Novell Identity Manager

3.5.1

www.novell.com

INSTALLATIONSHANDBUCH

28. September 2007

Novell®

Rechtliche Hinweise

Novell, Inc. übernimmt für Inhalt oder Verwendung dieser Dokumentation keine Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der 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 jegliche ausdrückliche oder stillschweigende 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 genannte 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). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Novell, Inc. besitzt gewerbliche Schutzrechte 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/) 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
U.S.A.
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).

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).

Materialien von Drittanbietern

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

Inhalt

Informationen zu dieser Dokumentation

Novell® Identity Manager, vormals DirXML®, ist ein Service für die Datenfreigabe und -synchronisierung, mit dessen Hilfe Anwendungen, Verzeichnisse und Datenbanken Informationen gemeinsam nutzen können. Es 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 einen Überblick über die Identity Manager-Technologien und eine Beschreibung der Installations-, Administrations- und Konfigurationsfunktionen von Identity Manager.

- Kapitel 1, „Überblick“, auf Seite 11
- Kapitel 2, „Planung“, auf Seite 39
- Kapitel 3, „Upgrades“, auf Seite 61
- Kapitel 4, „Installation von Identity Manager“, auf Seite 67
- Kapitel 5, „Installation der Benutzeranwendung“, auf Seite 99
- Kapitel 6, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 193

Zielgruppe

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

Aktualisierungen für Dokumentationen

Die neueste Version dieses Dokuments finden Sie auf der Website zur Identity Manager-Dokumentation (http://www.novell.com/documentation/idm35/index.html).

Zusätzliche Dokumentation

Die Dokumentation für andere Identity Manager-Treiber finden Sie auf der Website für Identity Manager-Treiber (http://www.novell.com/documentation/idm35drivers/index.html).

Konventionen in der Dokumentation

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

Ein Markensymbol (®, ™ usw.) kennzeichnet eine Marke von Novell. 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.

Überblick

1

1.1 Einführung in Identity Manager

Novell® Identity Manager ist eine vielfach ausgezeichnete Lösung für die Datenfreigabe und -synchronisierung, die die Verwaltung von Daten revolutioniert. Dieser Service verwendet eine zentrale Datenablage, das Identitätsdepot, um Daten anwendungs-, datenbank- und verzeichnisübergreifend zu synchronisieren, zu transformieren und zu verteilen.

Aber Identity Manager kann noch viel mehr. Zu den Funktionen von Identity Manager gehören:

- Passwortsynchronisierung
- Passwort-Selbstbedienung
- Services für die Protokollierung und Revision
- Benutzerverwaltung mithilfe der Benutzeranwendung
- Workflow-Bereitstellung
- Email-Benachrichtigung
- Entwerfen von Treibern und Richtlinien im Dienstprogramm „Designer“

Weitere Informationen zu neuen Funktionen dieser Komponenten in dieser Version von Identity Manager finden Sie in Abschnitt 1.3, „Neuerungen in Identity Manager 3.5.1“, auf Seite 14. Eine ausführlichere Anzeige der unterschiedlichen Komponenten und Services, aus denen Identity Manager besteht, finden Sie in Abschnitt 1.4, „Identity Manager - Installationsprogramme und Services“, auf Seite 19.

Mithilfe von Identity Manager kann ein verbundenes System (u. a. SAP*, PeopleSoft*, Lotus* Notes*, Microsoft* Exchange und Active Directory*) folgende Funktionen ausführen:

- Gemeinsame Nutzung von Daten über das Identitätsdepot.
- Synchronisieren und Transformieren gemeinsam genutzter Daten mit dem Identitätsdepot, wenn die Daten auf verbundenen Systemen geändert werden.
- Synchronisieren und Transformieren gemeinsam genutzter Daten mit den verbundenen Systemen, wenn die Daten im Identitätsdepot geändert werden.

Identity Manager stellt diese Funktionen im Rahmen eines bidirektionalen Frameworks zur Verfügung, über das Administratoren die Daten angeben können, die vom Identitätsdepot zur Anwendung und von der Anwendung zum Identitätsdepot fließen. Mittels XML liefert das

Framework Daten- und Ereignisübersetzungsfunktionen, die Identitätsdepot-Daten und -Ereignisse in das angegebene anwendungsspezifische Format konvertieren. Außerdem werden anwendungsspezifische Formate in ein Format konvertiert, das vom Identitätsdepot erkannt wird. Alle Interaktionen mit der Anwendung nutzen dabei die anwendungseigene API.

Identity Manager lässt nur die Auswahl von Attributen und Klassen zu, die spezifischen Datensätzen und Feldern des verbundenen Systems entsprechen. Für eine Verzeichnisdatenablage kann beispielsweise festgelegt werden, dass Objekte des Typs „Benutzer“ gemeinsam mit einer Personaldatenablage genutzt werden, Netzwerkressourcenobjekte wie Server, Drucker und Volumes jedoch nicht. Die Personaldatenablage kann wiederum die angegebenen Namen, Nachnamen, Initialien, Telefonnummern und Standorte eines Benutzers gemeinsam mit anderen Personen nutzen, jedoch nicht Daten des Benutzers, die von persönlicher Natur sind (z. B. Angaben zur Familie oder seine Personalakte).

Wenn das Identitätsdepot keine Klassen oder Attribute für von anderen Anwendungen gemeinsam genutzte Daten hat, können Sie das eDirectory™-Schema dahingehend erweitern. In diesem Fall wird aus dem Identitätsdepot eine Ablage von Informationen, die vom Identitätsdepot nicht benötigt werden, die aber von anderen Anwendungen verwendet werden können. Die anwendungsspezifische Datenablage verwaltet die Informationen, die nur von der Anwendung benötigt werden.

Identity Manager führt die folgenden Aufgaben aus:

- Anhand von Ereignissen Änderungen im Identitätsdepot erfassen.
- Datenverwaltung zentralisieren oder nach Aufgabenbereichen aufteilen, wobei Identity Manager als zentrale Sammelstelle dient, in der alle Daten zusammenlaufen.
- Directory-Daten werden im XML-Format bereitgestellt, damit diese von XML-Anwendungen oder von durch Identity Manager integrierte Anwendungen verarbeitet und gemeinsam genutzt werden können.
- Verknüpfungen zwischen Identitätsdepot-Objekten und Objekten in allen anderen integrierten Systemen werden sorgfältig verwaltet, um zu gewährleisten, dass Datenänderungen in allen verbundenen Systemen entsprechend implementiert werden.

Richtlinien bilden die Grundlage für die Datensynchronisierung. In einer Richtlinie kann Folgendes festgelegt werden:

- Der Datenfluss wird durch spezielle Filter gesteuert, die im System definierte Datenelemente beeinflussen.
- Mithilfe von Berechtigungen und Filtern wird sichergestellt, dass die Datenquellen autorisiert sind.
- Regeln werden auf XML-Daten der Datenablage angewendet. Diese Regeln bestimmen die Interpretation und die Umwandlung der Daten bei der Übertragung von Änderungen in DirXML.
- Die Daten aus XML werden in praktisch jedes beliebige Format konvertiert. Dadurch erhält Identity Manager die Möglichkeit, Daten mit jeder beliebigen Anwendung gemeinsam zu nutzen.

Mit Identity Manager können Sie in Ihrem Unternehmen Prozesse im Personalwesen vereinfachen, Kosten für die Datenverwaltung reduzieren, Kundenbeziehungen mithilfe äußerst flexibler Services aufbauen und Barrieren für die Interoperabilität entfernen, die den Erfolg beeinträchtigen. Im Folgenden finden Sie eine Liste mit Beispielen für Aktivitäten, die mit Identity Manager möglich sind:

Tabelle 1-1 *Nutzen durch Identity Manager*

Aktivität	Identity Manager-Lösung
Benutzerkonten verwalten	Mit einer einzigen Aktion haben Sie folgende Möglichkeiten: Identity Manager kann einem Mitarbeiter sofort Zugriff auf Ressourcen erteilen bzw. entziehen. Identity Manager verfügt über eine Funktion zur automatisierten Mitarbeiterbereitstellung, mit deren Hilfe einem neuen Mitarbeiter u. a. Zugriff auf das Netzwerk, Emails, Anwendungen und Ressourcen gewährt werden kann. Mithilfe der Workflow-Bereitstellung kann dieser Prozess so eingerichtet werden, dass ein Genehmigungsvorgang eingeleitet wird. Identity Manager kann auch bei Kündigung oder Beurlaubung den Zugriff einschränken oder deaktivieren.
Aufzeichnen und Integrieren von Bestandsinventar	Identity Manager kann für alle Elemente des Bestandsinventars (z. B. Computer, Monitore, Telefone, Bibliotheksbestand, Stühle und Schreibtische) Profile im Identitätsdepot erstellen und diese mit Benutzerprofilen, z. B. Personen, Abteilungen und Organisationen, integrieren.
Automatisieren von White/Yellow Page-Verzeichnissen	Identity Manager kann vereinheitlichte Verzeichnisse mit unterschiedlichen Informationsebenen für die interne und externe Verwendung erstellen. In externen Verzeichnissen werden beispielsweise nur Email-Adressen angezeigt, während die internen Verzeichnisse u. a. Ort, Telefon-, Fax- sowie Handynummer und die Privatadresse enthalten können.
Erweiterung von Benutzerprofilen	Identity Manager erweitert die Benutzerprofile, indem Informationen wie beispielsweise Email-Adresse, Telefonnummer, Adresse, Einstellungen, Vorgesetztenverhältnisse, Hardware-Bestand, Telefon, Schlüssel und Inventar hinzugefügt oder synchronisiert werden können.
Vereinheitlichung des Kommunikationszugriffs	Identity Manager vereinfacht den Zugriff auf das Netzwerk, Telefone, Pager, das Internet oder den kabellosen Zugriff für einzelne Benutzer oder Gruppen, indem die einzelnen Verzeichnisse zu einer gemeinsamen Verwaltungsoberfläche zusammengeführt werden.
Festigen von Partnerbeziehungen	Identity Manager festigt Beziehungen durch die Erstellung von Profilen (z. B. „Mitarbeiter“ oder „Kunde“) in Partnersystemen außerhalb der Firewall, sodass Partner bei Bedarf unmittelbar eine Serviceleistung anbieten können.
Verbesserung der Versorgungskette	Identity Manager verbessert den Kundendienst, da Instanzen von mehreren Konten pro Kunde erkannt und zusammengeführt werden.
Aufbau von Kundenloyalität	Identity Manager bietet neue Services, die die Anforderungen des Kunden berücksichtigen, der sich seine Daten im Zusammenhang und an einem einzigen Ort anzeigen lassen will, anstatt sie sich einzeln in verschiedenen Anwendungen zusammensuchen zu müssen.

Aktivität	Identity Manager-Lösung
Anpassen des Services	In Identity Manager verfügen Benutzer (z. B. Mitarbeiter, Kunden oder Partner) über Profile mit synchronisierten Informationen, einschließlich Beziehungen, Statuswerten und Servicedatensätzen. Mit diesen Profilen können verschiedene Zugriffsebenen auf Services und Informationen gewährt sowie angepasste Services in Echtzeit angeboten werden, die auf dem Stellenwert eines Kunden basieren.
Passwortverwaltung	Über die Benutzeranwendung können Administratoren Sicherheitsabfragen/-antworten einrichten und Benutzern die Möglichkeit geben, eigene Passwörter festzulegen. Die Client-Anmeldeerweiterung für Novell Identity Manager 3.5.1 erleichtert die Passwort-Selbstbedienung, indem ein Link zu den Novell- und Microsoft GINA-Anmelde-Clients hinzugefügt wird. Die Clients erlauben den Zugriff auf die Passwort-Selbstbedienungsfunktion der Identity Manager-Benutzeranwendung. Wenn der Identity Manager-Treiber die Passwortsynchronisierung unterstützt, können Passwörter in miteinander verbundenen Systemen synchronisiert werden.

1.2 Terminologieänderungen

Im Vergleich zu früheren Versionen wurden folgende Begriffe geändert:

Tabelle 1-2 *Terminologieänderungen*

Frühere Begriffe	Neue Begriffe
DirXML®	Identity Manager
DirXML-Server	Metaverzeichnis-Server
DirXML-Engine	Metaverzeichnis-Engine
eDirectory™	Identitätsdepot (sofern sich der Begriff nicht auf eDirectory-Attribute oder -Klassen bezieht)

1.3 Neuerungen in Identity Manager 3.5.1

- Abschnitt 1.3.1, „Identity Manager“, auf Seite 14
- Abschnitt 1.3.2, „Designer für Identity Manager“, auf Seite 16
- Abschnitt 1.3.3, „Benutzeranwendung“, auf Seite 18

1.3.1 Identity Manager

- „Unterstützung von Open Enterprise Server 2“ auf Seite 15
- „iManager-Plugins“ auf Seite 15

Unterstützung von Open Enterprise Server 2

Open Enterprise Server 2 enthält viele erforderliche Software-Komponenten, darunter SUSE® Linux Enterprise Server 10 Support Pack 1, NetWare® 6.5 Support Pack 7, eDirectory 8.8 Support Pack 2, iManager 2.7 und Security Services 2.0.5. Identity Manager wird sowohl auf der Linux- als auch auf der NetWare Open Enterprise Server 2-Plattform unterstützt.

iManager-Plugins

Die Plugins für iManager in dieser Version von Identity Manager sind auch mit Identity Manager 3.0 kompatibel. Zusätzlich zu der Abwärtskompatibilität enthält Identity Manager 3.5.1 Plugins, die der Treiber-Cache-Datei Informationen entnehmen können.

Unterstützung zusätzlicher Betriebssystemplattformen

Identity Manager bietet Unterstützung für alle Betriebssystemplattformen, die von der vorherigen Version von Identity Manager unterstützt werden. Zusätzlich können bestimmte Komponenten von Identity Manager auf Microsoft Windows Vista*, AIX* 5.3, Red Hat* 5 AS/ES 64 Bit und Open Enterprise Server 2, was SUSE Linux Enterprise Server 10 SP1 und NetWare 6.5 SP7 einschließt, ausgeführt werden.

Unterstützung zusätzlicher Anwendungen

Identity Manager bietet Unterstützung für alle Anwendungen, die von der vorherigen Version von Identity Manager unterstützt werden. Zusätzlich unterstützt Identity Manager auch eDirectory 8.8 SP2 und iManager 2.7 auf den Plattformen, auf denen diese Anwendungen ausgeführt werden können.

Nicht-Root-Installation

Identity Manager 3.5.1 enthält Informationen und Skripts für die Installation der Identity Manager-Metaverzeichnis-Engine in eine Nicht-Root-Installation von eDirectory. Die erforderlichen Schritte zum Durchführen einer Nicht-Root-Installation von Identity Manager sind in Abschnitt 4.9, „Nicht-Root-Installation von Identity Manager“, auf Seite 94 beschrieben.

Bundle-Komponenten

Identity Manager enthält die Client-Anmeldeerweiterung für Novell Identity Manager 3.5.1 und Designer 2.1.

Eine neue Komponente für Identity Manager, die Client-Anmeldeerweiterung für Novell Identity Manager 3.5.1, erleichtert die Passwort-Selbstbedienung, indem ein Link zu den Novell- und Microsoft GINA-Anmelde-Clients hinzugefügt wird. Wenn ein Benutzer in seinem Anmelde-Client auf den Link *Passwort vergessen* klickt, startet die Client-Anmeldeerweiterung einen eingeschränkten Browser zum Zugriff auf die Passwort-Selbstbedienungsfunktion der Identity Manager-Benutzeranwendung. Diese Funktion trägt dazu bei, die Anzahl der Anrufe beim Helpdesk aufgrund von vergessenen Passwörtern zu verringern.

Weitere Informationen zur Client-Anmeldeerweiterung für Novell Identity Manager 3.5.1 finden Sie unter „Client Login Extension for Novell Identity Manager 3.5.1“ im *Novell Identity Manager 3.5.1 Administrationshandbuch*. Weitere Informationen zu Designer 2.1 finden Sie unter Abschnitt 1.3.2, „Designer für Identity Manager“, auf Seite 16.

1.3.2 Designer für Identity Manager

In diesem Abschnitt werden Verbesserungen an Designer für Identity Manager beschrieben. Eine detaillierte Auflistung aller Verbesserungen und Änderungen an Designer 2.1 finden Sie unter Neuerungen (http://www.novell.com/documentation/designer21/index.html).

Gebietsschema-Unterstützung

In der Bereitstellungsansicht von Designer für Identity Manager können Sie nun Folgendes festlegen:

- Das Standard-Gebietsschema der Benutzeranwendung. (Dabei handelt es sich um das Gebietsschema, das zur Anzeige von Inhalten verwendet wird, wenn keine Übereinstimmung für das Gebietsschema des Benutzers gefunden wird.)
- Die vom Benutzeranwendungstreiber unterstützten Gebietsschemata.

Außerdem kann Designer jetzt Lokalisierungsdaten für Email-Schablonen importieren und exportieren.

Bereitstellungsteam-Editor

Designer für Identity Manager enthält jetzt ein Bereitstellungsteam-Editor-Plugin. Mit diesem neuen Editor können Sie eine Gruppe von Benutzern definieren, die für die Registerkarte *Anforderungen & Genehmigungen* der Benutzeranwendung als Team fungieren können. In der Teamdefinition ist festgelegt, wer mit diesem Team verbundene Bereitstellungsanforderungen und Genehmigungsaufgaben verwalten darf.

Der Bereitstellungsteam-Editor bietet eine Alternative zum iManager-Plugin für Team-Management.

Verbesserungen der Bedienungsfreundlichkeit in der Bereitstellungsansicht

Die Bereitstellungsansicht wurde verbessert, sodass Sie jetzt folgende Möglichkeiten haben:

- Die Organisation von Bereitstellungsanforderungsdefinitionen in Kategorien. Sie können den Editor für die Verzeichnisabstraktionsschicht zur Definition der Kategorien verwenden.
- Die Zuweisung verschiedener Eigenschaften (beispielsweise Trustee-Zuweisungen) für mehrere Bereitstellungsanforderungsdefinitionen gleichzeitig.

Email-Aktivität

Die Email-Aktivität bietet die Möglichkeit zum Versenden einer Email an interessierte Empfänger außerhalb einer Genehmigungsaktivität.

Genehmigungsaktivität

Die Genehmigungsaktivität ermöglicht nun das Erstellen eines neuen Formulars über die Eigenschaftsseite für die Genehmigungsaktivität.

Die Genehmigungsaktivität bietet auch die Möglichkeit, in Email-Benachrichtigungen ein Feld für eine Antwortadresse einzurichten, bei der es sich nicht um die Absenderadresse handelt.

Protokollaktivität

Mithilfe der Protokollaktivität können jetzt benutzerdefinierte Nachrichten zum Kommentarverlauf eines Workflows hinzugefügt werden.

Formularverbesserungen

Formulare unterstützen nun das Onload-Ereignis.

ECMA-Verbesserungen

Es werden nun die folgenden Feldmethoden unterstützt:

- getName()
- validate()
- hide()
- show()
- focus()
- select()
- activate()
- setRequired()

Verbesserungen für Anzeigenamen von Bereitstellungsanforderungsdefinitionen

Der Anzeigename einer Bereitstellungsanforderungsdefinition kann jetzt als statische Zeichenkette oder als übersetzbarer ECMA-Ausdruck definiert werden. Indem Sie einen Ausdruck definieren, können Sie den Anzeigenamen der Genehmigungsaufgabe anpassen. Dadurch können verschiedene Instanzen desselben Workflows eindeutige Einträge in der Aufgabenliste in der Benutzeranwendung anzeigen.

1.3.3 Benutzeranwendung

Verbesserungen der Benutzeroberfläche

Die Anzeige von Teamaufgaben wurde verbessert, sodass mehr Flexibilität auf der Benutzeroberfläche geboten und die Bedienung für den Benutzer optimiert wird. Die Seite „Teamaufgaben“ zeigt dynamische Inhalte in zwei neuen Präsentationsansichten an, der Schablonenansicht und der Komplettansicht. In beiden Formaten werden dem Benutzer Daten in einer Tabelle angezeigt. Der Benutzer kann wählen, welche Spalten und in welcher Reihenfolge diese angezeigt werden sollen, und er kann Aufgaben nach den Werten in einer Spalte sortieren.

Die Auswahl des Anzeigeformats wird vom Administrator gesteuert. Administratoren können eine bestimmte Ansicht auswählen, weil ihnen die Präsentation vielleicht besser gefällt, oder um die folgenden jeweils unterschiedlichen Funktionen nutzen zu können:

- Die Schablonenansicht (die Standardansicht) bietet Unterstützung für die Barrierefreiheit für sehbehinderte Benutzer. Zusätzlich enthält sie eine anpassbare Seitenwechselfunktion.
- Die Komplettansicht unterstützt die Filterung und bietet eine Möglichkeit für den Datenexport.

Plattformübergreifende Änderungen

In dieser Version wurde Laufzeitunterstützung für die folgenden Anwendungsserver-Plattformen hinzugefügt:

- JBoss* 4.2.0 auf SUSE Linux Enterprise Server 10.1, SUSE Linux Enterprise Server 9 SP2 und Windows 2003 Server SP1
- WebSphere* 6.1 auf Solaris* 10 und Windows 2003 SP1

  Das Installationsprogramm für die Benutzeranwendung installiert die WAR-Datei automatisch. Sie müssen die WAR-Datei jedoch manuell auf WebSphere bereitstellen.

  In WebSphere werden unter anderem die folgenden Datenbanken unterstützt: Oracle* 10g, MS SQL* 2005 SP1 und DB2.

  Eine vollständige Liste der unterstützten Plattformen finden Sie unter „Systemanforderungen für Identity Manager“ auf Seite 28.

In dieser Version wurde Unterstützung für die folgenden Browser-Umgebungen hinzugefügt:

- Internet Explorer 7 auf Windows 2000 Professional SP4, Windows XP SP2 und Windows Vista Enterprise Version 6
- Firefox* 2 auf Red Hat Enterprise Linux WS 4.0, Novell Linux Desktop 9, SUSE Linux 10.1 und SUSE Linux Enterprise Desktop 10

Änderungen an der Interoperabilität

In dieser Version wurden die folgenden Änderungen an der Interoperabilität vorgenommen:

- Der Administrator kann jetzt mithilfe einer Konfigurationseinstellung festlegen, ob in der Benutzeranwendung auf dem Bildschirm „Passwort vergessen“ der Hinweis angezeigt werden soll.
- Der Administrator kann jetzt mithilfe einer Konfigurationseinstellung die Funktion für die automatische Passworteingabe im Anmeldedialogfeld aktivieren oder deaktivieren. Dies legt fest, ob der Benutzer seinen Berechtigungsnachweis im Browser speichern kann.
- Der Anmeldevorgang unterstützt jetzt die Proxy-Smartcard-Authentifizierung über Access Manager. Dies wird ermöglicht, indem die Benutzeranwendung in den HTTP-Header eingespeiste SAML-Aussagen akzeptiert und diese dazu verwendet, eine SASL-Verbindung zum Verzeichnis herzustellen.

Verbesserungen an den SOAP-Endpunkten

In dieser Version wurden die folgenden Verbesserungen an den SOAP-Endpunkten vorgenommen:

- Ein neuer VDX-Service wurde hinzugefügt, um einen SOAP-Endpunkt zur Durchführung von Abfragen der Verzeichnisabstraktionsschicht zur Verfügung zu stellen.
- Ein neuer Benachrichtigungsservice wurde hinzugefügt, um einen SOAP-Endpunkt zum Versenden von Email-Benachrichtigungen zur Verfügung zu stellen.
- Die neue Methode getProcessesArray() wurde zum Bereitstellungsservice hinzugefügt. Sie enthält ein Argument, mit dem Sie die Anzahl der zurückgegebenen Prozesse begrenzen können.
- Die neue Methode startWithCorrelationId() wurde ebenfalls zum Bereitstellungsservice hinzugefügt, damit Sie einen Satz von zusammengehörigen Workflows starten und mithilfe einer Korrelations-ID verfolgen können.

Die SOAP-Endpunkte bieten Entwicklern die Möglichkeit, eigene Anwendungen zu erstellen. In der fertigen Benutzeroberfläche für die Benutzeranwendung sind sie nicht freigelegt.

Weitere Funktionsverbesserungen

In der Benutzeranwendung können Sie nun URL-Parameter angeben, um ein Bereitstellungsanforderungsformular direkt aufzurufen.

1.4 Identity Manager - Installationsprogramme und Services

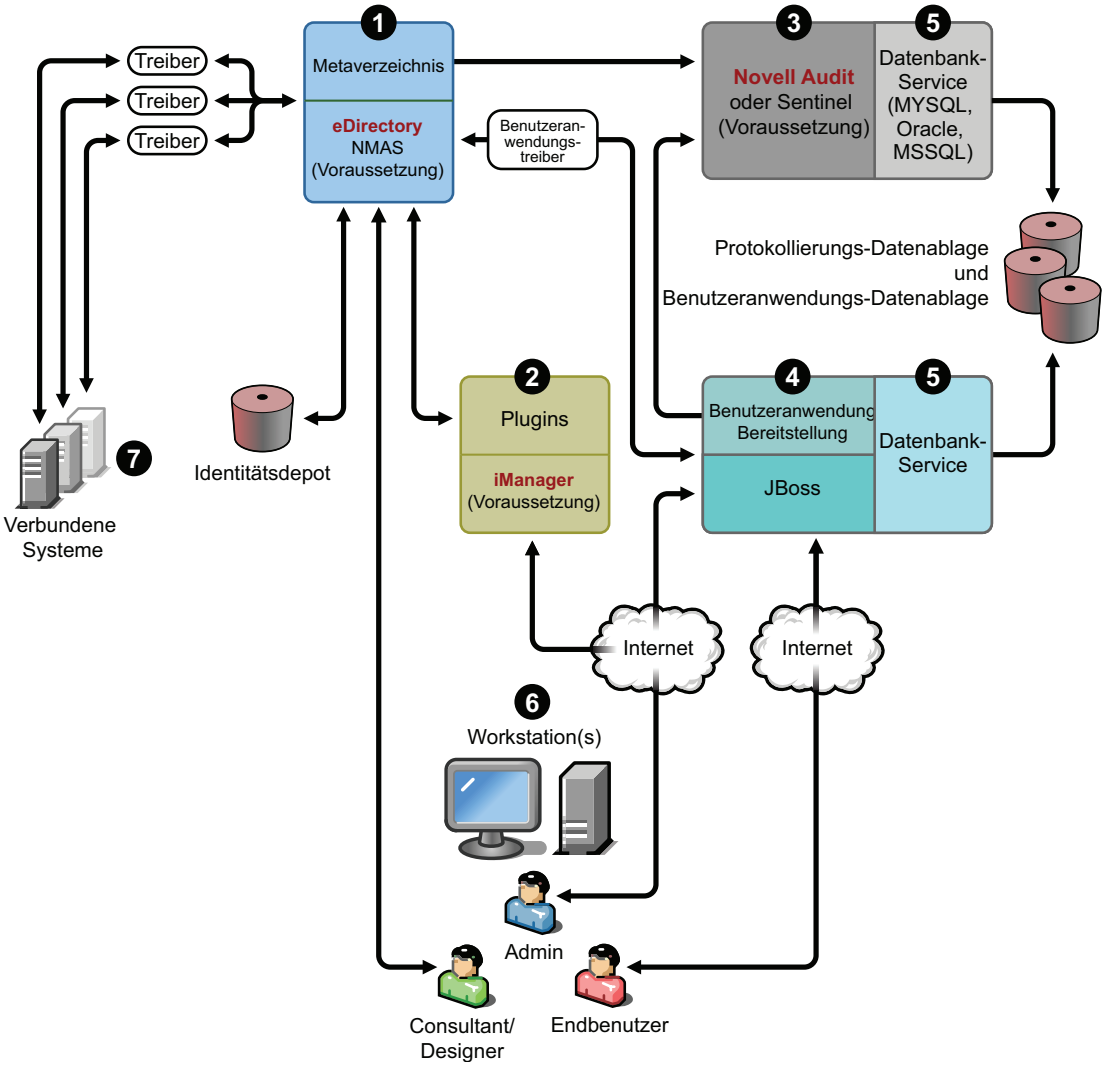
In den folgenden Abschnitten werden die Installationsprogramme und Services von Identity Manager erläutert. In diesem Abschnitt werden die verschiedenen Services aufgezeigt, die zu einem voll funktionsfähigen Identity Manager gehören.

- Abschnitt 1.4.1, „Installationsprogramme“, auf Seite 20
- Abschnitt 1.4.2, „Services“, auf Seite 21

1.4.1 Installationsprogramme

Identity Manager verfügt über drei verschiedene Installationsprogramme mit sieben Services, die installiert und konfiguriert werden müssen. In der folgenden Grafik erhalten Sie einen Überblick über alle Services, mit denen Identity Manager voll funktionsfähig wird.

Abbildung 1-1 *Grafischer Überblick über die sieben Identity Manager-Services*



Im Folgenden finden Sie eine Liste der Installationsprogramme und der Komponenten, die bei den einzelnen Installationsvorgängen installiert werden.

- „Installation des Identity Manager-Metaverzeichnis-Systems“ auf Seite 21
- „Installation der Benutzeranwendung und des Bereitstellungsmoduls“ auf Seite 21
- „Installation von Designer“ auf Seite 21

Hinweis: Vor der Installation der Identity Manager-Komponenten muss zunächst die hierfür erforderliche Software installiert werden: eDirectory 8.7.3.6 oder höher (für die Services, die an den Positionen 1 und 3 in der obigen Grafik angezeigt werden), Security Services 2.0.4 mit NMAS™ 3.1.3 (für die Positionen 1 und 3), iManager 2.6 oder höher (für Position 2) und Novell Audit 2.0.2 Starter Pack oder Sentinel™ 5.1.3 (für Position 3). Sie können die erforderliche Software von der Download-Website von Novell (http://download.novell.com) herunterladen. Eine ausführliche Liste der Voraussetzungen und Anforderungen finden Sie in Abschnitt 1.5, „Systemanforderungen für Identity Manager“, auf Seite 28.

Installation des Identity Manager-Metaverzeichnis-Systems

Der Installationsvorgang führt folgende Funktionen aus:

- Erweitert das eDirectory-Schema für das gesamte Identity Manager-Produkt.
- Installiert die Metaverzeichnis-Engine und den System-Service.
- Installiert die Identity Manager-Plugins für iManager.
- Installiert den Remote Loader des Metaverzeichnis-Systems (sofern ausgewählt).
- Installiert die Treiber der verbundenen Systeme. (Die Treiber werden installiert, sind aber bis zu ihrer Initiierung inaktiv.)
- Installiert die Identity Manager-Berichte sowie die Dienstprogramme und Werkzeuge des Metaverzeichnis-Systems.

Installation der Benutzeranwendung und des Bereitstellungsmoduls

Unter Linux* und Windows werden die folgenden Services installiert:

- JBoss und MySQL* (sofern ausgewählt).
- Die WAR-Datei erfordert das Ausführen der Benutzeranwendung.

Installation von Designer

Für Linux und Windows gibt es separate Installationsprogramme. Sie führen die folgenden Aufgaben aus:

- Installation des Eclipse*-Framework
- Installation der grundlegenden Plugins
- Installation der Metaverzeichnis-Plugins
- Installation der Verzeichnisabstraktionsschicht-Plugins
- Installation des Workflow-Editor-Plugins

1.4.2 Services

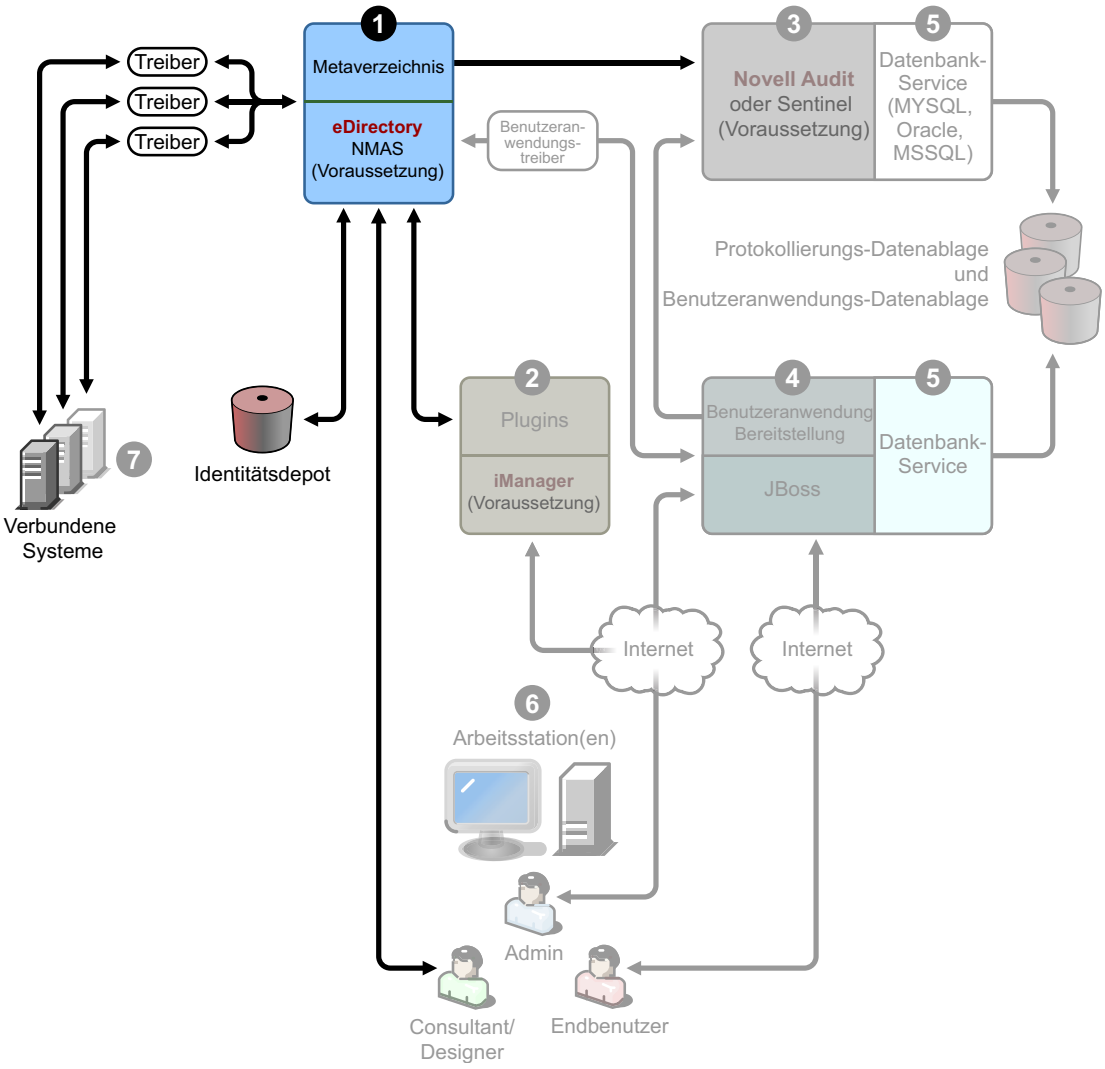
Identity Manager umfasst sieben Services, die Sie installieren und konfigurieren können. Alle sieben Services können auf einem einzelnen Computer installiert und konfiguriert werden, auch wenn dies in einer Produktionsumgebung nicht empfohlen wird. Sie können auch pro Computer nur einen Service anbieten bzw. eine beliebige Anzahl dazwischen. Die unterstützten Hardware- und

Software-Voraussetzungen für die einzelnen Services finden Sie in Abschnitt 1.5, „Systemanforderungen für Identity Manager“, auf Seite 28.

Metaverzeichnis-System-Service

Dieses System wird als Identitätsdepot verwendet. In einer Produktionsumgebung wird nur eine Instanz der Metaverzeichnis-Engine benötigt.

Abbildung 1-2 *Metaverzeichnis-Systemservice*

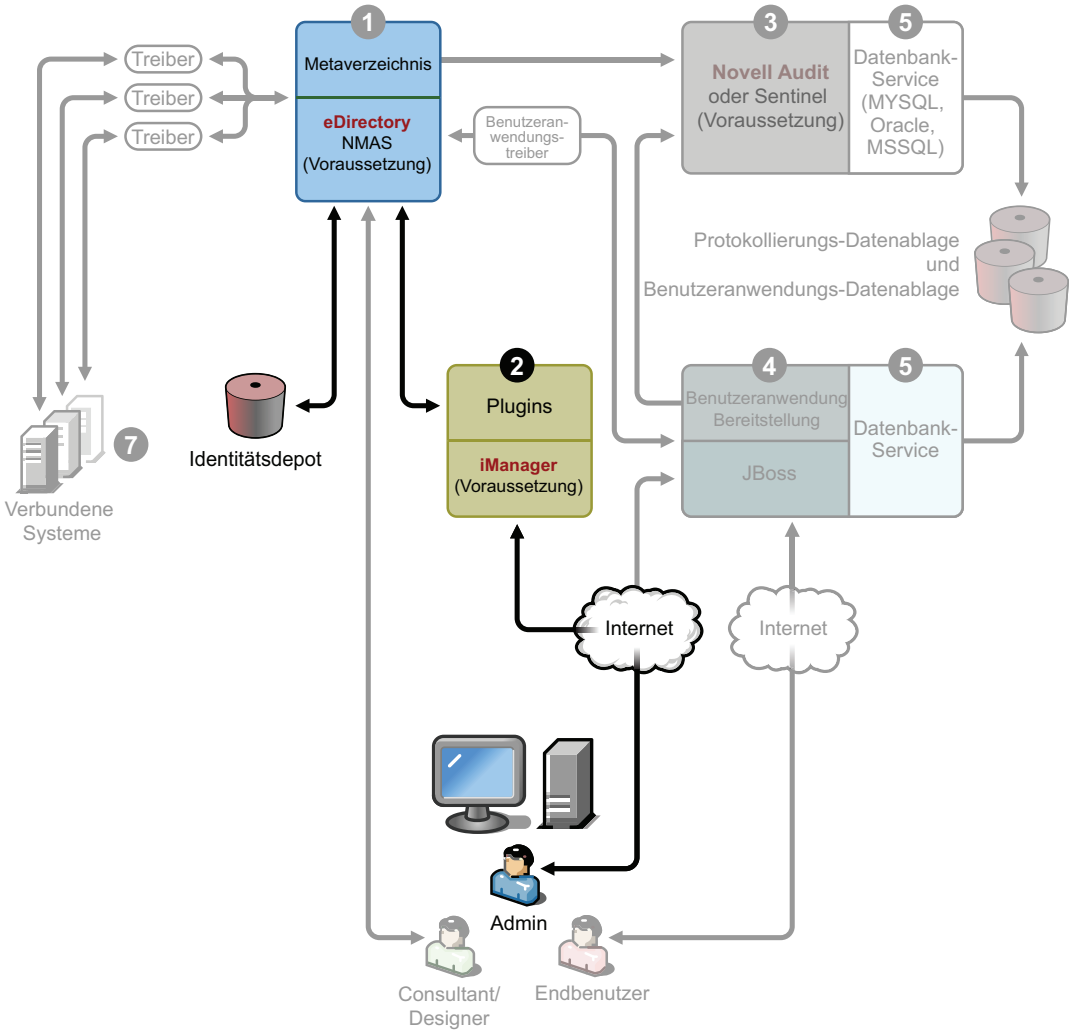


Wenn Daten in einem dieser Systeme geändert werden, erkennt die in Identity Manager enthaltene Metaverzeichnis-Engine diese Änderungen und gibt sie auf der Basis der definierten Geschäftsregeln an die verbundenen Systeme weiter. Mit dieser Lösung können Sie für beliebige Daten autorisierte Datenursprünge erzwingen (eine Anwendung zur Personalverwaltung ist beispielsweise Eigentümer der ID eines Benutzers, während ein Messaging-System möglicherweise Eigentümer der Email-Kontoinformationen eines Benutzers ist).

Informationen zum Installieren von Identity Manager und diesem Service finden Sie in Kapitel 4, „Installation von Identity Manager“, auf Seite 67. Eine Liste der Voraussetzungen, die vor der Installation von Identity Manager erfüllt sein müssen, finden Sie in den Systemanforderungen für „Metaverzeichnis-System“ auf Seite 29.

Webbasierte Administrationsservices

Abbildung 1-3 *Webbasierter Administrationsservice*

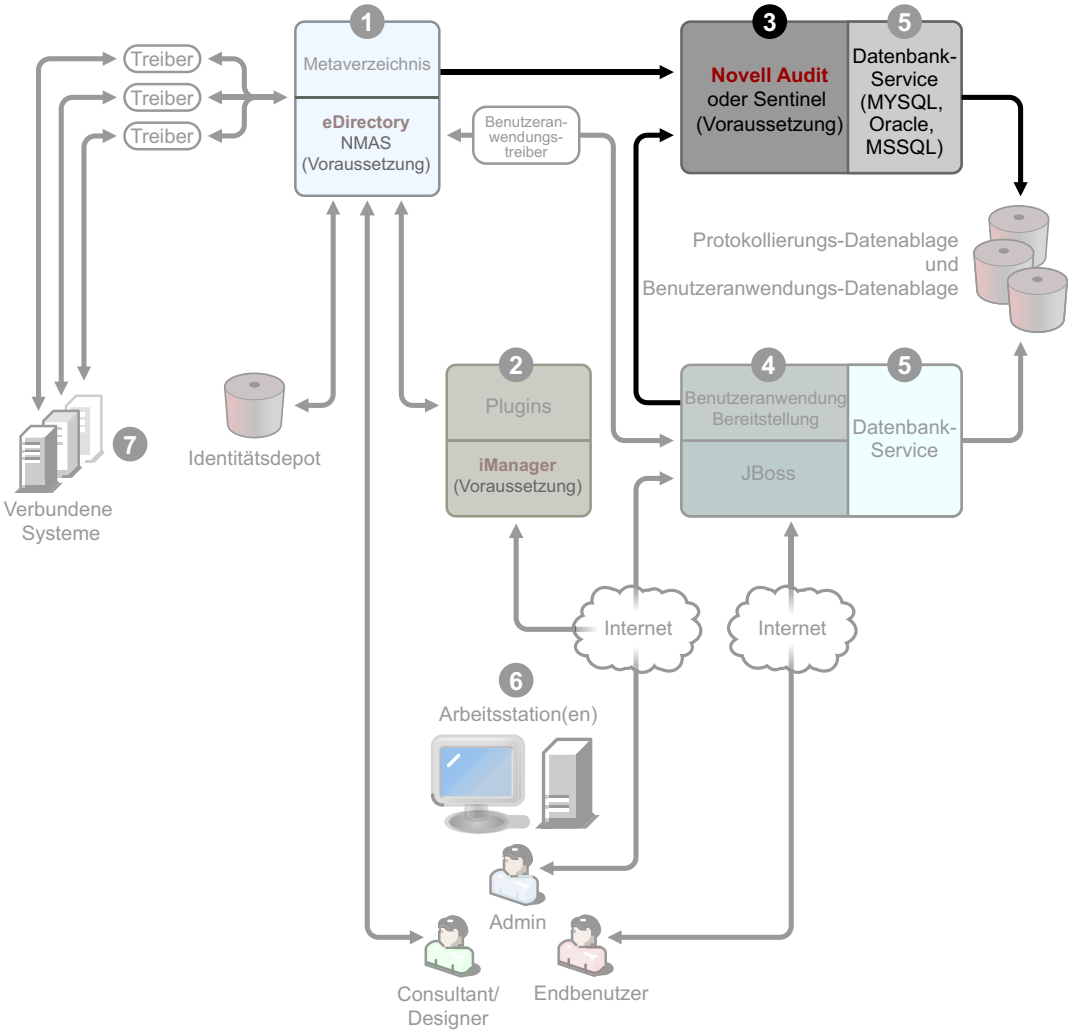


Verwenden Sie diesen Service für die Administration von eDirectory und des Metaverzeichnis-Systems mit iManager 2.5 und höher. Identity Manager und die Benutzeranwendungs-Plugins müssen installiert sein. Installieren Sie die Identity Manager-Plugins in iManager auf dem Server, auf dem Sie Identity Manager installieren. Informationen zum Installieren der Identity Manager-

Plugins und dieses Services finden Sie in Kapitel 4, „Installation von Identity Manager“, auf Seite 67.

Sichere Protokollservices

Abbildung 1-4 *Sicherer Protokollservice*

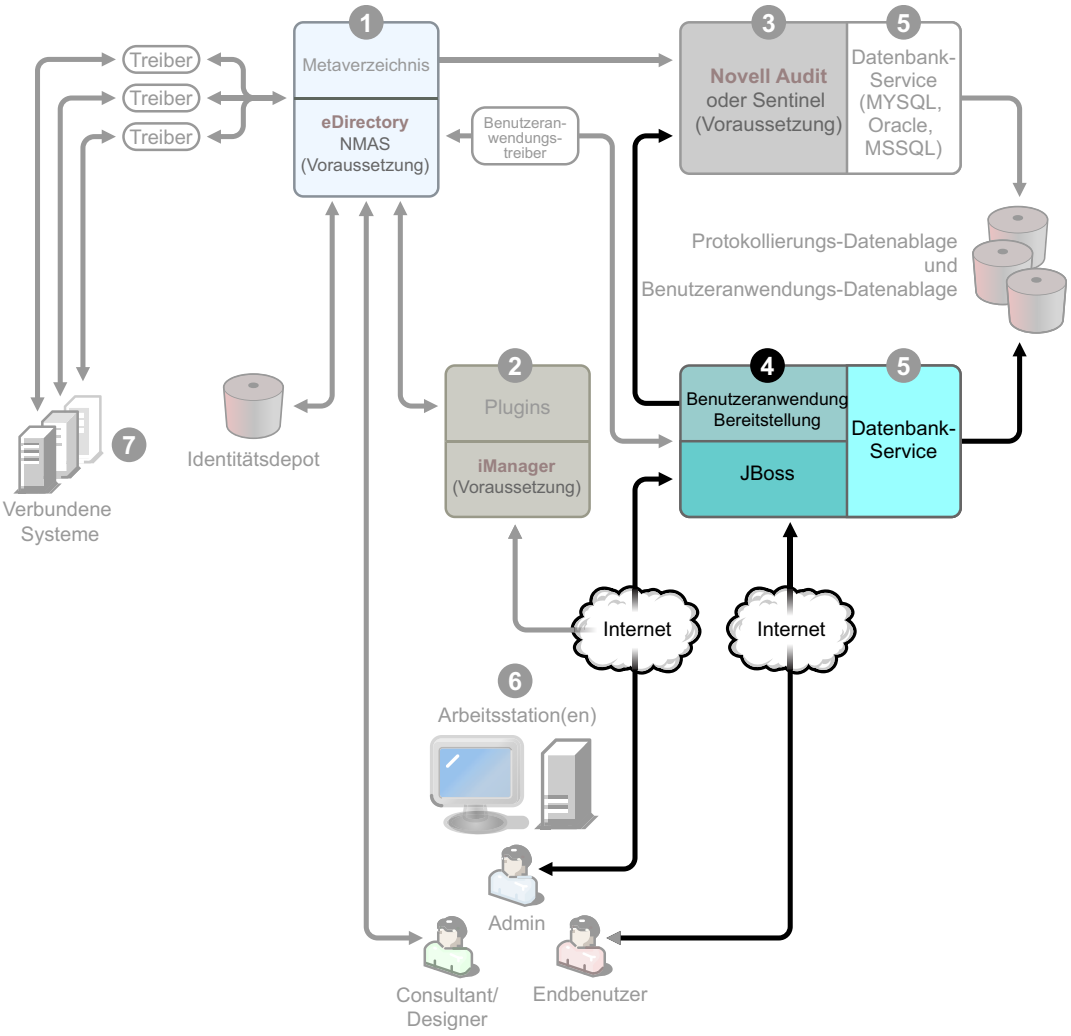


Repository für das Protokollieren von Ereignissen (die Identity Manager-Software wird nicht auf diesem Server installiert, aber ein sicherer Protokollservice ist obligatorisch). Dies ist ein zentraler Service, der von Identity Manager und den Benutzeranwendungs- und Workflow-System-Services verwendet wird und separat von der Download-Website von Novell (http://download.novell.com) heruntergeladen werden kann.

Wählen Sie auf der Download-Website im Pulldown-Menü *Produkt oder Technologie* die Option *Audit* und klicken Sie auf *Suchen*. Klicken Sie auf *Audit 2.0.2 Starter Pack*. Folgen Sie den Installationsanweisungen, die im Starter Pack enthalten sind.

Benutzeranwendung und Bereitstellungsmodul

Abbildung 1-5 *Benutzeranwendung und Bereitstellungsmodul*

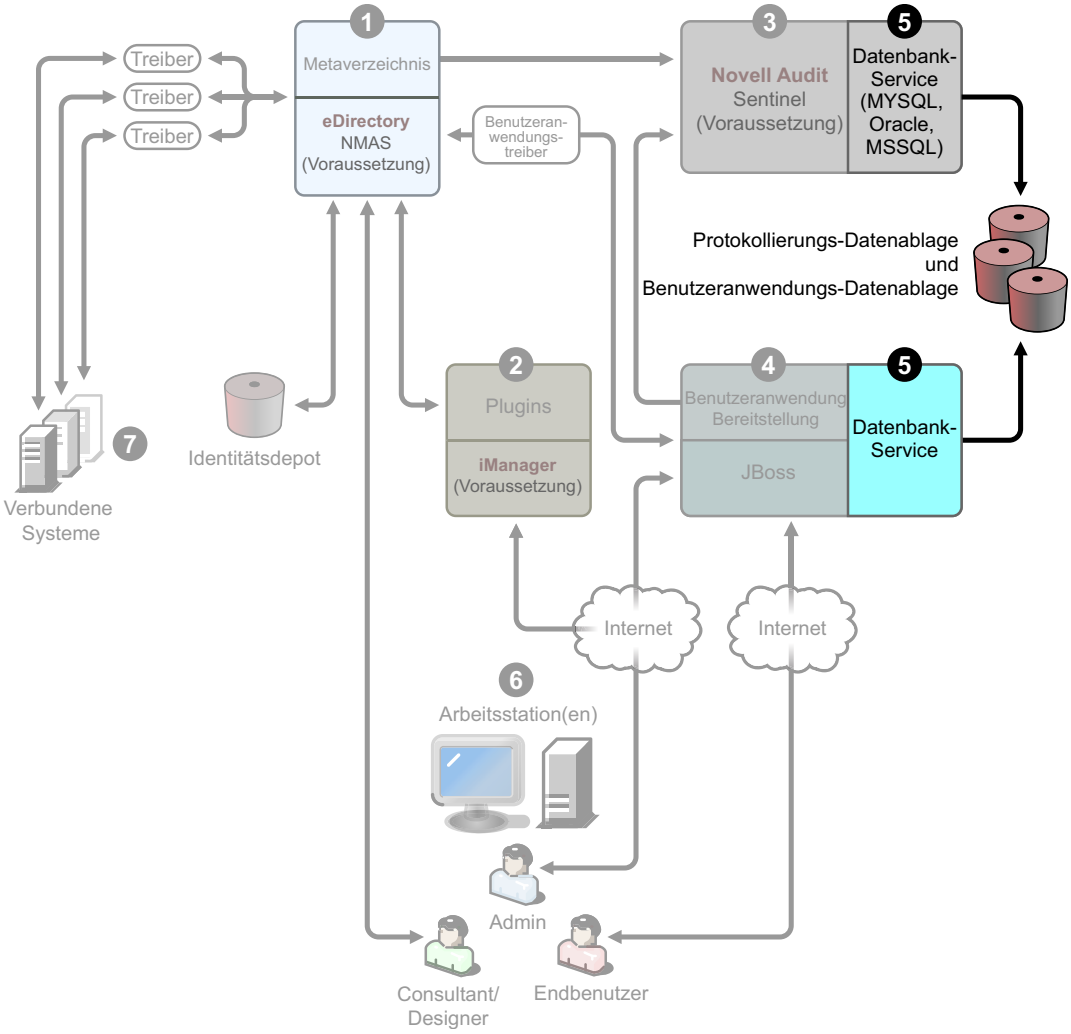


Informationen zum Installieren dieses Services finden Sie in Kapitel 5, „Installation der Benutzeranwendung“, auf Seite 99. Die unterstützten Hardware- und Software-Voraussetzungen für die einzelnen Services finden Sie in Abschnitt 5.1, „Voraussetzungen für die Installation“, auf Seite 99.

Datenbankservice

Sowohl für die sichere Protokollierung als auch für die Endbenutzeranwendung und das Workflow-System wird eine Datenbank benötigt. Sie können für beide Anwendungen dieselbe Datenbank einrichten oder jeder Anwendung eine eigene Datenbank zuordnen.

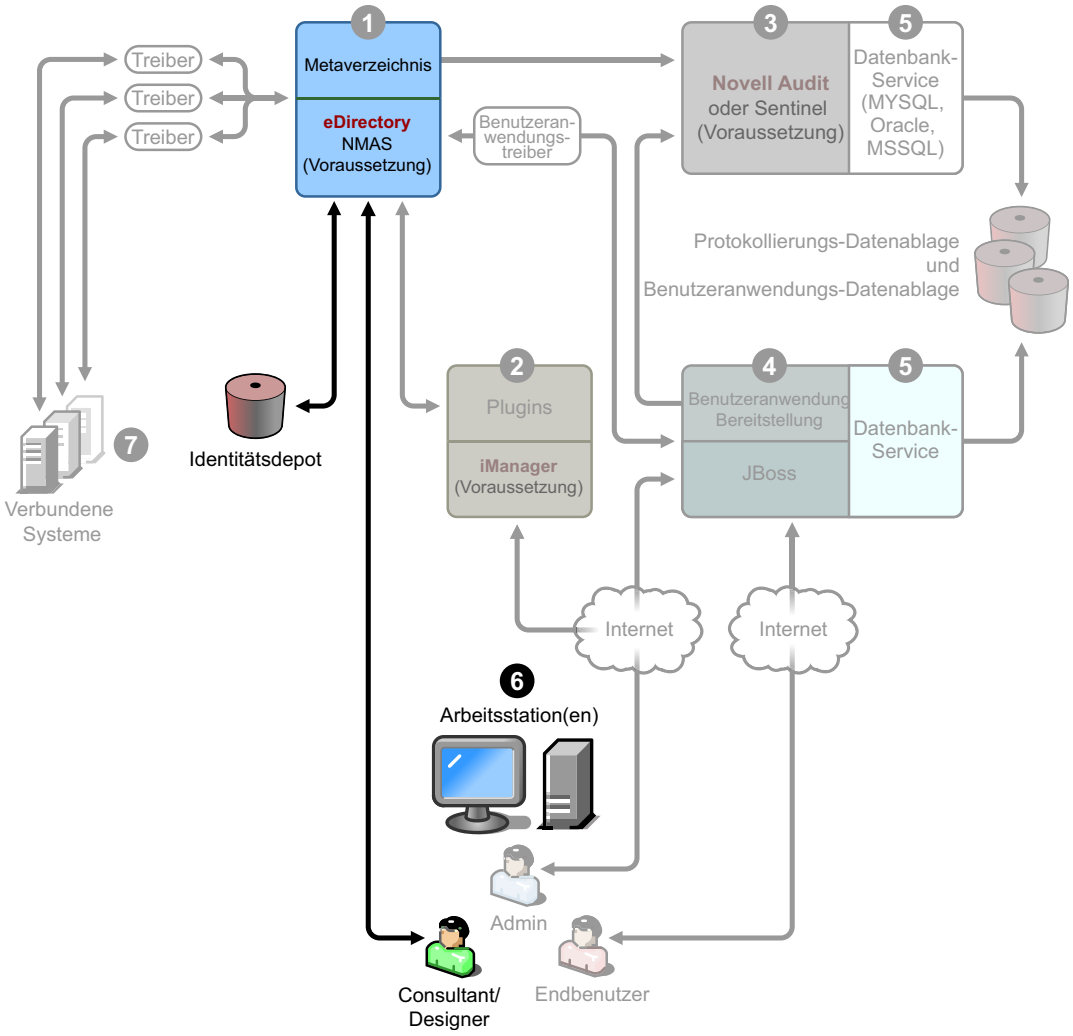
Abbildung 1-6 *Datenbankservice*



Die sichere Protokollierung umfasst keine spezielle Datenbank. Sie können jedoch auch die MySQL-Datenbank verwenden, die zum Lieferumfang der Benutzeranwendung und der Bereitstellung gehört. Die Benutzeranwendung enthält den JBoss-Anwendungsserver Version 4.2.0 und erfordert JRE* 1.5.0_10. Informationen zum Installieren dieses Services finden Sie in Abschnitt 5.2, „Installation und Konfiguration“, auf Seite 107.

