einem Identitätsdepot](#)“ im *Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6*.

Der letzte Schritt ist das Starten der Treiber. Weitere Informationen finden Sie in [Abschnitt 13.10](#), „[Starten der Treiber](#)“, auf [Seite 95](#).

14.2.2 Ändern der serverspezifischen Informationen in iManager

- 1 Klicken Sie in iManager auf , um die Identity Manager-Verwaltungsseite anzuzeigen.
- 2 Klicken Sie auf *Identity Manager-Überblick*.
- 3 Suchen Sie den Container, der den Treibersatz enthält, und wählen Sie ihn aus.
- 4 Klicken Sie auf den Treibersatznamen, um auf die Seite „Treibersatz-Überblick“ zuzugreifen.
- 5 Klicken Sie auf die obere rechte Ecke des Treibers und klicken Sie anschließend auf *Treiber anhalten*.
- 6 Klicken Sie auf die obere rechte Ecke des Treibers und klicken Sie anschließend auf *Eigenschaften bearbeiten*.
- 7 Sie müssen für jeden Treiberparameter, jeden Globalkonfigurationswert, jeden Engine-Steuerungswert, jedes benannte Passwort, jede Treiberauthentifizierungsinformation und jede Treiber-Startoption die Informationen des alten Servers in die des neuen Servers ändern.
- 8 Klicken Sie zum Speichern aller Änderungen auf *OK*.
- 9 Klicken Sie auf die obere rechte Ecke des Treibers, um ihn zu starten.
- 10 Wiederholen Sie [Schritt 5](#) bis [Schritt 9](#) für jeden Treiber im Treibersatz.

14.3 Entfernen des alten Servers aus dem Treibersatz

Wenn der neue Server alle Treiber ausführt, muss der alte Server aus dem Treibersatz entfernt werden.

- ♦ [Abschnitt 14.3.1](#), „[Mithilfe von Designer den alten Server aus dem Treibersatz entfernen](#)“, auf [Seite 100](#)
- ♦ [Abschnitt 14.3.2](#), „[Mithilfe von iManager den alten Server aus dem Treibersatz entfernen](#)“, auf [Seite 101](#)
- ♦ [Abschnitt 14.3.3](#), „[Stilllegen des alten Servers](#)“, auf [Seite 101](#)

14.3.1 Mithilfe von Designer den alten Server aus dem Treibersatz entfernen

- 1 Öffnen Sie Ihr Projekt in Designer.
- 2 Klicken Sie im Modellierer mit der rechten Maustaste auf den Treibersatz und wählen Sie anschließend *Eigenschaften*.
- 3 Wählen Sie *Serverliste*.

- 4 Wählen Sie den alten Identity Manager-Server in der Liste *Server auswählen* aus und klicken Sie anschließend auf „<“, um den Server aus der Liste *Server auswählen* zu entfernen.
- 5 Klicken Sie zum Speichern der Änderungen auf *OK*.

Diese Änderung muss im Identitätsdepot bereitgestellt werden. Weitere Informationen finden Sie unter „[Bereitstellen eines Treibersatzes in einem Identitätsdepot](#)“ im *Administrationshandbuch zu Designer 3.0.1 für Identity Manager 3.6*.

14.3.2 Mithilfe von iManager den alten Server aus dem Treibersatz entfernen

- 1 Klicken Sie in iManager auf , um die Identity Manager-Verwaltungsseite anzuzeigen.
- 2 Klicken Sie auf *Identity Manager-Überblick*.
- 3 Suchen Sie den Container, der den Treibersatz enthält und wählen Sie ihn aus.
- 4 Klicken Sie auf den Treibersatznamen, um auf die Seite „Treibersatz-Überblick“ zuzugreifen.
- 5 Klicken Sie auf *Server > Server entfernen*.
- 6 Wählen Sie den alten Identity Manager-Server aus und klicken Sie anschließend auf *OK*.

14.3.3 Stilllegen des alten Servers

Zu diesem Zeitpunkt hostet der alte Server keine Treiber mehr. Wenn Sie diesen Server nicht mehr benötigen, müssen Sie zusätzliche Schritte unternehmen, um diesen Server stillzulegen:

- 1 Entfernen Sie die eDirectory-Reproduktionen von diesem Server. Weitere Informationen finden Sie unter „[Deleting Replicas](http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html)“ (<http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html>) (Reproduktionen löschen) im *eDirectory Administrationshandbuch* (<http://www.novell.com/documentation/edir88/pdfdoc/edir88/edir88.pdf>).
- 2 Entfernen Sie eDirectory von diesem Server. Weitere Informationen finden Sie unter TID 10056593, „[Removing a Server From an NDS Tree Permanently](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=10056593&sliceId=&docTypeID=DT_TID_1_1&dialogID=35218849&stateId=0%20%202035214815)“ (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=10056593&sliceId=&docTypeID=DT_TID_1_1&dialogID=35218849&stateId=0%20%202035214815).

Deinstallation von Identity Manager

IV

Wenn Sie Identity Manager deinstallieren müssen, führen Sie die in den folgenden Abschnitten beschriebenen Verfahren in der angegebenen Reihenfolge durch.