Arbeitsstationen

Abbildung 1-7 *Arbeitsstationsservices für Designer*

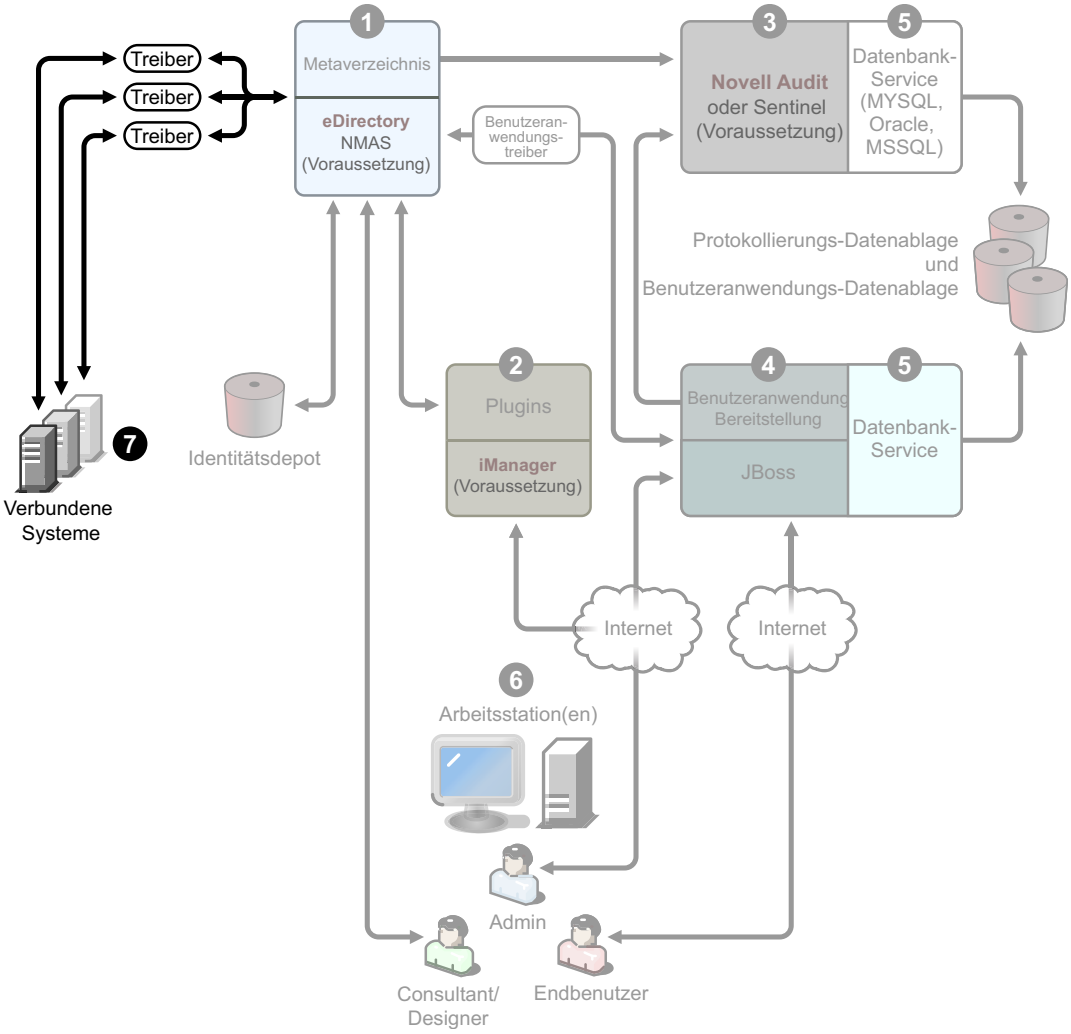


Sie werden für Designer verwendet, um das Identity Manager-System zu entwerfen, bereitzustellen und zu dokumentieren, sowie für Dienstprogramme, Berichte und Werkzeuge, die im Produkt enthalten sind. Informationen zum Installieren von Designer auf einer Arbeitsstation finden Sie im Abschnitt zur „Installation“ im Handbuch *Designer 2.1 für Identity Manager 3.5.1*.

Verbundene Systeme

Hier werden die Treiber gehostet. Verbundene Systeme können Anwendungen, Datenbanken, Server und andere Services sein. Jede verbundene Anwendung muss von Benutzern mit anwendungsspezifischen Kenntnissen und Verantwortlichkeiten bedient werden. Für jeden Treiber muss das verbundene System verfügbar sein und die relevanten APIs bereitgestellt werden.

Abbildung 1-8 *Verbundene Systeme*



Die Treiber werden als Teil der Installation von Identity Manager installiert. Informationen zum Installieren von Identity Manager und diesem Service finden Sie in Kapitel 4, „Installation von Identity Manager“, auf Seite 67. Wenn Sie mehr zur Konfiguration von Treibern erfahren möchten, lesen Sie die treiberspezifische Dokumentation auf der Website zur Identity Manager-Treiber-Dokumentation (http://www.novell.com/documentation/idmdrivers)

1.5 Systemanforderungen für Identity Manager

Novell Identity Manager enthält Komponenten, die innerhalb Ihrer Umgebung auf verschiedenen Systemen und Plattformen installiert werden können. Je nach Systemkonfiguration müssen Sie das Identity Manager-Installationsprogramm möglicherweise mehrmals ausführen, um die Komponenten von Identity Manager auf den entsprechenden Systemen zu installieren.

In der folgenden Tabelle sind die Installationskomponenten von Identity Manager und die jeweiligen Anforderungen aufgelistet.

Tabelle 1-3 *Anforderungen für Identity Manager-Systemkomponenten*

Systemkomponente	Systemanforderungen	Hinweise
Metaverzeichnis-System ◆ Metaverzeichnis-Engine ◆ Novell Audit Agent ◆ Service-Treiber ◆ Identity Manager-Treiber ◆ Dienstprogramme (einschließlich Anwendungs-Dienst-programmen und dem Werkzeug für das Novell Audit-Setup)	Eines der folgenden Betriebssysteme: ◆ NetWare 6.5 mit dem neuesten Support Pack ◆ Novell Open Enterprise Server (OES) 1.0 mit dem neuesten Support Pack ◆ Novell Open Enterprise Server (OES) 2.0 ◆ Windows Server 2000 mit dem neuesten Service Pack (32 Bit) ◆ Windows Server 2003 mit dem neuesten Service Pack (32 Bit) ◆ Linux Red Hat 3.0, 4.0 und 5.0 ES und AS (32- und 64-Bit-Unterstützung) ◆ SUSE Linux Enterprise Server 9 und 10 mit dem neuesten Support Pack (32- und 64-Bit-Unterstützung) ◆ Solaris 9 oder 10 ◆ AIX 5.2L, Version 5.2 und 5.3 Eine der folgenden Versionen von eDirectory: ◆ eDirectory 8.7.3.6 mit dem neuesten Support Pack ◆ eDirectory 8.8 mit dem neuesten Support Pack Security Services 2.0.5 (NMAS 3.1.3)	Wenn Sie eine Metaverzeichnis-System-Plattform verwenden, wird in Ihrer Implementierung VMWare* unterstützt. Alle Identity Manager-Softwarekomponenten in dieser Version sind 32-Bit-Komponenten, auch dann, wenn sie auf einem 64-Bit-Prozessor oder einem 64-Bit-Betriebssystem ausgeführt werden. Sofern nicht anders angegeben, unterstützen OES-, NetWare-, Windows- und Linux-Plattformen (Red Hat und SUSE) alle folgenden Prozessoren im 32-Bit-Modus: ◆ Intel* x86-32 ◆ AMD x86-32 ◆ Intel EM64T ◆ AMD Athlon64* und Opteron* Identity Manager unterstützt folgende Funktionen von eDirectory 8.8: ◆ Mehrere eDirectory-Instanzen auf demselben Server ◆ Verschlüsselte Attribute eDirectory 8.8 unterstützt Red Hat Linux 4.0, 64-Bit-Version. Es ist eine 64-Bit-Version der Passwortsynchronisierung auf Windows Server 2003 verfügbar. Stellen Sie sicher, dass Sie die eDirectory-Datenbank vor der Installation von eDirectory 8.8 vollständig sichern. eDirectory 8.8 rüstet Teile der Datenbankstruktur auf und lässt nach dem Aufrüsten kein Rollback zu. Die Xen-Virtualisierung wird nun auf SUSE Linux Enterprise Server 10 unterstützt, wenn die Xen Virtual Machine (VM) als Gast-Betriebssystem SLES 10 im paravirtualisierten Modus ausführt. Es wird ein Xen-Patch für SLES 10 benötigt (siehe TID-Artikel 3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=20406933&stateId=0%200%202020414606).

Systemkomponente	Systemanforderungen	Hinweise
Webbasierter Administrationsserver ◆ Passwort-synchronisierung ◆ iManager 2.6 und Plugins ◆ iManager 2.7 und Plugins ◆ Treiber-konfigurationen	Eines der folgenden Betriebssysteme: ◆ Novell Open Enterprise Server (OES) 1.0 unter NetWare mit dem neuesten Support Pack ◆ Novell Open Enterprise Server (OES) 2.0 ◆ NetWare 6.5 mit dem neuesten Support Pack ◆ Windows Server 2000 mit dem neuesten Service Pack (32 Bit) ◆ Windows Server 2003 mit dem neuesten Service Pack (32 Bit) ◆ Microsoft Windows Vista ◆ Linux Red Hat Linux 3.0, 4.0 und 5.0 ES und AS (32- und 64-Bit-Unterstützung) ◆ Solaris 9 oder 10 mit dem neuesten Support Pack ◆ SUSE Linux Enterprise Server 9 und 10 mit dem neuesten Support Pack (32- und 64-Bit-Unterstützung) Über die iManager-Arbeitsstation unterstützte Betriebssysteme: ◆ Windows 2000 Professional mit dem neuesten Service Pack ◆ Windows XP mit SP2 ◆ SUSE Linux Enterprise Desktop 10 ◆ SUSE Linux 10.1 Die folgende Software. ◆ Novell iManager 2.6 und 2.7 mit dem neuesten Support Pack und den neuesten Plugins	Alle Identity Manager-Softwarekomponenten in dieser Version sind 32-Bit-Komponenten, auch dann, wenn sie auf einem 64-Bit-Prozessor oder einem 64-Bit-Betriebssystem ausgeführt werden. Sofern nicht anders angegeben, unterstützen OES-, NetWare-, Windows- und Linux-Plattformen (Red Hat und SUSE) alle folgenden Prozessoren im 32-Bit-Modus: ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 und Opteron ◆ Die Browser-Unterstützung wird von iManager 2.6 festgelegt. Gegenwärtig umfasst diese Liste folgende Browser: ◆ Internet Explorer 6, SP1 und höher ◆ Internet Explorer 7 ◆ Firefox* 2.0 und höher ◆ Führen Sie den iManager-Konfigurationsassistenten oder das Designer-Dienstprogramm aus, um Portalinhalte in eDirectory zu installieren oder bereitzustellen. ◆ (Windows) Der Novell Client™ 4.9 ist auf der Download-Seite von Novell (http://download.novell.com/index.jsp) verfügbar. ◆ Wenn Sie sich zum Verwalten von Identity Manager Remote-Servern mit iManager bei anderen Bäumen anmelden, treten möglicherweise Fehler auf, wenn Sie für den Remote-Server anstelle der IP-Adresse den Servernamen angeben. ◆ Unter 64-Bit-Windows 2003 wird nur der Passwortsynchronisierungs-Agent unterstützt.

Systemkomponente	Systemanforderungen	Hinweise
Sicherer Protokollserver ◆ Der sichere Protokollserver ◆ Der Plattformagent (Client-Komponente) ◆ Novell Audit 2.0.2 oder Sentinel 5.1.3	Eines der folgenden Betriebssysteme für den sicheren Protokollserver: ◆ Novell Open Enterprise Server (OES) 1.0 und 2.0 mit dem neuesten Support Pack ◆ NetWare 6.5 mit dem neuesten Support Pack ◆ Windows Server 2000 mit dem neuesten Service Pack (32 Bit) ◆ Windows Server 2003 mit dem neuesten Service Pack (32 Bit) ◆ Red Hat Linux 3.0, 4.0 und 5.0 AS und ES (32 Bit und 64 Bit, Novell Audit läuft allerdings nur im 32-Bit-Modus) ◆ Solaris 9 oder 10 mit dem neuesten Support Pack ◆ SUSE Linux Enterprise Server 9 oder 10 (32 Bit und 64 Bit, Novell Audit läuft allerdings nur im 32-Bit-Modus) ◆ Novell eDirectory 8.7.3.6 oder 8.8 mit dem neuesten Support Pack (muss auf dem Secure Logging Server installiert sein) Eines der folgenden Betriebssysteme für den Plattformagenten: ◆ Novell Open Enterprise Server (OES) 1.0 SP1 oder das neueste Support Pack ◆ NetWare 6.5 mit dem neuesten Support Pack ◆ Windows 2000 oder 2000 Server, XP oder Windows Server 2003 mit dem neuesten Service Pack (32 Bit) ◆ Red Hat Linux 3 oder 4 AS und ES (32 Bit und 64 Bit, Novell Audit läuft allerdings nur im 32-Bit-Modus) ◆ Solaris 8, 9 oder 10 ◆ SUSE Linux Enterprise Server 9 oder 10 (32 Bit und 64 Bit, Novell Audit läuft allerdings nur im 32-Bit-Modus) iManager 2.6 und 2.7 mit dem neuesten Support Pack und den neuesten Plugins	OES-, NetWare-, Windows- und Linux-Plattformen (Red Hat und SUSE) unterstützen alle folgenden Prozessoren im 32-Bit-Modus: ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 und Opteron Mindestanforderungen für den sicheren Server: ◆ Einzelprozessor, PC der Serverklasse mit Pentium* II 400 MHz ◆ Mindestens 40 MB Festplattenspeicher ◆ 512 MB RAM Die eDirectory-Instrumentation, mit deren Hilfe eDirectory-Ereignisse protokolliert werden können, unterstützt folgende eDirectory-Versionen: ◆ eDirectory 8.7.3 (NetWare, Windows, Linux und Solaris) ◆ eDirectory 8.8 mit dem neuesten Support Pack Die NetWare-Instrumentation, mit deren Hilfe NetWare-Ereignisse protokolliert werden können, unterstützt folgende NetWare-Versionen: ◆ NetWare 5.1 mit dem neuesten Support Pack ◆ NetWare 6.0 mit dem neuesten Support Pack ◆ NetWare 6.5 oder NetWare 6.5 mit dem neuesten Support Pack ◆ Novell Open Enterprise Server (OES) mit dem neuesten Support Pack

Systemkomponente	Systemanforderungen	Hinweise
Benutzeranwendung	**Anwendungsserver** Die Benutzeranwendung kann auf JBoss und WebSphere ausgeführt werden, wie unten beschrieben. Folgende Server unterstützen JBoss 4.2.0: ◆ Novell Open Enterprise Server (OES) 1.0 SP2 oder das neueste Support Pack – nur Linux ◆ Novell Open Enterprise Server (OES) 2–SLES 10 SP1 und NetWare 6.5 SP7 ◆ SUSE Linux Enterprise Server 9 SP2 (in OES 1.0 SP2 enthalten) und 10.1.x (64-Bit-JVM*) ◆ Windows 2000 Server mit SP4 (32 Bit) ◆ Windows 2003 Server mit SP1 (32 Bit) ◆ Solaris 10 Support Pack mit Datum 6/06 Folgende Server unterstützen WebSphere 6.1: ◆ Solaris 10 (64-Bit-Modus) ◆ Windows 2003 SP1 Folgende Server unterstützen WebLogic 10: ◆ Solaris 10 (64-Bit-Modus) ◆ Windows Server 2003 SP1 Die Benutzeranwendung erfordert JRE* 1.5.0_10 (siehe Abschnitt 5.1, „Voraussetzungen für die Installation“, auf Seite 99) **Browser** Die Benutzeranwendung unterstützt Firefox und Internet Explorer, wie nachfolgend beschrieben. Firefox 2 wird in den folgenden Umgebungen unterstützt: ◆ Windows 2000 Professional mit SP4 ◆ Windows XP mit SP2 ◆ Red Hat Enterprise Linux WS 4.0 ◆ Novell Linux Desktop 9 ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 Internet Explorer 7 wird in den folgenden Umgebungen unterstützt: ◆ Windows 2000 Professional mit SP4 ◆ Windows XP mit SP2 ◆ Windows Vista Enterprise Version 6 Internet Explorer 6 wird in den folgenden Umgebungen unterstützt: ◆ Windows 2000 Professional mit SP4 ◆ Windows XP mit SP2	SUSE Linux Enterprise Server unterstützt im 32-Bit-Modus folgende Prozessoren: ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 und Opteron SUSE Linux Enterprise Server kann im 64-Bit-Modus auf folgenden Prozessoren ausgeführt werden: ◆ Intel EM64T ◆ AMD Athlon64 ◆ AMD Opteron ◆ Sun* SPARC* Die Xen*-Virtualisierung wird nun auf SUSE Linux Enterprise Server 10 unterstützt, wenn die Xen Virtual Machine (VM) als Gast-Betriebssystem SLES 10 im paravirtualisierten Modus ausführt. Es wird ein Xen-Patch für SLES 10 benötigt (siehe TID-Artikel 3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=20406933&stateId=0%200%200414606)).

Systemkomponente	Systemanforderungen	Hinweise
Datenbankserver für die Benutzeranwendung ◆ MySQL ◆ Oracle ◆ MS SQL ◆ DB2	Die folgenden Datenbanken werden mit JBoss unterstützt: ◆ MySQL Version 5.0.27 ◆ Oracle 9i (9.2.0.1.0 und 9.2.0.5.0) ◆ Oracle 10g Release 2 (10.2.0) ◆ MS SQL 2005 SP1 Die folgenden Datenbanken werden mit WebSphere unterstützt: ◆ Oracle 10g Release 2 (10.2.0) ◆ MS SQL 2005 SP1 ◆ DB2 DV2 Version 9.1.0.0	Die Benutzeranwendung verwendet eine Datenbank für viele Aufgaben, z. B. zum Speichern von Konfigurationsdaten und von Daten laufender Workflow-Aktivitäten. Sowohl für die sichere Protokollierung als auch für die Benutzeranwendung und die Workflow-Bereitstellung wird eine Datenbank benötigt. Sie können für beide Anwendungen dieselbe Datenbank einrichten oder jeder Anwendung eine unabhängige Datenbank zuordnen. Die sichere Protokollierung umfasst keine spezielle Datenbank. Oracle wird mit dem Thin-Client-Treiber und mit dem OCI-Client-Treiber unterstützt.
Arbeitsstationen ◆ Designer ◆ Webzugriff auf iManager	Designer wurde auf folgenden Plattformen getestet: Windows: ◆ Windows 2000 Professional mit dem neuesten Service Pack ◆ Windows XP SP2 ◆ Windows Server 2003 mit dem neuesten Service Pack (32 Bit) ◆ Microsoft Windows Vista Linux: ◆ SUSE Linux Enterprise Server 10 (nur Designer) ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 ◆ Red Hat Linux 4.0 (nur Designer) ◆ Red Hat Fedora* Core 5 (nur für Designer) ◆ Novell Linux Desktop 9 ◆ GNOME*, KDE, Red Hat Fedora	Designer verwendet Eclipse als seine Entwicklungsplattform. Plattformspezifische Informationen finden Sie auf der Eclipse-Website (http://www.eclipse.org/). Minimale und empfohlene Hardwareanforderungen: ◆ Mindestens 1 GHz, 2 GHz oder höher empfohlen. ◆ Mindestens 512 MB RAM, 1 GB RAM oder höher empfohlen. ◆ Mindestauflösung 1024 x 768, 1280 x 1024 empfohlen. Software-Voraussetzungen: ◆ Microsoft Internet Explorer 6.0 SP1 ◆ Microsoft Internet Explorer 7 ◆ oder Mozilla* Firefox 2.0

Systemkomponente	Systemanforderungen	Hinweise
Server für verbundenes System (Host auf einem separaten Server, auf dem Remote Loader ausgeführt wird) ◆ Remote Loader ◆ Remote Loader-Konfigurations-werkzeug (nur Windows) ◆ Novell Audit Agent ◆ Passwort-synchronisierungs-Agent ◆ Treiberschnitt-stellenmodul für das verbundene System ◆ Werkzeuge für das verbundene System	Für jeden Treiber muss das verbundene System verfügbar sein und die relevanten APIs müssen bereitgestellt werden. Informationen zu den systemspezifischen Anforderungen für das Betriebssystem und das verbundene System finden Sie in der Treiberdokumentation zu Identity Manager (http://www.novell.com/documentation/idmdrivers).	Jede verbundene Anwendung muss von Benutzern mit anwendungsspezifischen Kenntnissen und Zuständigkeiten bedient werden. Remote Loader-System: ◆ Windows NT* 4.0, Windows 2000 Server oder Windows Server 2003 mit den neuesten Support Packs ◆ Windows Server 2003 (64 Bit) mit dem neuesten Service Pack ◆ Der Passwortsynchronisierungs-Agent wird auf Windows Server 2003 (64 Bit) unterstützt ◆ Red Hat Linux 3.0, 4.0 und 5.0 ES und AS ◆ SUSE Linux Enterprise Server 9 oder 10 ◆ Solaris 9 oder 10 ◆ AIX 5.2L, Version 5.2 und 5.3 Java Remote Loader-System: ◆ HP-UX* 11i ◆ OS/400 ◆ zOS* ◆ Es sollte auf jedem System verwendet werden können, auf dem JVM 1.4.2 oder höher installiert ist

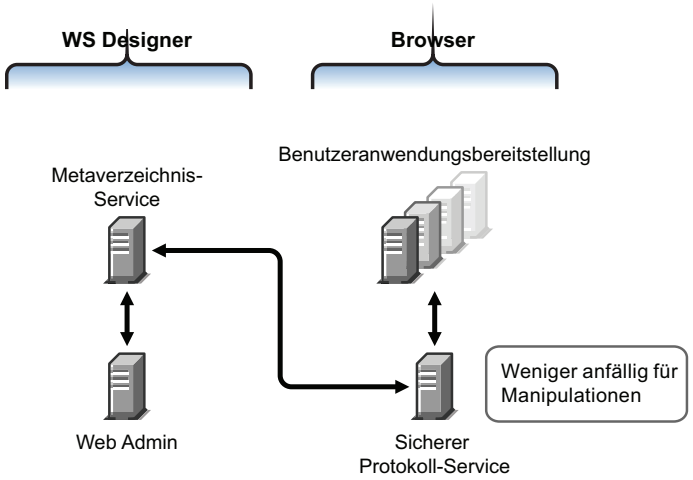
1.6 Empfohlene Bereitstellungsstrategien

In Identity Manager sind verschiedene Services integriert, die installiert und konfiguriert werden müssen. Alle erforderlichen Services können auf einem einzelnen Server installiert und konfiguriert werden, auch wenn dies in einer Produktionsumgebung nicht empfohlen wird. Sie können auch pro Server nur einen Service oder eine beliebige Anzahl dazwischen bereitstellen.

Der Hauptfaktor beim Entwerfen von Identity Manager-Bereitstellungen ist die Last. Je mehr Last verteilt werden kann, desto höher ist der potenzielle Durchsatz Ihrer Anwendungen.

Abbildung 1-3 zeigt eine mögliche Bereitstellungsstrategie, in der dem Metaverzeichnisservice, dem webbasierten Administrationsservice, dem sicheren Protokollierungsservice und den Benutzeranwendungs- und Bereitstellungsservices jeweils ein Server zugeordnet ist.

Abbildung 1-9 *Bereitstellungsstrategien für Identity Manager*



Metaverzeichnis-Service

Die Art der Bereitstellung der Identity Manager-Services hängt von der Servicelast ab. Sie können den Metaverzeichnis-Service von Identity Manager beispielsweise auf einem Server installieren, der mit den verbundenen Systemen kommuniziert. Sie müssen nur die Metaverzeichnis-Engine auf einem Server mit eDirectory installieren.

Wegen dem potenziell hohen Durchsatz mit iManager sollte der webbasierte Administrationsservice nicht zusammen mit dem Metaverzeichnis-Server installiert werden. Wenn Sie iManager auf demselben Server wie Identity Manager installieren, installieren Sie zunächst iManager und anschließend Identity Manager und seine Plugins.

Webbasierter Administrations-Service

Wenn auf einem Server bereits iManager 2.6 installiert ist, müssen Sie nur die Identity Manager-Installation ausführen und die Identity Manager-Plugins für iManager installieren. Wenn Sie die Benutzeranwendungs- und Bereitstellungsservices installieren, müssen Sie auch die Benutzeranwendungs-Installation ausführen und nur die Benutzeranwendungs-Plugins für iManager installieren. Dies müssen Sie entweder für die Benutzeranwendung oder für die Benutzeranwendung mit Bereitstellungsmodul durchführen (hierbei handelt es sich um zwei separate Produkte).

Benutzeranwendung und sichere Protokollierungsservices

Wenn Sie eine große Anzahl an Bereitstellungen vornehmen möchten, wird empfohlen, die Benutzeranwendung auf einem eigenen Server zu installieren. Sie können ggf. auch Clustering einrichten. MySQL 5.0.27-max wird mit der Benutzeranwendung zur Verfügung gestellt. Wird die Software als Teil der Installation der Benutzeranwendung oder der Benutzeranwendung mit Bereitstellungsmodul bereitgestellt, müssen Sie keinen weiteren Datenbankservice einrichten.

Der sichere Protokollierungsservice umfasst jedoch keine spezielle Datenbank, und sowohl für den sicheren Protokollierungsservice als auch für die Benutzeranwendungs- bzw. Bereitstellungsservices ist eine Datenbank erforderlich. Sie können für beide Anwendungen dieselbe Datenbank einrichten oder jedem Service eine eigene Datenbank zuordnen. Dies hängt von der Anzahl der Bereitstellungen und der Last des Protokollierungs-Services ab.

Hinweis: Wenn Oracle 9i oder 10g auf einem separaten (Remote-) Server eingerichtet werden soll, müssen Sie Oracle installieren und den Anwendungsserver so konfigurieren, dass eine Remote-Verbindung zur Datenbank möglich ist.

Verwendung der Remote Loader-Konfiguration

Sie können die Option *Server für verbundenes System* während der Installation von Identity Manager verwenden, wenn Sie die eDirectory-Services und die Metaverzeichnis-Engine nicht auf einem Server für ein verbundenes System installieren möchten. Der Remote Loader bietet durch die SSL-Technologie auch einen sicheren Kommunikationspfad zwischen der Metaverzeichnis-Engine und dem Treiber. Diese Punkte müssen bei der Verbindung von Systemen mit Identity Manager beachtet werden.

Weitere Informationen zur Planung des Identity Manager-Systems finden Sie in Kapitel 2, „Planung“, auf Seite 39.

1.7 Bezugsquellen für Identity Manager und -Services

So können Sie Identity Manager und -Services herunterladen:

1. Rufen Sie die Download-Website von Novell (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.

Die folgenden Identity Manager-Komponenten stehen zum Download bereit.

Tabelle 1-4 *Funktionsweise der ISO-Images*

Identity Manager-Komponenten	Plattformen	ISO
Identity Manager-DVD Die folgenden Identity Manager-Komponenten sind auf einem ISO-Image verfügbar und können auf DVD gebrannt werden. Diese Komponenten können auch einzeln heruntergeladen werden. ◆ Identity Manager und -Treiber ◆ Designer für Identity Manager	Identity Manager: Linux, NetWare, Windows und UNIX* Designer: Linux und Windows	Identity_Manager_3_5_1_DVD.iso
Identity Manager und -Treiber	NetWare und Windows	Identity_Manager_3_5_1_NW_Win.iso
Identity Manager und -Treiber	Linux	Identity_Manager_3_5_1_Linux.iso
Identity Manager und -Treiber	UNIX	Identity_Manager_3_5_1_Unix.iso
Benutzeranwendung Dies ist die Standardversion der Benutzeranwendung, die beim Kauf von Identity Manager 3 enthalten ist.	Linux und Windows	Identity_Manager_3_5_1_User_Application.iso
Benutzeranwendung mit dem Bereitstellungsmodul für Identity Manager Dies ist die Bereitstellungsversion der Benutzeranwendung. Hierbei handelt es sich um ein separat erhältliches Add-on für Identity Manager.	Linux und Windows	Identity_Manager_3_5_1_User_Application_Provisioning.iso
Designer für Identity Manager	Windows	Identity_Manager_3_5_1_Designer_Win.iso
Designer für Identity Manager	Linux	Identity_Manager_3_5_1_Designer_Linux.iso

Mit Identity Manager haben Sie Integrationsmodule für mehrere bekannte Kundensysteme erworben, für die Ihnen möglicherweise bereits Lizenzen vorliegen: Novell eDirectory, Microsoft Active Directory, Microsoft Windows NT, LDAP v3-Verzeichnisse, Novell GroupWise®, Microsoft Exchange und Lotus Notes. Alle anderen Identity Manager-Integrationsmodule sind separat erhältlich.

Die Benutzeranwendungskomponente wird in Form von zwei ISO-Images zur Verfügung gestellt: Das ISO-Image der Benutzeranwendung ist eine Standardversion, die im Kauf von Identity Manager-3 enthalten ist. Die Benutzeranwendung mit dem Bereitstellungsmodul für Identity Manager ist ein Add-on, das einen leistungsstarken Genehmigungs-Workflow integriert. Das Bereitstellungsmodul befindet sich auf einem separaten ISO-Image und ist separat erhältlich.

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.

1.7.1 Installation von Identity Manager 3.5.1

- Informationen zum Installieren von Identity Manager 3.5.1 unter Windows, NetWare, UNIX, und Linux finden Sie in Kapitel 4, „Installation von Identity Manager“, auf Seite 67.
- Informationen zum Installieren der Benutzeranwendung und der Benutzeranwendung mit Bereitstellungsmodul finden Sie in Kapitel 5, „Installation der Benutzeranwendung“, auf Seite 99.
- Informationen zum Installieren von Designer finden Sie im Abschnitt zur „Installation“ im Handbuch *Designer 2.1 für Identity Manager 3.5.1*.

Hinweis: Die Treiber-Installationsprogramme von Linux und UNIX (zuvor NIS), Mainframe und Midrange befinden sich im Verzeichnis `/platform/setup`. Diese Installationen müssen getrennt von den Identity Manager- und Benutzeranwendungs-Installationsprogrammen erfolgen.

Eine Liste der bekannten Probleme finden Sie in der `Readme`-Datei, die im Lieferumfang von Identity Manager enthalten ist.

1.7.2 Aktivieren von Identity Manager 3.5.1-Produkten

Die Identity Manager-Produkte müssen aktiviert werden (mit Ausnahme von Designer). Die folgenden Produkte können für einen Evaluierungszeitraum von 90 Tagen verwendet werden, bevor Sie sich für oder gegen den Erwerb einer Aktivierung entscheiden müssen.

- Identity Manager 3.5.1
- Benutzeranwendung mit dem Bereitstellungsmodul für Identity Manager
- Integrationsmodule

Wichtig: Damit die Benutzeranwendung ordnungsgemäß aktiviert werden kann, müssen Sie das richtige ISO-Image herunterladen. Wenn Sie beispielsweise Identity Manager erwerben, aber dann das Bereitstellungsmodul der Benutzeranwendung herunterladen, ohne das Bereitstellungsmodul separat zu erwerben, funktioniert die Benutzeranwendungs-Implementierung nach Ablauf von 90 Tagen nicht mehr.

Weitere Informationen zur Aktivierung finden Sie in Kapitel 6, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 193.

Planung

2

2.1 Planung der Projektmanagement-Aspekte der Identity Manager-Implementierung

In diesem Abschnitt werden die Projektmanagement-Aspekte der Identity Manager-Implementierung behandelt. (Die technischen Aspekte finden Sie in Abschnitt 2.3, „Planung der technischen Aspekte der Identity Manager-Implementierung“, auf Seite 55).

Diese Planungsmaterialien bieten einen Überblick über die Art der Aktivitäten, die in der Regel vom Beginn eines Identity Manager-Projekts bis hin zu seiner vollständigen Bereitstellung ausgeführt werden müssen. Zur Implementierung einer Identitätsmanagement-Strategie müssen Sie die Erfordernisse, die Projektbeteiligten und die am Projekt Interessierten in Ihrer Umgebung erkennen, eine Lösung entwerfen, das Buy-in der Beteiligten einholen und die Lösung testen und einführen. In diesem Abschnitt werden die Grundlagen dieses Prozesses erläutert, damit Sie aus Identity Manager den bestmöglichen Nutzen ziehen können.

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

Es wird empfohlen, eine Test-/Entwicklungsumgebung zu erstellen, in der Sie die Lösungen testen, analysieren und entwickeln können. Wenn alles wie gewünscht funktioniert, stellen Sie das Endprodukt in Ihrer Produktionsumgebung bereit.

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.

2.1.1 Novell Identity Manager-Bereitstellung

Bei der Bereitstellung von Identity Manager werden verschiedene Aktivitäten als Best Practices empfohlen.

- „Planung des Produktions-Rollout“ auf Seite 45
- „Produktionsbereitstellung“ auf Seite 46

Ermittlung

Es wird empfohlen, die Identity Manager-Implementierung mit einem Ermittlungsprozess zu starten, in dem Folgendes ermittelt wird:

- Identifikation der primären Ziele bei der Verwaltung von Identitätsinformationen
- Definieren und Klären der anzugehenden Geschäftsprobleme
- Festlegen der Initiativen, die zum Angehen ausstehender Probleme erforderlich sind
- Festlegen der Elemente, die zum Durchführen einer oder mehrerer dieser Initiativen erforderlich sind
- Entwicklung einer allgemeinen Strategie oder einer „Lösungs-Roadmap“ und eines Ausführungspfads

Mit der Ermittlung erhalten alle Projektbeteiligten einen allgemeinen Einblick in die Probleme und Lösungen. Dieses Werkzeug 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.

- Es verhilft allen Projektbeteiligten zu einem Grundverständnis
- Es kann wichtige Geschäfts- und Systeminformationen von den Projektbeteiligten abrufen
- Es kann eine Lösungs-Roadmap entwickeln

Das Ermittlungs-Werkzeug identifiziert auch die nächsten beiden Schritte, beispielsweise:

- Identifikation von Planungsaktivitäten zur Vorbereitung einer Anforderungs- und Entwurfsphase
- Definition zusätzlicher Schulungen für Projektbeteiligten

Ergebnisse

- Strukturierte Interviews mit den wichtigsten geschäftlichen und technischen Projektbeteiligten
- Allgemeine Zusammenfassung der geschäftlichen und technischen Aspekte
- Empfehlungen für die nächsten Schritte
- Eine Präsentation, in der das Ergebnis der Ermittlung zusammengefasst wird

Anforderungs- und Entwurfsanalyse

Diese Analyse erfasst die technischen und geschäftlichen Aspekte des Projekts im Detail und erzeugt das Datenmodell und einen allgemeinen Entwurf der Architektur von Identity Manager. Diese Aktivität ist ein entscheidender erster Schritt, auf dem die Implementierung der Lösung basiert.

Der Entwurf sollte besonders das Identitätsmanagement umfassen. Es können aber auch viele Elemente, die traditionell mit einem Ressourcen-Management-Verzeichnis, z. B. Archivierung und Drucken, behandelt werden. Hier finden Sie ein Beispiel für Elemente, die bewertet werden sollten:

- Welche Versionen der Systemsoftware werden verwendet?
- Ist der Verzeichnisentwurf zweckdienlich?
- Wird das Verzeichnis verwendet, um das Identitätsdepot und Identity Manager zu hosten, oder wird es zur Erweiterung anderer Services verwendet?
- Ist die Qualität der Daten in allen Systemen sachgemäß? (Wenn die Daten nicht verwendet werden können, wird die Geschäftsrichtlinie möglicherweise nicht wie gewünscht implementiert.)
- Ist in Ihrer Umgebung eine Datenmanipulation erforderlich?

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 möglichst umfassende Informationen und Dokumentationserfordernisse sammeln, damit kostspielige Fehler vermieden werden.

Bei der Bewertung der Anforderungen können folgende Aufgaben verarbeitet werden:

- „Definieren der Geschäftsanforderungen“ auf Seite 41
- „Analyse der Geschäftsprozesse“ auf Seite 42
- „Entwurf eines Enterprise-Datenmodells“ auf Seite 43

Definieren der Geschäftsanforderungen

Sammeln Sie die Geschäftsprozesse Ihres Unternehmens und die Geschäftsanforderungen, die diese Geschäftsprozesse definieren.

Beispiel: Eine Geschäftsanforderung bei der Kündigung eines Mitarbeiters könnte sein, dass am Tag der Kündigung der Zugriff des Mitarbeiters auf das Netzwerk und sein E-Mail-Konto gesperrt wird.

Die folgenden Aufgaben können Sie bei der Definition von Geschäftsanforderungen leiten:

- 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.
- Identifizieren Sie Daten, die von einem Format in ein anderes Format geändert werden sollen, 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.

Analyse der Geschäftsprozesse

Die Analyse von Geschäftsprozessen beginnt häufig mit der Befragung von Personen, beispielsweise Managern, Administratoren und Mitarbeitern, die mit der Anwendung oder dem System arbeiten. 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.

Entwurf eines Enterprise-Datenmodells

Nach der Definition der Geschäftsprozesse können Sie mit dem Entwurf eines Datenmodells beginnen, das Ihren aktuellen Geschäftsprozess widerspiegelt.

Das Modell sollte den Datenursprung sowie die Richtung des Datenflusses angeben und aufzeigen, wohin sie sich nicht bewegen dürfen. Außerdem sollte aufgezeigt sein, auf welche Weise sich kritische Ereignisse auf den Datenfluss auswirken.

Möglicherweise empfiehlt sich auch die Entwicklung eines Diagramms, das den vorgeschlagenen Geschäftsprozess und die Vorteile illustriert, 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, jedes Verzeichnissystem zu verstehen, in welcher Beziehung sie zueinander stehen und welche Objekte und Attribute systemübergreifend synchronisiert werden müssen.

Ergebnisse

- Datenmodell, das alle Systeme, autorisierte Datenursprünge, Ereignisse, Informationsfluss- und 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

Abhängigkeiten

- Mitarbeiter, die sich mit allen externen Systemen auskennen (z. B. der Administrator der Personaldatenbank, des Netzwerks und des Messaging-Systems)
- Verfügbarkeit von Systemschemata und Beispieldaten
- Datenmodell aus der Analyse- und Entwurfsphase
- Verfügbarkeit von Basisinformationen wie beispielsweise Organigramme sowie WAN- und Serverinfrastruktur

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.

Ergebnisse

- Ein funktionierendes Identity Manager Proof-of-Concept, in dem alle Systemverbindungen funktionsfähig sind

Abhängigkeiten

- Hardware-Plattform und -Ausrüstung
- Erforderliche Software
- Analyse- und Entwurfsphase, in der die erforderlichen Verbindungen identifiziert werden
- Verfügbarkeit und Zugriff auf andere Systeme zu Testzwecken
- Datenmodell aus der Analyse- und Entwurfsphase

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.

Ergebnisse

- Produktionsdatensätze, 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.
- Darüber hinaus werden Leistungsfaktoren mit der verwendeten Ausstattung und der gesamten verteilten Architektur der Identity Manager-Bereitstellung identifiziert und validiert.

Abhängigkeiten

- Datenmodell aus der Analyse- und Entwurfsphase (vorgeschlagene Strategie für den Datensatzabgleich und das Datenformat)
- Zugriff auf Produktionsdatensätze

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 gewünschte Ergebnisse der vorhergehenden Aktivitäten bestätigt und die Zustimmung für das Produktions-Rollout eingeholt werden.

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

Ergebnisse

- Die Prototyp-Lösung mit einem Live-Proof-of-Concept und der Validierung für das Datenmodell und die gewünschten Prozessergebnisse

Abhängigkeiten

- Alle vorherigen Aktivitäten (Analyse und Entwurf, Identity Manager-Technologieplattform)

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 der Einführung des Identitätsdepots in einer gemischten Umgebung
- Bestätigung der Partitionierungs- und Replizierungsstrategien
- Bestätigung der Identity Manager-Implementierung
- Planung der Umstellung auf den neuen Prozess
- Planung einer Rollback-Strategie für den Notfall

Ergebnisse

- Produktions-Rollout-Plan
- Plan für die Umstellung auf den neuen Prozess
- Rollback-Notfallplan

Abhängigkeiten

- Alle vorherigen Aktivitäten

Produktionsbereitstellung

In dieser Phase wird die Prototyp-Lösung auf alle Live-Daten in der Produktionsumgebung erweitert. In der Regel folgt die Bestätigung, dass der Produktions-Prototyp allen technischen und geschäftlichen Anforderungen entspricht.

Ergebnisse

- Produktionslösung bereit für den Übergang

Abhängigkeiten

- Alle vorherigen Aktivitäten

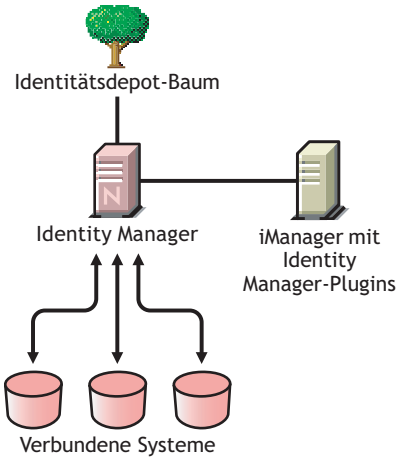
2.2 Planung allgemeiner Installationsszenarios

Die folgenden Szenarios sind Beispiele für eine Umgebung, in der Identity Manager verwendet werden kann. Für jedes Szenario finden Sie einige Richtlinien, die Sie bei der Implementierung unterstützen.

- Abschnitt 2.2.1, „Neue Installation von Identity Manager“, auf Seite 46
- Abschnitt 2.2.2, „Verwendung von Identity Manager und DirXML 1.1a in derselben Umgebung“, auf Seite 49
- Abschnitt 2.2.3, „Upgrade vom Starter Pack auf Identity Manager“, auf Seite 51
- Abschnitt 2.2.4, „Upgrade von Passwortsynchronisierung 1.0 auf die Identity Manager-Passwortsynchronisierung“, auf Seite 53

2.2.1 Neue Installation von Identity Manager

Abbildung 2-1 *Neue Installation*



Identity Manager ist eine Datenzugriffslösung, die das so genannte Identitätsdepot verwendet, um Daten anwendungs-, datenbank- und verzeichnisübergreifend zu synchronisieren, zu transformieren und zu verteilen.

Die Identity Manager-Lösung umfasst folgende Komponenten:

- „Identitätsdepot mit Identity Manager“ auf Seite 47
- „iManager-Server mit Identity Manager-Plugins“ auf Seite 47
- „Verbundene Systeme“ auf Seite 47
- „Allgemeine Identity Manager-Aufgaben“ auf Seite 47

Identitätsdepot mit Identity Manager

Das Identitätsdepot enthält die Benutzer- oder Objektdaten, die mit den verbundenen Systemen gemeinsam genutzt oder synchronisiert werden sollen. Es wird empfohlen, Identity Manager in einer eigenen eDirectory™-Instanz zu installieren und als Identitätsdepot zu verwenden.

iManager-Server mit Identity Manager-Plugins

Novell iManager und die Identity Manager-Plugins werden zur Verwaltung der Identity Manager-Lösung verwendet.

Verbundene Systeme

Die verbundenen Systeme enthalten möglicherweise andere Anwendungen, Verzeichnisse und Datenbanken, die mit dem Identitätsdepot gemeinsam Daten nutzen und synchronisieren sollen. Wenn Sie eine Verbindung zwischen dem Identitätsdepot und dem verbundenen System herstellen möchten, installieren Sie den entsprechenden Treiber für das System. Eine ausführliche Anleitung finden Sie in den entsprechenden Treiberimplementierungshandbüchern (http://www.novell.com/documentation/idm35drivers/index.html).

Allgemeine Identity Manager-Aufgaben

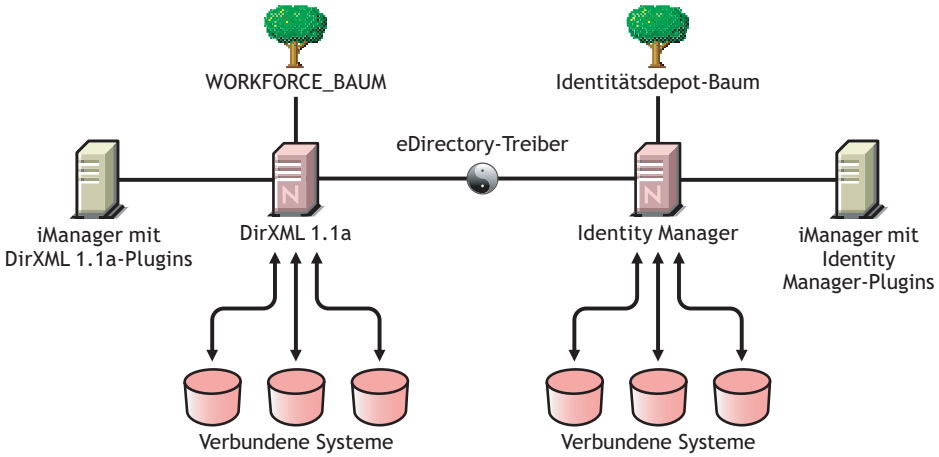
- **Installation der Systemkomponenten:** Da die Identity Manager-Lösung möglicherweise auf mehreren Computern, Servern oder Plattformen bereitgestellt wird, sollten Sie das Installationsprogramm ausführen und die entsprechenden Komponenten auf jedem System installieren. Weitere Informationen finden Sie in Abschnitt 1.4, „Identity Manager - Installationsprogramme und Services“, auf Seite 19.
- **Einrichtung verbundener Systeme:** Eine ausführliche Anleitung finden Sie in Abschnitt 1.4, „Identity Manager - Installationsprogramme und Services“, auf Seite 19 und in den entsprechenden Treiberimplementierungshandbüchern (http://www.novell.com/documentation/idm35drivers/index.html).
- **Aktivieren der Lösung:** Identity Manager-Produkte (Professional, Servereditionen, Integrationsmodule und Benutzeranwendungen) müssen innerhalb von 90 Tagen nach der Installation aktiviert werden. Siehe Kapitel 6, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 193.
- **Definieren von Geschäftsrichtlinien:** Mit Geschäftsrichtlinien können Sie für eine bestimmte Umgebung den Informationsfluss in das und aus dem Identitätsdepot anpassen. Außerdem können Sie mithilfe von Richtlinien neue Objekte erstellen, Attributwerte aktualisieren, Schema-Transformationen ausführen, Übereinstimmungskriterien definieren und Identity Manager-Verknüpfungen verwalten. Einen ausführlichen Leitfaden für Richtlinien finden Sie in *Richtlinien in iManager für Identity Manager 3.5.1*.
- **Konfiguration der Passwortverwaltung:** Mithilfe von Passwortrichtlinien kann die Sicherheit verbessert werden, indem Regeln zur Erstellung von Passwörtern durch Benutzer

eingerichtet werden. Darüber hinaus können die Helpdeskkosten reduziert werden, indem Benutzern Selbstbedienungsoptionen für vergessene Passwörter bereitgestellt werden. Ausführliche Informationen zur Passwortverwaltung finden Sie im Abschnitt zur Verwaltung von Passwörtern mithilfe von Passwortrichtlinien (http://www.novell.com/documentation/password_management31/index.html?page=/documentation/password_management31/pwm_administration/data/ampxjj0.html).

- **Konfigurieren von Berechtigungen:** Mithilfe von Berechtigungsdefinitionen können Sie auf verbundenen Systemen einer definierten Gruppe im Identitätsdepot Berechtigungen gewähren. Mithilfe von Berechtigungsrichtlinien lässt sich die Administration von Geschäftsrichtlinien vereinfachen und der Konfigurationsaufwand für die Identity Manager-Treiber wird reduziert. Weitere Informationen hierzu finden Sie unter „Creating and Using Entitlements“ (Erstellung und Verwendung von Berechtigungen) im *Novell Identity Manager 3.5.1 Administrationshandbuch*.
- **Protokollierung von Ereignissen mit Novell Audit:** Identity Manager kann mit Novell Audit zur Revision und Berichterstellung verwendet werden. Novell Audit besteht aus mehreren Modulen, die Funktionen zum Überwachen, zur Protokollierung, zur Berichterstellung und zur Benachrichtigung zur Verfügung stellen. Durch die Integration mit Novell Audit bietet Identity Manager detaillierte Informationen zum aktuellen und vergangenen Status der Treiber- und Engine-Aktivitäten. Diese Informationen werden von mehreren vorkonfigurierten Berichten, Standard-Benachrichtigungsservices und benutzerdefinierten Protokollierungen zur Verfügung gestellt. Weitere Informationen finden Sie unter „Using Status Logs“ (Statusprotokolle verwenden) in *Identity Manager 3.5.1 Logging and Reporting* (Identity Manager 3.5.1 Protokollierung und Berichterstellung).
- **Workflow-Genehmigung und Benutzeranwendung:** Die Novell Identity Manager-Benutzeranwendung ist eine leistungsstarke Webanwendung (mit unterstützenden Werkzeugen), die dem Benutzer ein umfangreiches, intuitives und flexibel konfigurierbares System auf der Grundlage eines hoch entwickelten Identitätsservices-Framework zur Verfügung stellt. Wenn die Identity Manager-Benutzeranwendung zusammen mit dem Bereitstellungsmodul für Identity Manager und Novell Audit verwendet wird, liefert sie eine umfassende Komplettlösung für die Bereitstellung, die sicher, skalierbar und einfach zu verwalten ist. Weitere Informationen hierzu finden Sie in der Dokumentation zur Benutzeranwendung (http://www.novell.com/documentation/idm35).

2.2.2 Verwendung von Identity Manager und DirXML 1.1a in derselben Umgebung

Abbildung 2-2 *Installation von Identity Manager und DirXML 1.1a im selben Baum*



Wenn Sie Identity Manager und DirXML® 1.1a in derselben Umgebung ausführen, müssen folgende Aspekte beachtet werden:

- „Erstellen eines Identitätsdepots“ auf Seite 49
- „Management-Tools“ auf Seite 49
- „Abwärtskompatibilität“ auf Seite 49
- „Passwortverwaltung“ auf Seite 50

Erstellen eines Identitätsdepots

Es wird empfohlen, Identity Manager in einer separaten eDirectory-Instanz zu installieren und als Identitätsdepot zu verwenden.

Management-Tools

- ConsoleOne® wird für DirXML 1.1a, nicht aber für Identity Manager unterstützt.
- Es werden zwei iManager-Server benötigt: einen für die DirXML 1.1a-Plugins und einen für die Identity Manager-Plugins. Dies ist erforderlich, weil die Plugins erweitert wurden und Identity Manager DirXML-Skript verwendet.
- iManager-Plugins für DirXML 1.1a können DirXML-Skript nicht lesen, das in den definierten Treiberkonfigurationen für die meisten Identity Manager-Treiber verwendet wird.
- Designer ist ein Werkzeug, mit dem Sie Identity Manager-Treiber entwerfen, testen, aktualisieren und dokumentieren können.

Abwärtskompatibilität

- Sie können DirXML 1.1a-Treiberschnittstellenmodule und -konfigurationen auf einem Identity Manager-Server ausführen und die Treiber des Treibersatzes in iManager unter „Identity Manager-Überblick“ anzeigen. Aber die Identity Manager-Plugins lassen die Anzeige oder

Bearbeitung der Treiberkonfigurationen erst nach einer Umwandlung in das Identity Manager-Format zu.

Wenn Sie in den Identity Manager-Plugins einen Treiber im 1.1a-Format auswählen, werden Sie aufgefordert, ihn zu konvertieren. Hierbei handelt es sich um einen einfachen Vorgang, der mithilfe eines Assistenten ausgeführt wird, und durch den die Funktionalität der Treiberkonfiguration nicht geändert wird. Als Teil des Vorgangs wird eine Sicherungskopie der DirXML 1.1a-Version gespeichert.

- Die Aktivierung für DirXML 1.1a-Treiber ist auch bei der Ausführung mit der Identity Manager-Engine noch gültig. Wenn Sie allerdings das Treiberschnittstellenmodul auf eine Identity Manager-Version aufrüsten, benötigen Sie für die Aktivierung einen neuen Berechtigungsnachweis. Weitere Informationen hierzu finden Sie in Anhang 6, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 193.
- In den meisten Fällen kann ein Identity Manager-Treiberschnittstellenmodul mit einer DirXML 1.1a-Konfiguration ausgeführt werden. Upgrade-Informationen finden Sie in den jeweiligen Treiberimplementierungshandbüchern (http://www.novell.com/documentation/idm35drivers/index.html).

  Es wird jedoch darauf hingewiesen, dass die Passwortsynchronisierung 1.0 unter Windows AD und Windows NT nach dem Upgrade des Treiberschnittstellenmoduls nur richtig ausgeführt wird, wenn weitere Treiberrichtlinien hinzugefügt werden. Eine Anleitung finden Sie in den Abschnitten zur Passwortsynchronisierung in den Treiber-Implementierungshandbüchern (http://www.novell.com/documentation/idm35drivers/index.html) zu den Identity Manager-Treibern für Active Directory und NT Domain.
- Die Ausführung von Identity Manager-Treiberschnittstellenmodulen und Treiberkonfigurationen mit der DirXML 1.1a-Engine wird nicht unterstützt.
- Die Ausführung von Identity Manager-Treiberkonfigurationen mit DirXML 1.1a-Treiberschnittstellenmodulen wird nicht unterstützt.
- Wenn auf mehreren Servern dieselbe Identity Manager-Treiberkonfiguration ausgeführt wird, stellen Sie sicher, dass auch dieselben Versionen von Identity Manager und eDirectory verwendet werden.

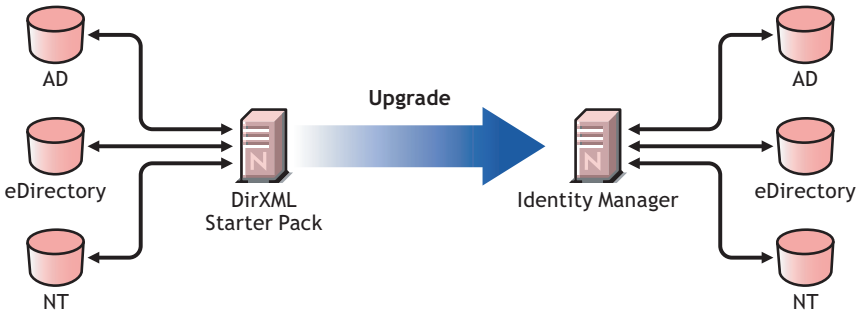
Passwortverwaltung

- Sie können Passwortrichtlinien einrichten, die den Benutzern Funktionen wie erweiterte Passwortregeln für sicherere Passwörter und Selbsthilfeoptionen bei vergessenen Passwörtern und zum Zurücksetzen von Passwörtern zur Verfügung stellen. Weitere Informationen hierzu finden Sie im Abschnitt zur Verwaltung der Passwortsynchronisierung im Handbuch zur Passwortverwaltung 3.1 (http://www.novell.com/documentation/password_management31/index.html).
- Wenn Sie bei der ersten Ausgabe von NetWare® 6.5 ein universelles Passwort verwendet haben, sind einige Upgrade-Schritte erforderlich, bevor die neuen Passwortrichtlinien-Funktionen verwendet werden können. Weitere Informationen hierzu finden Sie im Abschnitt zum Bereitstellen eines universellen Passworts (nur NetWare 6.5) im Handbuch zur Passwortverwaltung 3.1 (http://www.novell.com/documentation/password_management31/index.html). Diese Schritte sind nicht erforderlich, wenn Sie das universelle Passwort in NetWare 6.5 SP2 verwendet haben.
- Die Identity Manager-Passwortsynchronisierung bietet eine bidirektionale Passwortsynchronisierung und unterstützt mehr Plattformen als die Passwortsynchronisierung 1.0.

- Wenn Sie die Passwortsynchronisierung 1.0 unter Windows AD oder Windows NT verwendet haben, lesen Sie vor der Installation der neuen Treiberschnittstellenmodule die Upgrade-Anweisungen. Siehe Abschnitt 2.2.4, „Upgrade von Passwortsynchronisierung 1.0 auf die Identity Manager-Passwortsynchronisierung“, auf Seite 53.
- Es werden Treiberrichtlinien-Overlays zur Verfügung gestellt, mit denen Sie die bidirektionale Passwortsynchronisierung zu bestehenden Treibern hinzufügen können. Weitere Informationen hierzu finden Sie unter „Upgrading Existing Driver Configurations to Support Password Synchronization“ (Aufrüsten bestehender Treiberkonfigurationen zur Unterstützung der Passwortsynchronisierung) im *Novell Identity Manager 3.5.1 Administrationshandbuch*.

2.2.3 Upgrade vom Starter Pack auf Identity Manager

Abbildung 2-3 *Upgrade vom Starter Pack auf Identity Manager*



Die Lösungen des Identity Manager Starter Pack, die in anderen Novell-Produkten enthalten sind, stellen eine lizenzierte Synchronisierung von Informationen in NT-Domänen, Active Directory und eDirectory zur Verfügung. Weiterhin sind Evaluierungstreiber für verschiedene andere Systeme, z. B. PeopleSoft, GroupWise® und Lotus Notes enthalten, mit denen die Datensynchronisierung der anderen Systeme erkundet werden kann.

Diese Lösung bietet auch die Möglichkeit zur Synchronisierung von Benutzerpasswörtern. Mit PasswordSync muss ein Benutzer sich nur an ein einziges Passwort erinnern, über das er sich bei all diesen Systemen anmelden kann. Die Administratoren können die Passwörter in einem System ihrer Wahl verwalten. Wird ein Passwort in einer dieser Umgebungen geändert, wird es auch in den anderen Umgebungen aktualisiert.

Identity Manager Starter Packs, die in NetWare 6.5 und Nterprise™ Linux Services 1.0 enthalten sind, basieren auf der DirXML 1.1a-Technologie. Beim Upgrade von einem Starter Pack zu der neuesten Version von Identity Manager müssen folgende Aspekte beachtet werden:

- „Abwärtskompatibilität“ auf Seite 51
- „Passwortverwaltung“ auf Seite 52
- „Aktivierung“ auf Seite 52

Abwärtskompatibilität

- Sie können DirXML 1.1a-Treiberschnittstellenmodule und -konfigurationen auf einem Identity Manager-Server ausführen und die Treiber des Treibersatzes in iManager unter „Identity Manager-Überblick“ anzeigen. Aber die Identity Manager-Plugins lassen die Anzeige oder Bearbeitung der Treiberkonfigurationen erst nach einer Umwandlung in das Identity Manager-Format zu.

Wenn Sie in den Identity Manager-Plugins einen Treiber im 1.1a-Format auswählen, werden Sie aufgefordert, ihn zu konvertieren. Hierbei handelt es sich um einen einfachen Vorgang, der mithilfe eines Assistenten ausgeführt wird, und durch den die Funktionalität der Treiberkonfiguration nicht geändert wird. Als Teil des Vorgangs wird eine Sicherungskopie der DirXML 1.1a-Version gespeichert.

- Die Aktivierung für DirXML 1.1a-Treiber ist auch bei der Ausführung mit der Identity Manager-Engine noch gültig. Wenn Sie allerdings das Treiberschnittstellenmodul auf eine Identity Manager-Version aufrüsten, benötigen Sie eine neue Aktivierung.
- In den meisten Fällen kann ein Identity Manager-Treiberschnittstellenmodul mit einer DirXML 1.1a-Konfiguration ausgeführt werden. Upgrade-Informationen finden Sie in den jeweiligen Treiberimplementierungshandbüchern (http://www.novell.com/documentation/idm35drivers/index.html).

  Es wird jedoch darauf hingewiesen, dass die Passwortsynchronisierung 1.0 unter Windows AD und Windows NT nach dem Upgrade des Treiberschnittstellenmoduls nur richtig ausgeführt wird, wenn weitere Treiberrichtlinien hinzugefügt werden. Eine Anleitung finden Sie in den Abschnitten zur Passwortsynchronisierung in den Treiber-Implementierungshandbüchern (http://www.novell.com/documentation/idm35drivers/index.html) zu den Identity Manager-Treibern für Active Directory und NT Domain.
- Die Ausführung von Identity Manager-Treiberschnittstellenmodulen und Treiberkonfigurationen mit der DirXML 1.1a-Engine wird nicht unterstützt.
- Die Ausführung von Identity Manager-Treiberkonfigurationen mit DirXML 1.1a-Treiberschnittstellenmodulen wird nicht unterstützt.
- Wenn auf mehreren Servern dieselbe Identity Manager-Treiberkonfiguration ausgeführt wird, stellen Sie sicher, dass auch dieselben Versionen von Identity Manager und eDirectory verwendet werden.

Passwortverwaltung

- Die Passwortsynchronisierung 1.0, die in den Starter Packs (DirXML 1.1a) mitgeliefert wird, wird unter Windows AD und Windows NT nach dem Upgrade des Treiberschnittstellenmoduls nur richtig ausgeführt, wenn weitere Treiberrichtlinien hinzugefügt werden. Eine Anleitung finden Sie in den Abschnitten zur Passwortsynchronisierung in den Treiber-Implementierungshandbüchern (http://www.novell.com/documentation/idm35drivers/index.html) zu den Identity Manager-Treibern für Active Directory und NT Domain.
- Weitere Informationen zu diesem Upgrade-Prozess finden Sie in Abschnitt 2.2.4, „Upgrade von Passwortsynchronisierung 1.0 auf die Identity Manager-Passwortsynchronisierung“, auf Seite 53.

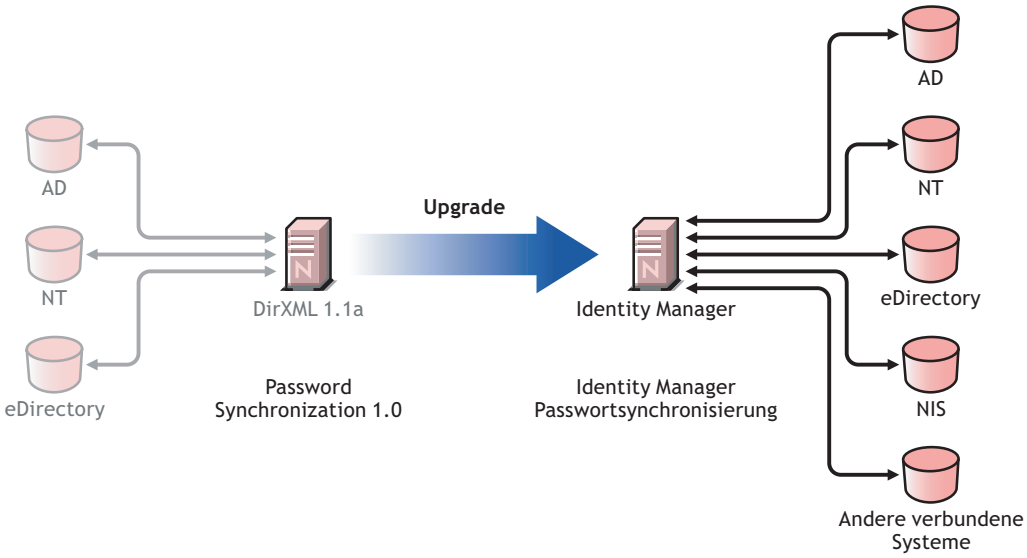
Aktivierung

- Alle Identity Manager-Produkte müssen innerhalb von 90 Tagen aktiviert werden. Wenn Sie weitere Novell-Software erworben haben, enthielt das DirXML Starter Pack Aktivierungen für die DirXML 1.1a-Engine und die NT-, AD- und eDirectory-Treiber. Erfolgt das Upgrade vom Identity Manager Starter Pack, müssen Sie möglicherweise die Berechtigungsnachweise für die Aktivierung dieser Treiber erneut verwenden.

  Weitere Informationen zur Aktivierung finden Sie in Anhang 6, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 193.

2.2.4 Upgrade von Passwortsynchronisierung 1.0 auf die Identity Manager-Passwortsynchronisierung

Abbildung 2-4 *Upgrade von Passwortsynchronisierung 1.0 auf die Identity Manager-Passwortsynchronisierung*



Die Identity Manager-Passwortsynchronisierung stellt viele Funktionen zur Verfügung, einschließlich bidirektionaler Passwortsynchronisierung, zusätzlichen Plattformen und Email-Benachrichtigung, falls bei der Passwortsynchronisierung ein Fehler auftritt.

Wenn Sie die Passwortsynchronisierung 1.0 mit Active Directory oder NT-Domäne verwenden, ist es sehr wichtig, vor der Installation der neuen Treiberschnittstellenmodule die Upgrade-Anleitung durchzulesen.

Wenn Sie Identity Manager 2.x mit der Passwortsynchronisierung 2.0 ausführen, müssen Sie diese Schritte nicht befolgen.

Allgemeine Informationen zur Identity Manager-Passwortsynchronisierung finden Sie unter „Password Synchronization across Connected Systems“ (Passwortsynchronisierung mit verbundenen Systemen) im *Novell Identity Manager 3.5.1 Administrationshandbuch*. Dieser Abschnitt enthält Informationen zur Konzeption sowie einen Vergleich alter und neuer Funktionen, Voraussetzungen, eine Liste mit den unterstützten Funktionen der verbundenen Systeme, Anweisungen zur Unterstützung vorhandener Treiber und verschiedene Szenarios, in denen dargestellt wird, wie Sie die neuen Funktionen verwenden können.

In diesem Abschnitt:

- „Upgrade der Passwortsynchronisierung für Active Directory oder Windows NT“ auf Seite 54
- „Upgrade der Passwortsynchronisierung für eDirectory“ auf Seite 54
- „Upgrade anderer Treiber verbundener Systeme“ auf Seite 54
- „Bearbeitung vertraulicher Informationen“ auf Seite 55

Upgrade der Passwortsynchronisierung für Active Directory oder Windows NT

Die neue Passwortsynchronisierung erfolgt nicht über einen separaten Agenten, sondern auf Basis von Treiberrichtlinien. Dies hat zur Folge, dass die Passwortsynchronisierung 1.0 auch weiterhin nur für vorhandene Benutzer funktioniert, wenn Sie das neue Treiberschnittstellenmodul installieren, ohne gleichzeitig auch ein Upgrade der Treiberkonfiguration durchzuführen. Für neue, verschobene oder umbenannte Benutzer funktioniert die Passwortsynchronisierung erst, wenn das Upgrade der Treiberkonfiguration abgeschlossen ist.

Führen Sie das Upgrade wie folgt durch:

1. Führen Sie ein Upgrade der Umgebung durch, sodass die Verwendung eines universellen Passworts unterstützt wird. Führen Sie ggf. auch ein Upgrade von Novell Client™ durch.
2. Installieren Sie das Identity Manager 3.5.1-Treiberschnittstellenmodul. Es ersetzt das DirXML 1.1a-Treiberschnittstellenmodul für Active Directory oder Windows NT.
3. Erstellen Sie direkt eine Abwärtskompatibilität mit der Passwortsynchronisierung 1.0, indem Sie der Treiberkonfiguration eine neue Richtlinie hinzufügen.

   Durch diesen Schritt funktioniert die Passwortsynchronisierung 1.0 auch weiterhin korrekt, bis die Umstellung auf die Identity Manager-Passwortsynchronisierung erfolgt.
4. Sorgen Sie mithilfe von Treiberrichtlinien für die Unterstützung der neuen Identity Manager-Passwortsynchronisierung.
5. Installieren und konfigurieren Sie neue Filter für die Passwortsynchronisierung.
6. Richten Sie ggf. SSL ein.
7. Aktivieren Sie ggf. mithilfe von Passwortrichtlinien das universelle Passwort.
8. Richten Sie das Szenario für die Identity Manager-Passwortsynchronisierung ein, das Sie verwenden möchten.

   Weitere Informationen hierzu finden Sie unter „Implementing Password Synchronization“ (Implementierung der Passwortsynchronisierung) im *Novell Identity Manager 3.5.1 Administrationshandbuch*.
9. Entfernen der Passwortsynchronisierung 1.0

Eine ausführliche Anleitung finden Sie in den Treiber-Implementierungshandbüchern (http://www.novell.com/documentation/idm35drivers/index.html) zu den Identity Manager-Treibern für Active Directory und NT-Domäne.

Upgrade der Passwortsynchronisierung für eDirectory

Das Upgrade für eDirectory ist recht unkompliziert. Sofern das Treiberschnittstellenmodul und die Konfiguration über die neuesten Patches verfügen, sollte das Treiberschnittstellenmodul mit der vorhandenen DirXML 1.1a-Treiberkonfiguration funktionieren, ohne dass Änderungen vorgenommen werden müssen. Eine Anleitung finden Sie im *Implementierungshandbuch zum Identity Manager 3.5.1-Treiber für eDirectory*.

Upgrade anderer Treiber verbundener Systeme

Die Identity Manager-Passwortsynchronisierung unterstützt mehr verbundene Systeme als die Passwortsynchronisierung 1.0.

Eine Liste der Funktionen, die für andere Systeme unterstützt werden, finden Sie unter „Connected System Support for Password Synchronization“ (Unterstützung von verbundenen Systemen bei der Passwortsynchronisierung) im *Novell Identity Manager 3.5.1 Administrationshandbuch*.

Es werden Treiberrichtlinien-Overlays zur Verfügung gestellt, mit denen Sie die bidirektionale Passwortsynchronisierung zu bestehenden Treibern verbundener Systeme hinzufügen können, die zuvor nicht unterstützt wurden. Weitere Informationen hierzu finden Sie unter „Upgrading Existing Driver Configurations to Support Password Synchronization“ (Aufrüsten bestehender Treiberkonfigurationen zur Unterstützung der Passwortsynchronisierung) im *Novell Identity Manager 3.5.1 Administrationshandbuch*.

Bearbeitung vertraulicher Informationen

Das universelle Passwort wird in eDirectory durch vier Verschlüsselungsstufen geschützt, sodass es in der Umgebung sehr sicher ist. Wenn Sie die bidirektionale Passwortsynchronisierung ausgewählt haben und Sie das universelle Passwort mit dem Verteilungspasswort synchronisieren, denken Sie daran, das Passwort aus eDirectory zu extrahieren und an andere verbundene Systeme zu senden. Sie müssen sowohl die Übertragung des Passworts als auch die verbundenen Systeme, mit denen es synchronisiert wird, absichern.

Zusätzlich zu den Passwörtern können Sie auch Novell SecretStore® und Novell SecureLogin für die Synchronisierungen von Berechtigungsnachweisen verwenden. Dies ermöglicht die Bereitstellung der SecureLogin-Passwortfrage und -antwort in Umgebungen, in denen absolute Eindeutigkeit erwünscht ist. Weitere Informationen hierzu finden Sie unter „Security: Best Practices“ (Sicherheit: Best Practices) im *Novell Identity Manager 3.5.1 Administrationshandbuch*.

2.3 Planung der technischen Aspekte der Identity Manager-Implementierung

2.3.1 Verwendung von Designer

Identity Manager enthält ein Dienstprogramm namens Designer. Mit Designer können Sie Identity Manager-Treiber entwerfen, testen und dokumentieren. Außerdem können Sie mit Designer den Ablauf der Passwortsynchronisierung und Datenflüsse anzeigen. Weitere Informationen hierzu finden Sie im *Administrationshandbuch zu Designer 2.1 für Identity Manager 3.5.1*.

2.3.2 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. Es wird empfohlen, 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 festgelegt haben (Regeln für die Bereichsfilterung).

  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 Einzelserver, 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 57.

- **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 beispielweise 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.

2.3.3 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.

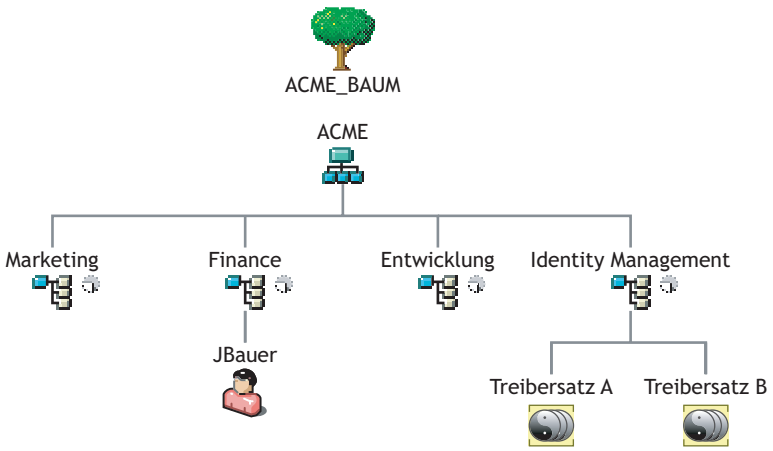
Hinweis: Sie sollten die Bereichsfilterung auch dann verwenden, wenn sich die Reproduktionen der Server gegenwärtig nicht überschneiden. Es könnte sein, dass zu einem

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 Identity Manager-Container, in dem die Treibersätze gespeichert sind. Jeder dieser Container ist eine separate Partition.

Abbildung 2-5 *Beispielbaum für die Bereichsfilterung*



In diesem Beispiel verfügt der Identity Manager-Administrator über zwei Identitätsdepot-Server, Server A und Server B (siehe Abbildung 2-6 auf Seite 59). 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.

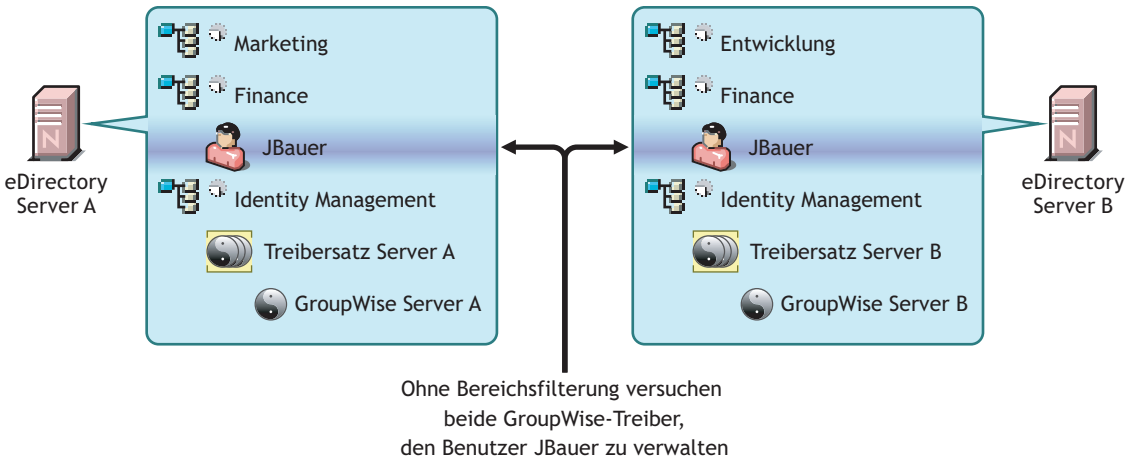
Der Administrator möchte, dass alle Benutzer im Baum vom GroupWise-Treiber synchronisiert werden, aber es sollen keine Reproduktionen der Benutzer auf einem einzelnen Server zusammengefasst werden. Stattdessen verwendet er zwei Instanzen des GroupWise-Treibers, von denen sich eine auf Server A, die andere 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.

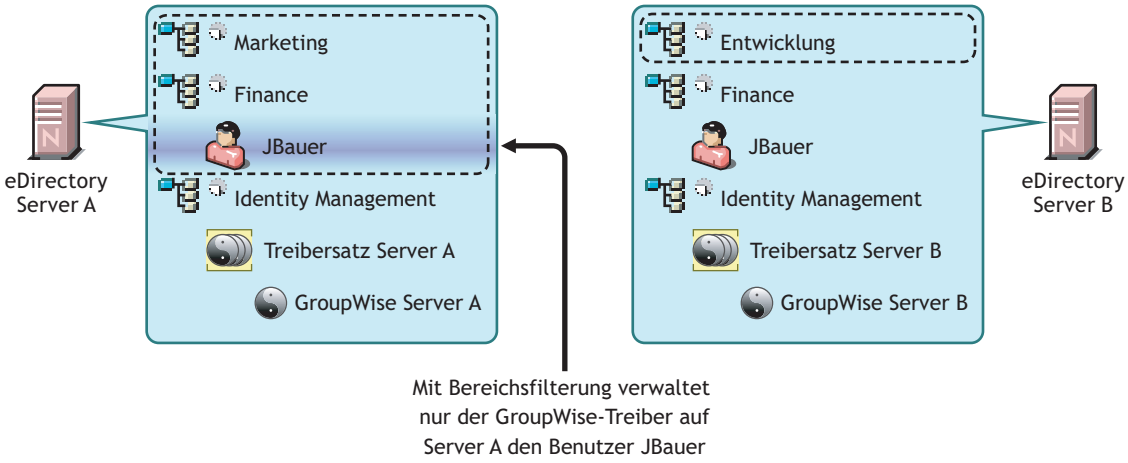
Da sich sowohl auf Server A als auch auf Server B eine Reproduktion des Containers „Finanzen“ befindet, ist auf beiden Servern der Benutzer „JBassad“ gespeichert, der sich im Container „Finanzen“ befindet. Ohne Bereichsfilterung nimmt sowohl GroupWise-Treiber A als auch GroupWise-Treiber B die Synchronisierung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

Abbildung 2-6 *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 2-7 *Die Bereichsfilterung definiert, welche Treiber die einzelnen Container synchronisieren*



In Identity Manager 3.5.1 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 *Richtlinien für Identity Manager 3.5.1*.

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“.

Upgrades

3

Identity Manager besteht aus vielen verschiedenen Teilen. Damit Identity Manager erfolgreich aufgerüstet werden kann, müssen Sie alle Aspekte des Produkts berücksichtigen.

Einige Upgrade-Szenarios werden in Abschnitt 2.2, „Planung allgemeiner Installationsszenarios“, auf Seite 46 beschrieben.

3.1 Upgrade-Pfade

Die Tabelle enthält die unterstützten Upgrade-Szenarios für die unterschiedlichen Versionen von Identity Manager. Für jedes Szenario ist angegeben, ob es unterstützt wird oder nicht.

Tabelle 3-1 *Upgrade-Pfad-Szenarios*

Installierte Version	Aktuelle Version	Wird ein Upgrade unterstützt?
DirXML® 1.1a	Identity Manager 3.5.1	Ja
Identity Manager 2.x	Identity Manager 3.5.1	Ja
Identity Manager 3.0x	Identity Manager 3.5.1	Ja

3.2 Änderungen an der Richtlinienarchitektur

Identity Manager 3.5 und 3.5.1 enthalten eine neuere Richtlinienarchitektur, die sich darauf auswirkt, wie Richtlinien aufeinander Bezug nehmen. Während die 3.5-Treiberarchitektur erweiterte Funktionen in der Identity Manager 3.5.1-Umgebung bietet, kann die 3.0.x-Metaverzeichnis-Engine keine 3.5-Treiberkonfigurationen ausführen.

Identity Manager 3.5 und 3.5.1 können jedoch 3.0.x-Treiberkonfigurationen ausführen. Wenn Sie über 3.0.x-Treiberkonfigurationen verfügen, die sowohl mit 3.0.x- als auch mit 3.5 -Metaverzeichnis-Engines verknüpft sind, aktualisieren Sie die 3.0.x-Treiber nicht. Die 3.0.x -Treiberkonfigurationen funktionieren in einer 3.5.1-Umgebung, sie besitzen jedoch nicht die erweiterten Funktionen, die Identity Manager 3.5 und höher bietet. Wenn 3.0.x -Treiberkonfigurationen nur mit einer Metaverzeichnis-Engine der Version 3.5 oder höher verknüpft sind, sollten Sie die 3.0.x-Treiber auf Version 3.5.1 aktualisieren.

Weitere Informationen zur Richtlinienarchitektur und dem Aktualisieren von Treibern auf Version 3.5.1 finden Sie unter „Upgrading Identity Manager Policies“ (Aufrüsten von Identity Manager-

Richtlinien) in *Understanding Policies for Identity Manager 3.5.1* (Richtlinien für Identity Manager 3.5.1).

3.3 Aufrüsten

Damit das Aufrüsten auf Identity Manager 3.5.1 erfolgreich ist, müssen die folgenden Schritte ausgeführt werden.

3.3.1 Export von Treibern

Der wichtigste Schritt vor dem Upgrade ist die Sicherung der aktuellen Treiber und deren Konfigurationsdaten. Bevor Sie die Treiber sichern können, müssen Sie sie exportieren.

Export aus ConsoleOne

1. Klicken Sie in ConsoleOne® mit der rechten Maustaste auf das Treibersatzobjekt und wählen Sie anschließend *Eigenschaften* > *DirXML* > *Treiber*.
2. Wählen Sie den Treiber aus, den Sie exportieren möchten, und klicken Sie anschließend auf *Exportieren*.
3. Geben Sie einen Dateinamen ein. Behalten Sie die Standarderweiterung `.xml` bei und klicken Sie anschließend auf *Speichern*.
4. Klicken Sie auf *Konfiguration exportieren*.

In iManager können Sie einen einzelnen Treiber oder den vollständigen Treibersatz exportieren. Beim Export des Treibersatzes wird eine einzelne Konfigurationsdatei erstellt. Wenn Sie die Treiber einzeln exportieren, wird für jeden Treiber eine Konfigurationsdatei erstellt.

Export aus iManager

1. Wählen Sie in iManager *DirXML-Dienstprogramme* > *Treiber exportieren*.
2. Wählen Sie den zu exportierenden Treiber bzw. Treibersatz aus und klicken Sie anschließend auf *Weiter*.
3. Lassen Sie die Eingabeaufforderungen leer, damit eine genaue Kopie des Treibers erstellt wird, und klicken Sie anschließend auf *Weiter*.
4. Wenn Sie das Treibersatzobjekt auswählen, wird für jeden Treiber eine Eingabeaufforderung angezeigt. Lassen Sie die Felder für jeden Treiber leer, damit eine genaue Kopie erstellt wird.
5. Klicken Sie auf *Speichern unter*.

6 Klicken Sie im Fenster zum Herunterladen von Dateien auf *Speichern*.

7 Wählen Sie einen Speicherort und einen Namen für die Datei aus und klicken Sie anschließend auf *Speichern*.

Wichtig: Bei der Speicherung muss die Datei über die Erweiterung `.xml` verfügen.

Wenn Ihnen die exportierte Datei vorliegt, testen Sie sie in einer Laborumgebung. Importieren Sie die exportierte Datei und testen Sie den Treiber, um sicherzustellen, dass alle Parameter richtig und alle Funktionen vorhanden sind.

Export aus Designer

1 Klicken Sie in Designer im Modellierer mit der rechten Maustaste auf das Treiber- oder Treibersatzobjekt und klicken Sie anschließend auf *In Konfigurationsdatei exportieren*.

2 Wählen Sie im Fenster „Treiberkonfiguration exportieren“ einen Speicherort und einen Namen für die Datei aus und klicken Sie anschließend auf *Speichern*.

3.3.2 Überprüfung der Mindestanforderungen

Für das Aufrüsten auf Identity Manager 3.5.1 müssen die Server, die die Identity Manager-Services ausführen, die Mindestanforderungen erfüllen. In Tabelle 1-3 auf Seite 29 finden Sie eine Liste der Mindestanforderungen für jede Plattform.

Wenn ein Upgrade der unterstützten Komponenten erfolgen muss, führen Sie die Upgrades in folgender Reihenfolge durch:

1. Führen Sie ein Upgrade des Betriebssystems auf eine unterstützte Version durch. Beispiel: Upgrade von NetWare® 6.0 auf NetWare 6.5.
2. Rüsten Sie eDirectory™ auf eDirectory 8.7.3.6 mit dem neuesten Support Pack oder auf eDirectory 8.8 mit dem neuesten Support Pack auf.
3. Es muss Security Services 2.0.5 mit NMAS™ 3.1.3 für die SSL-Unterstützung installiert sein.
4. Rüsten Sie iManager auf iManager 2.6 oder 2.7 mit dem neuesten Support Pack auf (dies schließt das Aufrüsten auf Apache 2.0.52 oder höher und Tomcat 4.1.18 oder höher ein).
5. Außerdem muss im Netzwerk Novell® Audit 2.0.2 mit Starter Pack oder Sentinel™ 5.1.3 installiert sein.
6. Informationen zur Identity Manager-Benutzeranwendung und -Bereitstellung finden Sie in Abschnitt 5.1, „Voraussetzungen für die Installation“, auf Seite 99.
7. Führen Sie ein Upgrade von Identity Manager durch.
8. Aktivieren Sie die Metaverzeichnis-Engine und die aufgerüsteten Treiber.

3.3.3 Upgrade der Engine

Nach dem Upgrade der unterstützten Komponenten erfolgt ein Upgrade der DirXML- oder Identity Manager-Engine.

1 Stellen Sie vor dem Upgrade sicher, dass Sie über eine fehlerfreie Exportdatei der Treiber verfügen. Weitere Informationen hierzu finden Sie in Abschnitt 3.3.1, „Export von Treibern“, auf Seite 62.

2 Halten Sie die Treiber an.

2a Klicken Sie in iManager auf *Identity Manager* > *Identity Manager-Überblick*.

2b Wählen Sie das Treibersatzobjekt aus und klicken Sie auf *Suchen*.

2c Klicken Sie auf die obere rechte Ecke des Treibersymbols und wählen Sie anschließend *Treiber anhalten*.

3 Legen Sie fest, dass die Treiber manuell gestartet werden sollen.

3a Klicken Sie in iManager auf *Identity Manager* > *Identity Manager-Überblick*.

3b Wählen Sie das Treibersatzobjekt aus und klicken Sie auf *Suchen*.

3c Klicken Sie in der oberen rechten Ecke des Treibersymbols auf *Eigenschaften bearbeiten*.

3d Wählen Sie auf der Seite „Treiberkonfiguration“ unter *Startoption* die Option *Manuell* aus.

4 Installieren Sie Identity Manager 3.5.1.

Die Schritte für das Aufrüsten auf Identity Manager 3.5.1 sind identisch mit den Schritten für die Installation von Identity Manager 3.5. Eine Anleitung für die Installation von Identity Manager finden Sie in Kapitel 4, „Installation von Identity Manager“, auf Seite 67.

Identity Manager 3.5.1 wird über frühere Versionen von Identity Manager kopiert. Gleichzeitig werden die Binärdateien aktualisiert. Sowohl iManager als auch Designer aktualisieren die Treiber auf die neue Funktionalität.

4a Klicken Sie in iManager auf die Treiber, um den Aufrüstungsassistenten für Treiber zu starten.

Wenn Designer alte Treiber erkennt, wird der Aufrüstungsassistent für Treiber automatisch gestartet.

5 Legen Sie die Treiber-Startoptionen fest.

5a Klicken Sie in iManager auf *Identity Manager* > *Identity Manager-Überblick*.

5b Wählen Sie das Treibersatzobjekt aus und klicken Sie auf *Suchen*.

5c Klicken Sie in der oberen rechten Ecke des Treibersymbols auf *Eigenschaften bearbeiten*.

5d Wählen Sie auf der Seite „Treiberkonfiguration“ unter *Startoption* die Option *Autom. starten* aus oder wählen Sie die gewünschte Methode für den Start des Treibers aus.

6 Überprüfen Sie, ob die Treiberparameter und -richtlinien wie gewünscht eingerichtet sind.

7 Starten Sie den Treiber.

7a Klicken Sie in iManager auf *Identity Manager* > *Identity Manager-Überblick*.

7b Wählen Sie das Treibersatzobjekt aus und klicken Sie auf *Suchen*.

7c Klicken Sie auf die obere rechte Ecke des Treibersymbols und wählen Sie anschließend *Treiber starten*.

3.3.4 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\` *`NamedesRemoteLoaders-config.txt`*

- Linux: Erstellen Sie im „rdxml“-Pfad Ihre eigene Konfigurationsdatei.

2. Halten Sie den Remote Loader-Service oder -Daemon an.
3. Führen Sie die Installationsprogramme für den Remote Loader aus.

   Hierdurch werden die Dateien und Binärdateien auf die aktuelle Version aufgerüstet. Weitere Informationen hierzu finden Sie unter „Installing the Remote Loader“ (Installieren von Remote Loadern) im *Novell Identity Manager 3.5.1 Administrationshandbuch*.

3.3.5 Aufrüsten in einer UNIX/Linux-Umgebung

Beim Aufrüsten von Identity Manager 3.0.1 auf Identity Manager 3.5.1 in einer UNIX- oder Linux-Umgebung werden zwei Deinstallationsverzeichnisse erstellt und die Pakete nicht vollständig entfernt. Wenn Sie beispielsweise mit einer UNIX-Plattform beginnen, z. B. SLES 9, und Identity Manager 3.0.1 installieren, befindet sich das Identity Manager-Deinstallationsverzeichnis im Verzeichnis `/root/dirXML`. Durch die Eingabe von `rpm -qa | grep -i dxml` wird angezeigt, wann die dxml-Pakete installiert wurden.

Wenn nun diese Bereitstellung auf Identity Manager 3.5.1 aufgerüstet wird, wird aufgrund der Namensänderung im Verzeichnis `/root/idm` ein neues Deinstallationsverzeichnis erstellt. Durch die Eingabe von `rpm -qa` wird angezeigt, wann die aktualisierten Pakete installiert wurden.

Wenn der Administrator Identity Manager 3.5.1 deinstalliert, werden aufgrund der Verzeichnisänderung nicht alle Pakete deinstalliert, obwohl gemeldet wird, dass alle Elemente erfolgreich entfernt wurden. Verwenden Sie das DirXML-Deinstallationsprogramm, um die restlichen Pakete zu deinstallieren.

3.4 Upgrade der Passwortsynchronisierung

Beim Aufrüsten von DirXML 1.1a auf Identity Manager 3.5.1 ist auch das Aufrüsten der Passwortsynchronisierung erforderlich. Weitere Informationen hierzu finden Sie unter „Upgrading Password Synchronization 1.0“ (Aufrüsten von Version 1.0 der Passwortsynchronisierung) im *Novell Identity Manager 3.5.1 Administrationshandbuch*.

Bei einem Upgrade von Identity Manager 2.x bleibt die Passwortsynchronisierung unverändert und wird nicht aufgerüstet.

3.5 Upgrade von RNS auf Novell Audit

Der Berichts- und Benachrichtigungsservice (RNS) ist veraltet, auch wenn die Engine weiterhin RNS-Funktionen verarbeitet, wenn sie derzeit RNS verwenden. Es wird ein Wechsel zu Novell Audit empfohlen, weil Novell Audit die von RNS zur Verfügung gestellte Funktionalität erweitert. Außerdem wird RNS in einer zukünftigen Version von Identity Manager möglicherweise nicht mehr unterstützt.

Weitere Informationen finden Sie unter „Querying and Reporting“ (Abfrage und Berichterstellung) in *Identity Manager 3.5.1 Logging and Reporting* (Identity Manager 3.5.1 Protokollierung und Berichterstellung).

3.6 Aufrüsten einer Treiberkonfiguration von DirXML 1.1a

Beim Aufrüsten von DirXML 1.1a auf Identity Manager 3.5.1 wird möglicherweise die Treiberkonfiguration aufgerüstet. Ein Upgrade der Treiberkonfigurationen hat zwei Aspekte:

- Konvertierung der DirXML-Regeln in Identity Manager-Richtlinien. Die Konvertierung wird von einem Konvertierungswerkzeug durchgeführt, ohne dass die Funktionalität des Treibers erweitert wird. Ältere Treiber funktionieren ohne diese Konvertierung, aber wenn Sie die Konvertierung durchführen, können Sie die bestehende Treiberkonfiguration in den Identity Manager iManager-Plugins anzeigen.

  Sie müssen eine sorgfältige Prüfung durchführen, um sicherzustellen, dass dieser Schritt funktioniert. Es wird empfohlen, eine Test-/Entwicklungsumgebung zu erstellen, in der Sie die Lösungen testen, analysieren und entwickeln können. Wenn alles wie gewünscht funktioniert, stellen Sie das Endprodukt in Ihrer Produktionsumgebung bereit.
- Upgrade der Treiberrichtlinien zum Hinzufügen neuer Funktionen. Identity Manager verwendet nun DirXML-Skript für die Funktionalität, die zuvor Teil der Formatvorlagen war. Diese Funktionalität sollte am besten von einem Identity Manager-Experten verwendet werden.

Weitere Informationen hierzu finden Sie unter „Upgrading a Driver Configuration from DirXML 1.1a to Identity Manager 3.5.1 Format“ (Aufrüsten einer Treiberkonfiguration von DirXML 1.1a auf ein Identity Manager 3.5.1-Format) und „Managing DirXML 1.1a Drivers in an Identity Manager Environment“ (Verwalten von DirXML 1.1a-Treibern in einer Identity Manager-Umgebung) im *Novell Identity Manager 3.5.1 Administrationshandbuch*.

Alternativ können Sie mit den Identity Manager-Treiberkonfigurationen beginnen und sie so anpassen, dass sie dieselben Funktionen wie Ihre DirXML 1.1a-Konfiguration ausführt.

3.7 Aktivieren von Identity Manager

Nach der Beendigung des Upgrades müssen Sie die Metaverzeichnis-Engine und die aufgerüsteten Treiber innerhalb von 90 Tagen aktivieren. Wenn die Engine und die Treiber nicht aktiviert werden, funktionieren sie nach Ablauf der 90 Tage nicht mehr. Eine Anleitung zur Aktivierung von Identity Manager finden Sie in Kapitel 6, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 193.

Installation von Identity Manager

4

Dieser Abschnitt enthält Anforderungen und Anweisungen für die Installation von Identity Manager und der Identity Manager-Treiber.

4.1 Vor der Installation

Lesen Sie vor der Installation von Identity Manager Kapitel 2, „Planung“, auf Seite 39.

4.2 Identity Manager-Komponenten und -Systemanforderungen

Novell® Identity Manager enthält Komponenten, die innerhalb Ihrer Umgebung auf verschiedenen Systemen und Plattformen installiert werden können. Je nach Systemkonfiguration müssen Sie das Identity Manager-Installationsprogramm möglicherweise mehrmals ausführen, um die Komponenten von Identity Manager auf den entsprechenden Systemen zu installieren.

In Tabelle 1-3, „Anforderungen für Identity Manager-Systemkomponenten“, auf Seite 29 werden die Installationskomponenten von Identity Manager und die Anforderungen für alle Systeme aufgeführt.

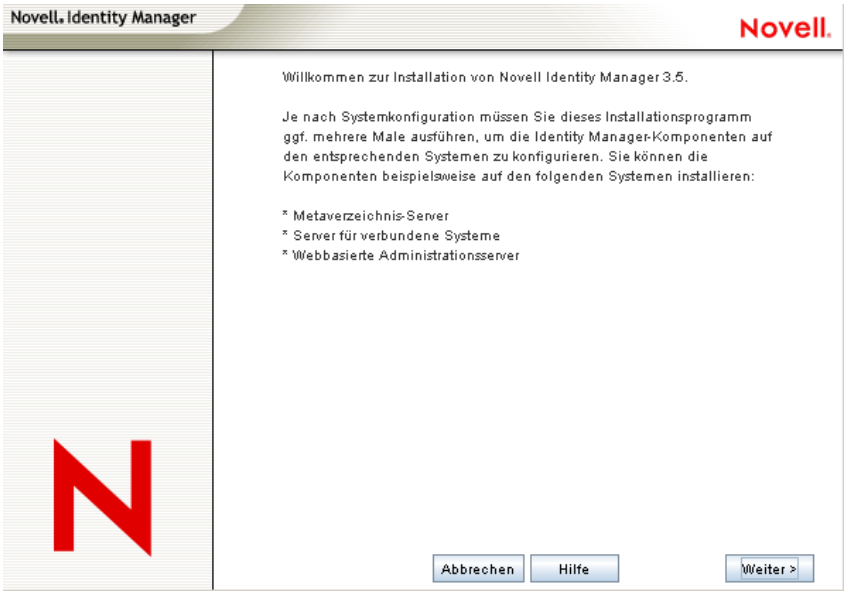
4.3 Installation von Identity Manager unter NetWare

Dieser Vorgang umfasst die Installation des Metaverzeichnis-Servers, der Webkomponenten und der Dienstprogramme für NetWare®. Stellen Sie vor Beginn sicher, dass Ihr System die in

Abschnitt 4.2, „Identity Manager-Komponenten und -Systemanforderungen“, auf Seite 67 aufgeführten Anforderungen erfüllt.

1. Laden Sie die erforderliche Identity Manager- `.iso`-Imagedatei herunter. Sie können die Identity Manager- `.iso`-Imagedateien von der Novell-Website (http://download.novell.com) herunterladen.

   Die NetWare-Installation von Identity Manager befindet sich auf `Identity_Manager_3_5_1_NW_Win.iso` oder `Identity_Manager_3_5_1_DVD.iso`.
2. Nachdem Sie die Datei extrahiert und die Imagedatei auf einem Datenträger gespeichert haben, legen Sie den Datenträger in das CD-Laufwerk des Servers ein und mounten Sie den Datenträger als Volume.
3. Starten Sie die NetWare-GUI (geben Sie in der Befehlszeile des Servers `STARTX` ein) und wählen Sie *Novell* > *Installieren*.
4. Wählen Sie im Fenster „Installierte Produkte“ *Hinzufügen* und geben Sie anschließend den Pfad zur `product.ini`-Datei von Identity Manager im Verzeichnis `\NW` ein. Klicken Sie auf *OK* und klicken Sie anschließend erneut auf *OK*, um das Identity Manager-Installationsprogramm zu starten.
5. Wenn der Kopiervorgang abgeschlossen ist, wird die Seite „Produktinstallation von Identity Manager“ angezeigt. Klicken Sie auf *Weiter*, um mit der Installation zu beginnen.



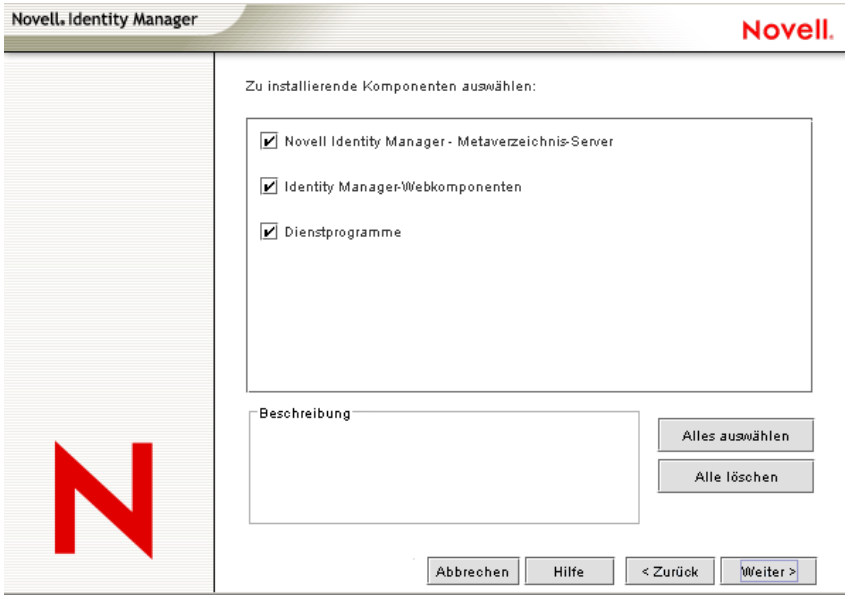
6. Wählen Sie die Sprache aus, in der die Lizenzvereinbarung angezeigt werden soll, oder verwenden Sie die Standardsprache (Englisch).

   Das Identity Manager-Installationsprogramm wird automatisch in der Sprache ausgeführt, die auf dem entsprechenden Computer verwendet wird. Wenn das Installationsprogramm nicht in die vom Computer verwendete Sprache übersetzt wurde, wird automatisch Englisch ausgewählt.
7. Lesen Sie die Lizenzvereinbarung und klicken Sie anschließend auf *Akzeptieren*.

8 Überprüfen Sie die Überblicksseiten, die eine Beschreibung der Systemtypen (einschließlich des Metaverzeichnis-Servers, der Webkomponenten und der Dienstprogramme) enthalten, und klicken Sie dann zum Fortfahren auf *Weiter*.

Diese Informationen finden Sie ebenfalls unter Tabelle 1-3 auf Seite 29.

9 Wählen Sie auf der Installationsseite von Identity Manager die zu installierenden Komponenten aus. Siehe Tabelle 1-3 auf Seite 29.



Wählen Sie eine der folgenden Optionen aus. Bei den meisten Installationen empfiehlt sich die Auswahl aller Komponenten.

- **Metaverzeichnis-Server:** Installiert die Metaverzeichnis-Engine und die Service-Treiber. Unter NetWare sind dies die Identity Manager-Treiber für Avaya, Text mit Begrenzungszeichen, eDirectory™, GroupWise®, JDBC*, JMS*, LDAP, Linux/UNIX-Einstellungen, RACF*, SOAP, SIF*, Top Secret und Work Order. Bei der Auswahl dieser Option wird auch das eDirectory-Schema erweitert.

  Wichtig: Diese Option kann nur installiert werden, wenn Novell eDirectory 8.7.3.6 oder höher und Security Services 2.0.5 (NMAS™ 3.1.3) mit den aktuellen Patches installiert sind. Installieren Sie die Metaverzeichnis-Server-Komponente an dem Speicherort, an dem die Metaverzeichnis-Engine für Identity Manager ausgeführt werden soll. Wenn Sie die falsche Version von NMAS installiert haben, wird Ihnen eine Warnmeldung angezeigt. Außerdem ist eine Weiterverwendung von Identity Manager nicht möglich.

- **Verbundenes System:** Installiert den Remote Loader, mit dessen Hilfe Sie eine Verknüpfung zwischen einem verbundenen System und einem Server herstellen können, auf dem die Metaverzeichnis-Engine ausgeführt wird.

  Für die NetWare-Installation von Identity Manager ist diese Option nicht verfügbar und wird nicht auf dem Installationsbildschirm angezeigt.

- **Identity Manager-Webkomponenten:** Mit dieser Option werden die Identity Manager-Plugins und -Treiberkonfigurationen installiert.

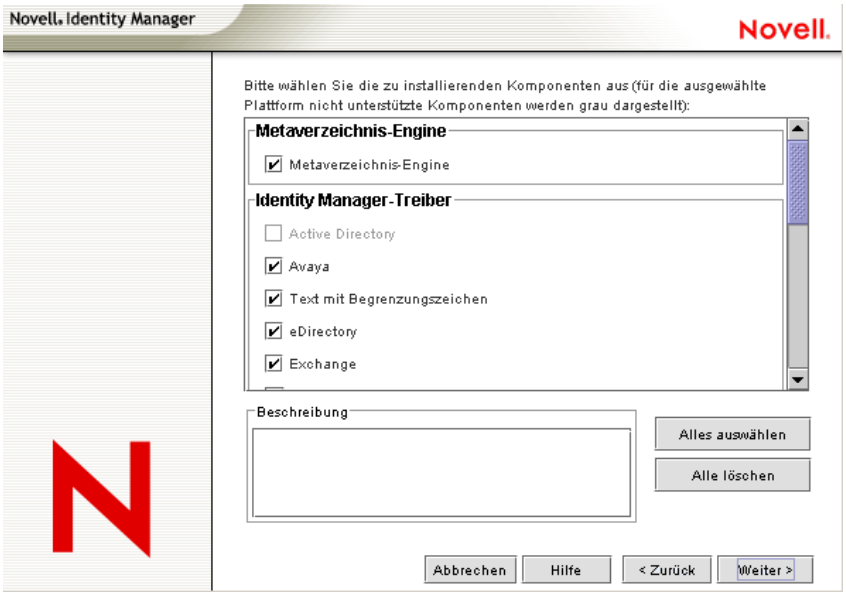
  Diese Option kann nur installiert werden, wenn Novell iManager installiert ist.

- **Dienstprogramme:** Installiert zusätzliche Skripts für den JDBC-Treiber und Dienstprogramme für andere Treiber. Die meisten Treiber verfügen nicht über ein verbundenes Dienstprogramm. Zu den Treiber-Dienstprogrammen können folgende Programme gehören:
  - SQL-Skripts für den JDBC-Treiber
  - JMS-Komponenten
  - PeopleSoft-Komponenten
  - Lizenzprüfungswerkzeug
  - Active Directory-Ermittlungswerkzeug
  - Lotus Notes-Ermittlungswerkzeug
  - SAP-Dienstprogramme

  Mithilfe eines anderen Dienstprogramms können Sie die Systemkomponenten von Novell Audit für Identity Manager registrieren (hierzu müssen vor Beginn der Installation des Dienstprogramms im Baum eine gültige eDirectory-Version und ein Novell Audit-Protokollserver installiert sein).

10 Klicken Sie auf *Weiter*.

11 Wählen Sie die zu installierenden Treiber aus und klicken Sie auf *Weiter*.



Auf der Seite „Treiber für die Engine-Installation auswählen“ wird angezeigt, welche Treiber auf der entsprechenden Plattform installiert werden können. Beispielsweise kann auf einem NetWare-Server kein Windows Active Directory-Treiber installiert werden.

In der Standardeinstellung sind für diese Option alle verfügbaren Treiber ausgewählt. Es wird empfohlen, alle ausgewählten Treiberdateien zu installieren, sodass Sie das Installationsprogramm nicht erneut ausführen müssen, wenn Sie zu einem späteren Zeitpunkt einen anderen Treiber benötigen. Die Treiberdateien werden erst verwendet, wenn ein Treiber über iManager oder Designer konfiguriert und anschließend bereitgestellt wird.

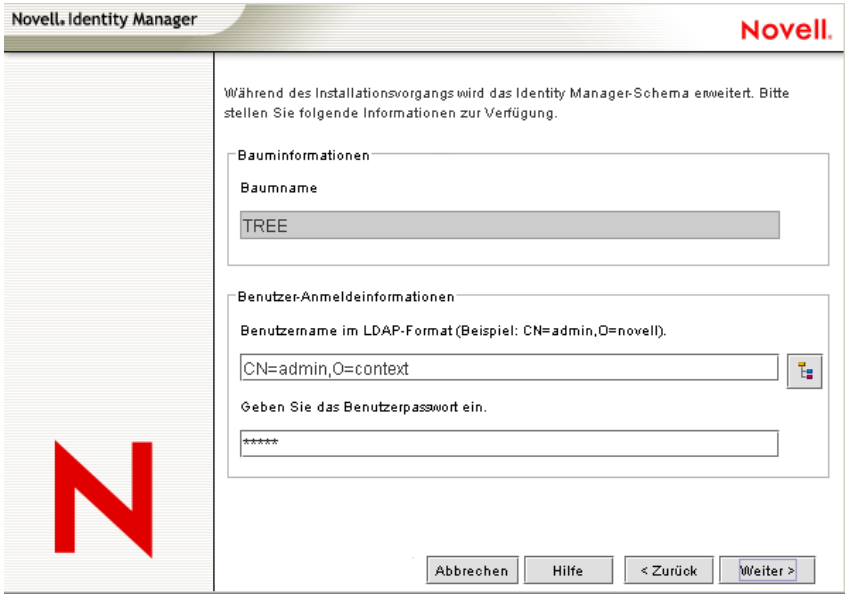
Wenn Sie nicht alle Treiber installieren möchten, können Sie entweder auf *Alle löschen* klicken und anschließend die gewünschten Treiber auswählen, oder Sie klicken auf die Treiber, die Sie

nicht installieren möchten, sodass deren Auswahl aufgehoben wird. Wenn Sie zu einem späteren Zeitpunkt einen Treiber benötigen, den Sie jetzt nicht ausgewählt haben, müssen Sie dieses Installationsprogramm erneut ausführen, um den Treiber zu installieren. Sie können auch mithilfe von Designer Treiberdateien erstellen, ändern und bereitstellen.

12 Wenn Info-Meldungen angezeigt werden, in denen Sie an die Produktaktivierung erinnert werden, klicken Sie auf *OK*.

Sie müssen die Treiber innerhalb von 90 Tagen nach der Installation aktivieren, anderenfalls werden sie außer Betrieb gesetzt.

13 Legen Sie auf der Seite „Schemaerweiterung“ Folgendes fest:



- **Benutzername:** Geben Sie den Benutzernamen (im LDAP-Format, z. B. CN=admin,O=novell) eines Benutzers ein, der über die erforderlichen Rechte zum Erweitern des Schemas verfügt. Wählen Sie auf dieser Seite einen Benutzer aus, der über die erforderlichen Rechte zum Erweitern des eDirectory-Schemas verfügt (ein Benutzer mit Supervisor-Rechten für den Stamm des Baums, beispielsweise ein Admin-Benutzer).
- **Benutzerpasswort:** Geben Sie das Passwort des Benutzers an.

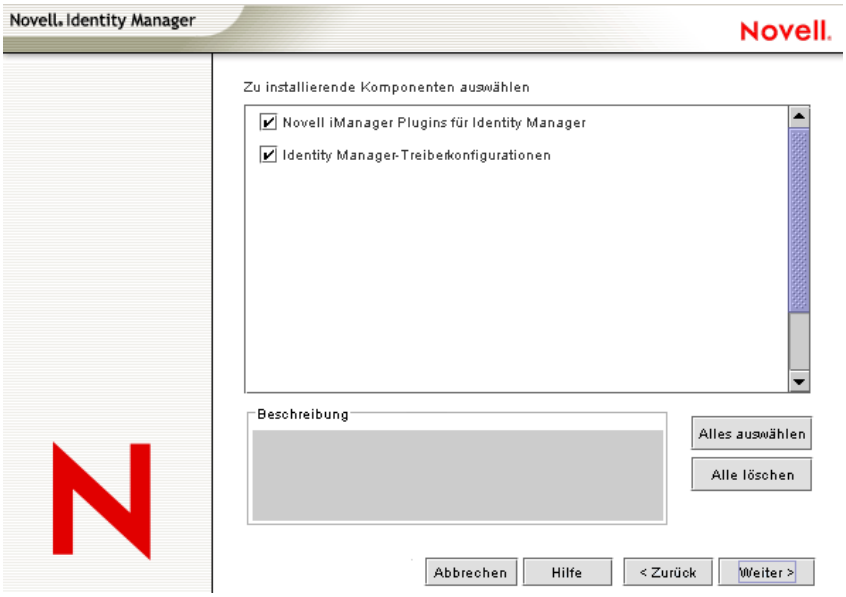
14 Klicken Sie auf *Weiter*.

Nach der Validierung der Benutzerinformationen wird die erste von zwei Komponentenseiten angezeigt.

Auf der ersten Komponentenseite ist *Novell Audit-Systemkomponenten für Identity Manager* ausgewählt, sofern Novell Audit auf dem Server installiert ist. Anderenfalls ist die Option nicht ausgewählt. Bei der Auswahl der *Anwendungskomponenten* werden Komponenten für Anwendungssysteme wie JDBC und PeopleSoft installiert.

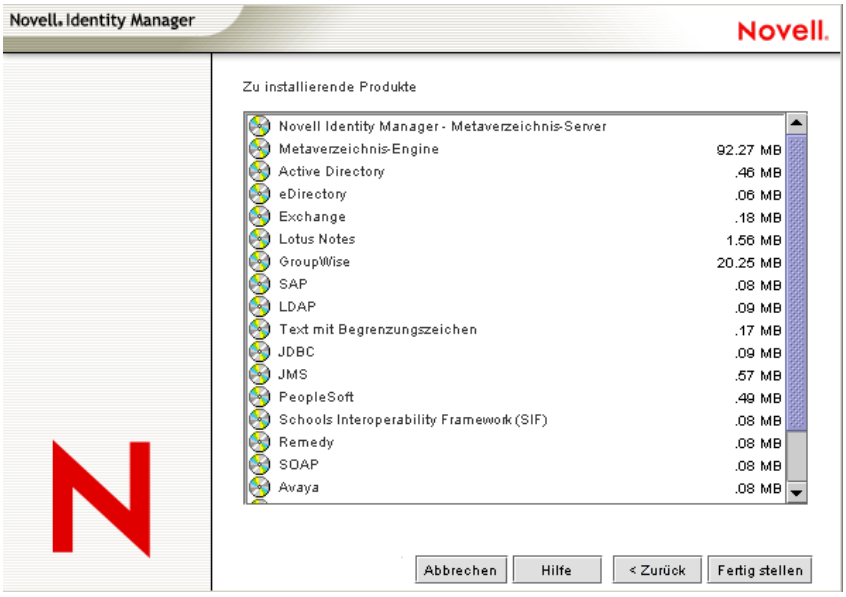
Wenn das Installationsprogramm vorhandene Treiberkonfigurationsdateien entdeckt, verschiebt es sie in einen Backup-Pfad.