- ♦ [Kapitel 15, „Entfernen von Objekten aus eDirectory“, auf Seite 105](#)
- ♦ [Kapitel 16, „Deinstallation des Metaverzeichnis-Servers und der Treiber“, auf Seite 107](#)
- ♦ [Kapitel 17, „Deinstallation von Designer“, auf Seite 109](#)

Entfernen von Objekten aus eDirectory

15

Im ersten Schritt der Deinstallation von Identity Manager müssen alle Identity Manager-Objekte aus dem Identitätsdepot gelöscht werden. Wenn es sich bei einem der Treibersatzobjekte um Stammobjekte der Partition in eDirectory™ handelt, muss die Partition mit der übergeordneten Partition zusammengeführt werden, bevor das Treibersatzobjekt gelöscht werden kann. Wenn der Treibersatz erstellt wird, fordert Sie der Assistent dazu auf, eine eigene Partition für den Treibersatz zu erstellen.

So können die Identity Manager-Objekte gelöscht werden:

- 1** Führen Sie eine Zustandsüberprüfung der eDirectory-Datenbank aus. Falls Fehler auftreten, beheben Sie diese, bevor Sie fortfahren. Weitere Informationen hierzu finden Sie unter [Keeping eDirectory Healthy \(http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html\)](http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html) (Funktionsfähigkeit von eDirectory aufrechterhalten) im *Novell eDirectory 8.8 Administrationshandbuch*.
- 2** Melden Sie sich bei iManager als Administrator mit vollständigen Berechtigungen für die eDirectory-Baumstruktur an.
- 3** Wählen Sie für Partitionen und Reproduktionen die Option zum Zusammenführen von Partitionen aus.
- 4** Wechseln Sie zum Treibersatzobjekt, das das root-Objekt der Partition ist, und markieren Sie es. Klicken Sie anschließend auf *OK*.
- 5** Warten Sie, bis der Zusammenführungsprozess abgeschlossen ist, und klicken Sie anschließend auf *OK*.
- 6** Löschen Sie das Treibersatzobjekt.
Wenn Sie das Treibersatzobjekt löschen, werden alle mit diesem Treibersatz verknüpften Treiberobjekte gelöscht.
- 7** Wiederholen Sie **Schritt 3** bis **Schritt 6** für alle Treibersatzobjekte in der eDirectory-Datenbank, bis alle gelöscht wurden.
- 8** Wiederholen Sie **Schritt 1**, um sicherzustellen, dass alle Zusammenführungen abgeschlossen sind und alle Objekte gelöscht wurden.

Fahren Sie mit **Kapitel 16**, „Deinstallation des Metaverzeichnis-Servers und der Treiber“, auf **Seite 107** fort.

Deinstallation des Metaverzeichnis-Servers und der Treiber

Wenn Identity Manager installiert ist, wird ein Deinstallationskript auf dem Identity Manager-Server abgelegt. Mithilfe des Skripts können Sie alle Services, Pakete und Verzeichnisse entfernen, die bei der Installation von Identity Manager erstellt wurden.

- ♦ [Abschnitt 16.1, „Deinstallation unter Windows“, auf Seite 107](#)
- ♦ [Abschnitt 16.2, „Deinstallation unter Linux/UNIX“, auf Seite 107](#)

16.1 Deinstallation unter Windows

So deinstallieren Sie Identity Manager unter Windows:

- ♦ Führen Sie für die 32-Bit-Version von Windows eine der folgenden Schritte aus:
 - ♦ Öffnen Sie auf dem Windows-Server die Systemsteuerung. Klicken Sie für Windows Server 2003 auf *Software*. Klicken Sie für Windows Server 2008 auf *Programme und Funktionen*.

Hinweis: Sie können diese Schritte nicht für Windows Server 2008 Server Core ausführen.

- ♦ Führen Sie das Skript zum Deinstallieren (`Uninstall Identity Manager.exe`) aus, das sich unter `C:\Programme\Novell\Identity Manager\Uninstall_Identity_Manager` befindet.
- ♦ Verwenden Sie für die 64-Bit-Version von Windows eines der folgenden Verfahren:
 - ♦ Öffnen Sie auf dem Windows-Server die Systemsteuerung. Klicken Sie für Windows Server 2003 auf *Software*. Klicken Sie für Windows Server 2008 auf *Programme und Funktionen*.

Hinweis: Sie können diese Schritte nicht für Windows Server 2008 Server Core ausführen.

- ♦ Führen Sie das Skript zum Deinstallieren (`Uninstall Identity Manager.exe`) aus, das sich unter `C:\Programme (x86)\Novell\Identity Manager\Uninstall_Identity_Manager` befindet.

16.2 Deinstallation unter Linux/UNIX

Führen Sie zur Deinstallation von Identity Manager unter Linux/UNIX das Deinstallationskript aus, das sich unter `~/idm/Uninstall_Identity_Manager/Uninstall_Identity_Manager` befindet. Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben:

```
./Uninstall_Identity_Manager.
```


Deinstallation von Designer

17

Die Deinstallation von Designer verläuft ähnlich wie die Deinstallation des Metaverzeichnis-Servers und -Treibers.

- ♦ Wählen Sie unter Windows in der Systemsteuerung die Option *Software*.
- ♦ Führen Sie unter Linux/UNIX das Deinstallationskript aus, das sich unter `~/designer/UninstallDesigner/Uninstall_Designer_for_Identity_Manager` befindet.