15 Klicken Sie auf *Weiter*.

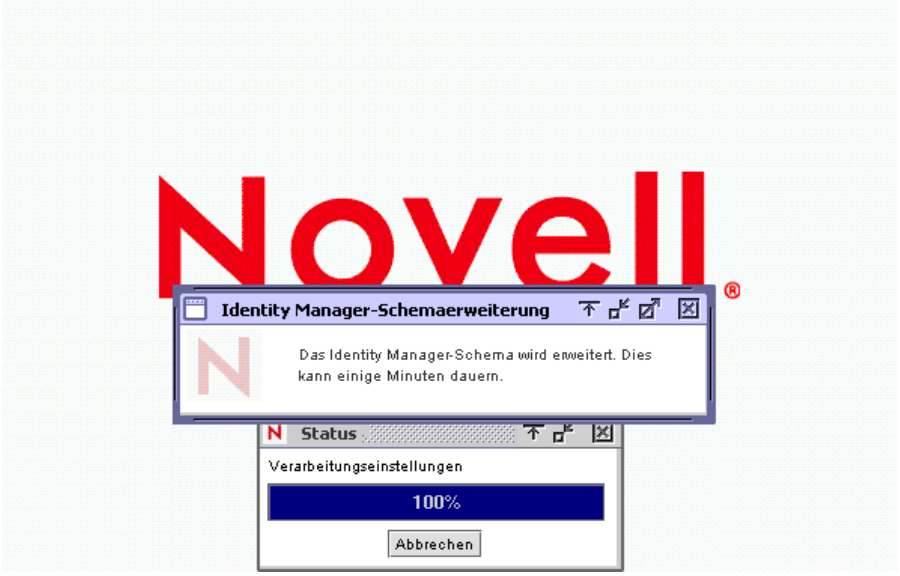


16 Auf der zweiten Komponentenseite werden die Dienstprogramme installiert. Plattformspezifische Dienstprogramme sind ausgeblendet, wenn sie nicht für die Plattform verfügbar sind, auf der Sie die Installation durchführen. Für NetWare stehen nur die Auswahlmöglichkeiten „SQL-Skripts für JDBC-Treiber“ und „JMC-Komponenten“ zur Verfügung. Wählen Sie die erforderlichen Komponenten aus und klicken Sie auf *Weiter*.

17 Überprüfen Sie die Einstellungen auf der Seite „Zusammenfassung“ und klicken Sie anschließend auf *Fertig stellen*.



Der Novell Identity Manager-Installationsvorgang fährt eDirectory zur Schemaerweiterung herunter. Der Installationsvorgang beginnt mit der Installation der ausgewählten Produkte und Komponenten.



18 Wenn nach Abschluss der Installation das Dialogfeld „Installation abgeschlossen“ angezeigt wird, klicken Sie auf die Schaltfläche *Schließen*.

19 Damit iManager die installierten Plugins erkennen kann, müssen Sie die Web Services jetzt neu starten und anschließend Tomcat neu starten.

Wenn Sie Identity Manager-Treiber installiert haben, verwenden Sie den Identity Manager-Konfigurationsassistenten ab iManager 2.6 oder konfigurieren Sie die Treiber mithilfe von Designer.

4.4 Installation von Identity Manager unter Windows

Dieser Vorgang umfasst die Installation des Metaverzeichnis-Servers, der Webkomponenten und der Dienstprogramme für Windows.

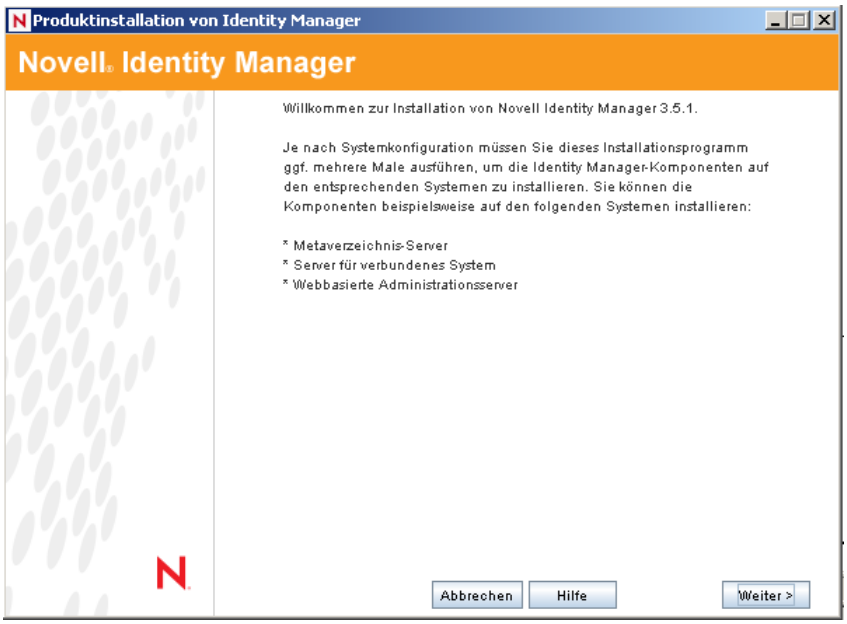
Stellen Sie vor Beginn sicher, dass Ihr System die in Tabelle 1-3 auf Seite 29 aufgeführten Anforderungen erfüllt.

1 Laden Sie die erforderliche `.iso`-Imagedatei herunter. Sie können die Identity Manager-`.iso`-Imagedateien von der Novell-Website (http://download.novell.com) herunterladen.

Die Windows-Installation von Identity Manager befindet sich auf `Identity_Manager_3_5_1_NW_Win.iso` oder `Identity_Manager_3_5_1_DVD.iso`.

2 Extrahieren Sie die Datei und doppelklicken Sie anschließend im Verzeichnis `\NT` auf die Datei `install.exe`.

Wenn der Kopiervorgang abgeschlossen ist, wird die Seite „Produktinstallation von Identity Manager“ angezeigt.



3 Klicken Sie auf *Weiter*, um mit der Installation zu beginnen.

4 Wählen Sie die Sprache aus, in der die Lizenzvereinbarung angezeigt werden soll, oder verwenden Sie die Standardsprache (Englisch).

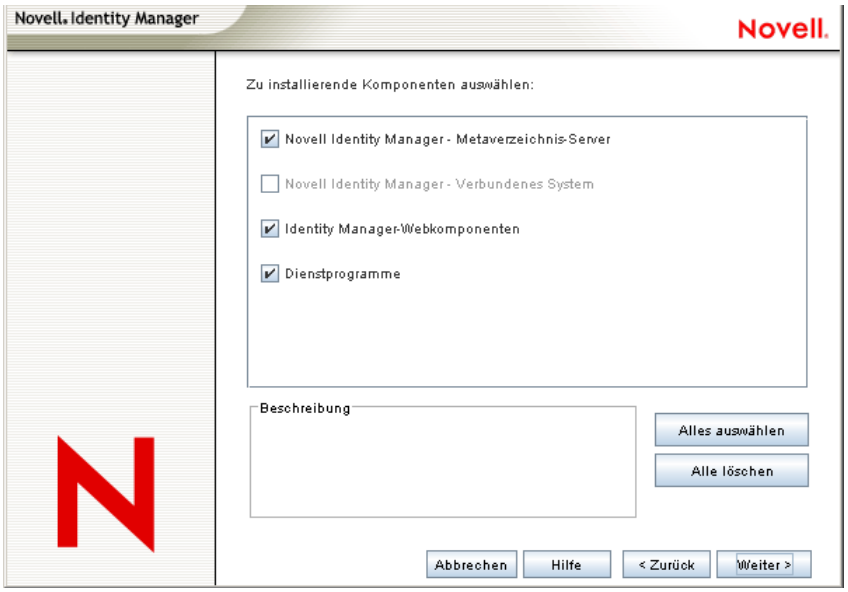
   Das Identity Manager-Installationsprogramm wird automatisch in der Sprache ausgeführt, die auf dem entsprechenden Computer verwendet wird. Wenn das Installationsprogramm nicht in die vom Computer verwendete Sprache übersetzt wurde, wird automatisch Englisch ausgewählt.

5 Lesen Sie die Lizenzvereinbarung und klicken Sie anschließend auf *Akzeptieren*.

6 Überprüfen Sie die Überblicksseiten, die eine Beschreibung der Systemtypen (einschließlich des Metaverzeichnis-Servers, der Webkomponenten und der Dienstprogramme) enthalten, und klicken Sie dann zum Fortfahren auf *Weiter*.

   Diese Informationen finden Sie ebenfalls in Tabelle 1-3 auf Seite 29.

7 Wählen Sie auf der Installationsseite von Identity Manager die zu installierenden Komponenten aus.



Es stehen folgende Optionen zur Auswahl:

- **Metaverzeichnis-Server:** Installiert die Metaverzeichnis-Engine und die Service-Treiber. Dies sind Identity Manager-Treiber für Active Directory, Avaya, Text mit Begrenzungszeichen, eDirectory, Exchange, GroupWise, JDBC, JMS, LDAP, Linux/UNIX-Einstellungen, Lotus Notes, PeopleSoft, RACF, Remedy, SOAP, SAP, SIF und Top Secret. Bei der Auswahl dieser Option wird auch das eDirectory-Schema erweitert.

  Wichtig: Diese Option kann nur installiert werden, wenn Novell eDirectory 8.7.3.6 oder 8.8 und Security Services 2.0.5 (NMAS 3.1.3) mit den aktuellen Patches installiert sind. Installieren Sie die Metaverzeichnis-Server-Komponente an dem Speicherort, an dem die Metaverzeichnis-Engine für Identity Manager ausgeführt werden soll. Wenn Sie die falsche Version von NMAS installiert haben, wird Ihnen eine Warnmeldung angezeigt. Außerdem ist eine Weiterverwendung von Identity Manager nicht möglich.

- **Verbundenes System:** Installiert den Remote Loader, mit dessen Hilfe Sie eine Verknüpfung zwischen einem verbundenen System und einem Server herstellen können, auf dem die Metaverzeichnis-Engine ausgeführt wird. Unter Windows werden mithilfe dieser Option folgende Treiber installiert: Treiber für Active Directory, Avaya, Text mit Begrenzungszeichen, eDirectory, Exchange, GroupWise, JDBC, JMS, LDAP, Linux/UNIX-Einstellungen, Lotus Notes, PeopleSoft, RACF, Remedy, SOAP, SAP, SIF und Top Secret.

  Installieren Sie das verbundene System, um eine Anwendungsverbindung von einem Anwendungsserver zu einem eDirectory-basierten Server, auf dem die Metaverzeichnis-Engine ausgeführt wird, zu ermöglichen. Dieser Vorgang wird in Abschnitt 4.5, „Installation der Option „Verbundenes System“ unter Windows“, auf Seite 79 beschrieben.

- **Webkomponenten:** Mit dieser Option werden Treiberkonfigurationen, iManager-Plugins sowie die Anwendungsskripts und Dienstprogramme installiert.

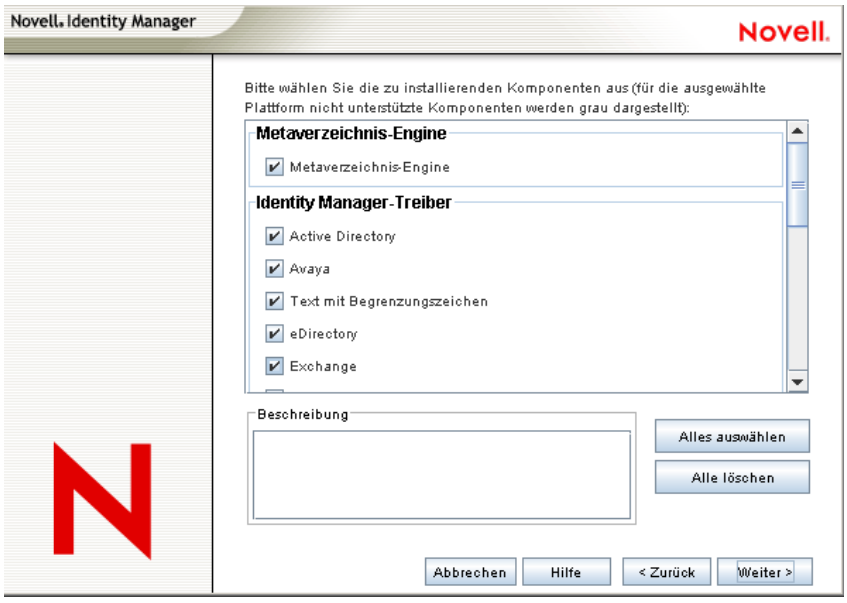
  Diese Option kann nur installiert werden, wenn Novell iManager installiert ist.

- **Dienstprogramme:** Installiert zusätzliche Skripts für den JDBC-Treiber und Dienstprogramme für andere Treiber. Die meisten Treiber verfügen nicht über ein verbundenes Dienstprogramm. Zu den Treiber-Dienstprogrammen können folgende Programme gehören:
  - SQL-Skripts für JDBC-Treiber
  - JMS-Komponenten
  - PeopleSoft-Komponenten
  - Lizenzprüfungswerkzeug
  - Active Directory-Ermittlungswerkzeug
  - Lotus Notes-Ermittlungswerkzeug
  - SAP-Dienstprogramme
  - Installationsprogramm und Konfigurationswerkzeug des Skripttreibers

  Mithilfe eines anderen Dienstprogramms können Sie die Systemkomponenten von Novell Audit für Identity Manager registrieren (hierzu müssen vor Beginn der Installation des Dienstprogramms im Baum eine gültige eDirectory-Version und ein Novell Audit-Protokollserver installiert sein).

8 Klicken Sie auf *Weiter*.

9 Wählen Sie die zu installierenden Treiber aus und klicken Sie auf *Weiter*.



Auf der Seite „Treiber für die Engine-Installation auswählen“ wird angezeigt, welche Treiber auf der entsprechenden Plattform installiert werden können. In der Standardeinstellung sind alle verfügbaren Treiber ausgewählt.

Es wird empfohlen, alle Treiberdateien zu installieren, sodass Sie das Installationsprogramm nicht erneut ausführen müssen, wenn Sie zu einem späteren Zeitpunkt einen anderen Treiber benötigen. Die Treiberdateien werden erst verwendet, wenn ein Treiber über iManager oder Designer konfiguriert wird.

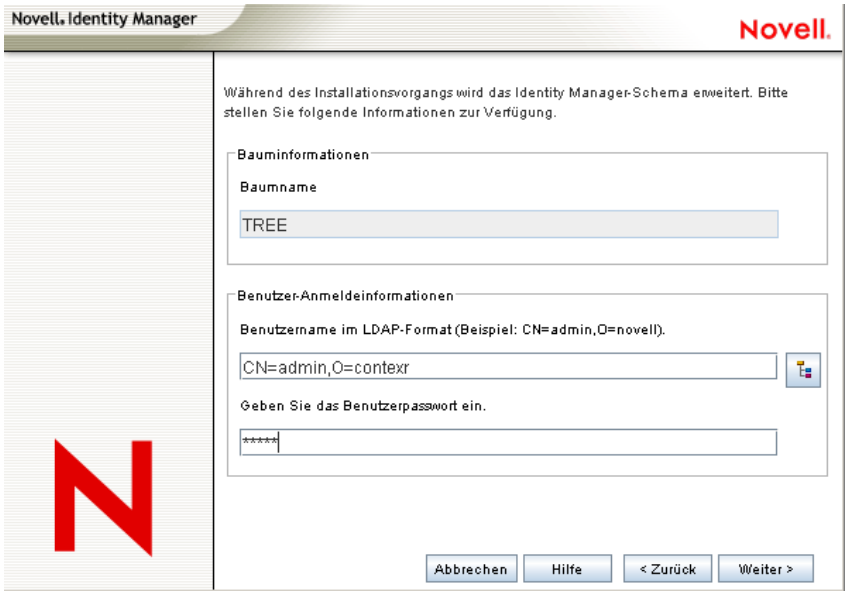
10 Wenn Info-Meldungen angezeigt werden, in denen Sie an die Produktaktivierung erinnert werden, klicken Sie auf *OK*.

Sie müssen die Treiber innerhalb von 90 Tagen nach der Installation aktivieren, anderenfalls werden sie außer Betrieb gesetzt.

11 Wenn die Meldung „Upgrade-Warnung für die Passwortsynchronisierung!“ angezeigt wird, klicken Sie auf *OK*.

Diese Meldung gilt für Windows-Server mit der Passwortsynchronisierung 1.0. Wenn Sie eine Abwärtskompatibilität für 1.0 wünschen, müssen Sie den Treiberkonfigurationsdateien zusätzliche Richtlinien hinzufügen. Ohne die Richtlinien funktioniert die Passwortsynchronisierung nur für bestehende Konten, aber nicht für neue oder umbenannte Konten.

12 Legen Sie auf der Seite „Schemaerweiterung“ Folgendes fest:



- **Benutzername:** Geben Sie den Benutzernamen (im LDAP-Format, z. B. CN=admin,O=novell) eines Benutzers an, der über die erforderlichen Rechte zum Erweitern des eDirectory-Schemas verfügt (ein Benutzer mit Supervisor-Rechten für den Stamm des Baums, beispielsweise ein Admin-Benutzer).
- **Benutzerpasswort:** Geben Sie das Passwort des Benutzers an.

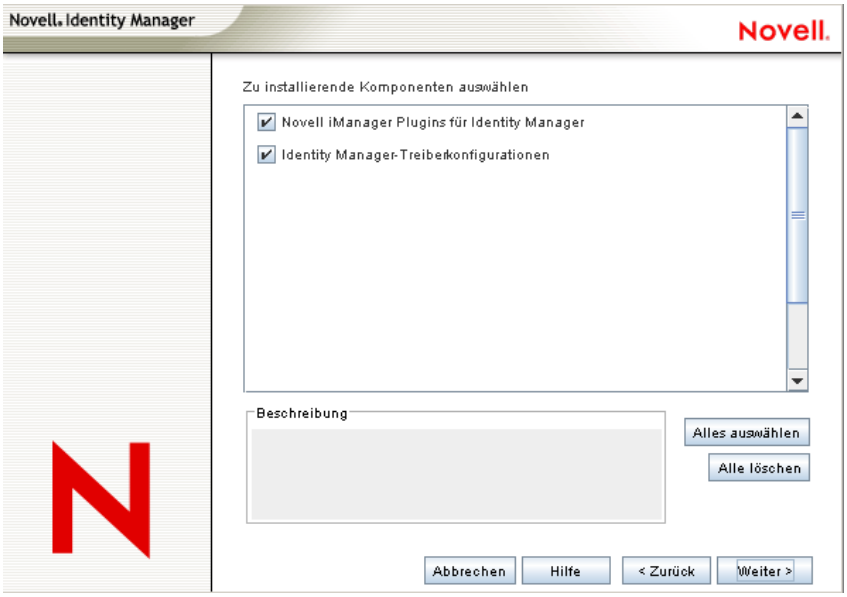
13 Klicken Sie auf *Weiter*. Nach der Validierung der Benutzerinformationen wird die erste von zwei Komponentenseiten angezeigt:

Auf der Seite „Zu installierende Komponenten auswählen“ ist die Option *Novell Audit-Systemkomponenten für Identity Manager registrieren* ausgewählt, sofern eine gültige Version von eDirectory und dem Novell Audit-Protokollserver auf dem Baum installiert sind. Anderenfalls ist die Option nicht ausgewählt. Bei der Auswahl der *Anwendungskomponenten* werden Komponenten für Anwendungssysteme wie JDBC und PeopleSoft installiert.

Wenn das Installationsprogramm vorhandene Treiberkonfigurationsdateien entdeckt, verschiebt es sie in einen Backup-Pfad.

Bei Auswahl von *Client Login Extension for Novell Identity Manager* wird das Installationsprogramm für die Client-Anmeldeerweiterung in Ihr Dateisystem kopiert. Weitere Informationen zur Client-Anmeldeerweiterung für Novell Identity Manager finden Sie unter „Client Login Extension for Novell Identity Manager 3.5.1“ im *Novell Identity Manager 3.5.1 Administrationshandbuch*.

14 Wählen Sie die zu installierenden Komponenten aus und klicken Sie auf *Weiter*.



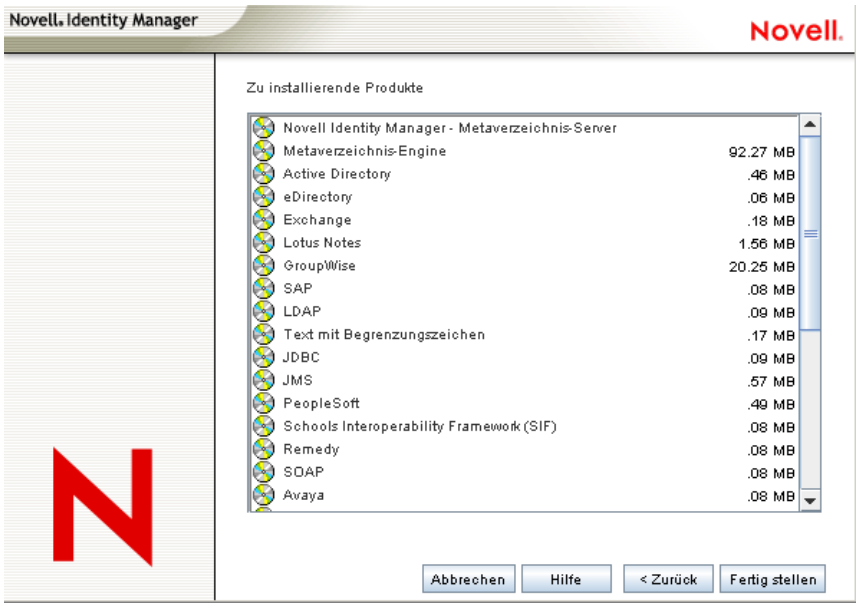
15 Es wird eine zusätzliche Seite für die Installation der Identity Manager-Plugins für iManager mithilfe des SSL-Ports 443 angezeigt. Klicken Sie auf *Weiter*.

16 Auf der zweiten Komponentenseite werden die Dienstprogramme installiert. Während der Windows-Installation wird eine zusätzliche Seite mit dem Verzeichnis angezeigt, in dem die Anwendungskomponenten abgelegt werden. Die Vorgabe ist `C:\Novell\NDS\DirXMLUtilities`. Klicken Sie auf *Weiter*.

17 Auf der Seite „Zu installierende Komponenten auswählen“ sind plattformspezifische Dienstprogramme ausgeblendet, wenn sie nicht für die Plattform verfügbar sind, auf der Sie die Installation durchführen. Für Windows stehen alle Komponenten zur Verfügung, einschließlich SQL-Skripts für JDBC-Treiber, JMS-Komponenten, PeopleSoft-Komponenten, des Lizenzprüfungswerkzeugs, des Active Directory-Ermittlungswerkzeugs, des Lotus Notes-Ermittlungswerkzeugs, SAP-Dienstprogrammen und des Installationsprogramms und Konfigurationswerkzeugs des Skripttreibers. Wählen Sie die erforderlichen Komponenten aus und klicken Sie auf *Weiter*.

18 Wenn Sie ausgewählt haben, dass das Installationsprogramm der Client-Anmeldeerweiterung für Novell Identity Manager in Ihr Dateisystem kopiert werden soll, wählen Sie einen Installationspfad aus oder verwenden Sie den Standardpfad `C:\Novell\NDS\DirXMLUtilities\cle`. Klicken Sie auf *Weiter*.

19 Überprüfen Sie die Einstellungen auf der Seite „Zusammenfassung“ und klicken Sie anschließend auf *Fertig stellen*.



Der Novell Identity Manager-Installationsvorgang fährt eDirectory zur Schemaerweiterung herunter. Der Installationsvorgang beginnt mit der Installation der ausgewählten Produkte und Komponenten.

20 Wenn nach Abschluss der Installation das Dialogfeld „Installation abgeschlossen“ angezeigt wird, klicken Sie auf die Schaltfläche *Schließen*.

21 Damit iManager die installierten Plugins erkennen kann, müssen Sie die Web Services jetzt neu starten und anschließend Tomcat neu starten.

Wenn Sie Identity Manager-Treiber installiert haben, verwenden Sie den Identity Manager-Konfigurationsassistenten ab iManager 2.6 oder konfigurieren Sie die Treiber mithilfe von Designer.

4.5 Installation der Option „Verbundenes System“ unter Windows

In Abschnitt 4.4, „Installation von Identity Manager unter Windows“, auf Seite 73 wurde die Installation des Metaverzeichnis-Servers, der Webkomponenten und der Dienstprogramme für Windows beschrieben. Für Windows-Server kann außerdem die Option „Verbundenes System“ ausgewählt werden.

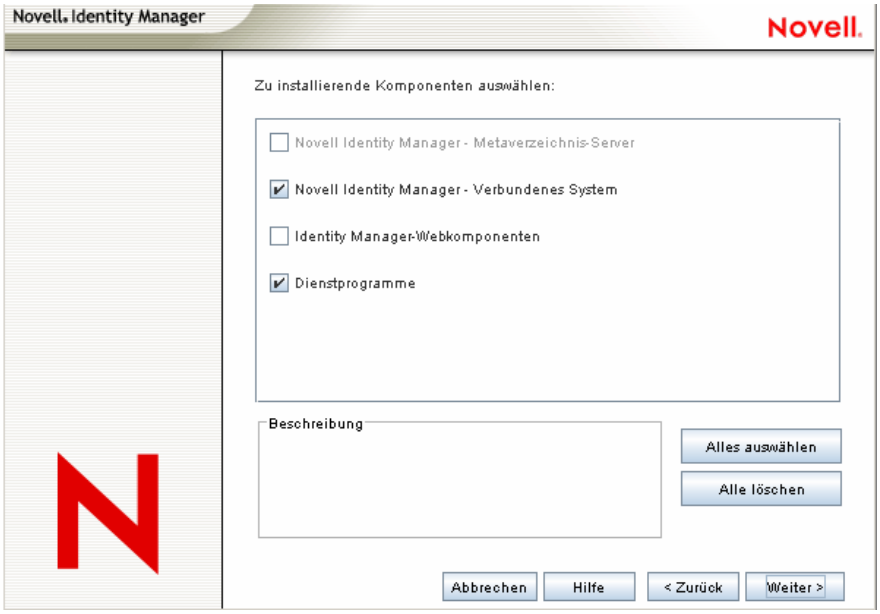
Diese Option sollte verwendet werden, wenn der Overhead der eDirectory-Services und der Metaverzeichnis-Engine nicht auf einem Anwendungsserver gespeichert werden sollen. Der Remote Loader ermöglicht die gewünschte Synchronisierung über Identity Manager, ohne dass Anwendungen geladen werden müssen, auf die von einem anderen Ort aus zugegriffen werden kann.

Stellen Sie vor Beginn sicher, dass Ihr System die in Tabelle 1-3 auf Seite 29 aufgeführten Anforderungen erfüllt.

1. Laden Sie die erforderliche `.iso`-Imagedatei herunter. Sie können die Identity Manager-`.iso`-Imagedateien von der Novell-Website (http://download.novell.com) herunterladen.

   Die Windows-Installation von Identity Manager befindet sich auf `Identity_Manager_3_5_1_NW_Win.iso` oder `Identity_Manager_3_5_1_DVD.iso`.
2. Führen Sie die Datei `install.exe` aus, die sich im Verzeichnis `\NT` befindet.
3. Lesen Sie die Begrüßungsinformationen und klicken Sie anschließend auf *Weiter*.
4. Wählen Sie die Sprache aus, in der die Lizenzvereinbarung angezeigt werden soll, oder verwenden Sie die Standardsprache (Englisch).

   Das Identity Manager-Installationsprogramm wird automatisch in der Sprache ausgeführt, die auf dem entsprechenden Computer verwendet wird. Wenn das Installationsprogramm nicht in die vom Computer verwendete Sprache übersetzt wurde, wird automatisch Englisch ausgewählt.
5. Lesen Sie die Lizenzvereinbarung und klicken Sie anschließend auf *Akzeptieren*.
6. Lesen Sie die Überblicksseiten der verschiedenen Systeme und Komponenten und starten Sie dann den Installationsvorgang, indem Sie auf *Weiter* klicken.
7. Klicken Sie zum Auswählen der Option „Verbundenes System“ zunächst auf *Alle löschen* und wählen Sie dann *Novell Identity Manager - Verbundenes System* und *Dienstprogramme* aus. Sie sollten auch die Option *Identity Manager-Webkomponenten* auswählen, wenn das iManager-Dienstprogramm auf dem Server installiert ist und die Identity Manager-Plugins für Identity Manager und Treiberkonfigurationen hinzugefügt werden sollen.



- **Verbundenes System:** Installiert den Remote Loader, mit dessen Hilfe Sie eine Verknüpfung zwischen einem verbundenen System und einem Server herstellen können, auf dem die Metaverzeichnis-Engine ausgeführt wird. Unter Windows werden mithilfe dieser Option folgende Treiber installiert: Treiber für Active Directory, Avaya, Text mit

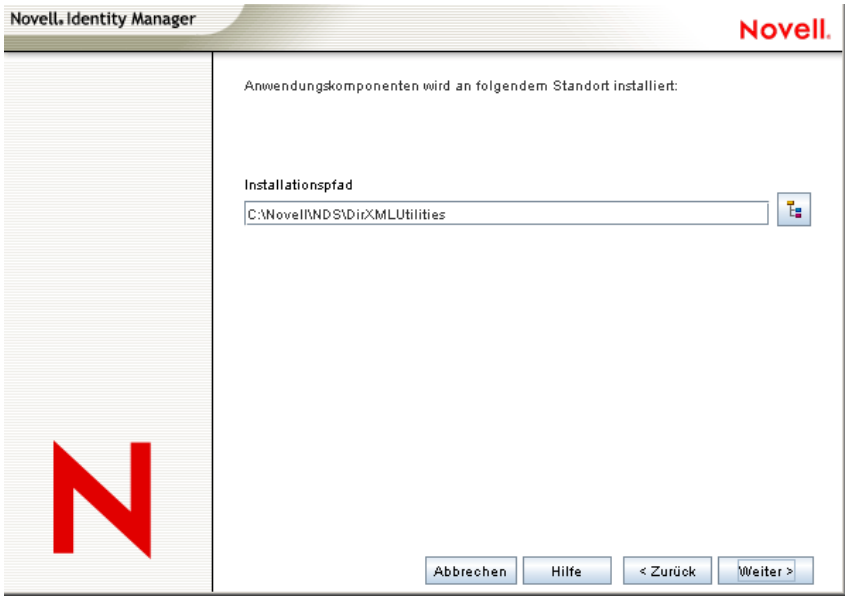
Begrenzungszeichen, eDirectory, Exchange, GroupWise, JDBC, JMS, LDAP, Linux/UNIX-Einstellungen, Lotus Notes, PeopleSoft, RACF, Remedy, SOAP, SAP, SIF und Top Secret.

- **Dienstprogramme:** Installiert zusätzliche Skripts für den JDBC-Treiber und Dienstprogramme für andere Treiber. Die meisten Treiber verfügen nicht über ein verbundenes Dienstprogramm. Zu den Treiber-Dienstprogrammen können folgende Programme gehören:
  - SQL-Skripts für JDBC-Treiber
  - JMS-Komponenten
  - PeopleSoft-Komponenten
  - Lizenzprüfungswerkzeug
  - Active Directory-Ermittlungswerkzeug
  - Lotus Notes-Ermittlungswerkzeug
  - SAP-Dienstprogramme
  - Installationsprogramm und Konfigurationswerkzeug des Skripttreibers

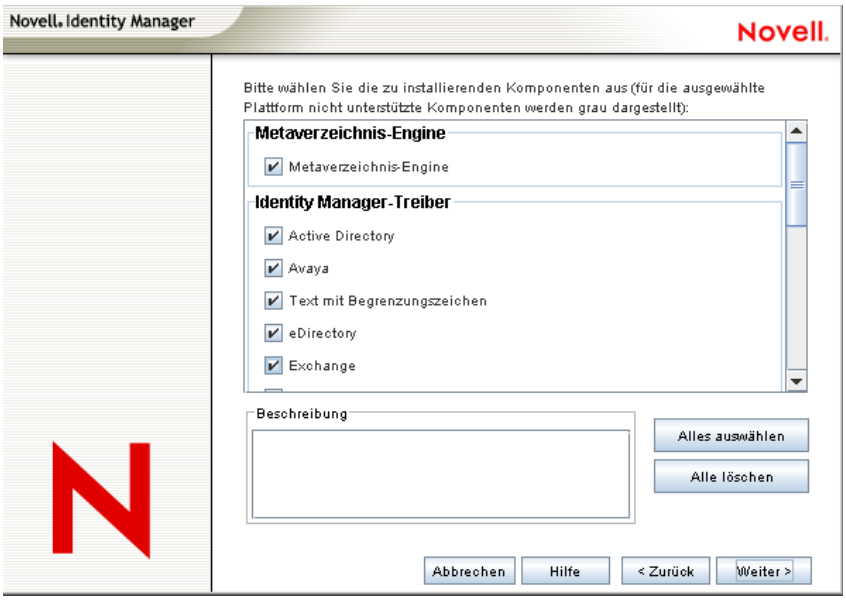
  Mithilfe eines anderen Dienstprogramms können Sie die Systemkomponenten von Novell Audit für Identity Manager registrieren (hierzu müssen vor Beginn der Installation des Dienstprogramms im Baum eine gültige eDirectory-Version und ein Novell Audit-Protokollserver installiert sein).

8 Klicken Sie auf *Weiter*.

9 Klicken Sie zum Übernehmen des Standardverzeichnispfads `C:\Novell\RemoteLoader` auf der Seite „Installationsverzeichnis“ auf *Weiter*.



10 Wählen Sie auf der Seite „Treiber für Remote Loader-Installation auswählen“ die zu ladenden Identity Manager-Treiber aus und klicken Sie anschließend auf *Weiter*.



Es können folgende Treiber ausgewählt werden: Treiber für Active Directory, Avaya, Text mit Begrenzungszeichen, eDirectory, Exchange, GroupWise, JDBC, JMS, LDAP, Linux/UNIX-Einstellungen, Lotus Notes, PeopleSoft, RACF, Remedy, SOAP, SAP, SIF und Top Secret.

Wenn Sie nicht alle Treiber installieren möchten, können Sie entweder auf *Alle löschen* klicken und anschließend die gewünschten Treiber auswählen, oder Sie klicken auf die Treiber, die Sie nicht installieren möchten, sodass deren Auswahl aufgehoben wird. Wenn Sie zu einem späteren Zeitpunkt einen Treiber benötigen, den Sie jetzt nicht ausgewählt haben, müssen Sie dieses Installationsprogramm erneut ausführen, um den Treiber zu installieren. Sie können auch mithilfe von Designer Treiberdateien erstellen, ändern und bereitstellen.

11 Wenn Info-Meldungen angezeigt werden, in denen Sie an die Produktaktivierung erinnert werden, klicken Sie auf *OK*.

Sie müssen die Treiber innerhalb von 90 Tagen nach der Installation aktivieren, anderenfalls werden sie außer Betrieb gesetzt.

12 Wenn die Meldung „Upgrade-Warnung für die Passwortsynchronisierung!“ angezeigt wird, klicken Sie auf *OK*.

Diese Meldung gilt für Windows-Server mit der Passwortsynchronisierung 1.0. Wenn Sie eine Abwärtskompatibilität für 1.0 wünschen, müssen Sie den Treiberkonfigurationsdateien zusätzliche Richtlinien hinzufügen. Ohne die Richtlinien funktioniert die Passwortsynchronisierung nur für bestehende Konten, aber nicht für neue oder umbenannte Konten..

13 Klicken Sie auf *Ja*, wenn auf dem Desktop eine Verknüpfung für die Remote Loader-Konsole erstellt werden soll. Wenn keine Verknüpfung erstellt werden soll, klicken Sie auf *Nein*.

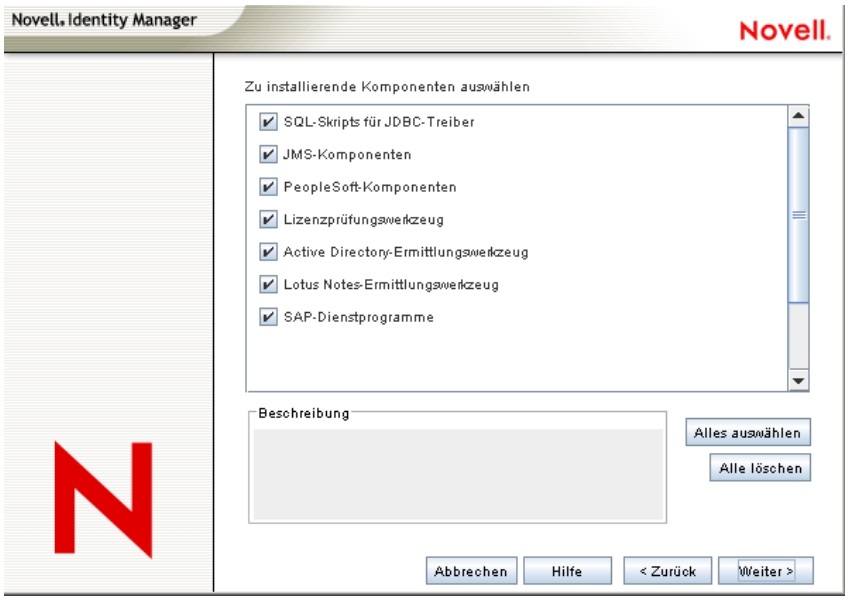
Auf der Seite „Zu installierende Komponenten auswählen“ ist die Option *Novell Audit-Systemkomponenten für Identity Manager registrieren* ausgewählt, sofern eine gültige Version von eDirectory und dem Novell Audit-Protokollserver auf dem Baum installiert sind. Anderenfalls ist die Option nicht ausgewählt. Bei der Auswahl der *Anwendungskomponenten* werden Komponenten für Anwendungssysteme wie JDBC und PeopleSoft installiert.

Bei Auswahl von *Client Login Extension for Novell Identity Manager* wird das Installationsprogramm für die Client-Anmeldeerweiterung in Ihr Dateisystem kopiert. Weitere Informationen zur Client-Anmeldeerweiterung für Novell Identity Manager finden Sie unter „Client Login Extension for Novell Identity Manager 3.5.1“ im *Novell Identity Manager 3.5.1 Administrationshandbuch*.

14 Wählen Sie die zu installierenden Komponenten aus und klicken Sie auf *Weiter*.

15 Klicken Sie zum Übernehmen des vorgegebenen Installationspfads für die Identity Manager-Dienstprogramme (`C:\Novell\NDS\DirXMLUtilities`) auf *Weiter*.

16 Wählen Sie die zu installierenden Treiberkomponenten und Dienstprogramme aus und klicken Sie anschließend auf *Weiter*.



17 Wenn Sie ausgewählt haben, dass das Installationsprogramm der Client-Anmeldeerweiterung für Novell Identity Manager in Ihr Dateisystem kopiert werden soll, wählen Sie einen Installationspfad aus oder verwenden Sie den Standardpfad `C:\Novell\NDS\DirXMLUtilities\cle`. Klicken Sie auf *Weiter*.

18 Überprüfen Sie die Elemente, die in der Zusammenfassung aufgeführt sind. Klicken Sie anschließend auf *Fertig stellen*, um die Komponenten zu installieren.

19 Klicken Sie zum Beenden des Installationsprogramms auf *Schließen*.

4.6 Installation von Identity Manager über die GUI-Schnittstelle auf UNIX/Linux-Plattformen

Stellen Sie vor Beginn sicher, dass Ihr System die in Abschnitt 4.2, „Identity Manager-Komponenten und -Systemanforderungen“, auf Seite 67 aufgeführten Anforderungen erfüllt.

1 Laden Sie die erforderliche `.iso`-Imagedatei herunter. Sie können die Identity Manager-`.iso`-Imagedateien von der Novell-Website (http://download.novell.com) herunterladen.

Die Linux-Installation für Identity Manager befindet sich auf `Identity_Manager_3_5_1_Linux.iso` oder `Identity_Manager_3_5_1_DVD.iso`, während sich AIX und Solaris auf

`Identity_Manager_3_5_1_Unix.iso` oder `Identity_Manager_3_5_1_DVD.iso` befinden.

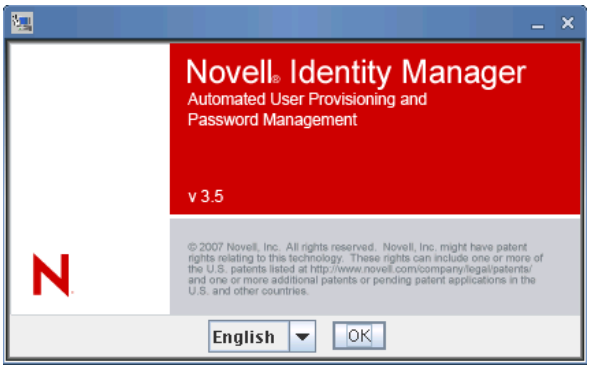
2 Melden Sie sich auf dem Host-Computer als `root`-Benutzer an.

3 Klicken Sie zum Ausführen des GUI-Installationsprogramms unter Linux im Stammverzeichnis auf die Datei `install.bin`. Sie werden gefragt, ob die Installationsdatei im Terminal- oder im Anzeigemodus ausgeführt werden soll. Wählen Sie *Terminal*. Die Datei `install.bin` überprüft, ob Xwindows vorhanden ist. Ist dies der Fall, wird das GUI-Installationsprogramm von Identity Manager für Linux angezeigt.

Hinweis: Wenn Sie auf `install.bin` klicken, aber das GUI-Installationsprogramm nicht gestartet wird, öffnen Sie ein Terminal-Fenster und führen Sie `install.bin` manuell aus. Wenn Sie einen Solaris-Server mit eDirectory 8.8.x verwenden, führen Sie das Identity Manager-Installationsprogramm ohne die GUI aus. Siehe Abschnitt 4.7, „Installation von Identity Manager auf UNIX/Linux-Plattformen mithilfe der Konsole“, auf Seite 88.

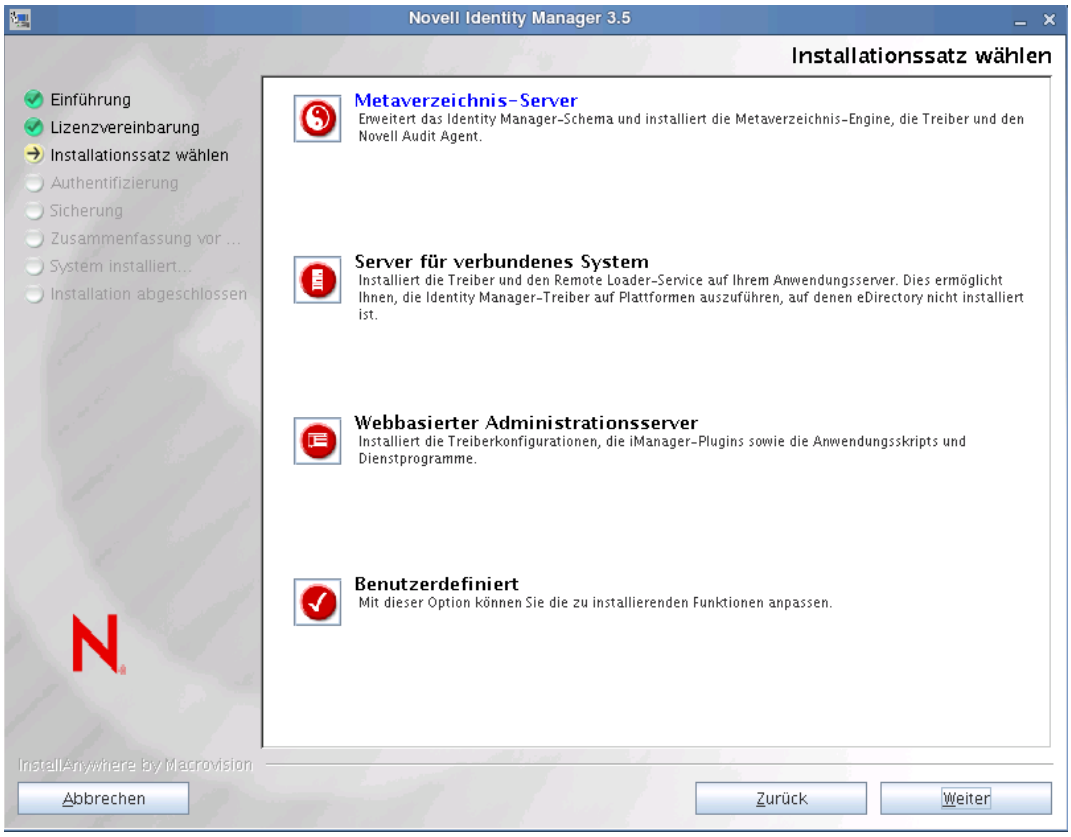
---

4 Wählen Sie die Sprache aus, in der das Installationsprogramm ausgeführt werden soll, oder verwenden Sie die Standardsprache (Englisch). Klicken Sie auf *OK*.



5 Überprüfen Sie die Begrüßungsinformationen und klicken Sie anschließend zum Fortsetzen der Installation auf *Weiter*.

6 Lesen Sie die Lizenzvereinbarung, klicken Sie zum Akzeptieren der Vereinbarung auf die entsprechende Schaltfläche und klicken Sie anschließend auf *Weiter*.



7 Wählen Sie den zu installierenden Installationssatz aus. Die Installationssätze enthalten folgende Komponenten:

- **Metaverzeichnis-Server:** Installiert die Metaverzeichnis-Engine und die Service-Treiber, Identity Manager-Treiber, Novell Audit Agent und erweitert das eDirectory-Schema.

  Diese Option kann nur installiert werden, wenn Novell eDirectory 8.7.3.6 oder höher und Security Services 2.0.5 (NMAS 3.1.3) mit den neuesten Support Packs installiert sind. Sind diese Komponenten nicht installiert, wird der Identity Manager-Installationsvorgang abgebrochen.

- **Server für verbundenes System:** Installiert den Remote Loader und die Treiber für Avaya, Text mit Begrenzungszeichen, GroupWise, JDBC, JMS, LDAP, Linux/UNIX-Einstellungen, Linux/UNIX (bidirektional), Lotus Notes, PeopleSoft, RACF, Remedy, SAP, SIF, Top Secret und Work Order. Wählen Sie die Option „Server für verbundenes System“, wenn der Overhead der eDirectory-Services und die Metaverzeichnis-Engine nicht auf Ihrem Anwendungsserver gespeichert werden sollen.

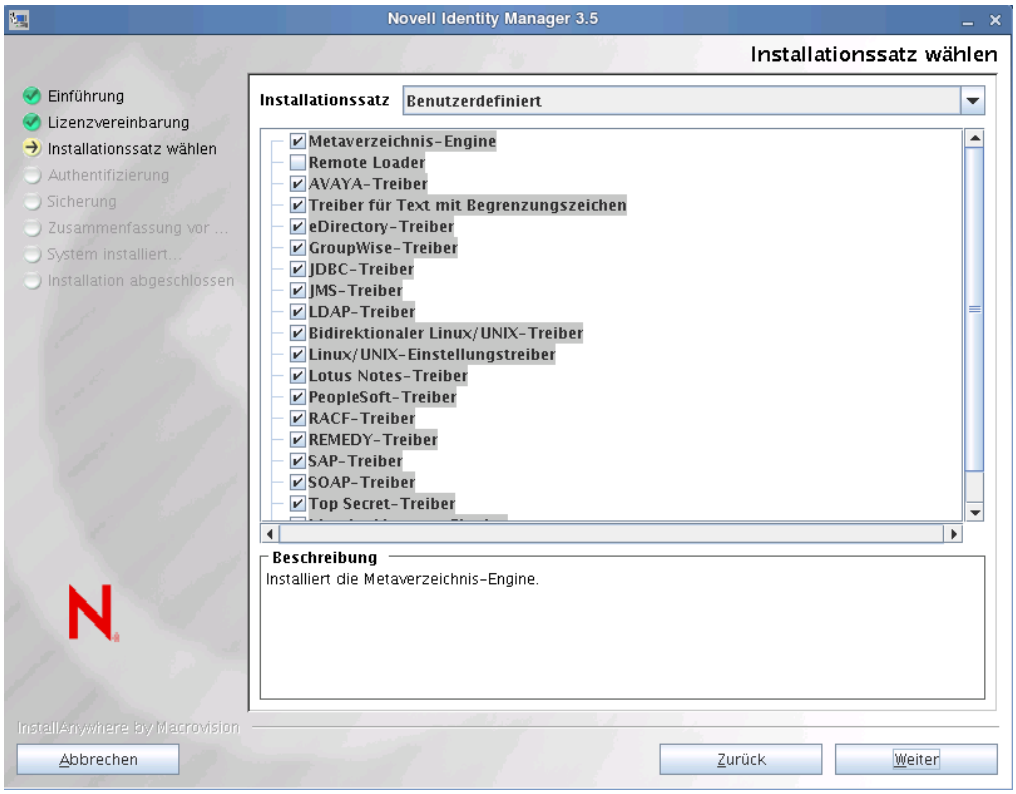
- **Webbasierter Administrationsserver:** Installiert die Identity Manager-Plugins und die Identity Manager-Treiberrichtlinien.

  Diese Option kann nur installiert werden, wenn Novell iManager installiert ist.

  In der Standardeinstellung werden Treiber-Dienstprogramme von Identity Manager nicht unter Linux/Unix installiert. Sie müssen die Dienstprogramme manuell von der Identity

Manager-Installations-CD auf den Identity Manager-Server kopieren. Alle Dienstprogramme befinden sich im *Plattform*-Verzeichnis `\setup\utilities`.

- **Benutzerdefiniert:** Installiert die Komponenten, die Sie in der Liste ausgewählt haben.

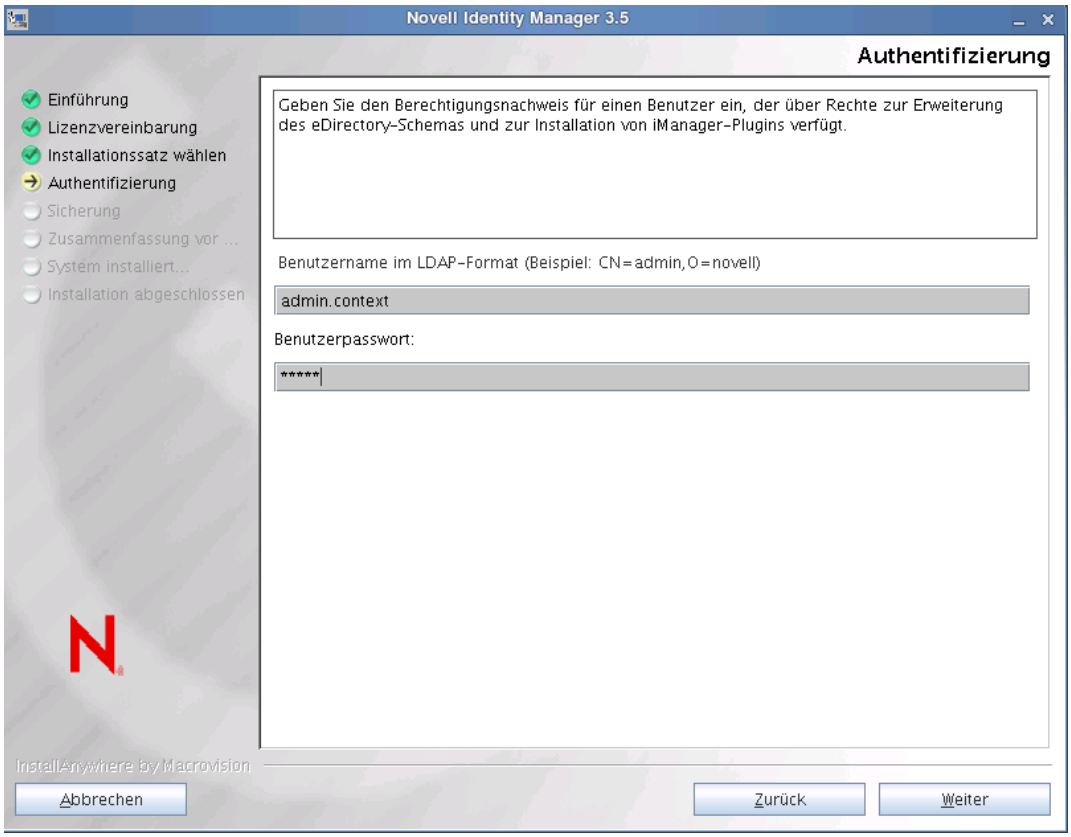


Mit *Zurück* können Sie zu vorherigen Menüs zurückkehren und die Installationsoptionen ändern.

8 (Optional) Abhängig davon, welche Option (z. B. den Metaverzeichnis-Server) Sie auswählen und ob Sie eDirectory v8.8 ausführen, werden Sie aufgefordert, die Umgebungsvariable LD_LIBRARY_PATH zu setzen. Führen Sie hierzu das Skript `/opt/novell/eDirectory/bin/ndspath` aus, indem Sie `. /opt/novell/eDirectory/bin/ndspath` eingeben und anschließend die Installation wiederholen.

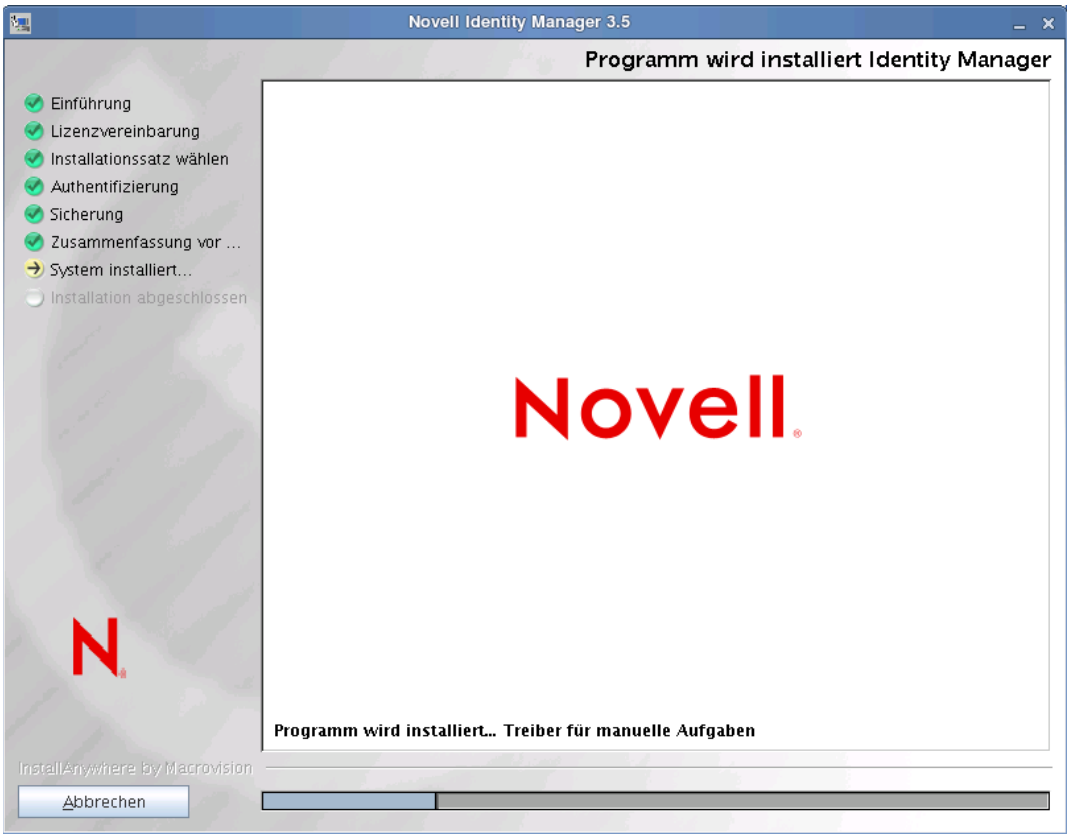
9 Bei der Installation des Metaverzeichnis-Servers werden Sie aufgefordert, den LDAP-Benutzernamen (CN=admin,O=novell) und das zugehörige Passwort einzugeben. Wählen Sie einen Benutzer aus, der über die erforderlichen Rechte zum Erweitern des eDirectory-Schemas

verfügt (ein Benutzer mit Supervisor-Rechten für den Stamm des Baums, beispielsweise ein Admin-Benutzer).



Wichtig: (Nur Solaris-Installationen) Wenn Sie den webbasierten Administrationsserver auf demselben Server wie eDirectory installieren, ändern Sie den Standardwert in einen freien Port, z. B. 8443, wenn Sie zur Eingabe des sicheren Webserver-Ports aufgefordert werden.

10 Überprüfen Sie die Angaben auf der Seite „Zusammenfassung vor der Installation“ und starten Sie anschließend die Installation der Pakete, indem Sie auf *Installieren* klicken.



eDirectory fährt bei der Installation der Metaverzeichnis-Engine und Schemadateien vorübergehend herunter. In der Standardeinstellung werden alle verfügbaren Treiber installiert, sodass Sie das Installationsprogramm nicht erneut ausführen müssen, wenn Sie zu einem späteren Zeitpunkt einen anderen Treiber benötigen. Die Treiberdateien werden erst verwendet, wenn ein Treiber über iManager oder Designer konfiguriert und anschließend bereitgestellt wird.

11 Wenn die Seite „Installation abgeschlossen“ angezeigt wird, klicken Sie zum Schließen des Installationsprogramms auf *Fertig*.

4.7 Installation von Identity Manager auf UNIX/ Linux-Plattformen mithilfe der Konsole

Stellen Sie vor Beginn sicher, dass Ihr System die in Tabelle 1-3 auf Seite 29 aufgeführten Anforderungen erfüllt.

1 Laden Sie die erforderliche `.iso`-Imagedatei herunter. Sie können die Identity Manager- `.iso`-Imagedateien von der Novell-Website (http://download.novell.com) herunterladen.

Die Linux-Installation für Identity Manager befindet sich auf `Identity_Manager_3_5_1_Linux.iso` oder `Identity_Manager_3_5_1_DVD.iso`, während sich AIX und Solaris auf

`Identity_Manager_3_5_1_Unix.iso` oder `Identity_Manager_3_5_1_DVD.iso` befinden.

2 Melden Sie sich auf dem Host-Computer als `root`-Benutzer an.

3 Führen Sie die `bin`-Datei aus dem Einrichtungsverzeichnis aus.

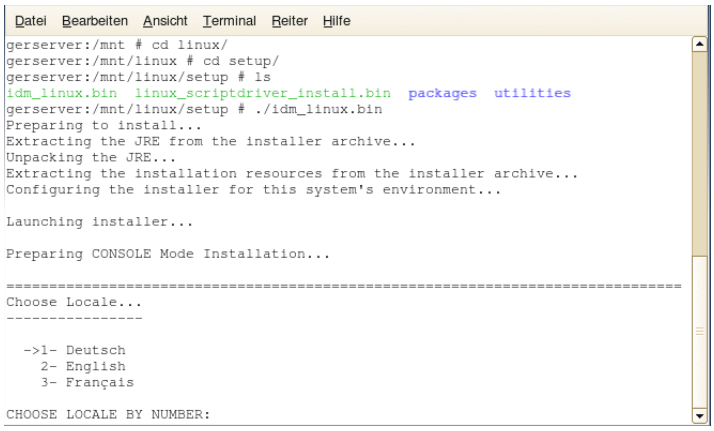
Ändern Sie das aktuelle Arbeitsverzeichnis in das Einrichtungsverzeichnis, in dem sich die Installation befindet. Geben Sie anschließend einen der folgenden Befehle ein, um den Installationsvorgang zu starten.

Plattform	Beispielpfad	Installationsdatei
Linux	`linux/setup/`	`idm_linux.bin`
Solaris	`solaris/setup/`	`idm_solaris.bin`
AIX	`aix/setup/`	`idm_aix.bin`

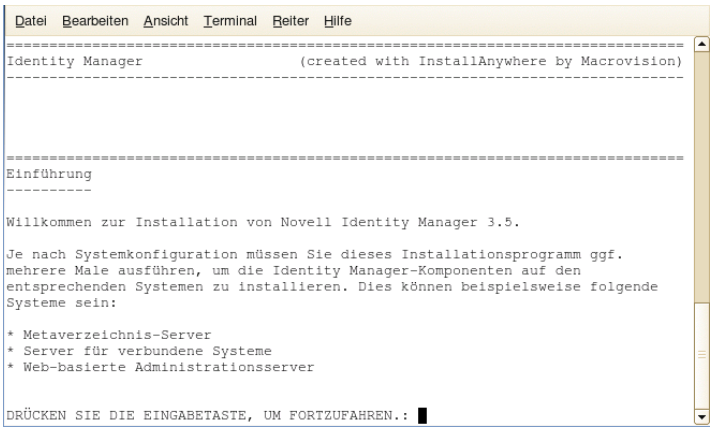
Diese Pfade sind relativ zum Stamm des Installations-Image, die sich an einem beliebigen Ort befinden können, an dem Sie es erweitert oder die CD gemountet haben. Dies ist auch abhängig von dem heruntergeladenen ISO-Image. Beispiel: Linux befindet sich auf `Identity_Manager_3_5_1_Linux.iso` oder `Identity_Manager_3_5_1_DVD.iso`, während sich AIX und Solaris auf `Identity_Manager_3_5_1_Unix.iso` oder `Identity_Manager_3_5_1_DVD.iso` befinden.

Das Installationsprogramm kann die zu installierenden Pakete nicht finden, sofern das aktuelle Arbeitsverzeichnis nicht das Verzeichnis ist, in dem sich das Installationsprogramm befindet.

4 Wählen Sie die Sprache aus, in der das Installationsprogramm ausgeführt werden soll, oder verwenden Sie die Standardsprache (Englisch). Geben Sie eine Ziffer ein und drücken Sie die Eingabetaste.



5 Lesen Sie die Begrüßungsinformationen und drücken Sie zum Fortsetzen der Installation die Eingabetaste.



6 Blättern Sie mithilfe der Eingabetaste durch die Lizenzvereinbarung. Geben Sie `Y` ein, wenn Sie mit den Nutzungsbedingungen einverstanden sind. Wenn Sie nicht einverstanden sind, geben Sie zum Beenden des Installationsprogramms `N` ein.

7 Geben Sie die Nummer des zu installierenden Installationssatzes (1-4) ein. Die Installationssätze enthalten folgende Komponenten:

- **1- Metaverzeichnis-Server:** Installiert die Metaverzeichnis-Engine und die Service-Treiber, Identity Manager-Treiber, Novell Audit Agent und erweitert das eDirectory-Schema.

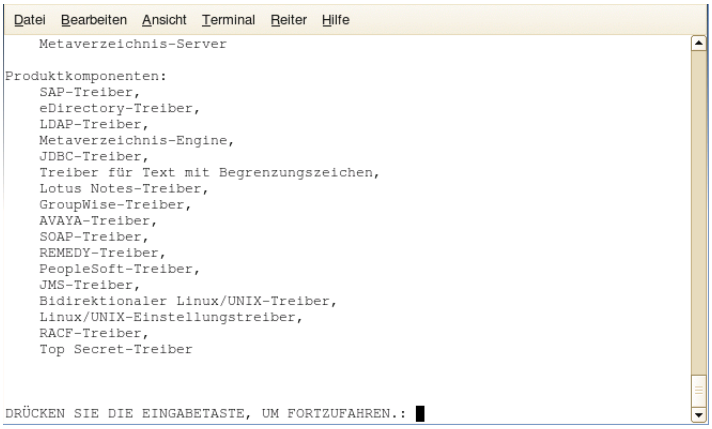
  Diese Option kann nur installiert werden, wenn Novell eDirectory 8.7.3.6 oder 8.8 und Security Services 2.0.5 (NMAS 3.1.3) mit den neuesten Support Packs installiert sind. Sind diese Komponenten nicht installiert, wird der Identity Manager-Installationsvorgang abgebrochen.

- **2- Server für verbundenes System:** Installiert den Remote Loader und die Treiber für Avaya, Text mit Begrenzungszeichen, GroupWise, JDBC, JMS, LDAP, Linux/UNIX-Einstellungen, Linux/UNIX (bidirektional), Lotus Notes, PeopleSoft, RACF, Remedy, SAP, SIF, Top Secret und Work Order. Sie können die Option *Server für verbundenes System* auswählen, wenn der Overhead der eDirectory-Services und die Metaverzeichnis-Engine nicht auf Ihrem Anwendungsserver gespeichert werden sollen.

- **3- Webbasierter Administrationsserver:** Installiert die Identity Manager-Plugins und die Identity Manager-Treiberrichtlinien.

  Diese Option kann nur installiert werden, wenn Novell iManager installiert ist.

  In der Standardeinstellung werden Treiber-Dienstprogramme von Identity Manager nicht unter Linux/Unix installiert. Sie müssen die Dienstprogramme manuell von der Identity Manager-Installations-CD auf den Identity Manager-Server kopieren. Alle Dienstprogramme befinden sich im *Plattform*-Verzeichnis `\setup\utilities`.
- **4- Benutzerdefiniert:** Installiert die Komponenten, die Sie in der Liste ausgewählt haben.



  Durch Eingabe von `prev` können Sie zu vorherigen Menüs zurückkehren und die Installationsoptionen ändern.

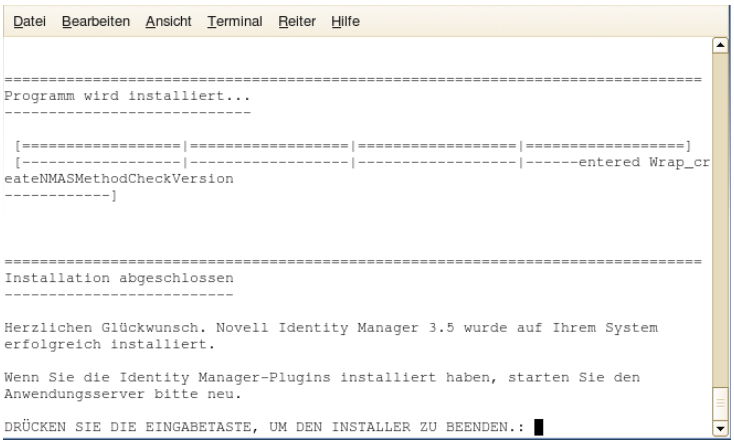
8 (Optional) Abhängig davon, welche Option (z. B. den Metaverzeichnis-Server) Sie auswählen und ob Sie eDirectory v8.8 ausführen, werden Sie aufgefordert, die Umgebungsvariable LD_LIBRARY_PATH zu setzen. Führen Sie hierzu das `/opt/novell/eDirectory/bin/ndspath`-Skript aus, indem Sie `/opt/novell/eDirectory/bin/dspath` eingeben und anschließend die Installation wiederholen.

9 Bei der Installation des Metaverzeichnis-Servers werden Sie aufgefordert, den LDAP-Benutzernamen (CN=admin,O=novell) und das zugehörige Passwort einzugeben. Wählen Sie einen Benutzer aus, der über die erforderlichen Rechte zum Erweitern des eDirectory-Schemas verfügt (ein Benutzer mit Supervisor-Rechten für den Stamm des Baums, beispielsweise ein Admin-Benutzer).

Wichtig: (Nur Solaris-Installationen) Wenn Sie den webbasierten Administrationsserver auf demselben Server wie eDirectory installieren, ändern Sie den Standardwert in einen freien Port, z. B. 8443, wenn Sie zur Eingabe des sicheren Webserver-Ports aufgefordert werden.

---

10 Überprüfen Sie die Angaben in der Zusammenfassung und starten Sie anschließend die Installation der Pakete, indem Sie die Eingabetaste drücken.



eDirectory fährt bei der Installation der Metaverzeichnis-Engine und Schemadateien vorübergehend herunter. In der Standardeinstellung werden alle verfügbaren Treiber installiert, sodass Sie das Installationsprogramm nicht erneut ausführen müssen, wenn Sie zu einem späteren Zeitpunkt einen anderen Treiber benötigen. Die Treiberdateien werden erst verwendet, wenn ein Treiber über iManager oder Designer konfiguriert und anschließend bereitgestellt wird.

11 Wenn der Bildschirm „Installation abgeschlossen“ angezeigt wird, drücken Sie die Eingabetaste, um das Installationsprogramm zu schließen.

4.8 Installation der Option „Verbundenes System“ unter UNIX/Linux mithilfe der Konsole

In Abschnitt 4.7, „Installation von Identity Manager auf UNIX/Linux-Plattformen mithilfe der Konsole“, auf Seite 88 wurde die Installation des Metaverzeichnis-Servers, der Webkomponenten und der Dienstprogramme auf UNIX-Plattformen beschrieben. Für UNIX- oder Linux-Server kann außerdem die Option „Verbundenes System“ ausgewählt werden.

Diese Option sollte verwendet werden, wenn der Overhead der eDirectory-Services und der Metaverzeichnis-Engine nicht auf einem Anwendungsserver gespeichert werden sollen. Der Remote Loader ermöglicht die gewünschte Synchronisierung über Identity Manager, ohne dass Anwendungen geladen werden müssen, auf die von einem anderen Ort aus zugegriffen werden kann.

Stellen Sie vor Beginn sicher, dass Ihr System die in Tabelle 1-3 auf Seite 29 aufgeführten Anforderungen erfüllt.

1 Laden Sie die erforderliche `.iso`-Imagedatei herunter. Sie können die Identity Manager-`.iso`-Imagedateien von der Novell-Website (http://download.novell.com) herunterladen.

Die Linux-Installation für Identity Manager befindet sich auf `Identity_Manager_3_5_1_Linux.iso` oder `Identity_Manager_3_5_1_DVD.iso`, während sich AIX und Solaris auf `Identity_Manager_3_5_1_Unix.iso` oder `Identity_Manager_3_5_1_DVD.iso` befinden.

2 Melden Sie sich auf dem Host-Computer als `root`-Benutzer an.

3 Führen Sie die `bin`-Datei aus dem Einrichtungsverzeichnis aus.

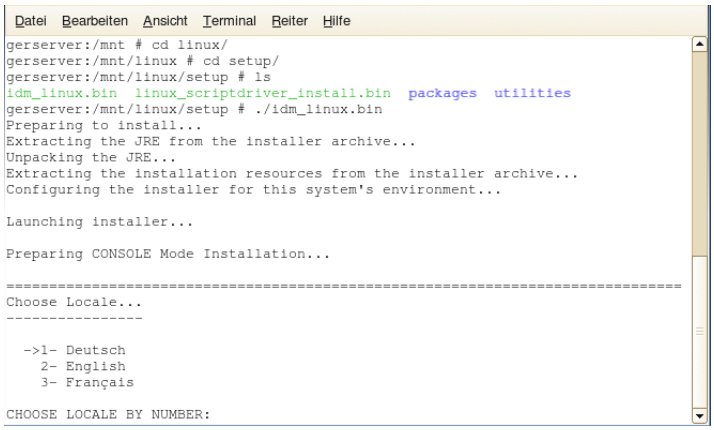
Ändern Sie das aktuelle Arbeitsverzeichnis in das Einrichtungsverzeichnis, in dem sich die Installation befindet. Geben Sie anschließend einen der folgenden Befehle ein, um den Installationsvorgang zu starten.

Plattform	Beispielpfad	Installationsdatei
Linux	`linux/setup/`	`idm_linux.bin`
Solaris	`solaris/setup/`	`idm_solaris.bin`
AIX	`aix/setup/`	`idm_aix.bin`

Diese Pfade sind relativ zum Stamm des Installations-Image, das sich an einem beliebigen Ort befinden kann, an dem Sie es erweitert oder die CD gemountet haben.

Das Installationsprogramm kann die zu installierenden Pakete nicht finden, sofern das aktuelle Arbeitsverzeichnis nicht das Verzeichnis ist, in dem sich das Installationsprogramm befindet.

4 Wählen Sie die Sprache aus, in der das Installationsprogramm ausgeführt werden soll, oder verwenden Sie die Standardsprache (Englisch). Geben Sie eine Ziffer ein und drücken Sie die Eingabetaste.



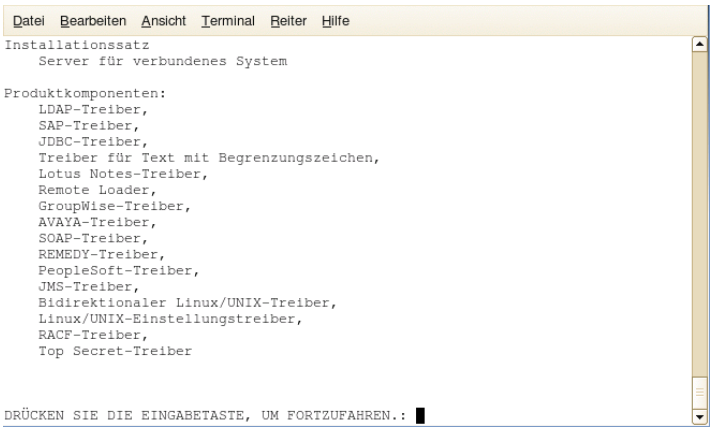
5 Lesen Sie die Begrüßungsinformationen und drücken Sie zum Fortsetzen der Installation die Eingabetaste.

6 Blättern Sie mithilfe der Eingabetaste durch die Lizenzvereinbarung. Geben Sie `Y` ein, wenn Sie mit den Nutzungsbedingungen einverstanden sind. Wenn Sie nicht einverstanden sind, geben Sie zum Beenden des Installationsprogramms `N` ein.

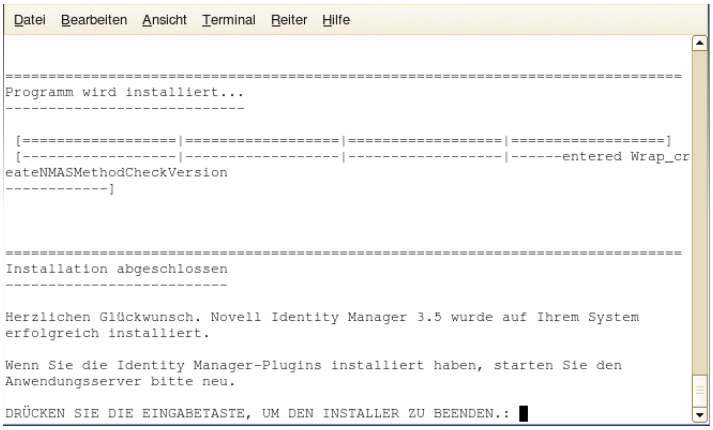
7 Wenn Sie den Server für ein verbundenes System installieren möchten, geben Sie die 2 ein.

Der Installationssatz enthält den Remote Loader und die folgenden Treiber: Treiber für Avaya, Text mit Begrenzungszeichen, GroupWise, JDBC, JMS, LDAP, Linux/UNIX-Einstellungen,

Linux/UNIX (bidirektional), Lotus Notes, PeopleSoft, RACF, Remedy, SAP, SIF, Top Secret und Work Order.



8 Überprüfen Sie die Elemente, die im Bildschirm „Zusammenfassung vor der Installation“ aufgeführt sind. Drücken Sie zum Installieren der Komponenten die Eingabetaste.



In der Standardeinstellung werden alle verfügbaren Treiber installiert, sodass Sie das Installationsprogramm nicht erneut ausführen müssen, wenn Sie zu einem späteren Zeitpunkt einen anderen Treiber benötigen. Die Treiberdateien werden erst verwendet, wenn ein Treiber über iManager oder Designer konfiguriert und anschließend bereitgestellt wird.

In der Standardeinstellung werden die Treiber-Dienstprogramme von Identity Manager nicht unter Linux/Unix installiert. Sie müssen die Dienstprogramme manuell von der Identity Manager-Installations-CD auf den Identity Manager-Server kopieren. Alle Dienstprogramme befinden sich im *Plattform*-Verzeichnis `\setup\utilities`.

9 Wenn der Bildschirm „Installation abgeschlossen“ angezeigt wird, drücken Sie die Eingabetaste, um das Installationsprogramm zu schließen.

4.9 Nicht-Root-Installation von Identity Manager

In dieser Identity Manager-Version können Sie die Metaverzeichnis-Engine in eine Nicht-Root-Installation von eDirectory installieren.

Diese Option kann nur installiert werden, wenn Novell Security Services 2.0.4 (NMAS 3.1.3) und eine Nicht-Root-Installation von eDirectory 8.8 mit den aktuellen Patches installiert sind. Weitere Informationen zur Installation von NICI als Nicht-Root-Benutzer finden Sie im Unterabschnitt „*Installing NICI*“ (Installation von NICI) unter der Überschrift „*3.0 Installing or Upgrading Novell eDirectory on Linux*“ (3.0 Installation oder Aufrüsten von Novell eDirectory auf Linux) im Novell eDirectory 8.8 Installationshandbuch (http://www.novell.com/documentation/edir88/index.html).

Befolgen Sie nach der Installation von NICI die Installationsanweisungen für Nicht-Root-eDirectory 8.8 im Unterabschnitt „*Nonroot User Installing eDirectory 8.8*“ (Installation von eDirectory 8.8 durch Nicht-Root-Benutzer) unter der Überschrift „*3.0 Installing or Upgrading Novell eDirectory on Linux*“ (3.0 Installation oder Aufrüsten von Novell eDirectory auf Linux) im Novell eDirectory 8.8 Installationshandbuch (http://www.novell.com/documentation/edir88/index.html).

1. Laden Sie die erforderliche `.iso`-Imagedatei herunter. Sie können die Identity Manager- `.iso`-Datei von der Novell-Website (http://download.novell.com) herunterladen.

   Linux befindet sich auf `Identity_Manager_3_5_1_Linux.iso` oder `Identity_Manager_3_5_1_DVD.iso`, während sich AIX und Solaris auf `Identity_Manager_3_5_1_Unix.iso` oder `Identity_Manager_3_5_1_DVD.iso` befinden. Das Nicht-Root-Installationsprogramm ist im `.iso`-Image enthalten.

2. Melden Sie sich auf dem Host-Computer als Benutzer mit Schreibberechtigungen für das Verzeichnis, in dem Sie das Nicht-Root-eDirectory installiert haben, an.

3. Führen Sie die Datei `idm-nonroot-install` aus dem Verzeichnis `/setup/` aus. Ändern Sie dazu das aktuelle Arbeitsverzeichnis in das Verzeichnis `setup` und geben Sie dann den folgenden Befehl ein, um die Nicht-Root-Installation auszuführen:

   ```
   ./idm-nonroot-install
   ```

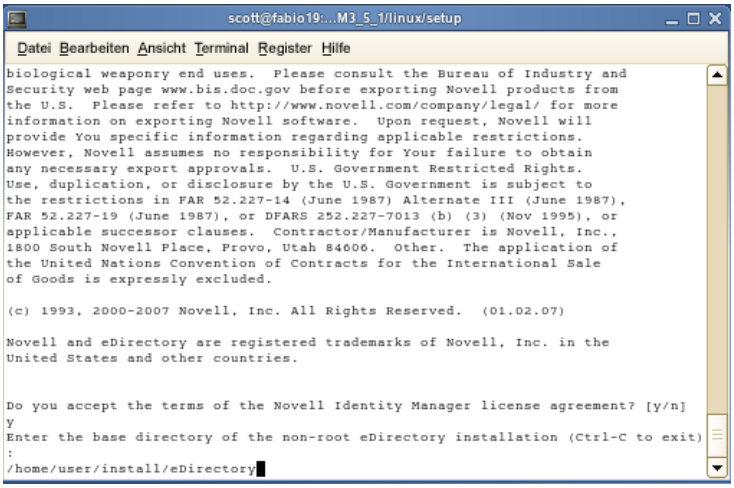
Plattform	Beispielpfad	Installationsdatei
Linux	`linux/setup/`	`idm-nonroot-install`
Solaris	`solaris/setup/`	`idm-nonroot-install`
AIX	`aix/setup/`	`idm-nonroot-install`

   Diese Pfade sind relativ zum Stamm des `iso`-Image, und das Installationsprogramm kann die zu installierenden Pakete nur dann finden, wenn das aktuelle Arbeitsverzeichnis das Verzeichnis ist, in dem sich das Installationsprogramm befindet.

4. Wenn Sie die Eingabetaste drücken, wird die Endbenutzer-Lizenzvereinbarung angezeigt. Sie können mithilfe der Leertaste darin blättern. Geben Sie `Y` ein, wenn Sie mit den Nutzungsbedingungen einverstanden sind. Wenn Sie nicht einverstanden sind, geben Sie zum Beenden des Installationsprogramms `N` ein.

5 Geben Sie den Pfad an, der auf den Speicherort des Nicht-Root-eDirectory verweist. Beispiel:

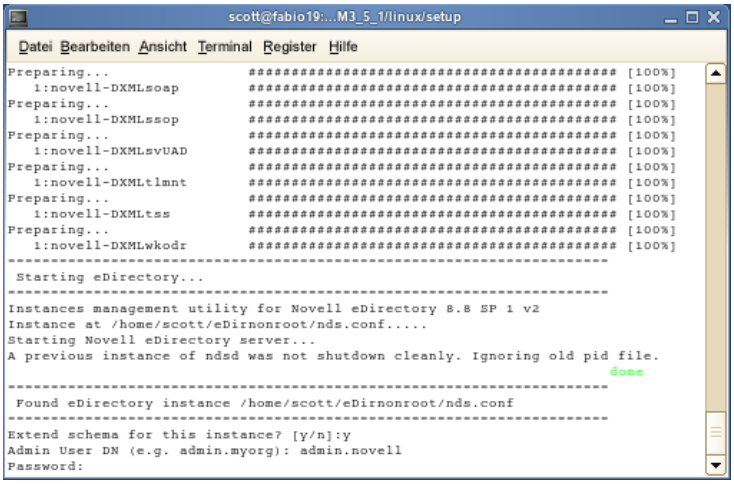
`/home/user/installed/eDirectory`



Das Installationsskript installiert Identity Manager daraufhin mit den folgenden Treibern: Treiber für Avaya, Text mit Begrenzungszeichen, GroupWise, JDBC, JMS, LDAP, Linux/UNIX-Einstellungen, Linux/UNIX (bidirektional), Lotus Notes, PeopleSoft, RACF, Remedy, SAP, SIF, Top Secret und Work Order.

6 Sie werden dann aufgefordert, das Schema für alle eDirectory-Instanzen, deren Besitzer der angemeldete Benutzer ist, zu erweitern. Geben Sie für jede Instanz `Y` ein, um das Schema für die betreffende Instanz zu erweitern, oder `N`, wenn Sie das Schema für diese Instanz nicht erweitern möchten.

7 Wenn Sie auswählen, dass das Schema erweitert werden soll, geben Sie den eindeutigen Namen (DN) der Person ein, die über die erforderlichen Rechte zum Erweitern des Schemas verfügt (beispielsweise admin.novell). Wählen Sie einen Benutzer aus, der über die erforderlichen Rechte zum Erweitern des eDirectory-Schemas verfügt (ein Benutzer mit Supervisor-Rechten für den Stamm des Baums, beispielsweise ein Admin-Benutzer).



8 Geben Sie das Passwort ein und drücken Sie die Eingabetaste. Sie müssen Schritt 7 und 8 für alle eDirectory-Instanzen durchführen, die Sie erweitern.

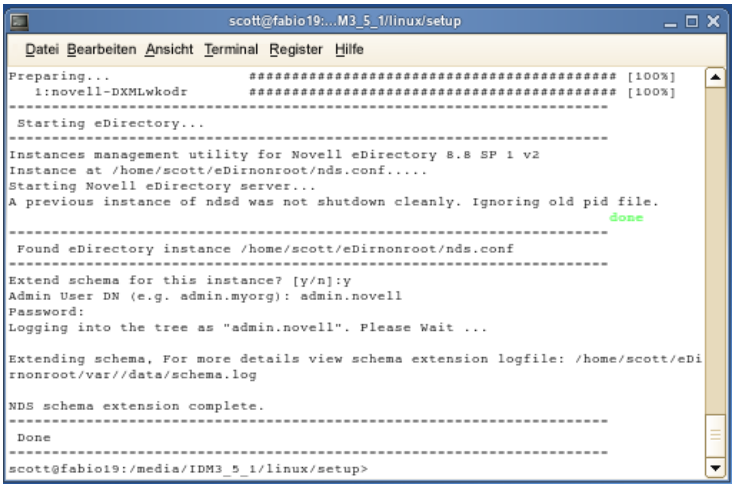
Wenn Sie das Schema zu einem späteren Zeitpunkt für andere eDirectory-Instanzen erweitern möchten, führen Sie das Skript `idm-nonroot-install` im Unterverzeichnis `opt/novell/eDirectory/bin` der Nicht-Root-eDirectory-Installation aus. Führen Sie das Skript aus, während Sie als Eigentümer der eDirectory-Instanz angemeldet sind, die Sie erweitern möchten.

Das Installationsskript meldet sich beim eDirectory-Baum an und erweitert das Schema. Wenn Sie weitere Details zum Schemaerweiterungsprozess erfahren möchten, wechseln Sie zur Datei `/home/user/eDirnonroot/var/data/schema.log`.

In der Standardeinstellung werden alle verfügbaren Treiber installiert, sodass Sie das Installationsprogramm nicht erneut ausführen müssen, wenn Sie zu einem späteren Zeitpunkt einen anderen Treiber benötigen. Die Treiberdateien werden erst verwendet, wenn ein Treiber über iManager oder Designer konfiguriert und anschließend bereitgestellt wird.

In der Standardeinstellung werden Treiber-Dienstprogramme von Identity Manager nicht unter Linux/Unix installiert. Sie müssen die Dienstprogramme manuell von der Identity Manager-Installations-CD auf den Identity Manager-Server kopieren. Alle Dienstprogramme befinden sich im *Plattform*-Verzeichnis `\setup\utilities`.

9 Wenn die Schemaerweiterung abgeschlossen ist, ist Identity Manager installiert.



4.10 Aufgaben nach Abschluss der Installation

Sie müssen Identity Manager nicht manuell laden oder entladen, weil das Identity Manager-Modul beim Start des Identity Manager-Treibers geladen wird. Wenn für einen Treiberparameter die Option „Autom. starten“ ausgewählt ist und wenn der Treiber und eDirectory ausgeführt werden, startet der Treiber automatisch das Identity Manager-Modul. Wenn für einen Treiberparameter die Option „Manuell“ ausgewählt ist, wird das Identity Manager-Modul beim Start eines Identity Manager-Treibers geladen.

Nach der Installation von Identity Manager müssen Sie die installierten Treiber konfigurieren, um die von Ihnen als Geschäftsvorgänge definierten Richtlinien und Anforderungen zu implementieren. Zu den Aufgaben nach der Installation gehören in der Regel die folgenden Elemente:

- Konfigurieren Sie ein verbundenes System. In der Dokumentation zu Identity Manager-Treibern (http://www.novell.com/documentation/dirxmldrivers) finden Sie treiberspezifische Konfigurationsanweisungen.

- Erstellen und konfigurieren Sie einen Treiber. Verwenden Sie iManager oder das Designer-Dienstprogramm, wenn Sie einen Treiber erstellen oder einen vorhandenen Treiber konfigurieren möchten. Weitere Informationen finden Sie unter „Importing a Driver Configuration File“ (Treiberkonfigurationsdatei importieren) im Handbuch *Designer 2.1 für Identity Manager 3.5.1*.
- Definieren Sie Richtlinien. Verwenden Sie iManager oder das Designer-Dienstprogramm, wenn Sie Richtlinien für Treiber definieren möchten, die den Anforderungen Ihres Unternehmens entsprechen. Weitere Informationen finden Sie unter „Creating a Policy“ (Richtlinie erstellen) im Handbuch *Richtlinien in Designer 2.1* oder im Handbuch *Richtlinien für Identity Manager 3.5.1*.
- Starten, stoppen oder starten Sie den Treiber erneut. Mit iManager oder dem Designer-Dienstprogramm können Sie die Aktivitäten eines Treibers verwalten. Weitere Informationen finden Sie unter „Importing a Driver Configuration File“ (Treiberkonfigurationsdatei importieren) im Handbuch *Designer 2.1 für Identity Manager 3.5.1*.
- Aktivieren Sie Identity Manager. Siehe Kapitel 6, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 193.

4.11 Benutzerdefinierten Treiber installieren

Ein benutzerdefinierter Treiber kann aus folgenden Elementen bestehen:

- Einem Satz `.jar`- oder nativen (`. dll`-, `. nlm`- oder `. so`-) Dateien
- XML-Regeldateien für die Konfiguration des Treibers
- Dokumentation

Weitere Informationen zum Erstellen oder Installieren eines benutzerdefinierten Treibers finden Sie im Entwicklungskit von Novell (http://developer.novell.com/ndk/dirxml-index.htm). Lesen Sie auch „Editing Driver Configuration Files“ (Treiberkonfigurationsdateien bearbeiten) im *Novell Identity Manager 3.5.1 Administrationshandbuch*.

Installation der Benutzeranwendung

5

In diesem Abschnitt wird beschrieben, wie Sie die Identity Manager-Benutzeranwendung installieren. Es werden u. a. folgende Themen erläutert:

5.1 Voraussetzungen für die Installation

Stellen Sie vor der Installation der Identity Manager-Benutzeranwendung sicher, dass die folgenden Anforderungen erfüllt sind:

Tabelle 5-1 *Voraussetzungen für die Installation*

Umgebungsvoraussetzungen	Beschreibung

Java* Development Kit	Laden Sie das Java 2 Platform Standard Edition Development Kit 5.0 herunter und installieren Sie es. Verwenden Sie die JRE-Version 1.5.0_10. Verwenden Sie auf WebSphere das IBM* JDK* mit den unbeschränkten Richtliniendateien.
	
	Setzen Sie die Umgebungsvariable JAVA_HOME so, dass sie auf das JDK verweist, das mit der Benutzeranwendung verwendet werden soll. Alternativ können Sie den Pfad während der Installation der Benutzeranwendung manuell eingeben, um JAVA_HOME zu überschreiben.
	
	◆ Geben Sie in der Linux- oder Solaris-Befehlszeile `echo $JAVA_HOME` ein. Zum Erstellen oder Ändern von JAVA_HOME erstellen oder bearbeiten Sie `~/.profile` (in SUSE® Linux):
	
	`# Java Home`
	
	`export JAVA_HOME=/usr/java/jdk1.5.0_10`
	
	`#JRE HOME`
	
	`export JRE_HOME=$JAVA_HOME/jre`
	
	◆ Unter Windows: *Systemsteuerung* > *System* > *Erweitert* > *Umgebungsvariablen* > *Systemvariablen*.

JBoss-Anwendungsserver	Wenn Sie JBoss verwenden, laden Sie den JBoss 4.2.0-Anwendungsserver herunter und installieren Sie ihn. (Starten Sie diesen Server nach der Installation der Benutzeranwendung. Weitere Informationen hierzu finden Sie in Abschnitt 5.9, „Aufgaben nach der Installation“, auf Seite 185). **RAM:** Für den JBoss-Anwendungsserver sollten mindestens 512 MB RAM zur Verfügung stehen, wenn die Benutzeranwendung ausgeführt wird. **Port:** Notieren Sie sich den Port, den der Anwendungsserver verwendet. (Die Vorgabe für den Anwendungsserver ist 8080.) **SSL:** Wenn Sie planen, die externe Passwortverwaltung zu verwenden, aktivieren Sie SSL auf den JBoss-Servern, auf denen Sie die Benutzeranwendung und die `IDMPwdMgt.war`-Datei bereitstellen. Eine Anleitung hierzu finden Sie in der JBoss-Dokumentation. Stellen Sie außerdem sicher, dass der SSL-Port über die Firewall geöffnet ist. Weitere Informationen zur `IDMPwdMgt.war-Datei` finden Sie in Abschnitt 5.9.4, „Zugriff auf die externe Passwort-WAR“, auf Seite 187 und im *IDM 3.5.1 Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idm35/index.html).
WebSphere Application Server	Wenn Sie WebSphere verwenden, laden Sie den WebSphere 6.1-Anwendungsserver herunter und installieren Sie ihn.
Aktivieren der Abmeldung über iChain	Aktivieren Sie die ICS-Abmeldung in der Identity Manager-Benutzeranwendung über die Option für die Cookieweiterleitung in Novell Access Manager™ oder iChain®.

Umgebungsvoraussetzungen	Beschreibung
Datenbank	Installieren Sie Ihre Datenbank und den Datenbanktreiber und erstellen Sie eine Datenbank oder eine Datenbankinstanz. Notieren Sie den Host und den Port, da Sie diese Angaben in Abschnitt 5.5.7, „Angabe von Datenbank-Host und -Port“, auf Seite 123 benötigen. Notieren Sie den Datenbanknamen, den Benutzernamen und das Benutzerpasswort, da Sie diese Angaben in Abschnitt 5.5.8, „Angabe des Datenbanknamens und des privilegierten Benutzers“, auf Seite 124 benötigen. Eine Ursprungsdatei muss auf die Datenbank verweisen. Dies wird je nach dem von Ihnen verwendeten Anwendungsserver unterschiedlich gehandhabt. Für JBoss erstellt das Installationsprogramm der Benutzeranwendung eine Ursprungsdatei der Benutzeranwendung, die auf die Datenbank verweist, und benennt die Datei anhand des Namens der WAR-Datei der Benutzeranwendung. Für WebSphere müssen Sie die Datenquelle vor der Installation manuell konfigurieren. Datenbanken müssen UTF-8-fähig sein. Lesen Sie Abschnitt 5.1.3, „Konfiguration der MySQL-Datenbank“, auf Seite 106, wenn Sie MySQL über die IDM-Benutzeranwendung oder eigenständig installieren. **Hinweis:** Wenn Sie die Migration einer Datenbank planen, starten Sie die entsprechende Datenbank und wählen Sie anschließend im Installationsprogramm die Option „Migration“. Wenn Sie keine Datenbank migrieren, muss die Datenbank während der Installation der Benutzeranwendung nicht geöffnet sein. Starten Sie sie einfach, bevor Sie den Anwendungsserver starten.
Bei der Installation der IDM 3.5.1-Benutzeranwendung unter Linux oder Solaris	Der vorgegebene Installationsordner ist `/opt/novell/idm`. Während der Installation können Sie ein anderes Standard-Installationsverzeichnis auswählen. Stellen Sie sicher, dass das Verzeichnis existiert und dass ein Nicht-`Root`-Benutzer Schreibzugriff darauf hat.
Bei der Installation der IDM 3.5.1-Benutzeranwendung unter Windows	**Installationsverzeichnis:** Der vorgegebene Installationsordner ist `C:\Novell\IDM` . Stellen Sie sicher, dass dieser Ordner vorhanden ist und beschrieben werden kann. Während der Installation können Sie ein anderes Standard-Installationsverzeichnis auswählen.
Identity Manager 3.5.1	Der Identity Manager 3.5.1-Metaverzeichnis-Server muss installiert sein, bevor Sie einen Benutzeranwendungstreiber erstellen und die Benutzeranwendung installieren können.
Benutzeranwendungstreiber	Der Benutzeranwendungstreiber muss bereits vor der Installation der Benutzeranwendung vorhanden (aber nicht eingeschaltet) sein.
Zugriff auf das Identitätsdepot	Die Benutzeranwendung benötigt einen Benutzer mit Administratorzugriff auf den Kontext, in dem sich die Benutzer der Benutzeranwendung befinden werden.
IDM-Benutzeranwendungsspeicher	Auf dem Computer, auf dem die Benutzeranwendung installiert wird, müssen mindestens 320 MB Speicherplatz verfügbar sein.

Wenn alle Voraussetzungen erfüllt sind, befolgen Sie die Installationsanweisungen in den folgenden Abschnitten:

- Abschnitt 5.1.1, „Installation des JBoss-Anwendungsservers und der MySQL-Datenbank“, auf Seite 102
- Abschnitt 5.1.2, „Installation des JBoss-Anwendungsservers als Dienst“, auf Seite 105
- Abschnitt 5.1.3, „Konfiguration der MySQL-Datenbank“, auf Seite 106

5.1.1 Installation des JBoss-Anwendungsservers und der MySQL-Datenbank

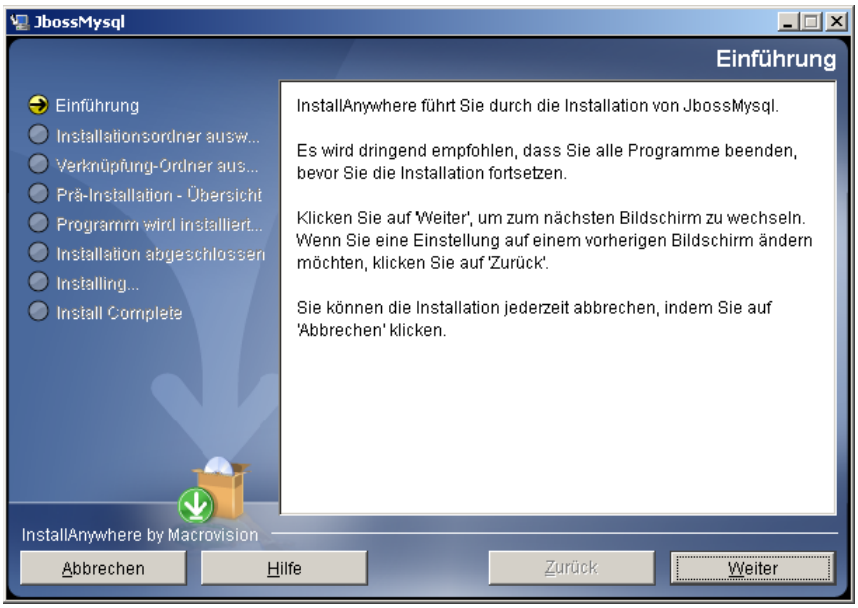
Verwenden Sie zum Installieren eines JBoss-Anwendungsservers und von MySQL auf Ihrem System das JbossMysql-Dienstprogramm.

Mit diesem Dienstprogramm kann der JBoss-Anwendungsserver nicht als Windows-Dienst installiert werden. Informationen zur Installation des JBoss-Anwendungsservers als Dienst unter Windows finden Sie in Abschnitt 5.1.2, „Installation des JBoss-Anwendungsservers als Dienst“, auf Seite 105.

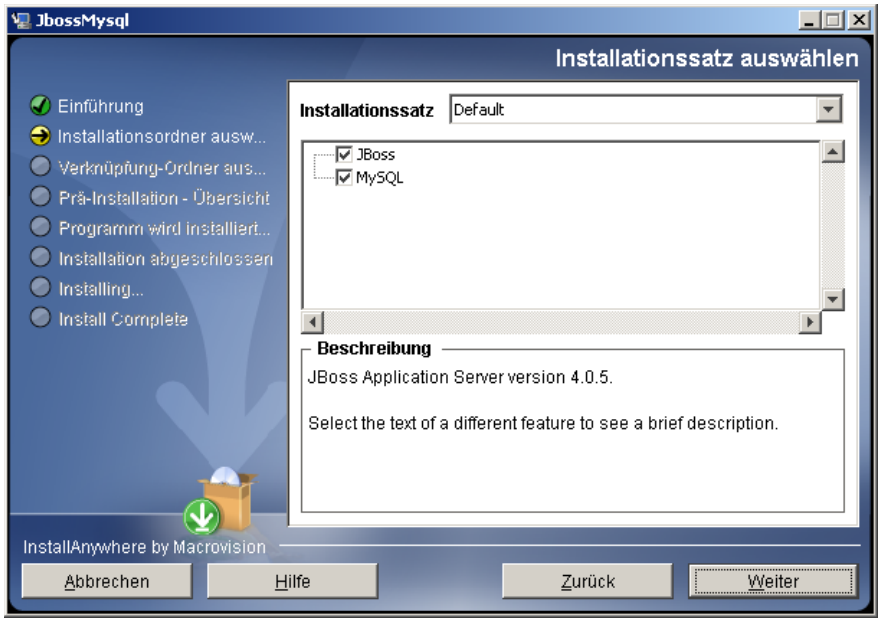
1. Führen Sie `JbossMysql.bin` oder `JbossMysql.exe` aus. Sie finden dieses Dienstprogramm mit dem Benutzeranwendungs-Installationsprogramm gebündelt unter

   `/linux/user_application` (für Linux)
   `/nt/user_application` (für Windows)

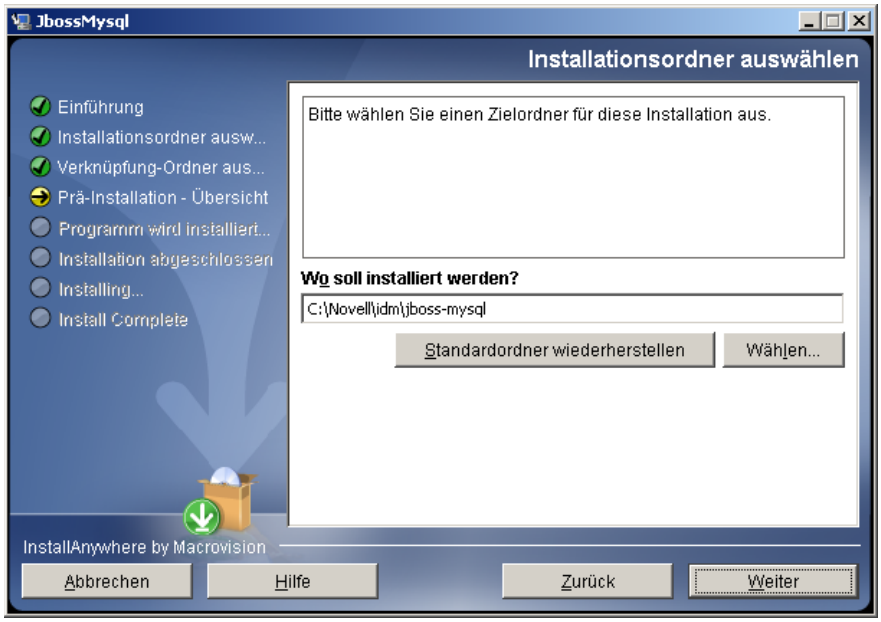
   Das Dienstprogramm ist für Solaris nicht verfügbar.
2. Wählen Sie Ihr Gebietsschema aus.
3. Lesen Sie die Einführung und klicken Sie anschließend auf *Weiter*.



4 Wählen Sie die zu installierenden Produkte aus und klicken Sie auf *Weiter*.

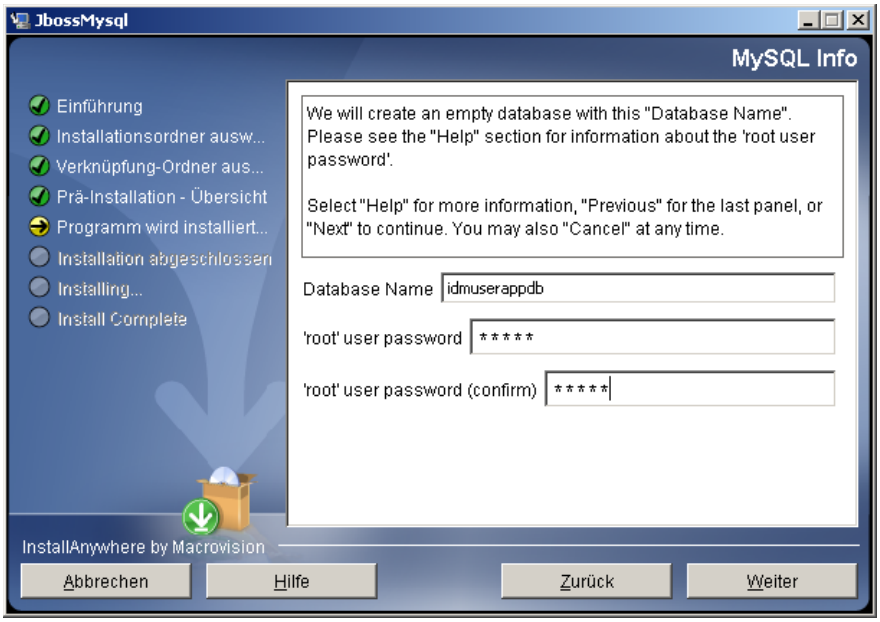


5 Klicken Sie zur Auswahl des Basisordners, in dem die ausgewählten Produkte installiert werden sollen, auf *Basisordner wählen* und anschließend auf *Weiter*.



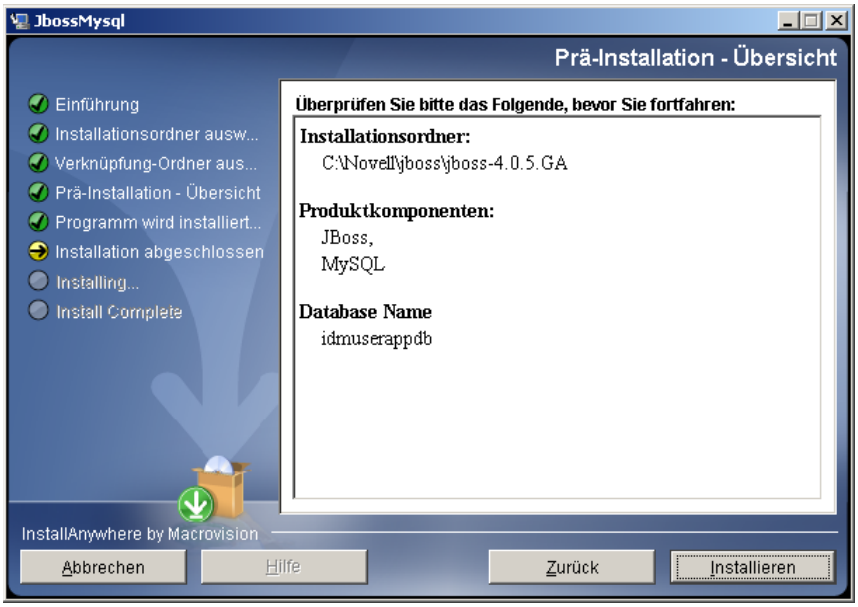
6 Legen Sie einen Namen für die Datenbank fest. Dieser Name ist bei der Installation der Benutzeranwendung erforderlich.

7 Geben Sie das Passwort für den `root`-Benutzer der Datenbank an.



8 Klicken Sie auf *Weiter*.

9 Überprüfen Sie Ihre Angaben auf der Seite „Zusammenfassung vor der Installation“ und klicken Sie anschließend auf *Installieren*.



Nach der Installation der ausgewählten Produkte wird eine Meldung zur erfolgreichen Installation angezeigt. Wenn Sie die MySQL-Datenbank installiert haben, fahren Sie mit Abschnitt 5.1.3, „Konfiguration der MySQL-Datenbank“, auf Seite 106 fort.

5.1.2 Installation des JBoss-Anwendungsservers als Dienst

Wenn der JBoss-Anwendungsserver als Dienst ausgeführt werden soll, verwenden Sie einen Java Service Wrapper oder ein Dienstprogramm eines Drittanbieters. Eine Anleitung von JBoss finden Sie unter http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows (http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows).

- „Verwendung eines Java Service Wrapper“ auf Seite 105
- „Verwendung eines Dienstprogramms eines Drittanbieters“ auf Seite 105

Verwendung eines Java Service Wrapper

Sie können mithilfe eines Java Service Wrapper den JBoss-Anwendungsserver als Windows-Dienst installieren, starten und anhalten. Im Internet finden Sie weitere Seiten mit verfügbaren Dienstprogrammen und Downloadsites.

Ein derartiger Wrapper befindet sich unter http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html): Verwalten Sie Ihn mit JMX (siehe http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss)). Dies sind einige Beispiel-Konfigurationsdateien:

```
wrapper.conf :
wrapper.java.command=%JAVA_HOME%/bin/java
wrapper.java.mainclass=org.tanukisoftware.wrapper.WrapperSimpleApp
wrapper.java.classpath.1=%JBOSS_HOME%/server/default/lib/
 wrapper.jar
wrapper.java.classpath.2=%JAVA_HOME%/lib/tools.jar
 wrapper.java.classpath.3=./run.jar
wrapper.java.library.path.1=%JBOSS_HOME%/server/default/lib
 wrapper.java.additional.1=-server
 wrapper.app.parameter.1=org.jboss.Main
 wrapper.logfile=%JBOSS_HOME%/server/default/log/wrapper.log
 wrapper.ntservice.name=JBoss wrapper.ntservice.displayname=JBoss
 Server
```

Warnung: Sie müssen Ihre Umgebungsvariable JBOSS_HOME korrekt setzen. Der Wrapper setzt diese nicht von allein.

```
java-service-wrapper-service.xml : <Xxml version="1.0"
encoding="UTF-8"?><!DOCTYPE server><server> <mbean
code="org.tanukisoftware.wrapper.jmx.WrapperManager"
name="JavaServiceWrapper:service=WrapperManager"/> <mbean
code="org.tanukisoftware.wrapper.jmx.WrapperManagerTesting"
name="JavaServiceWrapper:service=WrapperManagerTesting"/></server
```

Verwendung eines Dienstprogramms eines Drittanbieters

In früheren Versionen konnten Sie ein Dienstprogramm eines Drittanbieters, wie z. B. JavaService, verwenden, um den JBoss-Anwendungsserver als Windows-Dienst zu installieren, zu starten und anzuhalten.

Warnung: Die Verwendung von JavaService wird von JBoss nicht mehr empfohlen. Einzelheiten finden Sie unter http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService (http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService).

5.1.3 Konfiguration der MySQL-Datenbank

Die MySQL-Konfigurationseinstellungen müssen so konfiguriert sein, dass MySQL und Identity Manager 3.5.1 zusammenarbeiten. Wenn Sie MySQL eigenständig installieren, müssen Sie die Einstellungen selbst vornehmen. Wenn Sie MySQL mithilfe des JbossMysql-Dienstprogramms installieren, nimmt das Dienstprogramm die richtigen Einstellungen vor. Sie benötigen diese Werte allerdings für die folgenden Elemente:

- „Zeichensatz“ auf Seite 106
- „INNODB-Storage-Engine und Tabellentypen“ auf Seite 106
- „Beachtung der Groß- und Kleinschreibung“ auf Seite 106

Zeichensatz

Legen Sie UTF-8 als Zeichensatz für den gesamten Server oder nur für eine Datenbank fest. Legen Sie UTF-8 serverübergreifend fest, indem Sie die folgende Option in `my.cnf` (Linux oder Solaris) oder `my.ini` (Windows) aufnehmen:

`character-set-server=utf8` oder

Geben Sie den Zeichensatz für eine Datenbank bei ihrer Erstellung an, indem Sie den folgenden Befehl eingeben:

```
create database databasename character set utf8 collate utf8_bin;
```

Wenn Sie den Zeichensatz für die Datenbank festlegen, müssen Sie auch den Zeichensatz in der JDBC-URL in der Datei `IDM-ds.xml` festlegen. Beispiel:

```
<connection-url>jdbc:mysql://localhost:3306/
databasename?useUnicode=true&amp;characterEncoding
```

INNODB-Storage-Engine und Tabellentypen

Die Benutzeranwendung verwendet die INNODB-Storage-Engine, sodass Sie INNODB-Tabellentypen für MySQL auswählen können. Wenn Sie eine MySQL-Tabelle erstellen, ohne den Tabellentyp anzugeben, wird der Tabelle standardmäßig der Tabellentyp „MyISAM“ zugeordnet. Wenn Sie MySQL während der Installation von Identity Manager installieren, wird für MySQL der Tabellentyp „INNODB“ festgelegt. Sie können sicherstellen, dass Ihr MySQL-Server INNODB verwendet, indem Sie überprüfen, ob `my.cnf` (Linux oder Solaris) oder `my.ini` (Windows) die folgende Option enthält:

```
default-table-type=innodb
```

Die Option `skip-innodb` darf nicht enthalten sein.

Beachtung der Groß- und Kleinschreibung

Stellen Sie sicher, dass die Beachtung der Groß- und Kleinschreibung server- bzw. plattformübergreifend einheitlich geregelt ist, falls Daten server- bzw. plattformübergreifend

gesichert und wiederhergestellt werden. Sie können die Einheitlichkeit gewährleisten, indem Sie für `lower_case_table_names` in allen `my.cnf`-Dateien (Linux oder Solaris) oder `my.ini`-Dateien (Windows) denselben Wert angeben (0 oder 1), anstatt den vorgegebenen Wert zu übernehmen (die Windows-Vorgabe ist 0, die Linux-Vorgabe ist 1). Legen Sie diesen Wert fest, bevor Sie die Datenbank für die Identity Manager-Tabellen erstellen. Beispiel: Sie definieren

```
lower_case_table_names=1
```

in den `my.cnf`- und `my.ini`-Dateien für alle Plattformen, auf denen eine Datenbank gesichert und wiederhergestellt werden soll.

5.2 Installation und Konfiguration

1. Erstellen Sie den Benutzeranwendungstreiber und lassen Sie ihn deaktiviert.

   In diesem Schritt werden neue Objekte im Identitätsdepot erstellt. Einige Objekte haben Standard-Datenwerte. Weitere Informationen hierzu finden Sie in Abschnitt 5.3, „Erstellen des Benutzeranwendungstreibers“, auf Seite 107.

2. Führen Sie das Installationsprogramm der Benutzeranwendung aus.

   Weitere Informationen hierzu finden Sie unter Abschnitt 5.5, „Installation der Benutzeranwendung auf einem JBoss-Anwendungsserver von der GUI des Installationsprogramms“, auf Seite 114 oder Abschnitt 5.6, „Installation der Benutzeranwendung auf einem WebSphere-Anwendungsserver“, auf Seite 147.

   WebSphere-Benutzer müssen die WAR-Datei manuell implementieren.

Wichtig: Zur Installation der Identity Manager-Benutzeranwendung muss der Benutzeranwendungstreiber bereits vor der Installation der Anwendung vorhanden sein. Sie müssen den Treiber jedoch *nach* der Installation der Identity Manager-Benutzeranwendung starten. Anderenfalls treten möglicherweise Fehler auf.

5.3 Erstellen des Benutzeranwendungstreibers

Sie müssen für jede Benutzeranwendung einen separaten Benutzeranwendungstreiber erstellen, sofern sich die Benutzeranwendungen nicht in einem Cluster befinden. Benutzeranwendungen, die demselben Cluster angehören, müssen sich einen Benutzeranwendungstreiber teilen. Weitere Informationen zum Ausführen der Benutzeranwendung in einem Cluster finden Sie im *Identity Manager 3.5.1 Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idm35/index.html).

Die Benutzeranwendung speichert anwendungsspezifische Daten im Treiber, um die Anwendungsumgebung zu steuern und zu konfigurieren. Dazu gehören die Cluster-Informationen für den Anwendungsserver und die Workflow-Engine-Konfiguration.

Wichtig: Wird mehreren Benutzeranwendungen, die sich nicht in einem Cluster befinden, derselbe Treiber zugeordnet, führt dies bei einer oder mehreren Komponenten in der Benutzeranwendung zu Mehrdeutigkeiten und einer fehlerhaften Konfiguration. Der Ursprung der daraus entstehenden Probleme ist nur schwer zu erkennen.

So erstellen Sie einen Benutzeranwendungstreiber und verknüpfen ihn mit einem Treibersatz:

1. Melden Sie sich beim Identitätsdepot mit iManager an (falls Sie nicht bereits angemeldet sind).

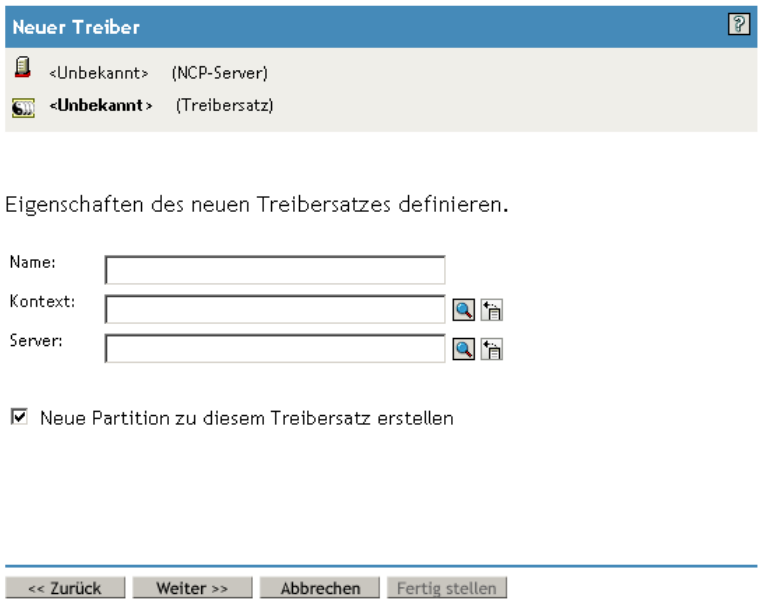
2 Wechseln Sie zu *Funktionen und Aufgaben* > *Identity Manager-Dienstprogramme* und wählen Sie *Neuer Treiber*, um den Assistenten zur Treibererstellung zu starten.

3 Wenn der Treiber in einem vorhandenen Treibersatz erstellt werden soll, wählen Sie die Option *In einem vorhandenen Treibersatz*. Klicken Sie anschließend auf das Symbol für die Objektauswahl, wählen Sie ein Treibersatzobjekt und klicken Sie auf *Weiter*. Fahren Sie dann mit Schritt 4 fort.

oder

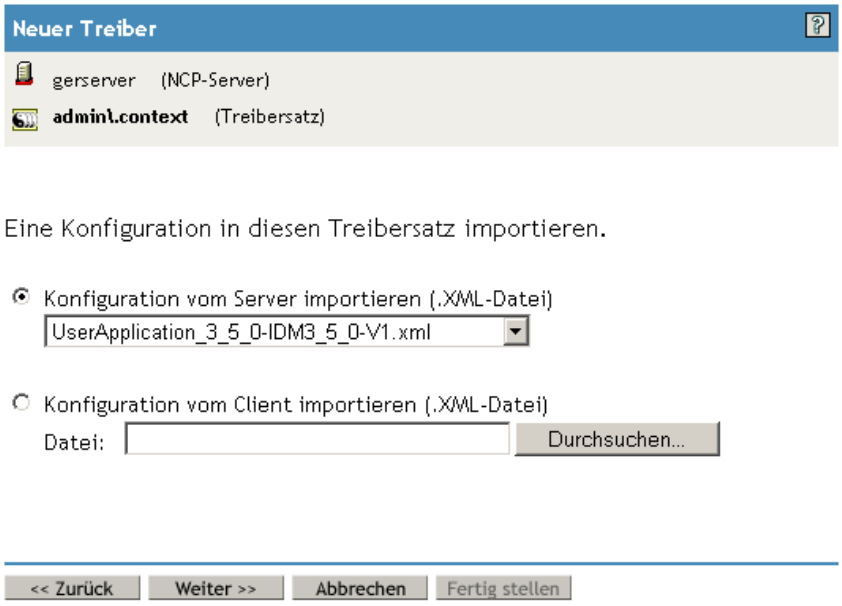
Wenn ein neuer Treibersatz erstellt werden soll (z. B. wenn der Benutzeranwendungstreiber auf einem anderen Server platziert werden soll als die anderen Treiber), wählen Sie *In einem neuen Treibersatz*, klicken Sie auf *Weiter* und definieren Sie anschließend die Eigenschaften des neuen Treibersatzes.

3a Geben Sie für den neuen Treibersatz einen Namen, einen Kontext und einen Server ein.



3b Klicken Sie auf *Weiter*.

4 Klicken Sie auf *Treiberkonfiguration vom Server importieren (.XML-Datei)*.



5 Wählen Sie in der Dropdown-Liste den Eintrag *UserApplication.xml*.

Dies ist die Konfigurationsdatei des neuen Treibers.

6 Klicken Sie auf *Weiter*.

Wenn *UserApplication.xml* nicht in der Dropdown-Liste angezeigt wird, wurde vermutlich bei der Installation von Identity Manager 3.5.1 der webbasierte Administrationsserver nicht installiert.

7 Sie werden aufgefordert, die Parameter für den Treiber einzugeben. (Blättern Sie durch die Elemente, um alle anzuzeigen.) Notieren Sie die Parameter, da Sie sie zur Installation der Benutzeranwendung benötigen.

Feld	Beschreibung
Treibername	Der Name des Treibers.
Authentifizierungs-ID	Der eindeutige Name des Benutzeranwendungsadministrators. Dies ist ein Benutzer, dem Sie die erforderlichen Rechte zur Verwaltung des Benutzeranwendungsportals erteilen. Verwenden Sie das eDirectory-Format (z. B. admin.orgunit.novell) oder wählen Sie den Benutzer aus. Die Eingabe in diesem Feld ist obligatorisch.
Passwort	Geben Sie das Passwort für den in der Authentifizierungs-ID angegebenen Administrator der Benutzeranwendung ein.
Anwendungskontext	Der Anwendungskontext der Benutzeranwendung. Dies ist der Kontextteil der URL für die WAR-Datei der Benutzeranwendung. Die Vorgabe ist „IDM“.
Host	Der Hostname oder die IP-Adresse des Anwendungsservers, auf dem die Identity Manager-Benutzeranwendung bereitgestellt wird. Wird der Anwendungsserver in einem Cluster ausgeführt, geben Sie den Hostnamen oder die IP-Adresse des Dispatchers ein.
Port	Der Port für den oben aufgeführten Host.
Überschreiben des Initiators zulassen: (gültige Werte: „Ja“ und „Nein“)	Wählen Sie *Ja*, damit der Bereitstellungsadministrator Workflows im Namen der Person starten darf, für die der Bereitstellungsadministrator als Vertretung benannt wurde.

8 Klicken Sie auf *Weiter*.

9 Klicken Sie zum Öffnen des Fensters „Sicherheitsäquivalenzen“ auf *Sicherheitsäquivalenzen definieren*. Wählen Sie einen Administrator oder ein anderes Supervisor-Objekt aus und klicken Sie auf *Hinzufügen*.

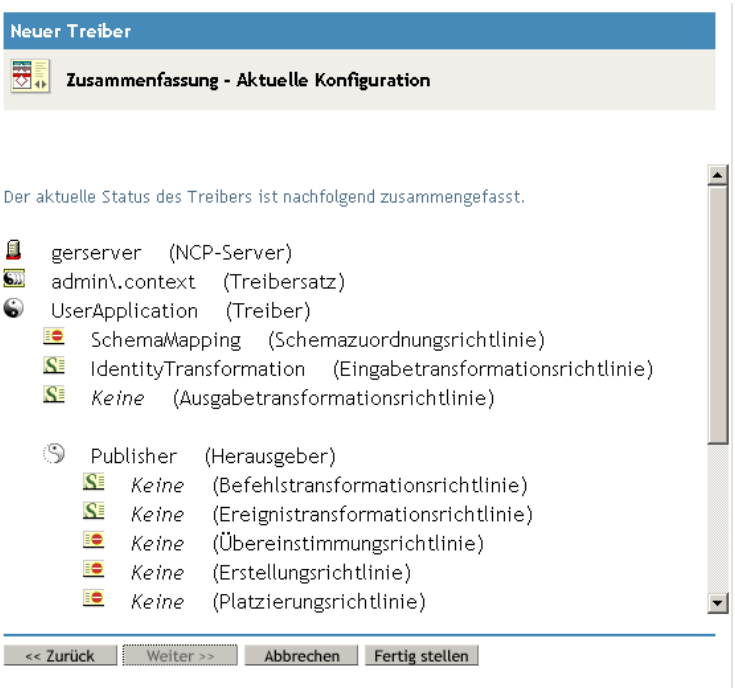
In diesem Schritt erhält der Treiber die erforderlichen Sicherheitsberechtigungen. Ausführliche Informationen zur Bedeutung dieses Schrittes finden Sie in der Dokumentation zu Identity Manager.

10 (Optional, aber empfohlen) Klicken Sie auf *Verwaltungsfunktionen ausschließen*.

11 Klicken Sie auf *Hinzufügen* und wählen Sie die Benutzer aus, die von Treiberaktionen ausgeschlossen sein sollen (z. B. Verwaltungsfunktionen).

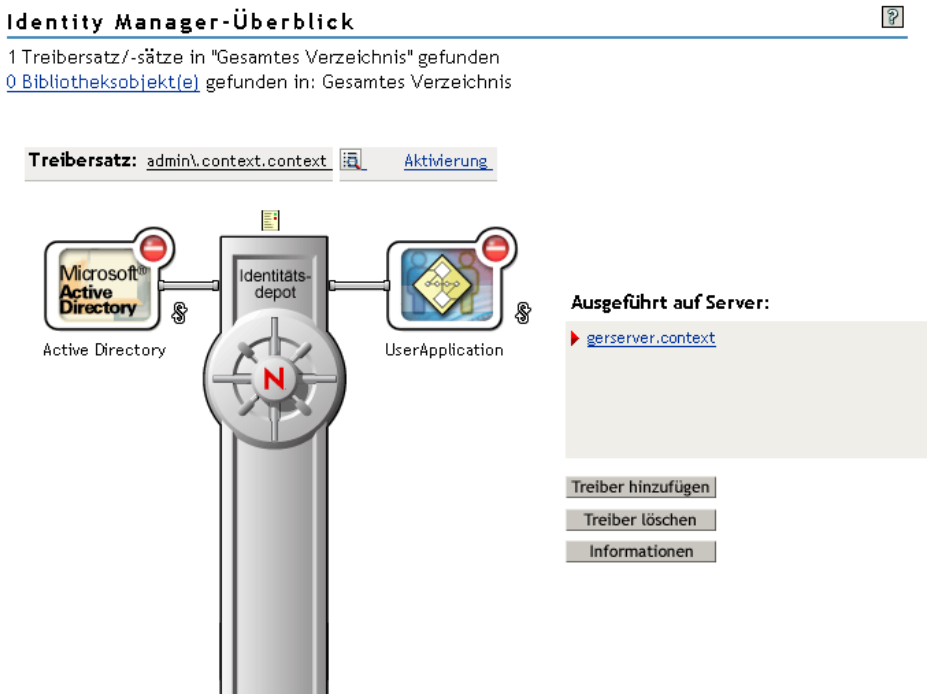
12 Klicken Sie zweimal auf *OK* und anschließend auf *Weiter*.

13 Klicken Sie auf *OK*, um das Fenster „Sicherheitsäquivalenzen“ zu schließen und eine Zusammenfassung anzuzeigen.



14 Sind die Angaben richtig, klicken Sie auf *Fertig stellen* oder *Fertig stellen – Überblick*.

Wichtig: In der Standardeinstellung ist der Treiber deaktiviert. Aktivieren Sie den Treiber erst nach der Installation der Benutzeranwendung.



5.4 Allgemeines zum Installationsprogramm

Das Installationsprogramm der Benutzeranwendung führt folgende Vorgänge durch:

- Festlegung einer vorhandenen Version eines zu verwendenden Anwendungsservers.
- Festlegung einer vorhandenen Version einer zu verwendenden Datenbank, z. B. MySQL, Oracle oder Microsoft SQL Server. Die Datenbank speichert Anwendungsdaten und Konfigurationsinformationen der Benutzeranwendung.
- Konfiguration der JDK-Zertifikatsdatei, sodass die Benutzeranwendung (die auf dem Anwendungsserver ausgeführt wird) sicher mit dem Identitätsdepot und mit der Benutzeranwendung kommunizieren kann.
- Konfiguration und Bereitstellung der Java-WAR-Datei (Web Application Archive) für die Novell Identity Manager-Benutzeranwendung und den JBoss-Anwendungsserver.
- Aktivierung der Protokollierung von Novell Audit, sofern ausgewählt.
- Möglichkeit zum Importieren eines vorhandenen Master-Schlüssels zur Wiederherstellung einer bestimmten Installation der Benutzeranwendung und zur Unterstützung von Clustern.

- Abschnitt 5.4.1, „Installations-Skripts und Programmdateien“, auf Seite 112.
- Abschnitt 5.4.2, „Für die Installation benötigte Werte“, auf Seite 113.

Das Installationsprogramm kann auf drei Arten gestartet werden:

- Über die grafische Benutzeroberfläche. Weitere Informationen hierzu finden Sie in Abschnitt 5.5, „Installation der Benutzeranwendung auf einem JBoss-Anwendungsserver von der GUI des Installationsprogramms“, auf Seite 114.
- Über die Konsolenschnittstelle (Befehlszeile). Weitere Informationen hierzu finden Sie in Abschnitt 5.7, „Installation der Benutzeranwendung über eine Konsolenschnittstelle“, auf Seite 176.
- Automatische Installation. Siehe Abschnitt 5.8, „Installation der Benutzeranwendung mit einem einzigen Befehl“, auf Seite 177.

5.4.1 Installations-Skripts und Programmdateien

Rufen Sie die Identity Manager 3.5.1-Installationsdateien durch eine der folgenden Methoden ab:

- Laden Sie das richtige `.iso`-Image oder die richtige `.zip`-Datei der Benutzeranwendung für Ihr System herunter: `Identity_Manager_3_5_1_User_Application.iso` oder `Identity_Manager_3_5_1_User_Application_Provisioning.iso`. Sie finden die Downloads auf der Website Novell Downloads (http://download.novell.com/index.jsp).
- Laden Sie die Produkt-DVD `Identity_Manager_3_5_1_DVD.iso` von Novell, Inc. herunter.

In Tabelle 5-2 sind alle Dateien und Skripts aufgeführt, die zur Installation der Identity Manager 3.5.1-Benutzeranwendung benötigt werden.

Tabelle 5-2 *Dateien und Skripts, die zur Installation der Identity Manager 3.5.1-Benutzeranwendung benötigt werden*

Datei	Beschreibung
WAR-Datei der Benutzeranwendung	Wählen Sie eine dieser Dateien: **IDM.war.** Enthält die Identity Manager 3.5.1-Benutzeranwendung mit Funktionen für die Identitätsselbstbedienung. **IDMProv.war.** Enthält die Identity Manager 3.5.1-Benutzeranwendung mit Funktionen für die Identitätsselbstbedienung und das Bereitstellungsmodul.

Die WAR-Dateien für Ihr System sowie die Dateien `IdmUserApp.jar` und `silent.properties` sind zunächst im folgenden Verzeichnis auf der Auslieferungs-CD für Ihr jeweiliges System verfügbar:

`/linux/user_application` (für Linux)
`/nt/user_application` (für Windows)
`/solaris/user_application` (für Solaris)

5.4.2 Für die Installation benötigte Werte

Tabelle 5-3 ist ein Arbeitsblatt, in dem Sie die Werte der Installationsparameter vermerken können, die bei der Installation auf JBoss verwendet werden sollen. Bei der Installation können außerdem Konfigurationsparameter für die Benutzeranwendung festgelegt werden. Informationen hierzu finden Sie in Abschnitt 5.5.14, „Konfiguration der Benutzeranwendung“, auf Seite 131.

Tabelle 5-3 *Installationsparameter – Arbeitsblatt für JBoss*

Parameter	Beispielwert	Ihr Wert
Installationsordner	C:\IDM\IDMinstalllocation	
Datenbankplattform	MySQL	
Datenbank-Host	localhost	
Datenbank-Port	3306	
Datenbankname (oder SID)	IDM	
Datenbankbenutzer	`Root`	
Datenbankbenutzer-Passwort		
Java-Stammordner	C:\Java\jdk1.5.0_10\	
(JBoss) Basisordner	C:\jboss	
JBoss-Host	localhost	
JBoss-Port	8080	

Parameter	Beispielwert	Ihr Wert
Workflow-Engine-ID (Für Cluster-Installationen. Jedem Mitglied des Clusters muss eine eindeutige ID zugeordnet werden.)		
Anwendungsname (URL-Kontext)	IDM	
Novell Audit-Server	[Name oder IP-Adresse]	
Verschlüsselter Master-Schlüssel. Siehe Abschnitt 5.5.13, „Angabe eines Master-Schlüssels“, auf Seite 129.	_+FEJEefMAglH0A= =:3VRmp04lub21Y3GpdaXCY)LG qS1nBaL/	

5.5 Installation der Benutzeranwendung auf einem JBoss-Anwendungsserver von der GUI des Installationsprogramms

In diesem Abschnitt wird die Installation der Identity Manager-Benutzeranwendung auf einem JBoss-Anwendungsserver über die grafische Benutzeroberfläche des Installationsprogramms erläutert.

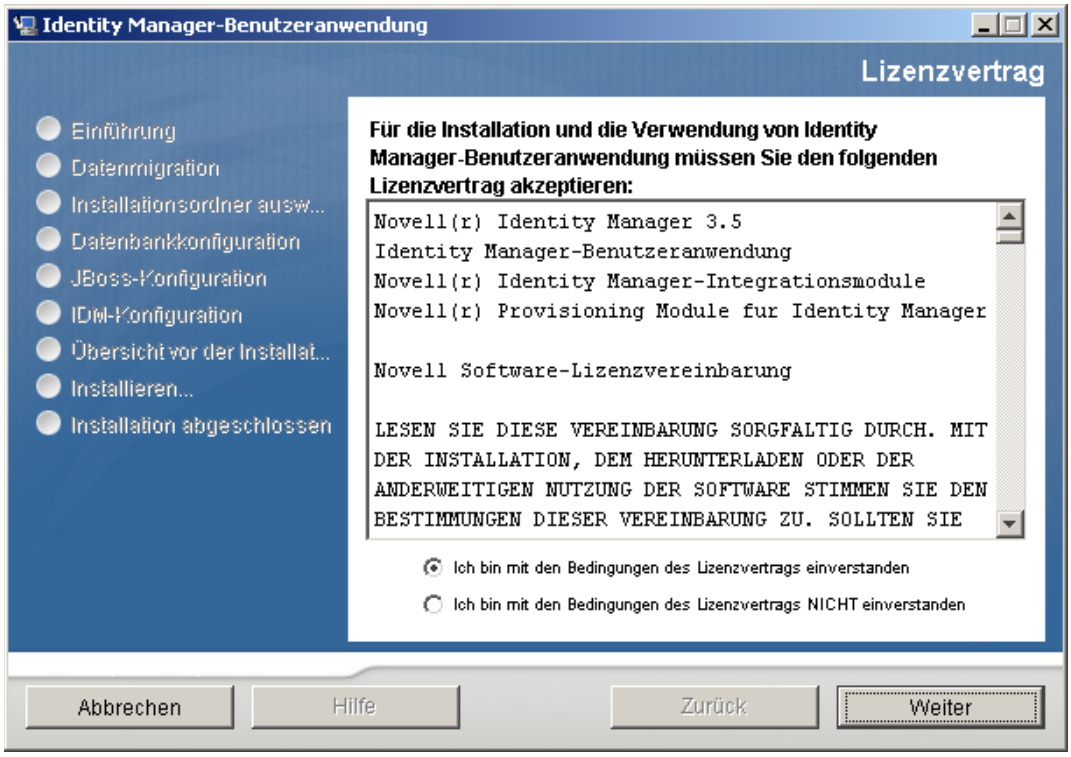
5.5.1 Starten der GUI des Installationsprogramms

1. Rufen Sie das Verzeichnis mit den in Tabelle 5-2 auf Seite 113 beschriebenen Installationsdateien auf.
2. Starten Sie das Installationsprogramm für Ihre Plattform über die Befehlszeile:

   ```
   java -jar IdmUserApp.jar
   ```

3. Wählen Sie im Dropdown-Menü eine Sprache aus und klicken Sie anschließend auf *OK*.

4. Lesen Sie die Lizenzvereinbarung, klicken Sie zur Bestätigung auf die entsprechende Schaltfläche und klicken Sie anschließend auf *Weiter*.

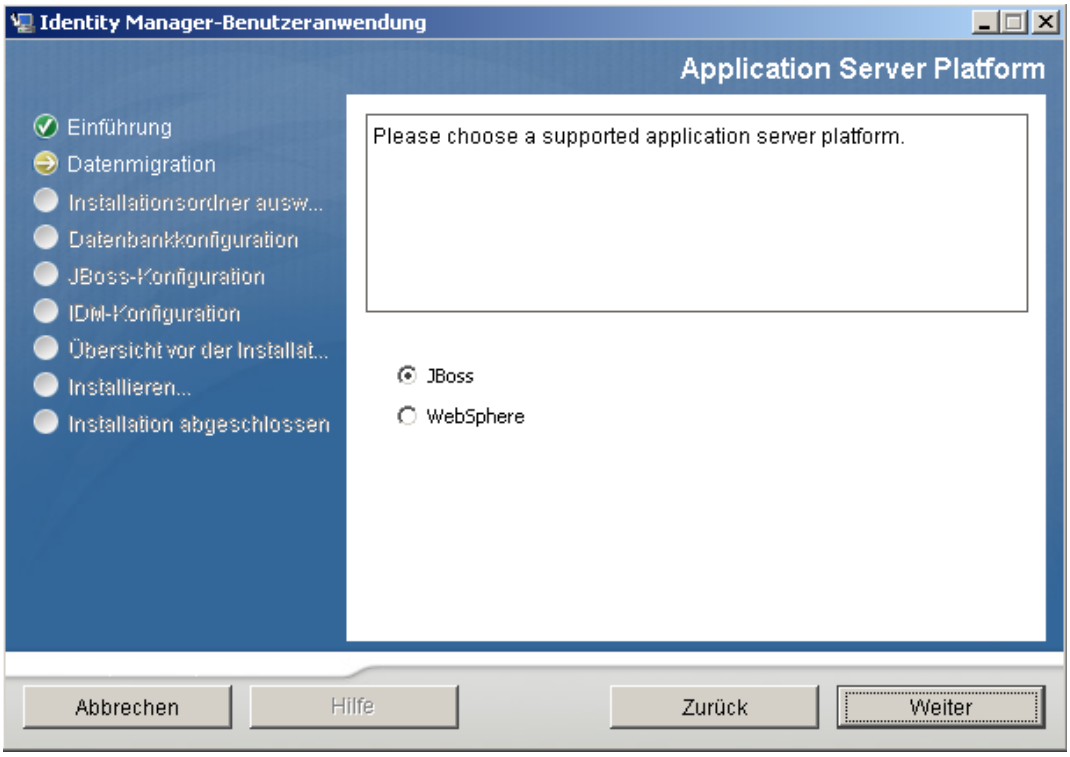


5 Lesen Sie die Einführungsseite des Installationsassistenten und klicken Sie anschließend auf *Weiter*.

6 Fahren Sie mit Abschnitt 5.5.2, „Auswahl einer Anwendungsserver-Plattform“, auf Seite 116 fort.

5.5.2 Auswahl einer Anwendungsserver-Plattform

1 Wählen Sie die JBoss-Anwendungsserver-Plattform aus und klicken Sie auf *Weiter*.



5.5.3 Migration einer Datenbank

Wenn Sie keine Datenbank migrieren möchten, klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.5.4, „Angabe des Speicherorts der WAR-Datei“, auf Seite 118 fort.

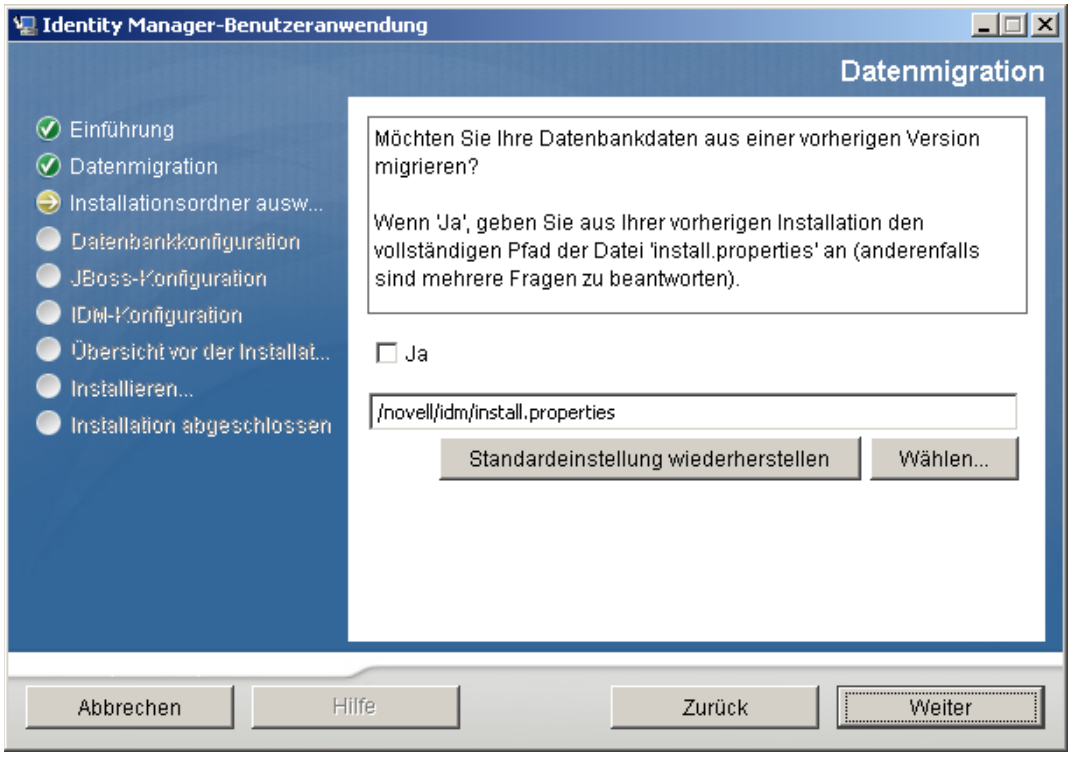
Wenn Sie weiterhin eine bestehende Datenbank der Version 3.0 oder 3.01 der Benutzeranwendung verwenden möchten, müssen Sie die Datenbank migrieren.

1 Überprüfen Sie, dass die zu migrierende Datenbank gestartet wurde.

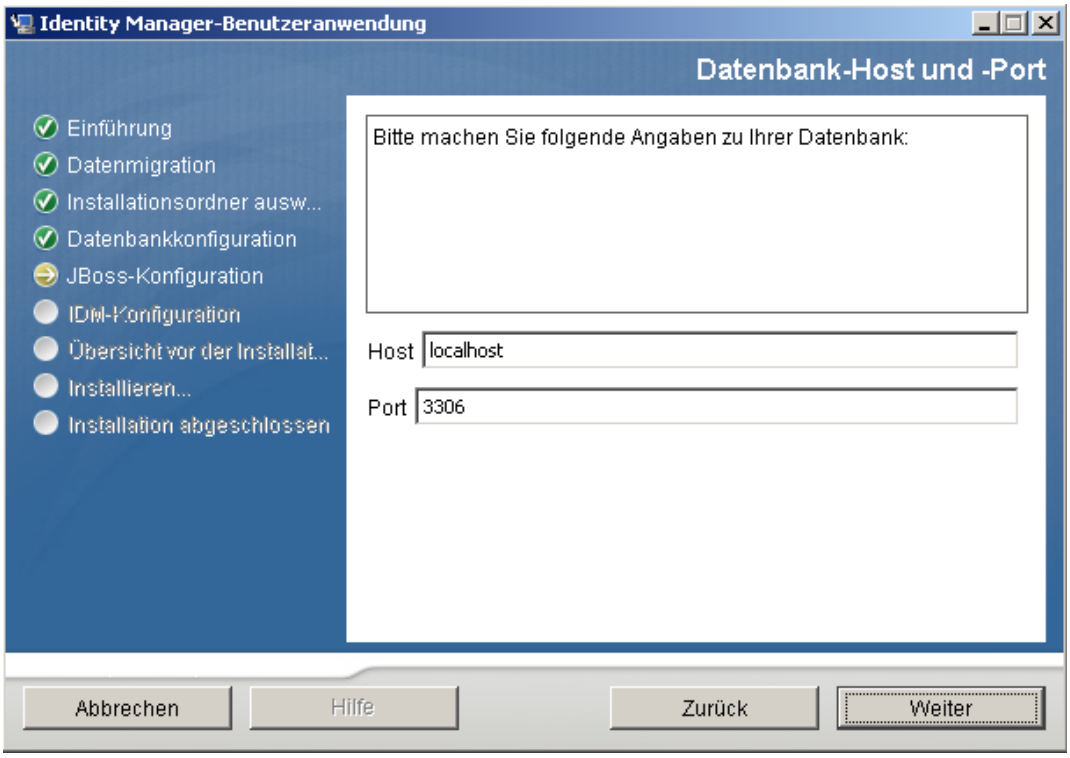
2 Klicken Sie auf der Seite „Datenmigration“ des Installationsprogramms auf *Ja*.

3 Navigieren Sie zur Datei `install.properties` im Installationsverzeichnis der Identity Manager 3.0 oder 3.01-Benutzeranwendung, indem Sie auf die Schaltfläche zum *Auswählen* klicken.

Wenn Sie den Speicherort der Datei `install.properties` von der vorherigen Installation angeben, verringert sich die Anzahl der Elemente, die Sie auf den folgenden Seiten festlegen müssen.



4 Sie werden aufgefordert, den Datenbanktyp, den Hostnamen und den Port zu bestätigen. Bestätigen Sie diese Angaben und klicken Sie auf *Weiter*.



5 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.5.4, „Angabe des Speicherorts der WAR-Datei“, auf Seite 118 oder Abschnitt 5.5.5, „Auswahl eines Installationsordners“, auf Seite 119 fort.

Das Installationsprogramm der Benutzeranwendung rüstet die Benutzeranwendung auf und migriert Daten aus der Datenbank der Version 3.0 oder 3.0.1 in die Datenbank, die für Version 3.5.1 verwendet wird. Weitere Informationen zur Migration einer Datenbank finden Sie im *Migrationshandbuch zur Identity Manager-Benutzeranwendung* (http://www.novell.com/documentation/idm35/index.html).

5.5.4 Angabe des Speicherorts der WAR-Datei

Wenn sich die WAR-Datei der Identity Manager-Benutzeranwendung nicht im selben Verzeichnis befindet wie das Installationsprogramm, werden Sie aufgefordert, den Pfad zur WAR-Datei einzugeben.

1 Wenn sich die WAR-Datei am Standardspeicherort befindet, klicken Sie auf *Standard wiederherstellen*.

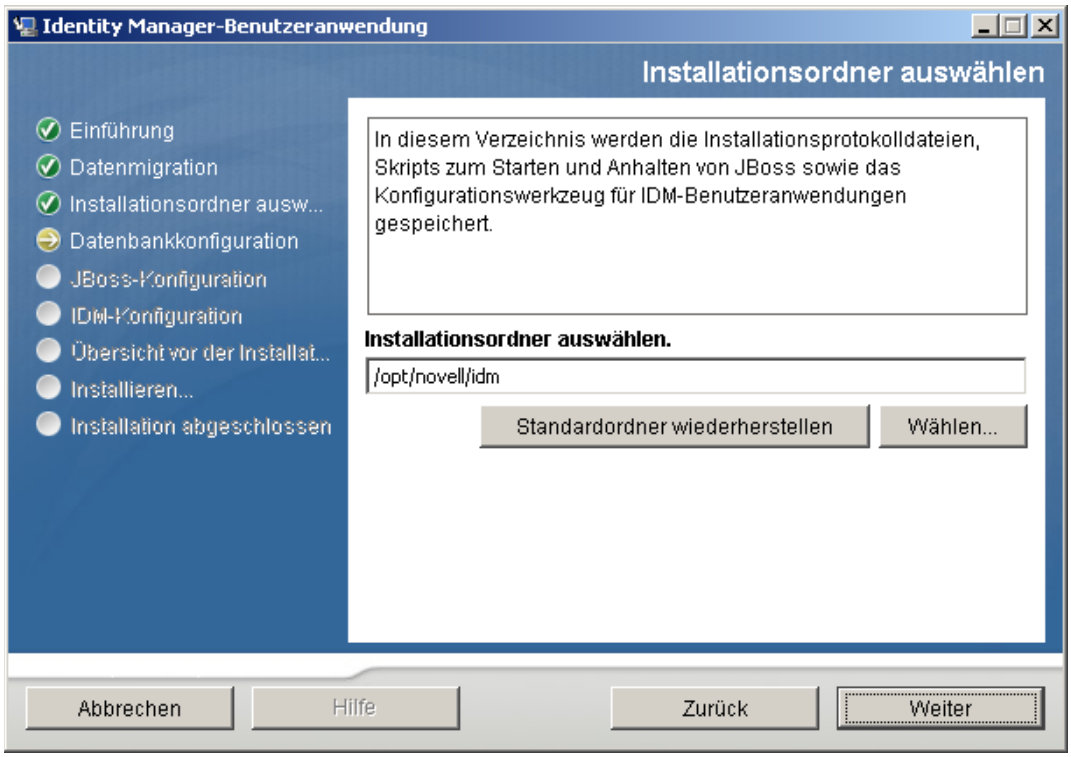
Sie können stattdessen auch auf die Schaltfläche zum *Auswählen* klicken und einen Speicherort auswählen, um den Speicherort der WAR-Datei anzugeben.

2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.5.5, „Auswahl eines Installationsordners“, auf Seite 119 fort.

5.5.5 Auswahl eines Installationsordners

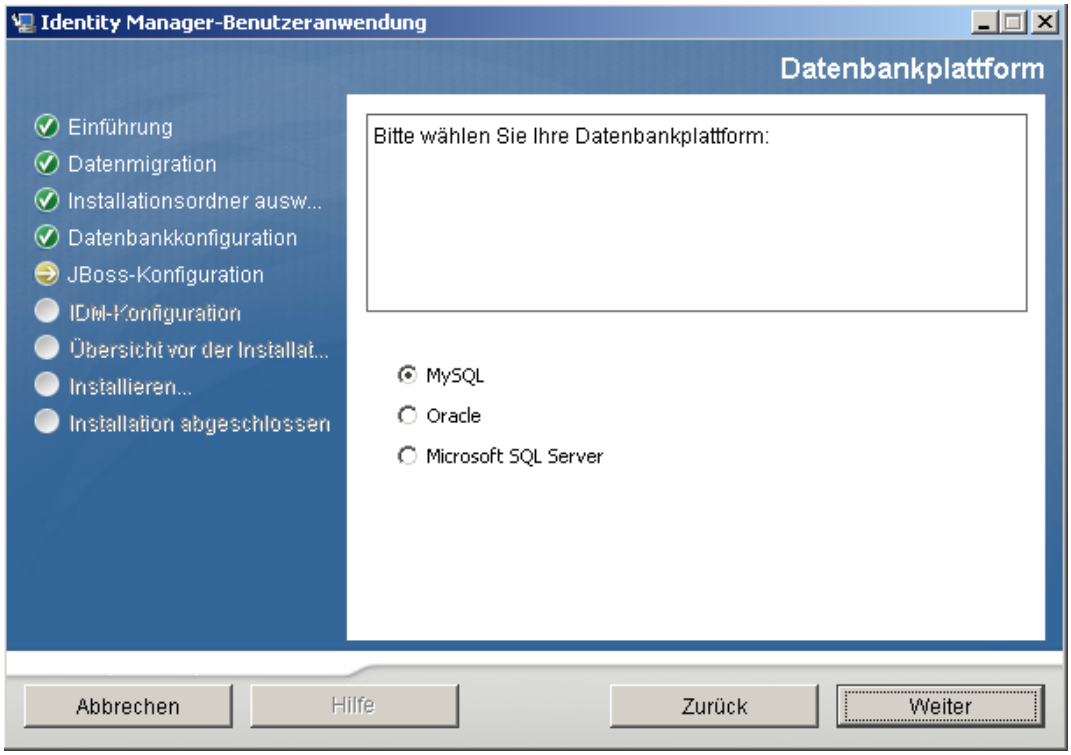
1 Geben Sie auf der Seite „Installationsordner auswählen“ die Stelle an, an der die Benutzeranwendung installiert werden soll. Wenn Sie den Standardspeicherort speichern und verwenden möchten, klicken Sie auf *Standard wiederherstellen* oder auf die Schaltfläche zum *Auswählen*, um einen anderen Speicherort für die Installationsdateien auszuwählen.

2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.5.6, „Auswahl einer Datenbankplattform“, auf Seite 121 fort.



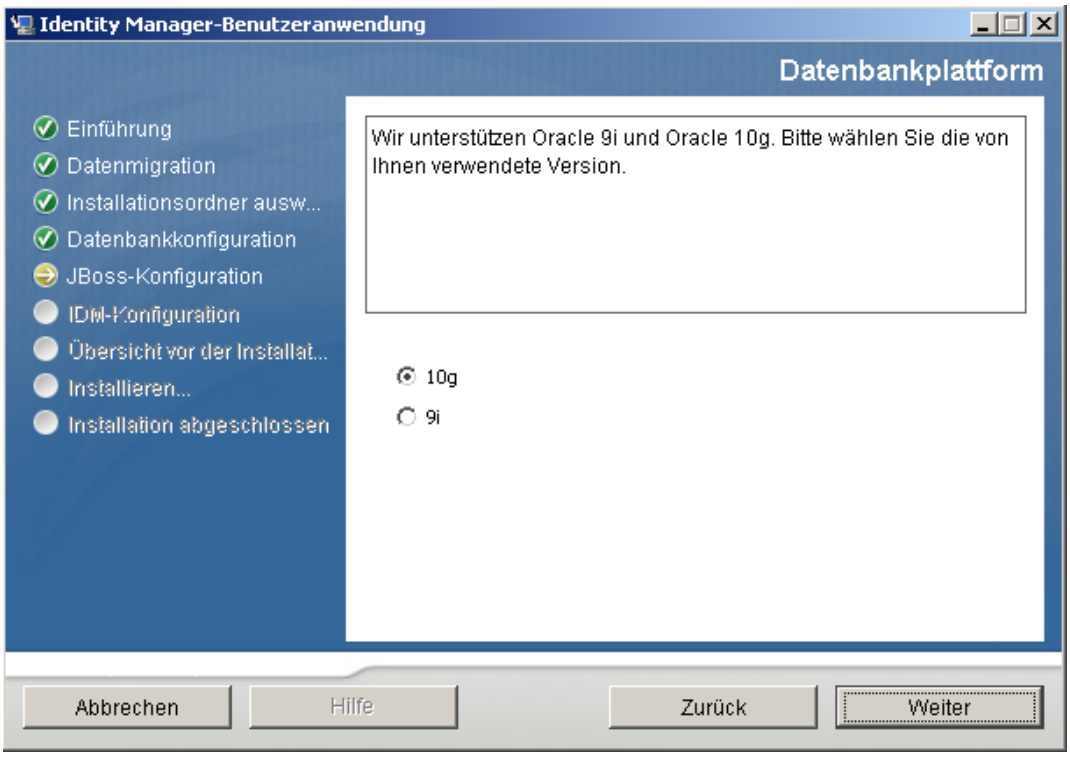
5.5.6 Auswahl einer Datenbankplattform

1 Wählen Sie die gewünschte Datenbank aus.



2 Wenn Sie eine Oracle-Datenbank verwenden, fahren Sie mit Schritt 3 fort. Fahren Sie anderenfalls mit Schritt 4 fort.

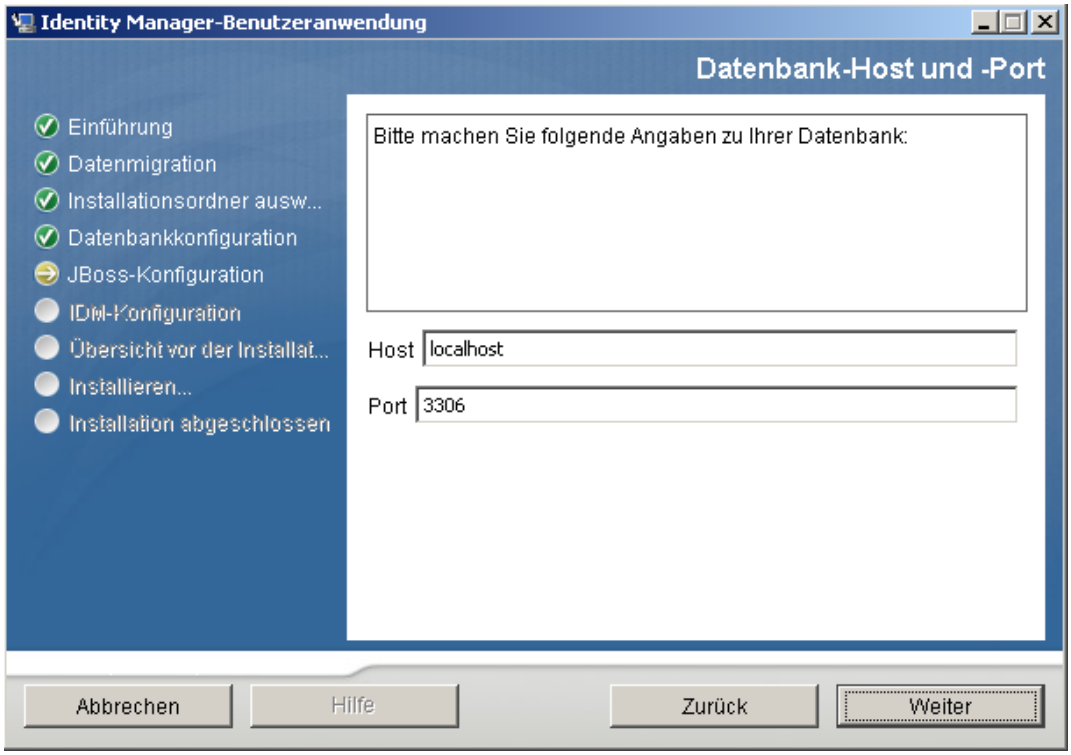
3 Bei Verwendung einer Oracle-Datenbank fragt Sie das Installationsprogramm nach deren Version. Wählen Sie die entsprechende Version aus.



4 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.5.7, „Angabe von Datenbank-Host und -Port“, auf Seite 123 fort.

5.5.7 Angabe von Datenbank-Host und -Port

1 Vervollständigen Sie die folgenden Felder:

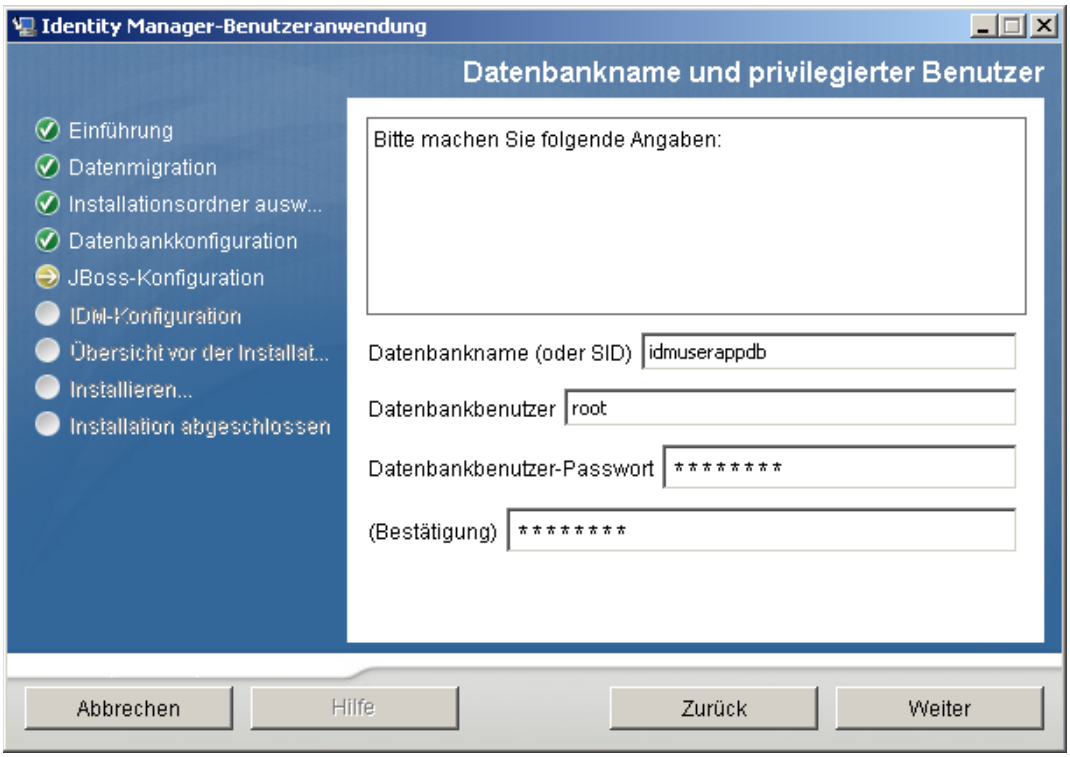


Feld	Beschreibung
Host	Geben Sie den Host oder die IP-Adresse des Datenbankservers an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Hostname bzw. dieselbe IP-Adresse angegeben werden.
Port	Geben Sie die Listener-Portnummer der Datenbank an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Port angegeben werden.

2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.5.8, „Angabe des Datenbanknamens und des privilegierten Benutzers“, auf Seite 124 fort.

5.5.8 Angabe des Datenbanknamens und des privilegierten Benutzers

1 Vervollständigen Sie die folgenden Felder:

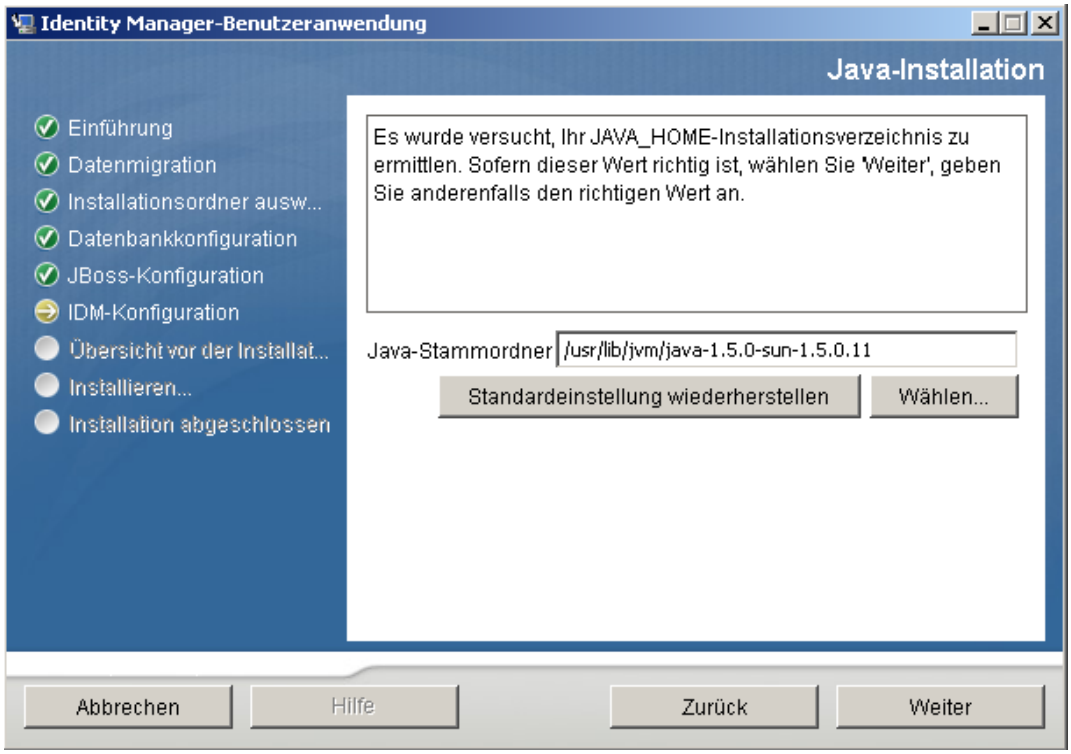


Feld	Beschreibung
Datenbankname (oder SID)	Geben Sie für MySQL oder MS SQL Server den Namen der vorkonfigurierten Datenbank an. Geben Sie für Oracle den zuvor erstellten Oracle System Identifier (SID) ein. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Datenbankname bzw. derselbe SID angegeben werden.
Datenbankbenutzer	Geben Sie den Datenbankbenutzer an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied dieselbe Datenbank angegeben werden.
Passwort und Bestätigungspasswort der Datenbank	Geben Sie das Passwort der Datenbank an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied dasselbe Passwort angegeben werden.

2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.5.9, „Angabe des Java-Stammordners“, auf Seite 125 fort.

5.5.9 Angabe des Java-Stammordners

1 Klicken Sie zum Wechseln in den Java-Stammordner auf die Schaltfläche zum *Auswählen*. Wenn Sie den Standardspeicherort verwenden möchten, klicken Sie auf *Standardeinstellung wiederherstellen*.



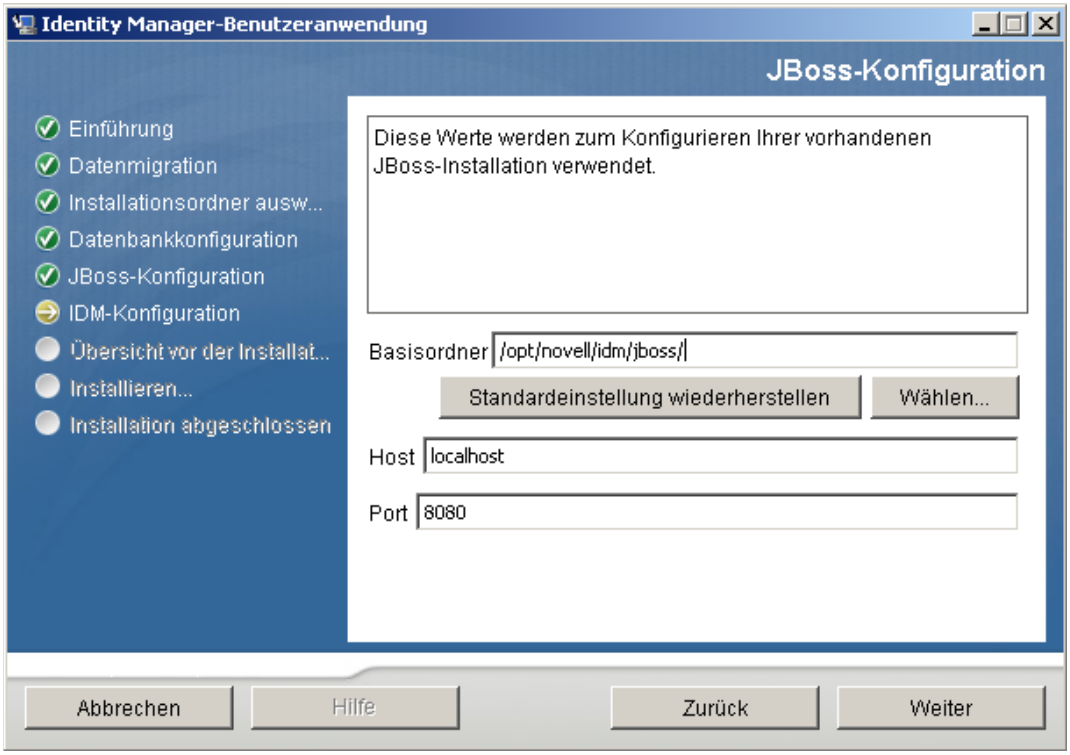
2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.5.10, „Angabe der Einstellungen für den JBoss-Anwendungsserver“, auf Seite 125 fort.

5.5.10 Angabe der Einstellungen für den JBoss-Anwendungsserver

Geben Sie auf dieser Seite den Pfad zum JBoss-Anwendungsserver an.

Bei diesem Installationsvorgang wird der JBoss-Anwendungsserver nicht installiert. Eine Anleitung für die Installation des JBoss-Anwendungsservers finden Sie in Abschnitt 5.1.1, „Installation des JBoss-Anwendungsservers und der MySQL-Datenbank“, auf Seite 102.

1 Geben Sie den Basisordner, den Host und den Port an:

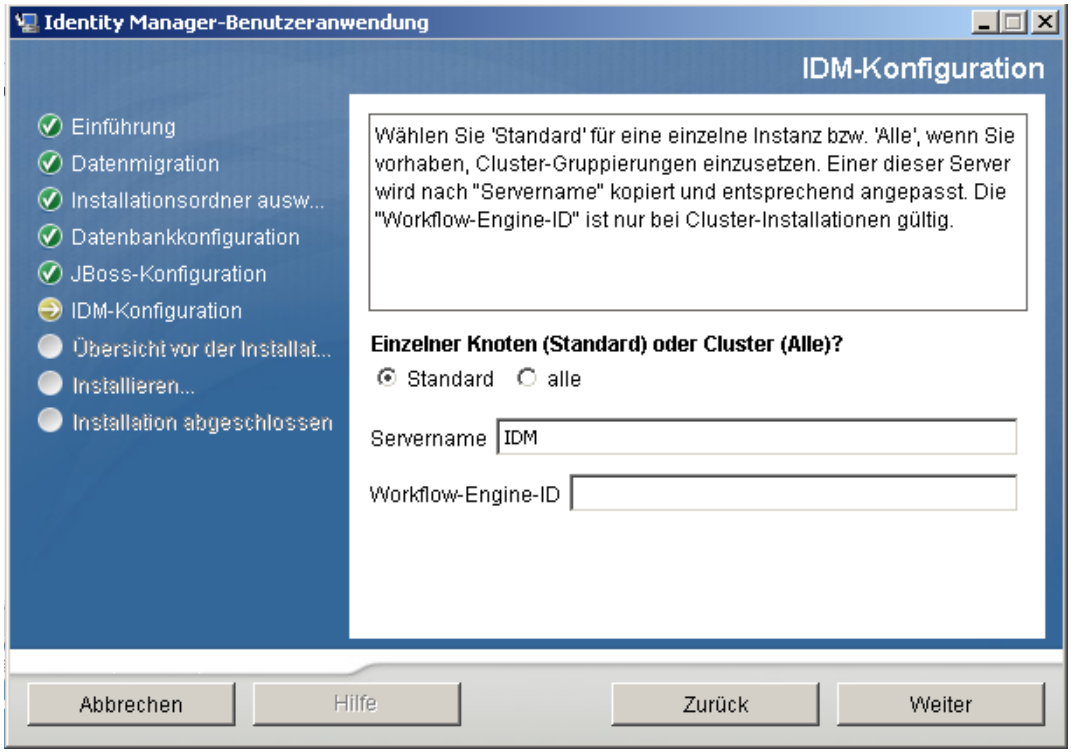


Feld	Beschreibung
Basisordner	Geben Sie den Speicherort des Anwendungsservers an.
Host	Geben Sie den Hostnamen oder die IP-Adresse des Anwendungsservers an.
Port	Geben Sie die Listener-Portnummer des Anwendungsservers an. Der JBoss-Standardport ist 8080.

2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.5.11, „Auswahl des Anwendungsserver-Konfigurationstyps“, auf Seite 127 fort.

5.5.11 Auswahl des Anwendungsserver-Konfigurationstyps

1 Vervollständigen Sie die folgenden Felder:



Option	Beschreibung
Einzelner Knoten (Standard) oder *Cluster* (Alle)	Wählen Sie den Anwendungsserver-Konfigurationstyp: ◆ Wählen Sie *Alle*, wenn diese Installation für ein Cluster erfolgt. ◆ Wählen Sie *Standard*, wenn diese Installation für einen einzelnen Knoten erfolgt, der nicht Teil eines Clusters ist.
Servername	Geben Sie den Servernamen an. Der Servername ist der Name der Konfiguration des Anwendungsservers, der Name der WAR-Datei der Anwendung und der Name des URL-Kontexts. Das Installations-Skript erstellt eine Serverkonfiguration und benennt die Konfiguration standardmäßig auf der Basis des *Anwendungsnamens*. Notieren Sie den Anwendungsnamen und fügen Sie ihn in die URL ein, wenn Sie die Identity Manager-Benutzeranwendung über einen Browser starten.

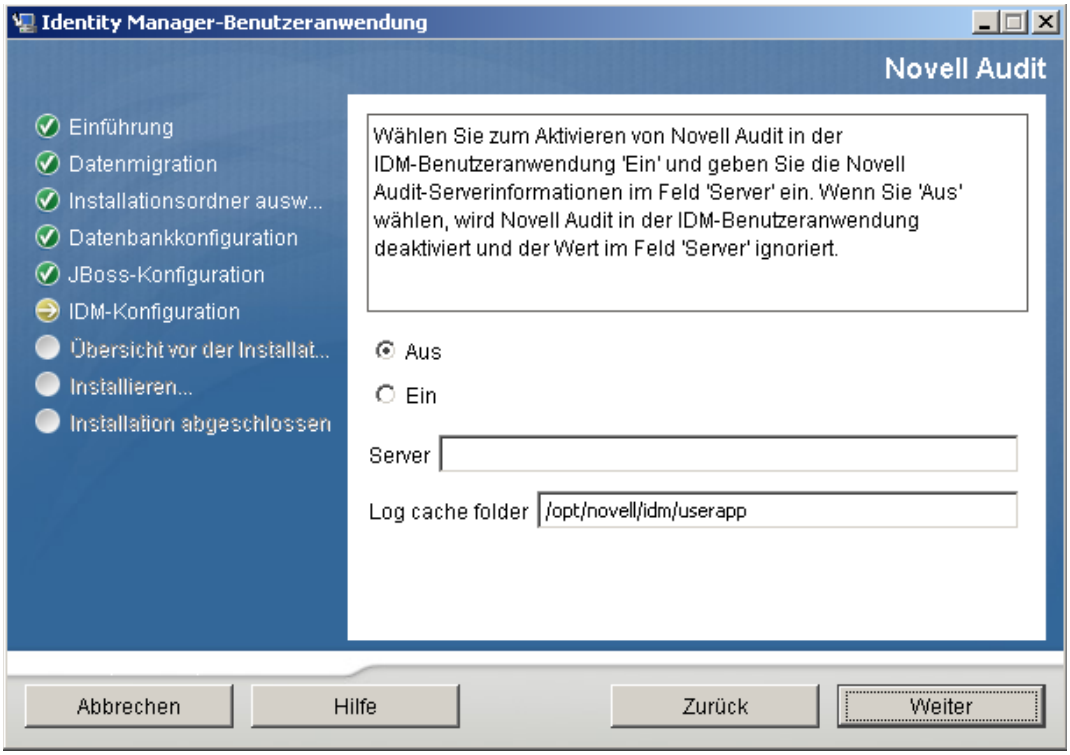
Option	Beschreibung
Workflow-Engine-ID	Jeder Server in einem Cluster muss eine eindeutige Workflow-Engine-ID besitzen. Weitere Informationen zu Workflow-Engine-IDs finden Sie im *Identity Manager-Benutzeranwendung: Administrationshandbuch* in Abschnitt 3.5.4 zur Konfiguration von Workflows für das Clustering.

2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.5.12, „Aktivieren der Novell Audit-Protokollierung“, auf Seite 128 fort.

5.5.12 Aktivieren der Novell Audit-Protokollierung

(Optional) So aktivieren Sie die Novell Audit-Protokollierung für die Benutzeranwendung:

1 Vervollständigen Sie die folgenden Felder:



Option	Beschreibung
Ein	Aktiviert die Novell Audit-Protokollierung für die Benutzeranwendung. Weitere Informationen zum Einrichten der Novell Audit-Protokollierung finden Sie im *Identity Manager-Benutzeranwendung: Administrationshandbuch*.
Aus	Deaktiviert die Novell Audit-Protokollierung für die Benutzeranwendung. Sie können sie zu einem späteren Zeitpunkt in der Benutzeranwendung über die Registerkarte *Administration* aktivieren. Weitere Informationen zur Aktivierung der Novell Audit-Protokollierung finden Sie im *Identity Manager-Benutzeranwendung: Administrationshandbuch*.
Server	Wenn Sie die Novell Audit-Protokollierung aktivieren, geben Sie den Hostnamen oder die IP-Adresse des Novell Audit-Servers an. Wenn Sie die Protokollierung deaktivieren, wird dieser Wert ignoriert.

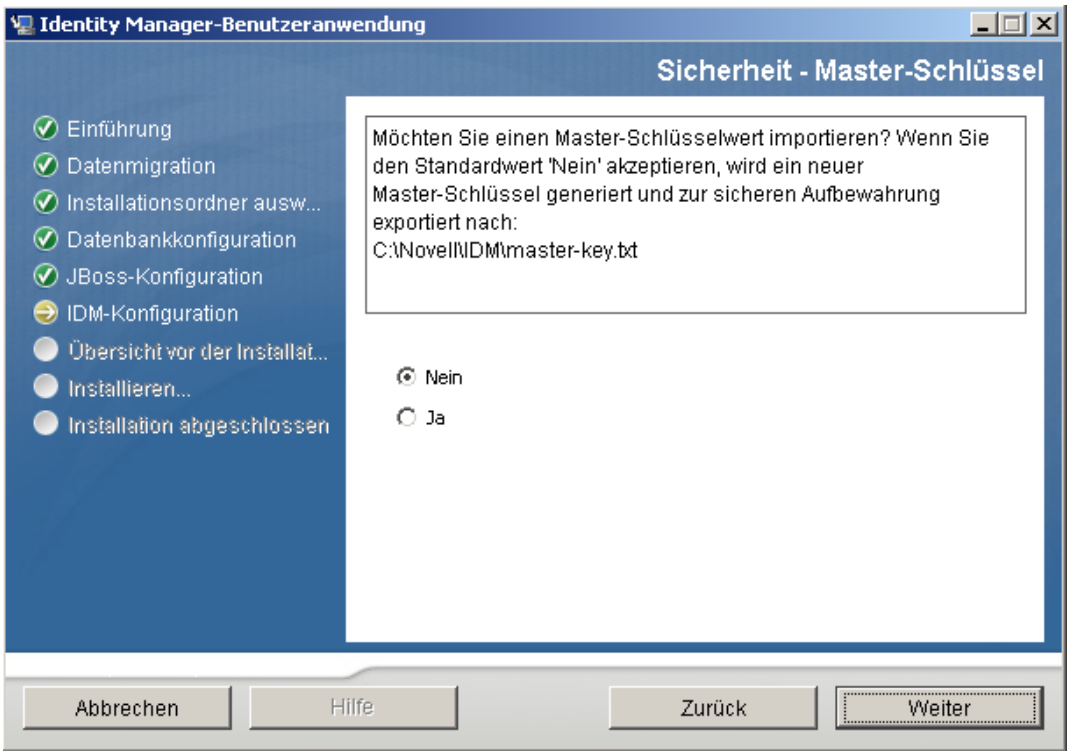
2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.5.14, „Konfiguration der Benutzeranwendung“, auf Seite 131 fort.

5.5.13 Angabe eines Master-Schlüssels

Geben Sie an, ob Sie einen vorhandenen Master-Schlüssel importieren oder einen neuen erstellen möchten. Mögliche Gründe für den Import eines vorhandenen Master-Schlüssels:

- Sie verlagern Ihre Installation aus einem Staging-System in ein Produktionssystem und möchten auch weiterhin auf die Datenbank des Staging-Systems zugreifen.
- Sie haben die Benutzeranwendung als erstes Mitglied eines JBoss-Clusters installiert und führen nun die Installation auf nachfolgenden Cluster-Mitgliedern durch (für die derselbe Master-Schlüssel benötigt wird).
- Bedingt durch einen Festplattenfehler müssen Sie die Benutzeranwendung wiederherstellen. Sie müssen die Benutzeranwendung neu installieren und den Master-Schlüssel der vorherigen Installation angeben. Auf diese Weise erhalten Sie Zugriff auf zuvor gespeicherte verschlüsselte Daten.

1 Klicken Sie auf *Ja*, um einen vorhandenen Master-Schlüssel zu importieren, oder auf *Nein*, um einen neuen Master-Schlüssel zu erstellen.



2 Klicken Sie auf *Weiter*.

Bei der Installation wird der verschlüsselte Master-Schlüssel im Installationsverzeichnis in die Datei `master-key.txt` geschrieben.

Wenn Sie *Nein* gewählt haben, fahren Sie mit Abschnitt 5.5.14, „Konfiguration der Benutzeranwendung“, auf Seite 131 fort. Nach Abschluss der Installation müssen Sie den Master-Schlüssel manuell speichern, wie in Abschnitt 5.9.1, „Aufzeichnen des Master-Schlüssels“, auf Seite 186 beschrieben.

Wenn Sie *Ja* gewählt haben, fahren Sie mit Schritt 3 fort.

3 Wenn ein vorhandener verschlüsselter Master-Schlüssel importiert werden soll, kopieren Sie den Schlüssel und fügen Sie ihn in das Fenster des Installationsvorgangs ein.

4 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.5.14, „Konfiguration der Benutzeranwendung“, auf Seite 131 fort.

5.5.14 Konfiguration der Benutzeranwendung

Bei der Installation der Benutzeranwendung können Sie Konfigurationsparameter für die Benutzeranwendung festlegen. Die meisten dieser Parameter können auch nach der Installation in der Datei `configupdate.sh` oder `configupdate.bat` bearbeitet werden. Auf Ausnahmen wird in den Parameterbeschreibungen hingewiesen.

In einer Clusterkonfiguration müssen für alle Cluster-Mitglieder dieselben Konfigurationsparameter für die Benutzeranwendung angegeben werden.

1 Geben Sie die wichtigsten Konfigurationsparameter für die Benutzeranwendung wie in Tabelle 5-4 beschrieben an und fahren Sie dann mit Schritt 2 fort.

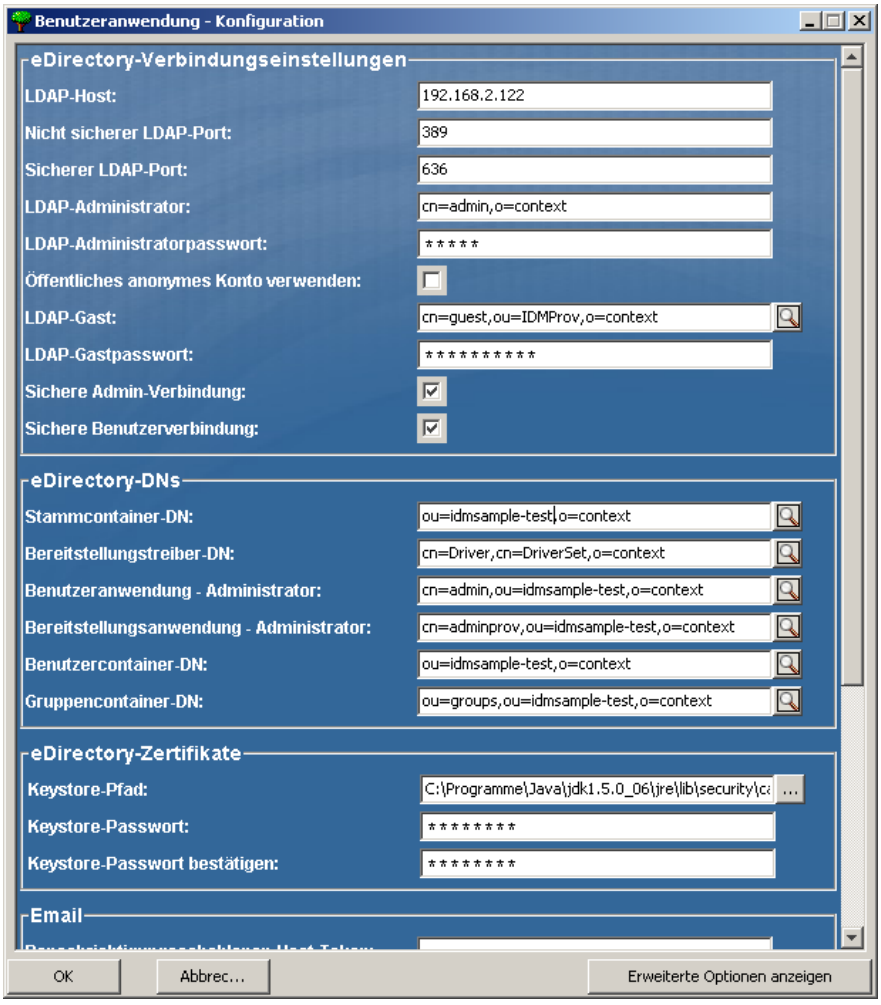


Tabelle 5-4 *Konfiguration der Benutzeranwendung: Wichtigste Parameter*

Einstellungstyp	Feld	Beschreibung
eDirectory-Verbindungs-einstellungen	*LDAP-Host*	Erforderlich. Geben Sie den Hostnamen oder die IP-Adresse sowie den sicheren Port des LDAP-Servers an. Beispiel: `myLDAPhost`
	Nicht sicherer LDAP-Port	Geben Sie den nicht sicheren Port des LDAP-Servers an. Beispiel: 389.
	Sicherer LDAP-Port	Geben Sie den sicheren Port des LDAP-Servers an. Beispiel: 636.
	LDAP-Administrator	Erforderlich. Geben Sie die Berechtigungsnachweise für den LDAP-Administrator an. Dieser Benutzer muss bereits vorhanden sein. Die Benutzeranwendung verwendet dieses Konto für eine administrative Verbindung zum Identitätsdepot. Dieser Wert ist mit dem Master-Schlüssel verschlüsselt.
	LDAP-Administratorpasswort	Erforderlich. Geben Sie das LDAP-Administratorpasswort an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
	Öffentliches anonymes Konto verwenden	Ermöglicht nicht angemeldeten Benutzern den Zugriff auf das öffentliche anonyme LDAP-Konto.
	LDAP-Gast	Ermöglicht nicht angemeldeten Benutzern den Zugriff auf zulässige Portlets. Dieses Benutzerkonto muss bereits im Identitätsdepot vorhanden sein. Deaktivieren Sie das Kontrollkästchen *Öffentliches anonymes Konto verwenden*, um „LDAP-Gast“ zu aktivieren. Aktivieren Sie das Kontrollkästchen *Öffentliches anonymes Konto verwenden*, um „LDAP-Gast“ zu deaktivieren.
	LDAP-Gastpasswort	Geben Sie das LDAP-Gastpasswort an.
	Sichere Admin-Verbindung	Wählen Sie diese Option aus, wenn die gesamte Kommunikation über das Admin-Konto über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung beeinträchtigen).
	Sichere Benutzerverbindung	Wählen Sie diese Option aus, wenn die gesamte Kommunikation über das Konto des angemeldeten Benutzers über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung beeinträchtigen).

Einstellungstyp	Feld	Beschreibung
eDirectory-DNs	*Stammcontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen des Stammcontainers an. Diese Angabe wird als Standard-Suchstamm der Entitätsdefinition verwendet, sofern in der Verzeichnisabstraktionsschicht kein Suchstamm angegeben wurde.
	Bereitstellungstreiber-DN	Erforderlich. Geben Sie den eindeutigen Namen des Benutzeranwendungstreibers an, den Sie zuvor in Abschnitt 5.3, „Erstellen des Benutzeranwendungstreibers“, auf Seite 107 erstellt haben. Wenn Ihr Treiber beispielsweise „myDriverSet“ und der Treibersatz „myDriverSet“ ist und sich der Treibersatz in einem Kontext „o=myDriverSet“ befindet, geben Sie folgenden Wert ein: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Benutzeranwendung - Administrator	Erforderlich. Ein vorhandener Benutzer im Identitätsdepot mit den Rechten zum Ausführen von administrativen Tätigkeiten für den in der Benutzeranwendung angegebenen Benutzercontainer. Dieser Benutzer hat die Möglichkeit, über die Registerkarte *Administration* der Benutzeranwendung das Portal zu verwalten. Wenn der Benutzeranwendungsadministrator in iManager, Novell Designer für Identity Manager oder der Benutzeranwendung (Registerkarte *Anforderungen und Genehmigungen*) freigelegte Aufgaben zur Workflow-Administration bearbeitet, müssen Sie dem entsprechenden Administrator ausreichende Trustee-Rechte auf Objektinstanzen gewähren, die im Benutzeranwendungstreiber enthalten sind. Weitere Informationen finden Sie im *Administrationshandbuch zur IDM-Benutzeranwendung*. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden.
	Bereitstellungsanwendung - Administrator	Diese Funktion ist in der Bereitstellungsversion von Identity Manager 3.5.1 verfügbar. Der Administrator für die Bereitstellungsanwendung kann die Funktionen des Bereitstellungs-Workflows über die Registerkarte *Bereitstellung* (in der Registerkarte *Administration*) verwalten. Auf diese Funktionen können die Benutzer über die Registerkarte *Anforderungen und Genehmigungen* der Benutzeranwendung zugreifen. Dieser Benutzer muss im Identitätsdepot vorhanden sein, bevor ihm die Rolle des Administrators für die Bereitstellungsanwendung zugewiesen werden kann. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden.

Einstellungstyp	Feld	Beschreibung
eDirectory-DNs (Fortsetzung)	*Benutzercontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Benutzercontainers an. Diese Angabe definiert den Suchbereich für Benutzer und Gruppen. Benutzer in diesem Container (und unterhalb) dürfen sich bei der Benutzeranwendung anmelden. **Wichtig:** Stellen Sie sicher, dass der bei der Installation des Benutzeranwendungstreibers angegebene Benutzeranwendungsadministrator in diesem Container vorhanden ist, wenn dieser Benutzer Workflows ausführen soll.
	Gruppencontainer-DN	Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Gruppencontainers an. Wird von Entitätsdefinitionen innerhalb der Verzeichnisabstraktionsschicht verwendet.
eDirectory-Zertifikate	*Keystore-Pfad*	Erforderlich. Geben Sie den vollständigen Pfad zur Keystore-Datei (`cacerts`) des JDK an, die der Anwendungsserver für die Ausführung verwendet, oder klicken Sie auf die kleine Browser-Schaltfläche und navigieren Sie zur `cacerts`-Datei. Unter Linux oder Solaris benötigt der Benutzer eine entsprechende Berechtigung zum Schreiben in diese Datei.
	Keystore-Passwort/Keystore-Passwort bestätigen	Erforderlich. Geben Sie das `cacerts`-Passwort an. Die Vorgabe ist `changeit`.

Einstellungstyp	Feld	Beschreibung
Email	*Benachrichtigungsschablonen-Host-Token*	Geben Sie den Anwendungsserver an, der die Identity Manager-Benutzeranwendung hostet. Beispiel: `myapplication serverServer` Dieser Wert ersetzt das $HOST$-Token in Email-Schablonen. Die erstellte URL ist eine Verknüpfung zu Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen.
	Benachrichtigungsschablonen-Port-Token	Ersetzt das $PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungsaufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Token für den sicheren Port der Benachrichtigungsschablone	Ersetzt das $SECURE_PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Benachrichtigungs-SMTP-Email-Von:	Geben Sie an, dass die Email vom Benutzer in der Bereitstellungs-Email stammt.
	Benachrichtigungs-SMTP-Email-Host:	Geben Sie den SMTP-Email-Host für die Bereitstellungs-Email an. Dies kann eine IP-Adresse oder ein DNS-Name sein.
Passwort-verwaltung	*Externe WAR-Datei für Passwort verwenden*	Mithilfe dieser Funktion können Sie eine Seite „Passwort vergessen“ in einer externen WAR-Datei „Passwort vergessen“ sowie eine URL angeben, die die externe WAR-Datei „Passwort vergessen“ für den Rückruf der Benutzeranwendung über einen Webservice verwendet. Wenn *Externe WAR-Datei für Passwort verwenden* aktiviert ist, müssen auch Werte für *'Passwort vergessen'-Link* und *Link zurück zu 'Passwort vergessen'* angegeben werden. Wenn *Externe WAR-Datei für Passwort verwenden* nicht aktiviert ist, verwendet IDM die interne Standardfunktion zur Passwortverwaltung. `/jsps/pwdmgt/ForgotPassword.jsf` (ohne http(s) am Anfang) zu verwenden. Hierdurch wird der Benutzer nicht zu einer externen WAR-Datei, sondern zur in der Benutzeranwendung integrierten Funktionalität „Passwort vergessen“ umgeleitet.

Einstellungstyp	Feld	Beschreibung
	'Passwort vergessen'-Link	Diese URL verweist auf die Funktionsseite „Passwort vergessen“. Erstellen Sie in einer externen oder in einer internen WAR-Datei für die Passwortverwaltung eine Datei namens `ForgotPassword.jsf`. Weitere Informationen finden Sie in „Verwendung von Passwort-WAR-Dateien“ auf Seite 145.
	Link zurück zu 'Passwort vergessen'	Bei Verwendung einer externen WAR-Datei für die Passwortverwaltung müssen Sie den Pfad angeben, den diese WAR-Datei für den Rückruf der Benutzeranwendung über die Web-Services verwendet. Beispiel: `https://idmhost:sslport/idm`.

2 Klicken Sie zum Festlegen zusätzlicher Konfigurationsparameter für die Benutzeranwendung auf *Erweiterte Optionen anzeigen*. (Blättern Sie durch die Optionen, um das gesamte Teilfenster anzuzeigen.) In Tabelle 5-5 werden die Parameter der erweiterten Optionen erläutert.

Wenn Sie in diesem Schritt keine der beschriebenen zusätzlichen Parameter festlegen möchten, fahren Sie mit Schritt 3 fort.

Tabelle 5-5 *Konfiguration der Benutzeranwendung: Alle Parameter*

Einstellungstyp	Feld	Beschreibung
eDirectory-Verbindungs-einstellungen	*LDAP-Host*	Erforderlich. Geben Sie den Hostnamen oder die IP-Adresse des LDAP-Servers an. Beispiel: myLDAPhost
	Nicht sicherer LDAP-Port	Geben Sie den nicht sicheren Port des LDAP-Servers an. Beispiel: 389.
	Sicherer LDAP-Port	Geben Sie den sicheren Port des LDAP-Servers an. Beispiel: 636.
	LDAP-Administrator	Erforderlich. Geben Sie die Berechtigungsnachweise für den LDAP-Administrator an. Dieser Benutzer muss bereits vorhanden sein. Die Benutzeranwendung verwendet dieses Konto für eine administrative Verbindung zum Identitätsdepot. Dieser Wert ist mit dem Master-Schlüssel verschlüsselt.
	LDAP-Administratorpasswort	Erforderlich. Geben Sie das LDAP-Administratorpasswort an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
	Öffentliches anonymes Konto verwenden	Ermöglicht nicht angemeldeten Benutzern den Zugriff auf das öffentliche anonyme LDAP-Konto.
	LDAP-Gast	Ermöglicht nicht angemeldeten Benutzern den Zugriff auf zulässige Portlets. Dieses Benutzerkonto muss bereits im Identitätsdepot vorhanden sein. Deaktivieren Sie das Kontrollkästchen *Öffentliches anonymes Konto verwenden*, um „LDAP-Gast“ zu aktivieren. Aktivieren Sie das Kontrollkästchen *Öffentliches anonymes Konto verwenden*, um „LDAP-Gast“ zu deaktivieren.
	LDAP-Gastpasswort	Geben Sie das LDAP-Gastpasswort an.
	Sichere Admin-Verbindung	Wählen Sie diese Option aus, wenn die gesamte Kommunikation über das Admin-Konto über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung beeinträchtigen).
	Sichere Benutzerverbindung	Wählen Sie diese Option aus, wenn die gesamte Kommunikation über das Konto des angemeldeten Benutzers über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung stark beeinträchtigen).

Einstellungstyp	Feld	Beschreibung
eDirectory-DNs	*Stammcontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen des Stammcontainers an. Diese Angabe wird als Standard-Suchstamm der Entitätsdefinition verwendet, sofern in der Verzeichnisabstraktionsschicht kein Suchstamm angegeben wurde.
	Bereitstellungstreiber-DN	Erforderlich. Geben Sie den eindeutigen Namen des Benutzeranwendungstreibers an, den Sie zuvor in Abschnitt 5.3, „Erstellen des Benutzeranwendungstreibers“, auf Seite 107 erstellt haben. Wenn Ihr Treiber beispielsweise „UserApplicationDriver“ und der Treibersatz „myDriverSet“ ist und sich der Treibersatz in einem Kontext „o=myCompany“ befindet, geben Sie folgenden Wert ein: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Benutzeranwendung - Administrator	Erforderlich. Ein vorhandener Benutzer im Identitätsdepot mit den Rechten zum Ausführen von administrativen Tätigkeiten für den in der Benutzeranwendung angegebenen Benutzercontainer. Dieser Benutzer hat die Möglichkeit, über die Registerkarte *Administration* der Benutzeranwendung das Portal zu verwalten. Wenn der Benutzeranwendungsadministrator in iManager, Novell Designer für Identity Manager oder der Benutzeranwendung (Registerkarte *Anforderungen und Genehmigungen*) freigelegte Aufgaben zur Workflow-Administration bearbeitet, müssen Sie dem entsprechenden Administrator ausreichende Trustee-Rechte auf Objektinstanzen gewähren, die im Benutzeranwendungstreiber enthalten sind. Weitere Informationen finden Sie im *Administrationshandbuch zur IDM-Benutzeranwendung*. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden.
	Bereitstellungs-anwendung - Administrator	Diese Funktion ist in der Bereitstellungsversion von Identity Manager 3.5.1 verfügbar. Der Administrator der Bereitstellungsanwendung verwaltet die Funktionen des Bereitstellungs-Workflows, die über die Registerkarte *Anforderungen und Genehmigungen* der Benutzeranwendung verfügbar sind. Dieser Benutzer muss im Identitätsdepot vorhanden sein, bevor ihm die Rolle des Administrators für die Bereitstellungsanwendung zugewiesen werden kann. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden.

Einstellungstyp	Feld	Beschreibung
Benutzeridentität für Metaverzeichnis	*Benutzercontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Benutzercontainers an. Diese Angabe definiert den Suchbereich für Benutzer und Gruppen. Benutzer in diesem Container (und unterhalb) dürfen sich bei der Benutzeranwendung anmelden. **Wichtig:** Stellen Sie sicher, dass der bei der Installation des Benutzeranwendungstreibers angegebene Benutzeranwendungsadministrator in diesem Container vorhanden ist, wenn dieser Benutzer Workflows ausführen soll.
	Benutzerobjektklasse	Die LDAP-Benutzerobjektklasse (in der Regel inetOrgPerson).
	Anmeldeattribut	Das LDAP-Attribut (z. B. CN), das den Anmeldenamen des Benutzers repräsentiert.
	Benennungsattribut	Das als ID verwendete LDAP-Attribut beim Nachschlagen von Benutzern oder Gruppen. Dieses Attribut ist nicht identisch mit dem Anmeldeattribut, das nur für die Anmeldung, nicht aber bei der Suche nach Benutzern oder Gruppen verwendet wird.
	Benutzermitglied-schaftsattribut	Optional. Das LDAP-Attribut, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.
Benutzergruppen für Metaverzeichnis	*Gruppencontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Gruppencontainers an. Wird von Entitätsdefinitionen innerhalb der Verzeichnisabstraktionsschicht verwendet.
	Gruppenobjektklasse	Die Objektklasse für die LDAP-Gruppen (in der Regel groupofNames).
	Gruppenmitglied-schaftsattribut	Das Attribut, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.
	Dynamische Gruppen verwenden	Wählen Sie diese Option, wenn Sie dynamische Gruppen verwenden möchten.
	Klasse für dynamisches Gruppenobjekt	Die Objektklasse für die dynamische Gruppe (in der Regel dynamicGroup).

Einstellungstyp	Feld	Beschreibung
eDirectory-Zertifikate	*Keystore-Pfad*	Erforderlich. Geben Sie den vollständigen Pfad zur Keystore-Datei (`cacerts`) der JRE an, die der Anwendungsserver für die Ausführung verwendet, oder klicken Sie auf die kleine Browser-Schaltfläche und navigieren Sie zur `cacerts`-Datei. Während der Installation der Benutzeranwendung wird die Keystore-Datei geändert. Unter Linux oder Solaris benötigt der Benutzer eine entsprechende Berechtigung zum Schreiben in diese Datei.
	Keystore-Passwort *Keystore-Passwort bestätigen*	Erforderlich. Geben Sie das `cacerts`-Passwort an. Die Vorgabe ist `changeit`.
Speicher für privaten Schlüssel	*Pfad für privaten Keystore*	Der private Keystore enthält den privaten Schlüssel und die Zertifikate der Benutzeranwendung. Reserviert. Wenn Sie keine Eingabe vornehmen, lautet der Standardpfad `/jre/lib/security/cacerts`.
	Passwort für privaten Keystore	Das Passwort lautet `changeit`, sofern Sie kein anderes Passwort festgelegt haben. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
	Alias für privaten Schlüssel	Dieser Alias lautet `novellIDMUserApp`, sofern Sie keinen anderen Namen festgelegt haben.
	Passwort für privaten Schlüssel	Das Passwort lautet `novellIDM`, sofern Sie kein anderes Passwort festgelegt haben. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
Speicher für Herkunftsverbürgungs-schlüssel	*Pfad für Herkunftsverbürgungs-speicher*	Der Speicher für Herkunftsverbürgungsschlüssel enthält alle verbürgten Zertifikate der Signierer, die zum Validieren digitaler Signaturen verwendet werden. Wurde kein Pfad angegeben, ruft die Benutzeranwendung den Pfad von der Systemeigenschaft `javax.net.ssl.trustStore` ab. Wurde kein Pfad angegeben, wird `jre/lib/security/cacerts` verwendet.
	Passwort für Herkunftsverbürgungs-speicher	Wurde kein Passwort angegeben, ruft die Benutzeranwendung das Passwort von der Systemeigenschaft `javax.net.ssl.trustStorePassword` ab. Ist dort kein Wert angegeben, lautet das Passwort `changeit`. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.

Einstellungstyp	Feld	Beschreibung
Novell Audit-Digitalsignatur-Zertifikat und Schlüssel		Enthält das Novell Audit-Digitalsignatur-Zertifikat und den Schlüssel.
	Novell Audit-Digitalsignatur-Zertifikat	Zeigt das Digitalsignatur-Zertifikat an.
	Privater Schlüssel für Novell Audit-Digitalsignatur	Zeigt den privaten Schlüssel für die Digitalsignatur an. Dieser Schlüssel ist mit dem Master-Schlüssel verschlüsselt.
iChain-Einstellungen	*ICS-Abmeldung aktiviert*	Bei Auswahl dieser Option unterstützt die Benutzeranwendung die gleichzeitige Abmeldung von der Benutzeranwendung und iChain® bzw. Novell Access Manager. Bei der Abmeldung leitet die Benutzeranwendung den Benutzer bei Vorhandensein des iChain- oder Novell Access Manager-Cookies zur ICS-Abmeldungsseite um.
	ICS-Abmeldungsseite	Die URL zur iChain- oder Novell Access Manager-Abmeldungsseite, wobei die URL ein von iChain oder Novell Access Manager erwarteter Hostname ist. Wenn die ICS-Protokollierung aktiviert ist und sich ein Benutzer von der Benutzeranwendung abmeldet, wird der Benutzer auf diese Seite umgeleitet.

Einstellungstyp	Feld	Beschreibung
Email	*Benachrichtigungs-schablonen-Host-Token*	Geben Sie den Anwendungsserver an, der die Identity Manager-Benutzeranwendung hostet. Beispiel: `myapplication serverServer` Dieser Wert ersetzt das $HOST$-Token in Email-Schablonen. Die erstellte URL ist eine Verknüpfung zu Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen.
	Benachrichtigungs-schablonen-Port-Token	Ersetzt das $PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungsaufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Token für den sicheren Port der Benachrichtigungs-schablone	Ersetzt das $SECURE_PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Benachrichtigungs-schablonen-Protokoll-Token	Bezieht sich auf ein nicht sicheres Protokoll, HTTP. Ersetzt das $PROTOCOL$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Token für das sichere Protokoll der Benachrichtigungs-schablone	Bezieht sich auf ein sicheres Protokoll, HTTPS. Ersetzt das $SECURE_PROTOCOL$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Benachrichtigungs-SMTP-Email-Von:	Geben Sie Emails an, die von einem Benutzer in der Bereitstellungs-Email stammen.
	Benachrichtigungs-SMTP-Email-Host:	Geben Sie den SMTP-Email-Host für die Bereitstellungs-Email an. Dies kann eine IP-Adresse oder ein DNS-Name sein.

Einstellungstyp	Feld	Beschreibung
Passwortverwaltung		
	Externe WAR-Datei für Passwort verwenden	Mithilfe dieser Funktion können Sie eine Seite „Passwort vergessen“ in einer externen WAR-Datei „Passwort vergessen“ sowie eine URL angeben, die die externe WAR-Datei „Passwort vergessen“ für den Rückruf der Benutzeranwendung über einen Webservice verwendet. Wenn *Externe WAR-Datei für Passwort verwenden* aktiviert ist, müssen auch Werte für *'Passwort vergessen'-Link* und *Link zurück zu 'Passwort vergessen'* angegeben werden. Wenn *Externe WAR-Datei für Passwort verwenden* nicht aktiviert ist, verwendet IDM die interne Standardfunktion zur Passwortverwaltung. `/jsps/pwdmgt/ForgotPassword.jsf` (ohne http(s) am Anfang) zu verwenden. Hierdurch wird der Benutzer nicht zu einer externen WAR-Datei, sondern zur in der Benutzeranwendung integrierten Funktionalität „Passwort vergessen“ umgeleitet.
	'Passwort vergessen'-Link	Diese URL verweist auf die Funktionsseite „Passwort vergessen“. Erstellen Sie in einer externen oder in einer internen WAR-Datei für die Passwortverwaltung eine Datei namens `ForgotPassword.jsf`. Weitere Informationen finden Sie in „Verwendung von Passwort-WAR-Dateien“ auf Seite 145.
	Link zurück zu 'Passwort vergessen'	Bei Verwendung einer externen WAR-Datei für die Passwortverwaltung müssen Sie den Pfad angeben, den diese WAR-Datei für den Rückruf der Benutzeranwendung über die Web-Services verwendet. Beispiel: `https://idmhost:sslport/idm`.
Sonstige	*Sitzungszeit-überschreitung*	Die Sitzungszeitüberschreitung der Anwendung.
	OCSP-URI	Wenn für die Client-Installation das OSCP (On-Line Certificate Status Protocol) verwendet wird, stellen Sie eine URI (Uniform Resource Identifier) bereit. Beispiel für das Format: http://host:port/ocspLocal. Die OCSP-URI aktualisiert den Status der verbürgten Zertifikate online.
	Konfigurationspfad für Autorisierung	Vollständig qualifizierter Name der Konfigurationsdatei für die Autorisierung.

Einstellungstyp	Feld	Beschreibung
Containerobjekt	*Ausgewählt*	Wählen Sie alle zu verwendenden Containerobjekttypen aus.
	Containerobjekttyp	Wählen Sie die Typen aus den folgenden Standard-Containern aus: Standort-, Länder-, Organisationseinheits-, Organisations- und Domänenobjekte. Sie können in iManager auch eigene Container erstellen und mithilfe der Option *Neues Containerobjekt hinzufügen* hinzufügen.
	Containerattributname	Listet den mit dem Containerobjekttyp verknüpften Attributnamen auf.
	Neues Containerobjekt hinzufügen: Containerobjekttyp	Geben Sie den LDAP-Namen einer Objektklasse aus dem Identitätsdepot an, die als Container dienen kann. Weitere Informationen zu Containern finden Sie im *Administrationshandbuch zu Novell iManager 2.6 (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*.
	Neues Containerobjekt hinzufügen: Containerattributname	Geben Sie den Attributnamen des Containerobjekts an.

Hinweis: Die meisten Einstellungen in dieser Datei können nach der Installation bearbeitet werden. Führen Sie hierzu das `configupdate.sh`-Skript oder die Windows-Datei `configupdate.bat` aus, die sich im Installations-Unterverzeichnis befinden. Denken Sie daran, dass die Einstellungen in dieser Datei in einem Cluster für alle Cluster-Mitglieder identisch sein müssen.

3 Klicken Sie nach der Konfiguration dieser Einstellungen auf *OK* und fahren Sie anschließend mit Abschnitt 5.5.15, „Prüfen der Auswahl und Installation“, auf Seite 146 fort. .

Verwendung von Passwort-WAR-Dateien

Geben Sie für den Konfigurationsparameter *'Passwort vergessen'-Link* den Standort einer WAR-Datei mit der Funktionalität „Passwort vergessen“ an. Hierbei kann es sich um eine externe oder interne WAR-Datei handeln.

Angabe einer externen WAR-Datei für die Passwortverwaltung

1 Sie können die externe WAR-Datei während des Installationsvorgangs oder über das „configupdate“-Dienstprogramm angeben.

2 Aktivieren Sie in den Konfigurationsparametern der Benutzeranwendung das Kontrollkästchen *Externe WAR-Datei für Passwort verwenden*.

3 Geben Sie für den Konfigurationsparameter *'Passwort vergessen'-Link* den Speicherort der externen Passwort-WAR-Datei an.

Nehmen Sie den Host und den Port auf, z. B. `http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`. Eine externe Passwort-WAR kann sich außerhalb der schützenden Firewall der Benutzeranwendung befinden.

4 Geben Sie für *Link zurück zu 'Passwort vergessen'* den Pfad ein, den die externe WAR-Datei für die Passwortverwaltung für den Rückruf der Benutzeranwendung über die Web Services verwendet, z. B. `https://idmhost:sslport/idm`.

Der Link zurück zu 'Passwort vergessen' muss SSL verwenden, sodass eine sichere Web-Service-Kommunikation mit der Benutzeranwendung gewährleistet ist. Siehe auch Abschnitt 5.9.3, „Konfiguration der SSL-Kommunikation zwischen JBoss-Servern“, auf Seite 187.

5 Wenn Sie das Installationsprogramm verwenden, lesen Sie die Informationen in diesem Schritt und fahren Sie dann mit Schritt 6 fort.

Bei Verwendung des configupdate-Dienstprogramms zur Aktualisierung der externen Passwort-WAR im Stammverzeichnis der Installation: Lesen Sie die Informationen in diesem Schritt und benennen Sie die WAR-Datei manuell in das erste Verzeichnis um, das unter *'Passwort vergessen'-Link* angegeben ist. Fahren Sie dann mit Schritt 6 fort.

Vor dem Abschluss der Installation benennt das Installationsprogramm `IDMPwdMgt.war` (Teil der Installationsroutine) in den Namen des ersten angegebenen Verzeichnisses um. Die umbenannte Datei `IDMPwdMgt.war` wird zu Ihrer externen Passwort-WAR. Beispiel: Wenn Sie `http://www.idmpwdmgthost.com/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf` angeben, benennt das Installationsprogramm `IDMPwdMgt.war` in `ExternalPwd.war` um. Anschließend verschiebt das Installationsprogramm die umbenannte WAR in das Stammverzeichnis der Installation.

6 Kopieren Sie `ExternalPwd.war` in den Bereitstellungsordner des Remote-JBoss-Servers, auf dem die Funktionalität der externen Passwort-WAR ausgeführt wird.

Angabe einer internen WAR-Datei für die Passwortverwaltung

1 Lassen Sie die Option *Externe WAR-Datei für Passwort verwenden* deaktiviert.

2 Übernehmen Sie den vorgegebenen Speicherort unter *'Passwort vergessen'-Link* oder geben Sie eine URL zu einer anderen Passwort-WAR an.

3 Bestätigen Sie den vorgegebenen Wert für *Link zurück zu 'Passwort vergessen'*.

5.5.15 Prüfen der Auswahl und Installation

1 Überprüfen Sie auf der Seite „Zusammenfassung vor der Installation“ die Einstellungen der Installationsparameter.

2 Wenn Sie Änderungen vornehmen möchten, können Sie über die Schaltfläche *Zurück* vorherige Installationsseiten aufrufen.

Die Werte auf der Seite „Benutzeranwendung - Konfiguration“ werden nicht gespeichert, daher müssen Sie die Einstellungen auf dieser Seite erneut vornehmen, wenn Sie vorherige Seiten des Installationsvorgangs ändern.

3 Wenn Sie die gewünschten Änderungen an den Installations- und Konfigurationsparametern vorgenommen haben, kehren Sie zur Seite „Zusammenfassung vor der Installation“ zurück und klicken Sie auf *Installieren*.

5.5.16 Anzeigen der Protokolldateien

1. Wenn die Installation ohne Fehler abgeschlossen wurde, fahren Sie mit Abschnitt 5.9, „Aufgaben nach der Installation“, auf Seite 185 fort.
2. Sofern bei der Installation Fehler- oder Warnmeldungen ausgegeben wurden, ermitteln Sie die Probleme anhand der Protokolldateien:
   - Die Datei `Identity_Manager_User_Application_InstallLog.log` enthält die Ergebnisse der wichtigsten Installationsaufgaben.
   - Die Datei `Novell-Custom-Install.log` enthält Informationen zur Konfiguration der Benutzeranwendung, die während der Installation vorgenommen wurde.

   Informationen zur Behebung von Problemen finden Sie in Abschnitt 5.11, „Fehlersuche“, auf Seite 191.

5.6 Installation der Benutzeranwendung auf einem WebSphere-Anwendungsserver

In diesem Abschnitt wird die Installation der IDM-Benutzeranwendung auf einem WebSphere-Anwendungsserver über die grafische Benutzeroberfläche des Installationsprogramms erläutert.

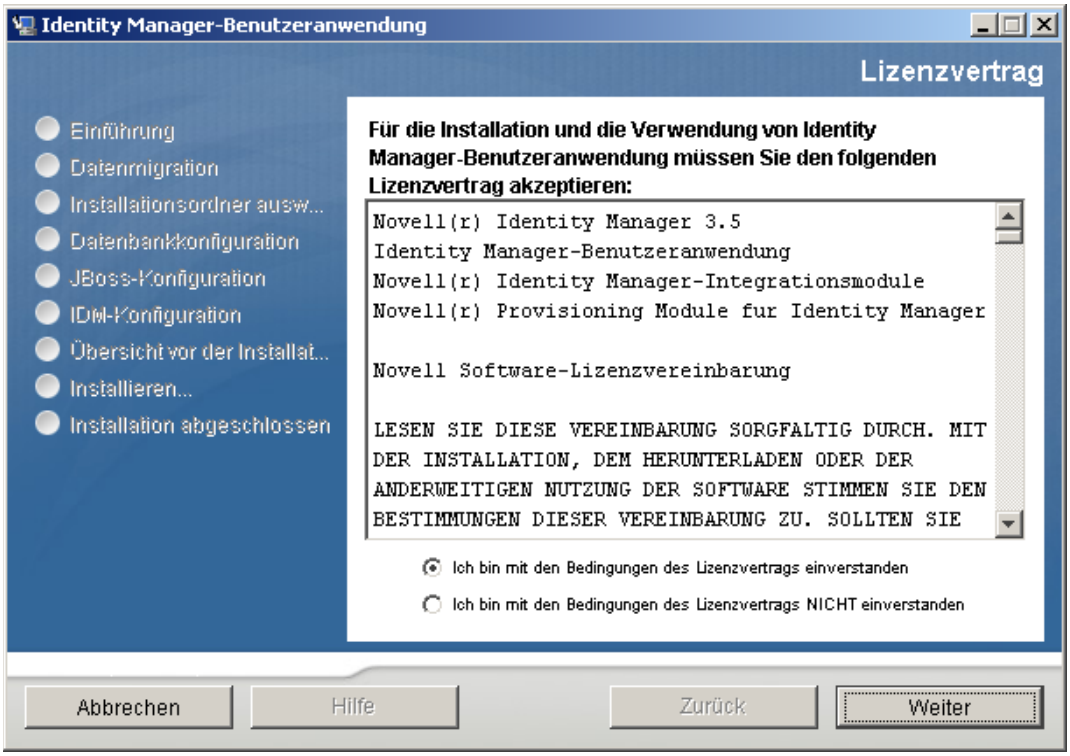
5.6.1 Starten der GUI des Installationsprogramms

1. Rufen Sie das Verzeichnis mit den Installationsdateien auf.
2. Starten Sie das Installationsprogramm:

   ```
   java -jar IdmUserApp.jar
   ```

3 Wählen Sie im Dropdown-Menü eine Sprache aus und klicken Sie anschließend auf OK.

4 Lesen Sie die Lizenzvereinbarung, klicken Sie zur Bestätigung auf die entsprechende Schaltfläche und klicken Sie anschließend auf *Weiter*.



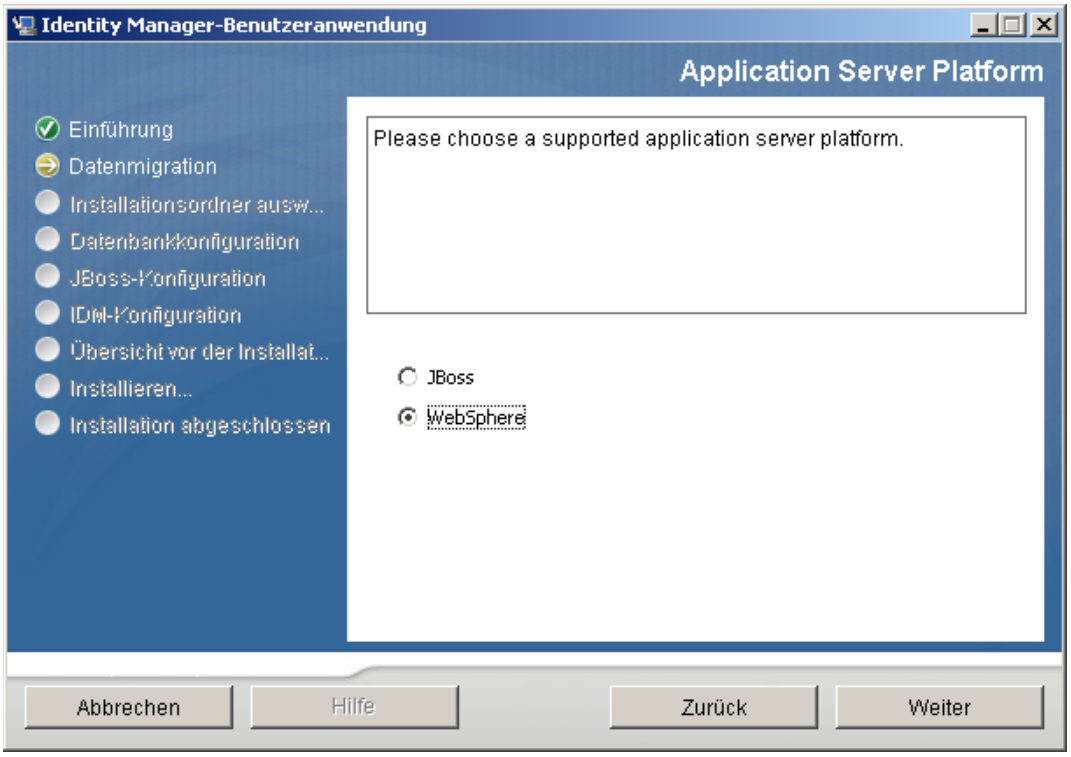
5 Lesen Sie die Einführungsseite des Installationsassistenten und klicken Sie anschließend auf *Weiter*.

6 Fahren Sie mit Abschnitt 5.6.2, „Auswahl einer Anwendungsserver-Plattform“, auf Seite 149 fort.

5.6.2 Auswahl einer Anwendungsserver-Plattform

1 Wählen Sie im Fenster zur Auswahl einer Anwendungsserver-Plattform die WebSphere-Anwendungsserver-Plattform aus.

2 Wählen Sie *Weiter*. Fahren Sie dann mit Abschnitt 5.6.3, „Angabe des Speicherorts der WAR-Datei“, auf Seite 149 fort.



5.6.3 Angabe des Speicherorts der WAR-Datei

Wenn sich die WAR-Datei der Identity Manager-Benutzeranwendung nicht im selben Verzeichnis befindet wie das Installationsprogramm, werden Sie aufgefordert, den Pfad zur WAR-Datei einzugeben.

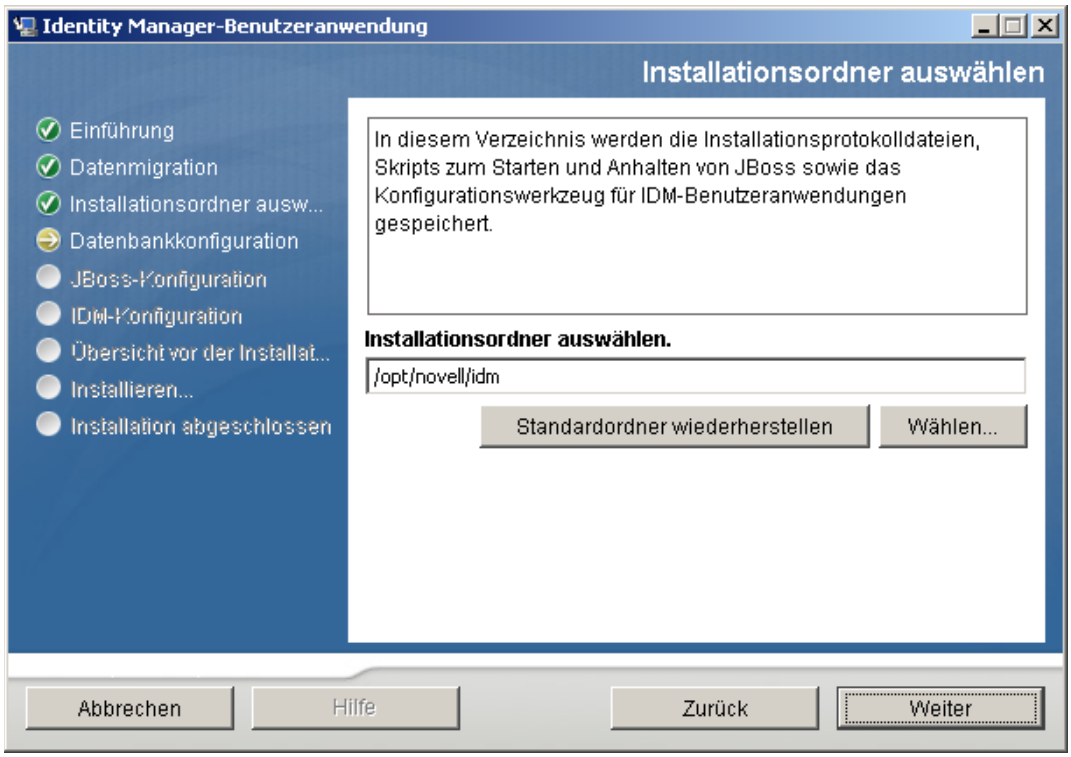
1 Wenn sich die WAR-Datei am Standardspeicherort befindet, können Sie auf *Standard wiederherstellen* klicken.

Sie können stattdessen auch auf die Schaltfläche zum *Auswählen* klicken und einen Speicherort auswählen, um den Speicherort der WAR-Datei anzugeben.

2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.6.4, „Auswahl eines Installationsordners“, auf Seite 151 fort.

5.6.4 Auswahl eines Installationsordners

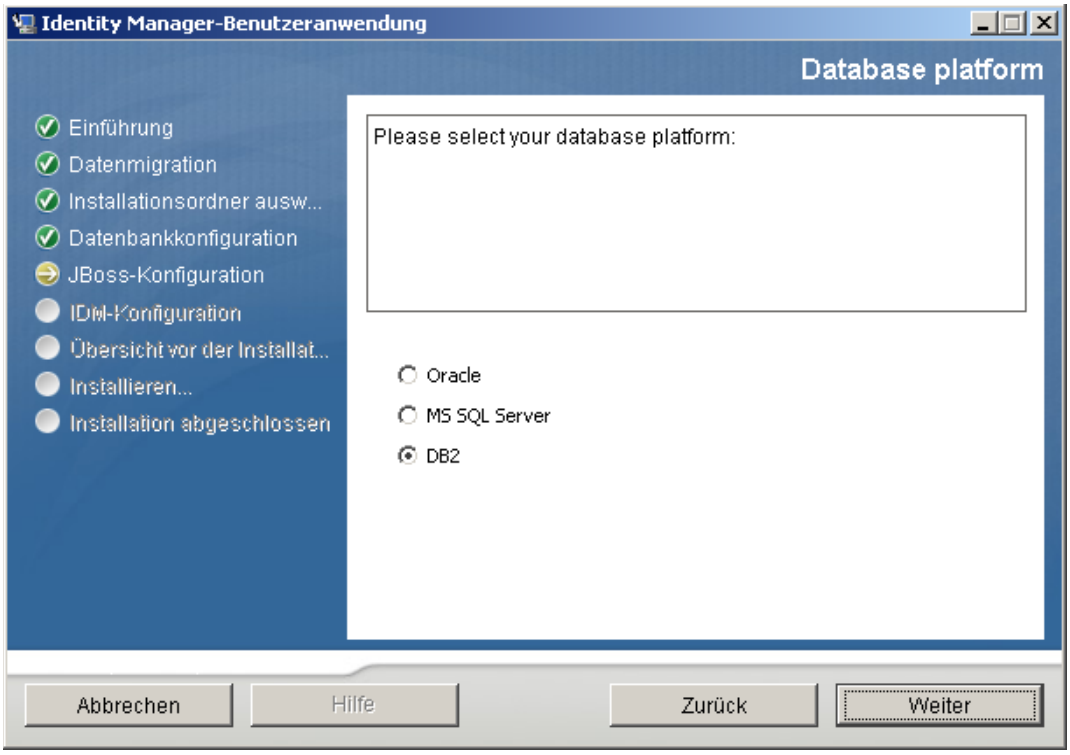
1 Geben Sie auf der Seite „Installationsordner auswählen“ die Stelle an, an der die Benutzeranwendung installiert werden soll. Wenn Sie den Standardspeicherort verwenden möchten, klicken Sie auf *Standard wiederherstellen*, oder klicken Sie auf die Schaltfläche zum *Auswählen*, um einen anderen Speicherort für die Installationsdateien auszuwählen.



2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.6.5, „Auswahl einer Datenbankplattform“, auf Seite 152 fort.

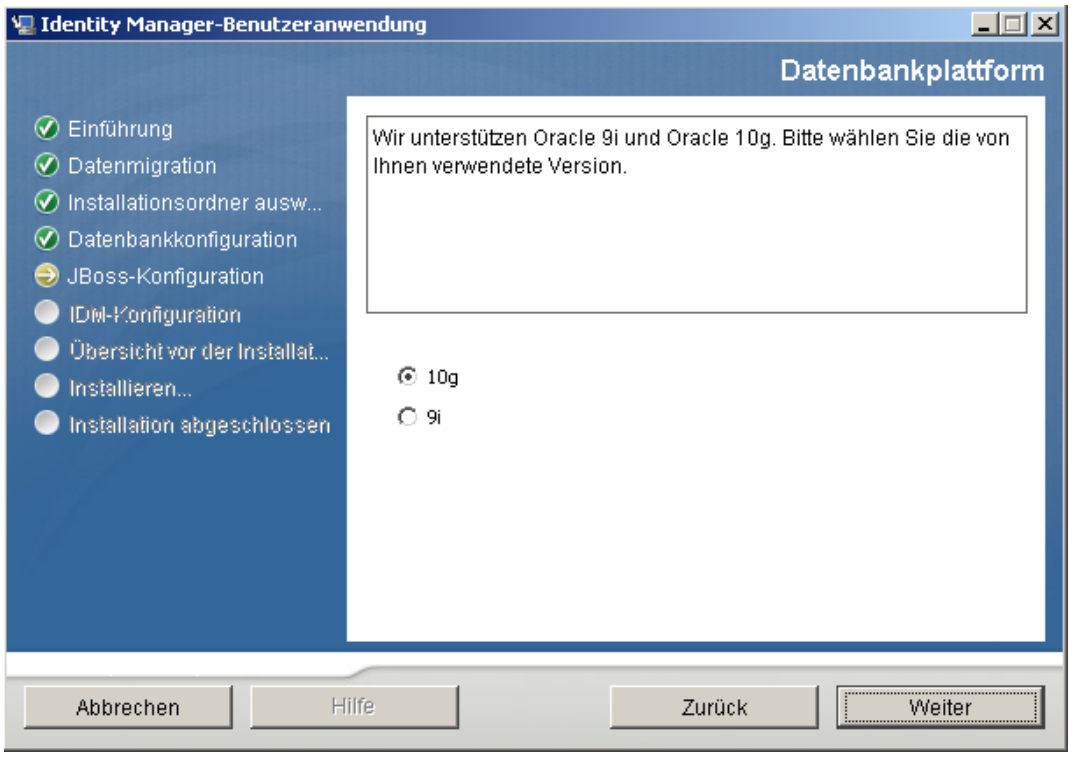
5.6.5 Auswahl einer Datenbankplattform

1 Wählen Sie die gewünschte Datenbank aus.



2 Wenn Sie eine Oracle-Datenbank verwenden, fahren Sie mit Schritt 3 fort. Fahren Sie anderenfalls mit Schritt 4 fort.

3 Bei Verwendung einer Oracle-Datenbank fragt Sie das Installationsprogramm nach deren Version. Wählen Sie die entsprechende Version aus.

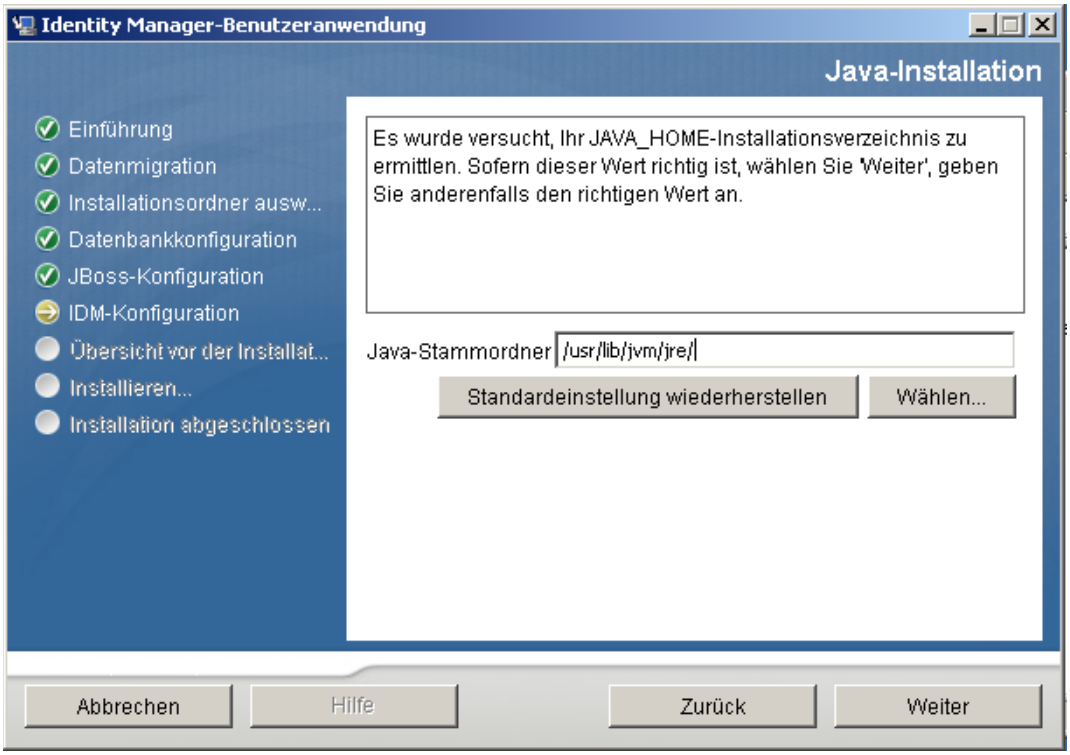


4 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.6.6, „Angabe des Java-Stammordners“, auf Seite 154 fort.

5.6.6 Angabe des Java-Stammordners

Hinweis: Mit WebSphere müssen Sie das IBM JDK mit den unbeschränkten Richtliniendateien verwenden.

1 Klicken Sie zum Wechseln in den Java-Stammordner auf die Schaltfläche zum *Auswählen*. Wenn Sie den Standardspeicherort verwenden möchten, klicken Sie auf *Standardeinstellung wiederherstellen*.

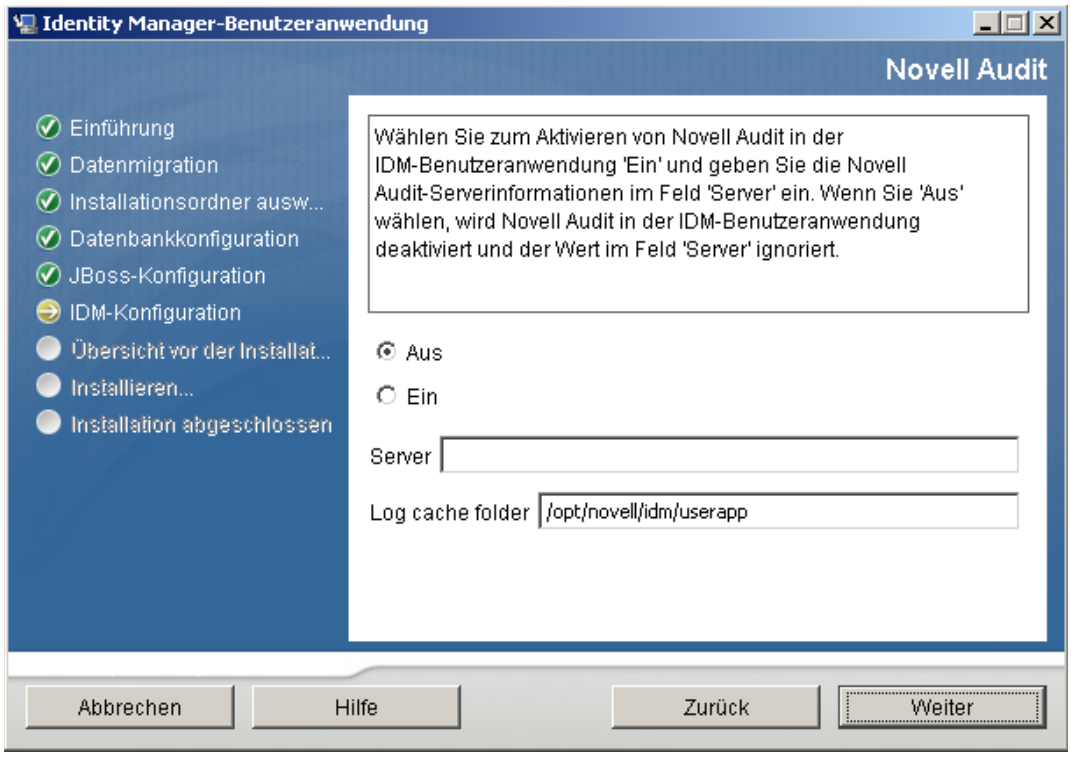


2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.6.7, „Aktivieren der Novell Audit-Protokollierung“, auf Seite 155 fort.

5.6.7 Aktivieren der Novell Audit-Protokollierung

So aktivieren Sie die Novell Audit-Protokollierung (optional) für die Benutzeranwendung:

1 Füllen Sie die folgenden Felder aus:



Option	Beschreibung
Aus	Deaktiviert die Novell Audit-Protokollierung für die Benutzeranwendung. Sie können sie zu einem späteren Zeitpunkt in der Benutzeranwendung über die Registerkarte *Administration* aktivieren. Weitere Informationen zur Aktivierung der Novell Audit-Protokollierung finden Sie im *Identity Manager-Benutzeranwendung: Administrationshandbuch*.
Ein	Aktiviert die Novell Audit-Protokollierung für die Benutzeranwendung. Weitere Informationen zum Einrichten der Novell Audit-Protokollierung finden Sie im *Identity Manager-Benutzeranwendung: Administrationshandbuch*.
Server	Wenn Sie die Novell Audit-Protokollierung aktivieren, geben Sie den Hostnamen oder die IP-Adresse des Novell Audit-Servers an. Wenn Sie die Protokollierung deaktivieren, wird dieser Wert ignoriert.
Ordner für Protokoll-Cache	Geben Sie das Verzeichnis für den Protokoll-Cache an.

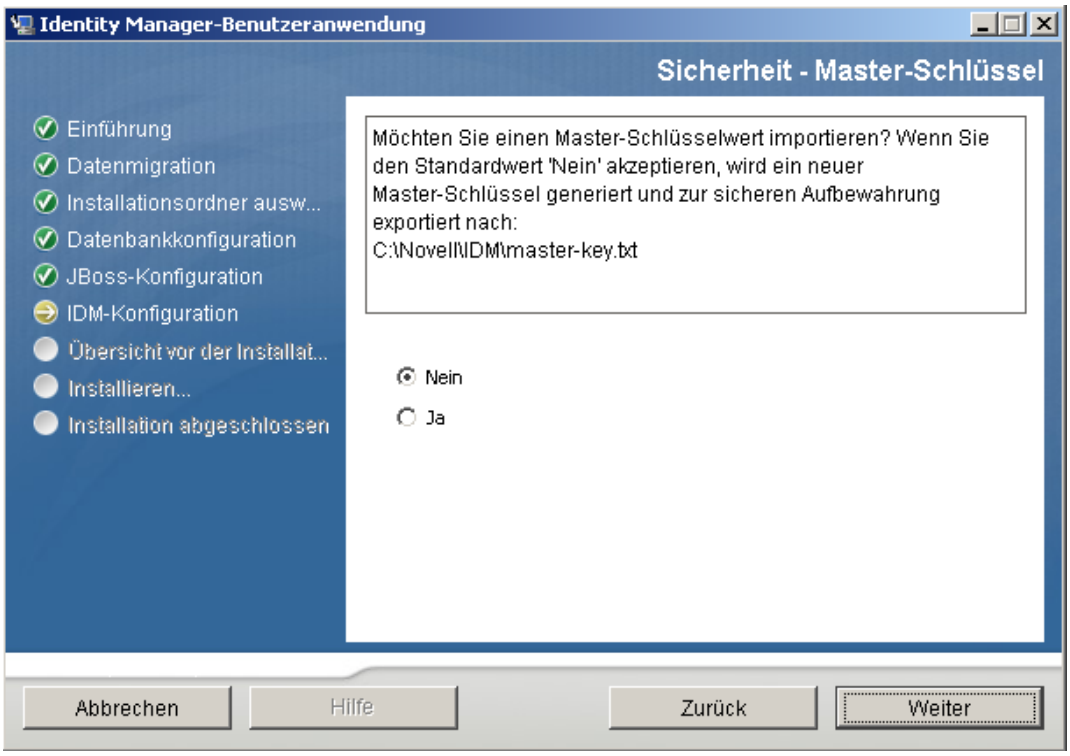
2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.6.8, „Angabe eines Master-Schlüssels“, auf Seite 156 fort.

5.6.8 Angabe eines Master-Schlüssels

Geben Sie an, ob Sie einen vorhandenen Master-Schlüssel importieren oder einen neuen erstellen möchten. Mögliche Gründe für den Import eines vorhandenen Master-Schlüssels:

- Sie verlagern Ihre Installation aus einem Staging-System in ein Produktionssystem und möchten auch weiterhin auf die Datenbank des Staging-Systems zugreifen.
- Sie haben die Benutzeranwendung als erstes Mitglied eines Clusters installiert und führen nun die Installation auf nachfolgenden Cluster-Mitgliedern durch (für die derselbe Master-Schlüssel benötigt wird).
- Bedingt durch einen Festplattenfehler müssen Sie die Benutzeranwendung wiederherstellen. Sie müssen die Benutzeranwendung neu installieren und den Master-Schlüssel der vorherigen Installation angeben. Auf diese Weise erhalten Sie Zugriff auf zuvor gespeicherte verschlüsselte Daten.

1 Klicken Sie auf *Ja*, um einen vorhandenen Master-Schlüssel zu importieren, oder auf *Nein*, um einen neuen Master-Schlüssel zu erstellen.



2 Klicken Sie auf *Weiter*.

Bei der Installation wird der verschlüsselte Master-Schlüssel im Installationsverzeichnis in die Datei `master-key.txt` geschrieben.

Wenn Sie *Nein* gewählt haben, fahren Sie mit Abschnitt 5.6.9, „Konfiguration der Benutzeranwendung“, auf Seite 157 fort. Nach Abschluss der Installation müssen Sie den Master-Schlüssel manuell speichern. Wenn Sie *Ja* gewählt haben, fahren Sie mit Schritt 3 fort.

3 Wenn ein vorhandener verschlüsselter Master-Schlüssel importiert werden soll, kopieren Sie den Schlüssel und fügen Sie ihn in das Fenster des Installationsvorgangs ein.

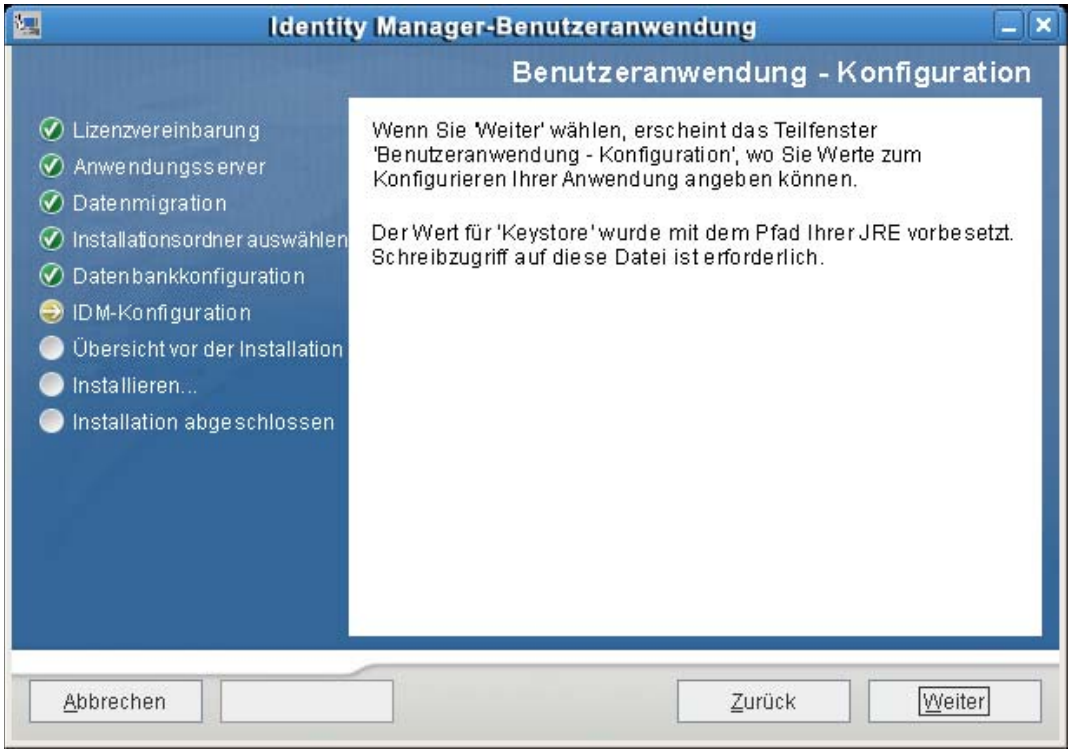
4 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 5.6.9, „Konfiguration der Benutzeranwendung“, auf Seite 157 fort.

5.6.9 Konfiguration der Benutzeranwendung

Bei der Installation der Benutzeranwendung können Sie Konfigurationsparameter für die Benutzeranwendung festlegen. Die meisten dieser Parameter können auch nach der Installation in der Datei `configupdate.sh` oder `configupdate.bat` bearbeitet werden. Auf Ausnahmen wird in den Parameterbeschreibungen hingewiesen. In einer Clusterkonfiguration müssen für alle

Cluster-Mitglieder dieselben Konfigurationsparameter für die Benutzeranwendung angegeben werden.

1 Klicken Sie auf der ersten Seite zur Konfiguration der Benutzeranwendung auf *Weiter*.



2 Geben Sie die wichtigsten Konfigurationsparameter für die Benutzeranwendung wie in Tabelle 5-6 auf Seite 160 beschrieben an und fahren Sie dann mit Schritt 3 fort.

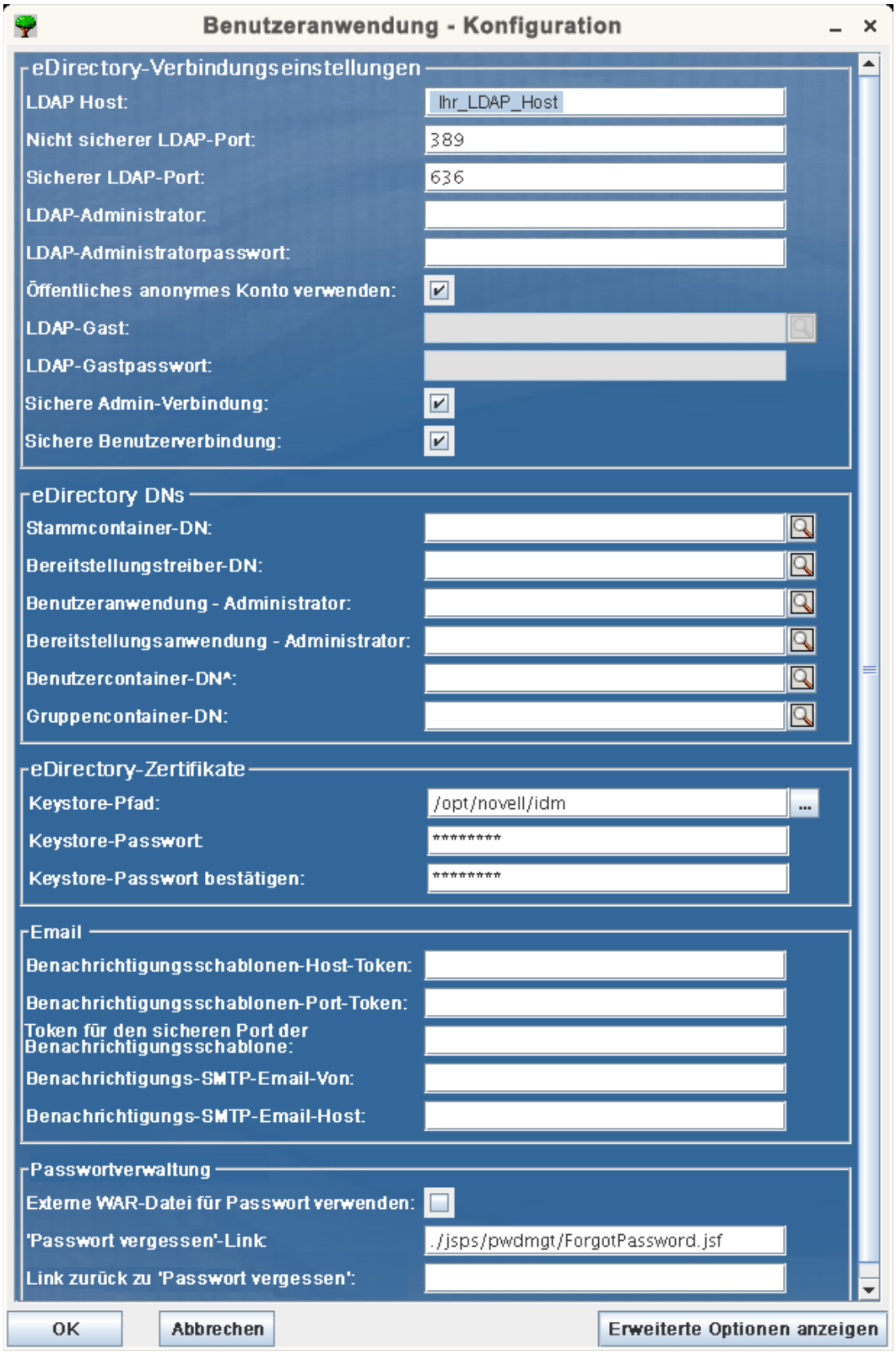


Tabelle 5-6 *Konfiguration der Benutzeranwendung: Wichtigste Parameter*

Einstellungstyp	Feld	Beschreibung
eDirectory-Verbindungs-einstellungen	*LDAP-Host*	Erforderlich. Geben Sie den Hostnamen oder die IP-Adresse sowie den sicheren Port des LDAP-Servers an. Beispiel: `myLDAPhost`
	Nicht sicherer LDAP-Port	Geben Sie den nicht sicheren Port des LDAP-Servers an. Beispiel: 389.
	Sicherer LDAP-Port	Geben Sie den sicheren Port des LDAP-Servers an. Beispiel: 636.
	LDAP-Administrator	Erforderlich. Geben Sie die Berechtigungsnachweise für den LDAP-Administrator an. Dieser Benutzer muss bereits vorhanden sein. Die Benutzeranwendung verwendet dieses Konto für eine administrative Verbindung zum Identitätsdepot. Dieser Wert ist mit dem Master-Schlüssel verschlüsselt.
	LDAP-Administratorpasswort	Erforderlich. Geben Sie das LDAP-Administratorpasswort an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
	Öffentliches anonymes Konto verwenden	Ermöglicht nicht angemeldeten Benutzern den Zugriff auf das öffentliche anonyme LDAP-Konto.
	LDAP-Gast	Ermöglicht nicht angemeldeten Benutzern den Zugriff auf zulässige Portlets. Dieses Benutzerkonto muss bereits im Identitätsdepot vorhanden sein. Deaktivieren Sie das Kontrollkästchen *Öffentliches anonymes Konto verwenden*, um „LDAP-Gast“ zu aktivieren. Aktivieren Sie das Kontrollkästchen *Öffentliches anonymes Konto verwenden*, um „LDAP-Gast“ zu deaktivieren.
	LDAP-Gastpasswort	Geben Sie das LDAP-Gastpasswort an.
	Sichere Admin-Verbindung	Wählen Sie diese Option aus, wenn die gesamte Kommunikation über das Admin-Konto über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung beeinträchtigen).
	Sichere Benutzerverbindung	Wählen Sie diese Option aus, wenn die gesamte Kommunikation über das Konto des angemeldeten Benutzers über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung beeinträchtigen).

Einstellungstyp	Feld	Beschreibung
eDirectory-DNs	*Stammcontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen des Stammcontainers an. Diese Angabe wird als Standard-Suchstamm der Entitätsdefinition verwendet, sofern in der Verzeichnisabstraktionsschicht kein Suchstamm angegeben wurde.
	Bereitstellungstreiber-DN	Erforderlich. Geben Sie den eindeutigen Namen für den Benutzeranwendungstreiber an. Wenn Ihr Treiber beispielsweise „myDriverSet“ und der Treibersatz „myDriverSet“ ist und sich der Treibersatz in einem Kontext „o=myDriverSet“ befindet, geben Sie folgenden Wert ein: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Benutzeranwendung - Administrator	Erforderlich. Ein vorhandener Benutzer im Identitätsdepot mit den Rechten zum Ausführen von administrativen Tätigkeiten für den in der Benutzeranwendung angegebenen Benutzercontainer. Dieser Benutzer hat die Möglichkeit, über die Registerkarte *Administration* der Benutzeranwendung das Portal zu verwalten. Wenn der Benutzeranwendungsadministrator in iManager, Novell Designer für Identity Manager oder der Benutzeranwendung (Registerkarte *Anforderungen und Genehmigungen*) freigelegte Aufgaben zur Workflow-Administration bearbeitet, müssen Sie dem entsprechenden Administrator ausreichende Trustee-Rechte auf Objektinstanzen gewähren, die im Benutzeranwendungstreiber enthalten sind. Weitere Informationen finden Sie im *Administrationshandbuch zur IDM-Benutzeranwendung*. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden.
	Bereitstellungsanwendung - Administrator	Diese Funktion ist in der Bereitstellungsversion von Identity Manager 3.5.1 verfügbar. Der Administrator für die Bereitstellungsanwendung kann die Funktionen des Bereitstellungs-Workflows über die Registerkarte *Bereitstellung* (in der Registerkarte *Administration*) verwalten. Auf diese Funktionen können die Benutzer über die Registerkarte *Anforderungen und Genehmigungen* der Benutzeranwendung zugreifen. Dieser Benutzer muss im Identitätsdepot vorhanden sein, bevor ihm die Rolle des Administrators für die Bereitstellungsanwendung zugewiesen werden kann. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden.

Einstellungstyp	Feld	Beschreibung
eDirectory-DNs (Fortsetzung)	*Benutzercontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Benutzercontainers an. Diese Angabe definiert den Suchbereich für Benutzer und Gruppen. Benutzer in diesem Container (und unterhalb) dürfen sich bei der Benutzeranwendung anmelden. **Wichtig:** Stellen Sie sicher, dass der bei der Installation des Benutzeranwendungstreibers angegebene Benutzeranwendungsadministrator in diesem Container vorhanden ist, wenn dieser Benutzer Workflows ausführen soll.
	Gruppencontainer-DN	Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Gruppencontainers an. Wird von Entitätsdefinitionen innerhalb der Verzeichnisabstraktionsschicht verwendet.
eDirectory-Zertifikate	*Keystore-Pfad*	Erforderlich. Geben Sie den vollständigen Pfad zur Keystore-Datei (`cacerts`) des JDK an, die der Anwendungsserver für die Ausführung verwendet, oder klicken Sie auf die kleine Browser-Schaltfläche und navigieren Sie zur `cacerts`-Datei. Unter Linux oder Solaris benötigt der Benutzer eine entsprechende Berechtigung zum Schreiben in diese Datei.
	Keystore-Passwort/Keystore-Passwort bestätigen	Erforderlich. Geben Sie das `cacerts`-Passwort an. Die Vorgabe ist `changeit`.

Einstellungstyp	Feld	Beschreibung
Email	*Benachrichtigungsschablonen -Host-Token*	Geben Sie den Anwendungsserver an, der die Identity Manager-Benutzeranwendung hostet. Beispiel: `myapplication serverServer` Dieser Wert ersetzt das $HOST$-Token in Email-Schablonen. Die erstellte URL ist eine Verknüpfung zu Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen.
	Benachrichtigungsschablonen -Port-Token	Ersetzt das $PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungsaufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Token für den sicheren Port der Benachrichtigungsschablone	Ersetzt das $SECURE_PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Benachrichtigungs-SMTP-Email-Von:	Geben Sie an, dass die Email vom Benutzer in der Bereitstellungs-Email stammt.
	Benachrichtigungs-SMTP-Email-Host:	Geben Sie den SMTP-Email-Host für die Bereitstellungs-Email an. Dies kann eine IP-Adresse oder ein DNS-Name sein.
Passwort-verwaltung	*Externe WAR-Datei für Passwort verwenden*	Mithilfe dieser Funktion können Sie eine Seite „Passwort vergessen“ in einer externen WAR-Datei „Passwort vergessen“ sowie eine URL angeben, die die externe WAR-Datei „Passwort vergessen“ für den Rückruf der Benutzeranwendung über einen Webservice verwendet. Wenn *Externe WAR-Datei für Passwort verwenden* aktiviert ist, müssen auch Werte für *'Passwort vergessen'-Link* und *Link zurück zu 'Passwort vergessen'* angegeben werden. Wenn *Externe WAR-Datei für Passwort verwenden* nicht aktiviert ist, verwendet IDM die interne Standardfunktion zur Passwortverwaltung. `/jsps/pwdmgt/ForgotPassword.jsf` (ohne http(s) am Anfang) zu verwenden. Hierdurch wird der Benutzer nicht zu einer externen WAR-Datei, sondern zur in der Benutzeranwendung integrierten Funktionalität „Passwort vergessen“ umgeleitet.

Einstellungstyp	Feld	Beschreibung
	'Passwort vergessen'-Link	Diese URL verweist auf die Funktionsseite „Passwort vergessen“. Erstellen Sie in einer externen oder in einer internen WAR-Datei für die Passwortverwaltung eine Datei namens `ForgotPassword.jsf`.
	Link zurück zu 'Passwort vergessen'	Bei Verwendung einer externen WAR-Datei für die Passwortverwaltung müssen Sie den Pfad angeben, den diese WAR-Datei für den Rückruf der Benutzeranwendung über die Web-Services verwendet. Beispiel: `https://idmhost:sslport/idm`.

3 Klicken Sie zum Festlegen zusätzlicher Konfigurationsparameter für die Benutzeranwendung auf *Erweiterte Optionen anzeigen*. (Blättern Sie durch die Optionen, um das gesamte Teilfenster anzuzeigen.) In Tabelle Tabelle 5-7 auf Seite 165 werden die Parameter der erweiterten Optionen erläutert. Wenn Sie in diesem Schritt keine der beschriebenen zusätzlichen Parameter festlegen möchten, fahren Sie mit Schritt 4 fort.

Tabelle 5-7 *Konfiguration der Benutzeranwendung: Alle Parameter*

Einstellungstyp	Feld	Beschreibung
eDirectory-Verbindungs-einstellungen	*LDAP-Host*	Erforderlich. Geben Sie den Hostnamen oder die IP-Adresse des LDAP-Servers an. Beispiel: myLDAPhost
	Nicht sicherer LDAP-Port	Geben Sie den nicht sicheren Port des LDAP-Servers an. Beispiel: 389.
	Sicherer LDAP-Port	Geben Sie den sicheren Port des LDAP-Servers an. Beispiel: 636.
	LDAP-Administrator	Erforderlich. Geben Sie die Berechtigungsnachweise für den LDAP-Administrator an. Dieser Benutzer muss bereits vorhanden sein. Die Benutzeranwendung verwendet dieses Konto für eine administrative Verbindung zum Identitätsdepot. Dieser Wert ist mit dem Master-Schlüssel verschlüsselt.
	LDAP-Administratorpasswort	Erforderlich. Geben Sie das LDAP-Administratorpasswort an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
	Öffentliches anonymes Konto verwenden	Ermöglicht nicht angemeldeten Benutzern den Zugriff auf das öffentliche anonyme LDAP-Konto.
	LDAP-Gast	Ermöglicht nicht angemeldeten Benutzern den Zugriff auf zulässige Portlets. Dieses Benutzerkonto muss bereits im Identitätsdepot vorhanden sein. Deaktivieren Sie das Kontrollkästchen *Öffentliches anonymes Konto verwenden*, um „LDAP-Gast“ zu aktivieren. Aktivieren Sie das Kontrollkästchen *Öffentliches anonymes Konto verwenden*, um „LDAP-Gast“ zu deaktivieren.
	LDAP-Gastpasswort	Geben Sie das LDAP-Gastpasswort an.
	Sichere Admin-Verbindung	Wählen Sie diese Option aus, wenn die gesamte Kommunikation über das Admin-Konto über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung beeinträchtigen).
	Sichere Benutzerverbindung	Wählen Sie diese Option aus, wenn die gesamte Kommunikation über das Konto des angemeldeten Benutzers über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung stark beeinträchtigen).

Einstellungstyp	Feld	Beschreibung
eDirectory-DNs	*Stammcontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen des Stammcontainers an. Diese Angabe wird als Standard-Suchstamm der Entitätsdefinition verwendet, sofern in der Verzeichnisabstraktionsschicht kein Suchstamm angegeben wurde.
	Bereitstellungstreiber-DN	Erforderlich. Geben Sie den eindeutigen Namen für den Benutzeranwendungstreiber an. Wenn Ihr Treiber beispielsweise „UserApplicationDriver“ und der Treibersatz „myDriverSet“ ist und sich der Treibersatz in einem Kontext „o=myCompany“ befindet, geben Sie folgenden Wert ein: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Benutzeranwendung - Administrator	Erforderlich. Ein vorhandener Benutzer im Identitätsdepot mit den Rechten zum Ausführen von administrativen Tätigkeiten für den in der Benutzeranwendung angegebenen Benutzercontainer. Dieser Benutzer hat die Möglichkeit, über die Registerkarte *Administration* der Benutzeranwendung das Portal zu verwalten. Wenn der Benutzeranwendungsadministrator in iManager, Novell Designer für Identity Manager oder der Benutzeranwendung (Registerkarte *Anforderungen und Genehmigungen*) freigelegte Aufgaben zur Workflow-Administration bearbeitet, müssen Sie dem entsprechenden Administrator ausreichende Trustee-Rechte auf Objektinstanzen gewähren, die im Benutzeranwendungstreiber enthalten sind. Weitere Informationen finden Sie im *Administrationshandbuch zur IDM-Benutzeranwendung*. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden.
	Bereitstellungs-anwendung - Administrator	Diese Funktion ist in der Bereitstellungsversion von Identity Manager 3.5.1 verfügbar. Der Administrator der Bereitstellungsanwendung verwaltet die Funktionen des Bereitstellungs-Workflows, die über die Registerkarte *Anforderungen und Genehmigungen* der Benutzeranwendung verfügbar sind. Dieser Benutzer muss im Identitätsdepot vorhanden sein, bevor ihm die Rolle des Administrators für die Bereitstellungsanwendung zugewiesen werden kann. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden.

Einstellungstyp	Feld	Beschreibung
Benutzeridentität für Metaverzeichnis	*Benutzercontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Benutzercontainers an. Diese Angabe definiert den Suchbereich für Benutzer und Gruppen. Benutzer in diesem Container (und unterhalb) dürfen sich bei der Benutzeranwendung anmelden. **Wichtig:** Stellen Sie sicher, dass der bei der Installation des Benutzeranwendungstreibers angegebene Benutzeranwendungsadministrator in diesem Container vorhanden ist, wenn dieser Benutzer Workflows ausführen soll.
	Benutzerobjektklasse	Die LDAP-Benutzerobjektklasse (in der Regel inetOrgPerson).
	Anmeldeattribut	Das LDAP-Attribut (z. B. CN), das den Anmeldenamen des Benutzers repräsentiert.
	Benennungsattribut	Das als ID verwendete LDAP-Attribut beim Nachschlagen von Benutzern oder Gruppen. Dieses Attribut ist nicht identisch mit dem Anmeldeattribut, das nur für die Anmeldung, nicht aber bei der Suche nach Benutzern oder Gruppen verwendet wird.
	Benutzermitgliedschafts attribut	Optional. Das LDAP-Attribut, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.
Benutzergruppen für Metaverzeichnis	*Gruppencontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Gruppencontainers an. Wird von Entitätsdefinitionen innerhalb der Verzeichnisabstraktionsschicht verwendet.
	Gruppenobjektklasse	Die Objektklasse für die LDAP-Gruppen (in der Regel groupofNames).
	Gruppenmitgliedschafts attribut	Das Attribut, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.
	Dynamische Gruppen verwenden	Wählen Sie diese Option, wenn Sie dynamische Gruppen verwenden möchten.
	Klasse für dynamisches Gruppenobjekt	Die Objektklasse für die dynamische Gruppe (in der Regel dynamicGroup).

Einstellungstyp	Feld	Beschreibung
eDirectory-Zertifikate	*Keystore-Pfad*	Erforderlich. Geben Sie den vollständigen Pfad zur Keystore-Datei (`cacerts`) der JRE an, die der Anwendungsserver für die Ausführung verwendet, oder klicken Sie auf die kleine Browser-Schaltfläche und navigieren Sie zur `cacerts`-Datei. Während der Installation der Benutzeranwendung wird die Keystore-Datei geändert. Unter Linux oder Solaris benötigt der Benutzer eine entsprechende Berechtigung zum Schreiben in diese Datei.
	Keystore-Passwort *Keystore-Passwort bestätigen*	Erforderlich. Geben Sie das `cacerts`-Passwort an. Die Vorgabe ist `changeit`.
Speicher für privaten Schlüssel	*Pfad für privaten Keystore*	Der private Keystore enthält den privaten Schlüssel und die Zertifikate der Benutzeranwendung. Reserviert. Wenn Sie keine Eingabe vornehmen, lautet der Standardpfad `/jre/lib/security/cacerts`.
	Passwort für privaten Keystore	Das Passwort lautet `changeit`, sofern Sie kein anderes Passwort festgelegt haben. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
	Alias für privaten Schlüssel	Dieser Alias lautet `novellIDMUserApp`, sofern Sie keinen anderen Namen festgelegt haben.
	Passwort für privaten Schlüssel	Das Passwort lautet `novellIDM`, sofern Sie kein anderes Passwort festgelegt haben. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
Speicher für Herkunftsverbürgungs-schlüssel	*Pfad für Herkunftsverbürgungs-speicher*	Der Speicher für Herkunftsverbürgungsschlüssel enthält alle verbürgten Zertifikate der Signierer, die zum Validieren digitaler Signaturen verwendet werden. Wurde kein Pfad angegeben, ruft die Benutzeranwendung den Pfad von der Systemeigenschaft `javax.net.ssl.trustStore` ab. Wurde kein Pfad angegeben, wird `jre/lib/security/cacerts` verwendet.
	Passwort für Herkunftsverbürgungs-speicher	Wurde kein Passwort angegeben, ruft die Benutzeranwendung das Passwort von der Systemeigenschaft `javax.net.ssl.trustStorePassword` ab. Ist dort kein Wert angegeben, lautet das Passwort `changeit`. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.

Einstellungstyp	Feld	Beschreibung
Novell Audit-Digitalsignatur-Zertifikat und Schlüssel		Enthält das Novell Audit-Digitalsignatur-Zertifikat und den Schlüssel.
	Novell Audit-Digitalsignatur-Zertifikat	Zeigt das Digitalsignatur-Zertifikat an.
	Privater Schlüssel für Novell Audit-Digitalsignatur	Zeigt den privaten Schlüssel für die Digitalsignatur an. Dieser Schlüssel ist mit dem Master-Schlüssel verschlüsselt.
iChain-Einstellungen	*ICS-Abmeldung aktiviert*	Bei Auswahl dieser Option unterstützt die Benutzeranwendung die gleichzeitige Abmeldung von der Benutzeranwendung und iChain bzw. Novell Access Manager. Bei der Abmeldung leitet die Benutzeranwendung den Benutzer bei Vorhandensein des iChain- oder Novell Access Manager-Cookies zur ICS-Abmeldungsseite um.
	ICS-Abmeldungsseite	Die URL zur iChain- oder Novell Access Manager-Abmeldungsseite, wobei die URL ein von iChain oder Novell Access Manager erwarteter Hostname ist. Wenn die ICS-Protokollierung aktiviert ist und sich ein Benutzer von der Benutzeranwendung abmeldet, wird der Benutzer auf diese Seite umgeleitet.

Einstellungstyp	Feld	Beschreibung
Email	*Benachrichtigungs-schablonen-Host-Token*	Geben Sie den Anwendungsserver an, der die Identity Manager-Benutzeranwendung hostet. Beispiel: `myapplication serverServer` Dieser Wert ersetzt das $HOST$-Token in Email-Schablonen. Die erstellte URL ist eine Verknüpfung zu Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen.
	Benachrichtigungs-schablonen-Port-Token	Ersetzt das $PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungsaufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Token für den sicheren Port der Benachrichtigungs-schablone	Ersetzt das $SECURE_PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Benachrichtigungs-schablonen-Protokoll-Token	Bezieht sich auf ein nicht sicheres Protokoll, HTTP. Ersetzt das $PROTOCOL$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Token für das sichere Protokoll der Benachrichtigungs-schablone	Bezieht sich auf ein sicheres Protokoll, HTTPS. Ersetzt das $SECURE_PROTOCOL$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Benachrichtigungs-SMTP-Email-Von:	Geben Sie Emails an, die von einem Benutzer in der Bereitstellungs-Email stammen.
	Benachrichtigungs-SMTP-Email-Host:	Geben Sie den SMTP-Email-Host für die Bereitstellungs-Email an. Dies kann eine IP-Adresse oder ein DNS-Name sein.

Einstellungstyp	Feld	Beschreibung
Passwortverwaltung		
	Externe WAR-Datei für Passwort verwenden	Mithilfe dieser Funktion können Sie eine Seite „Passwort vergessen“ in einer externen WAR-Datei „Passwort vergessen“ sowie eine URL angeben, die die externe WAR-Datei „Passwort vergessen“ für den Rückruf der Benutzeranwendung über einen Webservice verwendet. Wenn *Externe WAR-Datei für Passwort verwenden* aktiviert ist, müssen auch Werte für *'Passwort vergessen'-Link* und *Link zurück zu 'Passwort vergessen'* angegeben werden. Wenn *Externe WAR-Datei für Passwort verwenden* nicht aktiviert ist, verwendet IDM die interne Standardfunktion zur Passwortverwaltung. `/jsps/pwdmgt/ForgotPassword.jsf` (ohne http(s) am Anfang) zu verwenden. Hierdurch wird der Benutzer nicht zu einer externen WAR-Datei, sondern zur in der Benutzeranwendung integrierten Funktionalität „Passwort vergessen“ umgeleitet.
	'Passwort vergessen'-Link	Diese URL verweist auf die Funktionsseite „Passwort vergessen“. Erstellen Sie in einer externen oder in einer internen WAR-Datei für die Passwortverwaltung eine Datei namens `ForgotPassword.jsf`.
	Link zurück zu 'Passwort vergessen'	Bei Verwendung einer externen WAR-Datei für die Passwortverwaltung müssen Sie den Pfad angeben, den diese WAR-Datei für den Rückruf der Benutzeranwendung über die Web-Services verwendet. Beispiel: `https://`*`idmhost:sslport`*`/idm`.
Sonstige	*Sitzungszeitüber-schreitung*	Die Sitzungszeitüberschreitung der Anwendung.
	OCSP-URI	Wenn für die Client-Installation das OSCP (On-Line Certificate Status Protocol) verwendet wird, stellen Sie eine URI (Uniform Resource Identifier) bereit. Beispiel für das Format: http://host:port/ocspLocal. Die OCSP-URI aktualisiert den Status der verbürgten Zertifikate online.
	Konfigurationspfad für Autorisierung	Vollständig qualifizierter Name der Konfigurationsdatei für die Autorisierung.
	eDirectory-Index erstellen	
	Server-DN	

Einstellungstyp	Feld	Beschreibung
Containerobjekt	*Ausgewählt*	Wählen Sie alle zu verwendenden Containerobjekttypen aus.
	Containerobjekttyp	Wählen Sie die Typen aus den folgenden Standard-Containern aus: Standort-, Länder-, Organisationseinheits-, Organisations- und Domänenobjekte. Sie können in iManager auch eigene Container erstellen und mithilfe der Option *Neues Containerobjekt hinzufügen* hinzufügen.
	Containerattributname	Listet den mit dem Containerobjekttyp verknüpften Attributnamen auf.
	Neues Containerobjekt hinzufügen: Containerobjekttyp	Geben Sie den LDAP-Namen einer Objektklasse aus dem Identitätsdepot an, die als Container dienen kann. Weitere Informationen zu Containern finden Sie im *Administrationshandbuch zu Novell iManager 2.6 (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*.
	Neues Containerobjekt hinzufügen: Containerattributname	Geben Sie den Attributnamen des Containerobjekts an.

4 Klicken Sie nach der Konfiguration dieser Einstellungen auf *OK* und fahren Sie anschließend mit Abschnitt 5.6.10, „Prüfen der Auswahl und Installation“, auf Seite 172 fort.

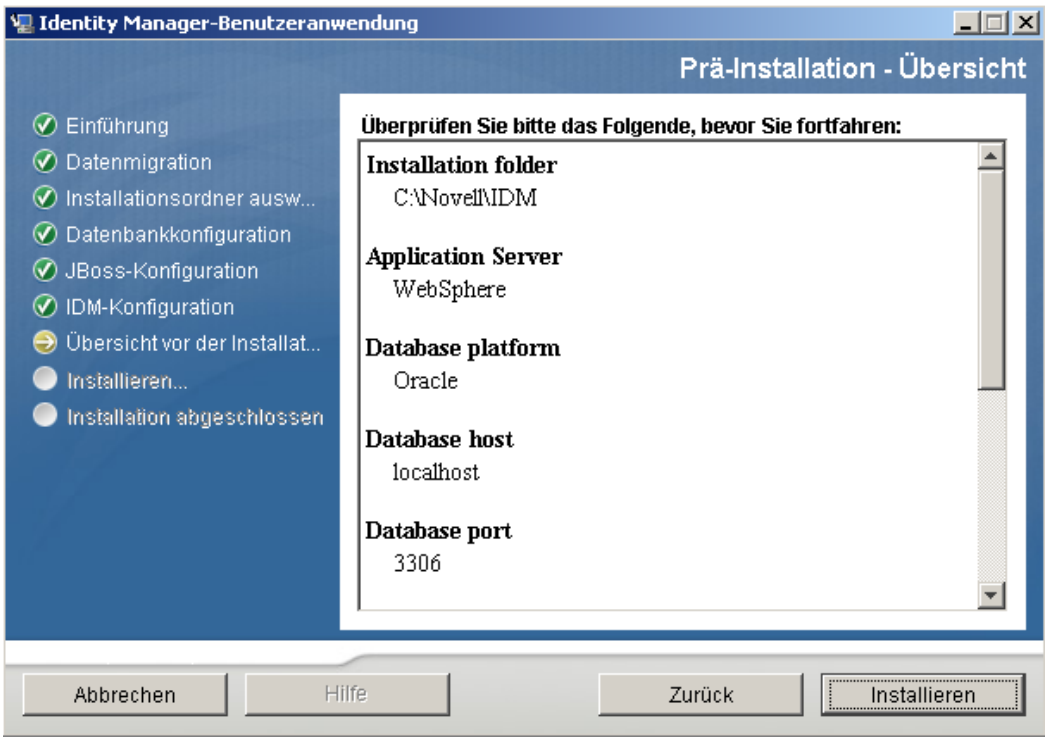
5.6.10 Prüfen der Auswahl und Installation

1 Überprüfen Sie auf der Seite „Zusammenfassung vor der Installation“ die Einstellungen der Installationsparameter.

2 Wenn Sie Änderungen vornehmen möchten, können Sie über die Schaltfläche *Zurück* vorherige Installationsseiten aufrufen.

Die Werte auf der Seite „Benutzeranwendung - Konfiguration“ werden nicht gespeichert, daher müssen Sie die Einstellungen auf dieser Seite erneut vornehmen, wenn Sie vorherige Seiten des Installationsvorgangs ändern.

3 Wenn Sie die gewünschten Änderungen an den Installations- und Konfigurationsparametern vorgenommen haben, kehren Sie zur Seite „Zusammenfassung vor der Installation“ zurück und klicken Sie auf *Installieren*. Fahren Sie mit Abschnitt 5.6.11, „Anzeigen der Protokolldateien“, auf Seite 173 fort.



5.6.11 Anzeigen der Protokolldateien

Wenn die Installation ohne Fehler abgeschlossen wurde, fahren Sie mit Abschnitt 5.6.12, „Hinzufügen von Benutzeranwendungs-Konfigurationsdateien und JVM-Systemeigenschaften“, auf Seite 173 fort.

Sofern bei der Installation Fehler- oder Warnmeldungen ausgegeben wurden, ermitteln Sie die Probleme anhand der Protokolldateien:

- Die Datei `Identity_Manager_User_Application_InstallLog.log` enthält die Ergebnisse der wichtigsten Installationsaufgaben.
- Die Datei `Novell-Custom-Install.log` enthält Informationen zur Konfiguration der Benutzeranwendung, die während der Installation vorgenommen wurde.

5.6.12 Hinzufügen von Benutzeranwendungs-Konfigurationsdateien und JVM-Systemeigenschaften

1. Kopieren Sie die Datei `sys-configuration-xmldata.xml` aus dem Installationsverzeichnis der Benutzeranwendung in ein Verzeichnis auf dem Computer, der den WebSphere-Server hostet, beispielsweise `/UserAppConfigFiles`. Das Installationsverzeichnis der Benutzeranwendung ist das Verzeichnis, in dem Sie die Benutzeranwendung installiert haben.
2. Geben Sie den Pfad zur Datei `sys-configuration-xmldata.xml` in den JVM-Systemeigenschaften an. Melden Sie sich dazu als Admin-Benutzer bei der Administrationskonsole von WebSphere an.
3. Rufen Sie in der linken Kontrollleiste *Server* > *Anwendungsserver* auf.

4 Klicken Sie in der Serverliste auf den Servernamen, z. B. „server1“.

5 Rufen Sie in der Liste der Einstellungen auf der rechten Seite unter *Server Infrastructure* die Option *Java and Process Management* auf.

6 Erweitern Sie den Link und wählen Sie *Process Definition*.

7 Wählen Sie aus der Liste von *zusätzlichen Eigenschaften* die Option *Java Virtual Machine*.

8 Wählen Sie unter der Überschrift *Additional Properties* für die JVM-Seite die Option *Custom Properties*.

9 Klicken Sie auf *New*, um eine neue JVM-Systemeigenschaft hinzuzufügen.

9a Geben Sie als *Namen* `extend.local.config.dir` an.

9b Geben Sie als *Wert* das Verzeichnis an, beispielsweise `/UserAppConfigFiles`, in das Sie die Datei `sys-configuration-xmldata.xml` kopiert haben.

9c Geben Sie als *Beschreibung* eine Beschreibung für die Eigenschaft an, beispielsweise `Pfad zu sys-configuration-xmldata.xml`.

9d Klicken Sie auf *OK*, um die Eigenschaft zu speichern.

10 Klicken Sie auf *New*, um eine weitere neue JVM-Systemeigenschaft hinzuzufügen.

10a Geben Sie als *Namen* `idmuserapp.logging.config.dir` an.

10b Geben Sie als *Wert* das Verzeichnis an, beispielsweise `/UserAppConfigFiles`, in das Sie die Datei `sys-configuration-xmldata.xml` kopiert haben.

10c Geben Sie als *Beschreibung* eine Beschreibung für die Eigenschaft an, beispielsweise `Pfad zu sys-configuration-xmldata.xml`.

10d Klicken Sie auf *OK*, um die Eigenschaft zu speichern.

Hinweis: Die Datei `idmuserapp-logging.xml` muss nicht in diesem Verzeichnis vorhanden sein. Sie wird erstellt, wenn Änderungen an der Protokollierungskonfiguration vorgenommen werden.

---

11 Fahren Sie mit dem Abschnitt Abschnitt 5.6.13, „Importieren der eDirectory-Herkunftsverbürgung in den WebSphere-Keystore“, auf Seite 174 fort.

5.6.13 Importieren der eDirectory-Herkunftsverbürgung in den WebSphere-Keystore

1 Der Installationsvorgang der Benutzeranwendung exportiert die eDirectory-Herkunftsverbürgungszertifikate in das Verzeichnis, in dem Sie die Benutzeranwendung installieren. Kopieren Sie diese Zertifikate auf den Computer, der den WebSphere-Server hostet.

2 Importieren Sie die Zertifikate in den WebSphere-Keystore. Sie können dies mithilfe der WebSphere-Administrationskonsole („Zertifikate mit der WebSphere-Administrationskonsole importieren“ auf Seite 174) oder über die Befehlszeile („Zertifikate über die Befehlszeile importieren“ auf Seite 175) tun.

3 Fahren Sie nach dem Importieren der Zertifikate mit Abschnitt 5.6.14, „Bereitstellung der IDM WAR-Datei“, auf Seite 175 fort.

Zertifikate mit der WebSphere-Administrationskonsole importieren

1 Melden Sie sich bei der Administrationskonsole von WebSphere als Admin-Benutzer an.

2 Rufen Sie in der linken Kontrollleiste *Security* > *SSL Certificate and Key Management* auf.

3 Rufen Sie in der Liste der Einstellungen auf der rechten Seite unter *Additional Properties* die Option *Key stores and certificates* auf.

4 Wählen Sie *NodeDefaultTrustStore* (oder den Verbürgungsspeicher, den Sie verwenden).

5 Wählen Sie rechts unter *Additional Properties* die Option *Signer Certificates* aus.

6 Klicken Sie auf *Add*.

7 Geben Sie den Aliasnamen und den vollständigen Pfad zur Zertifikatsdatei ein.

8 Ändern Sie den Datentyp in der Dropdown-Liste in *Binary DER data*.

9 Klicken Sie auf *OK*. Jetzt sollte das Zertifikat in der Liste der Signierzertifikate angezeigt werden.

Zertifikate über die Befehlszeile importieren

1 Führen Sie in der Befehlszeile auf dem Computer, der den WebSphere-Server hostet, das Keytool aus, um das Zertifikat in den WebSphere-Keystore zu importieren.

Hinweis: Sie müssen das WebSphere-Keytool ausführen, damit dies funktioniert. Vergewissern Sie sich außerdem, dass der Store-Typ PKCS12 ist.

Das WebSphere-Keytool befindet sich unter `/IBM/WebSphere/AppServer/java/bin`.

Beispiel für einen Keytool-Befehl

```
keytool -import -trustcacerts -file servercert.der -alias
myserveralias -keystore trust.p12 -storetype PKCS12
```

Wenn sich auf Ihrem System mehrere `trust.p12`-Dateien befinden, müssen Sie ggf. den vollständigen Pfad zu der Datei angeben.

5.6.14 Bereitstellung der IDM WAR-Datei

1 Melden Sie sich bei der Administrationskonsole von WebSphere als Admin-Benutzer an.

2 Rufen Sie in der linken Kontrollleiste *Applications* > *Install New Application* auf.

3 Wechseln Sie zum Speicherort der IDM WAR-Datei. (Die IDM WAR-Datei wird während der Installation der Benutzeranwendung konfiguriert. Sie befindet sich im Installationsverzeichnis der Benutzeranwendung, das Sie während der Installation der Benutzeranwendung angegeben haben.)

4 Geben Sie den Kontextstamm für die Anwendung ein, beispielsweise `IDMProv`. Dies ist der URL-Pfad.

5 Stellen Sie sicher, dass die Option *Prompt me only when additional information is required* ausgewählt ist, und klicken Sie dann auf *Next*, um zur Seite für die *Auswahl der Installationsoptionen* zu wechseln.

6 Übernehmen Sie die Standardeinstellungen für diese Seite und klicken Sie auf *Next*, um zum Bildschirm *Map modules to servers* zu wechseln.

7 Übernehmen Sie die Standardeinstellungen für diese Seite und klicken Sie auf *Next*, um zur Seite *Map resource references to resources* zu wechseln.

8 Wählen Sie für die Authentifizierungsmethode die Option *User default method*. Wählen Sie dann im Dropdown-Menü *Authentication data entry* den zuvor erstellten Alias aus, z. B. `MeinServerNode01/MeinAlias`.

9 Suchen Sie in der Tabelle unter den Authentifizierungseinstellungen das Modul, das Sie bereitstellen. Klicken Sie unter der Spalte mit der Überschrift `Target Resource JNDI Name` auf die Schaltfläche zum Durchsuchen, um einen JNDI-Namen anzugeben. Daraufhin sollte eine Liste von Ressourcen angezeigt werden. Wählen Sie die zuvor erstellte Datenquelle aus, z. B. `MeineDatenquelle`, und klicken Sie auf die Schaltfläche *Apply*, um zur Seite `Map resource references to resources` zurückzukehren.

10 Wählen Sie *Next*, um zur Seite *Map virtual hosts for Web modules* zu wechseln.

11 Übernehmen Sie die Standardeinstellungen für diese Seite und klicken Sie auf *Next*, um zur Seite *Summary* zu wechseln.

12 Klicken Sie auf *Finish*, um die Bereitstellung abzuschließen.

13 Klicken Sie nach dem Abschluss der Bereitstellung auf *Save*, um die Änderungen zu speichern.

14 Fahren Sie mit Abschnitt 5.6.15, „Anwendung starten“, auf Seite 176 fort.

5.6.15 Anwendung starten

1 Melden Sie sich bei der Administrationskonsole von WebSphere als Admin-Benutzer an.

2 Rufen Sie in der linken Navigationsleiste *Applications* > *Enterprise Applications* auf.

3 Wählen Sie das Kontrollkästchen neben der Anwendung aus, die Sie starten möchten, und klicken Sie anschließend auf *Start*.

Nach dem Start wird in der Spalte *Application status* ein grüner Pfeil angezeigt.

5.6.16 Zugriff auf das Benutzeranwendungsportal

1 Sie können mithilfe des Kontexts, den Sie während der Bereitstellung festgelegt haben, auf das Portal zugreifen.

Der Standardport für den Web-Container auf WebSphere ist 9080 bzw. 9443 für den sicheren Port. Die URL hat das folgende Format:

`http://<Server>:9080/IDMProv`

5.7 Installation der Benutzeranwendung über eine Konsolenschnittstelle

In diesem Abschnitt wird die Installation der Identity Manager-Benutzeranwendung über die Konsolenversion (Befehlszeile) des Installationsprogramms erläutert.

1 Rufen Sie die in Tabelle 5-2 auf Seite 113 beschriebenen Installationsdateien ab.

2 Melden Sie sich an und eröffnen Sie eine Terminalsitzung.

3 Starten Sie das Installationsprogramm für Ihre Plattform mit Java über den folgenden Befehl:

```
java -jar IdmUserApp.jar -i console
```

4 Befolgen Sie die unter Abschnitt 5.5, „Installation der Benutzeranwendung auf einem JBoss-Anwendungsserver von der GUI des Installationsprogramms“, auf Seite 114 für die grafische

Benutzeroberfläche beschriebenen Schritte. Beachten Sie die Eingabeaufforderungen und geben Sie die Antworten in der Befehlszeile ein. Führen Sie die Schritte zum Importieren oder Erstellen des Master-Schlüssels aus.

5 Starten Sie das configupdate-Dienstprogramm, um die Konfigurationsparameter für die Benutzeranwendung festzulegen. Geben Sie in der Befehlszeile `configupdate.sh` (Linux oder Solaris) oder `configupdate.bat` (Windows) ein und geben Sie die Werte, wie in Abschnitt 5.5.14, „Konfiguration der Benutzeranwendung“, auf Seite 131 beschrieben, ein.

6 Wenn Sie eine externe WAR-Datei für die Passwortverwaltung verwenden, kopieren Sie sie manuell in das Installationsverzeichnis und in das Bereitstellungsverzeichnis des Remote-JBoss-Servers, auf dem die externe Passwort-WAR ausgeführt wird.

7 Fahren Sie mit Abschnitt 5.9, „Aufgaben nach der Installation“, auf Seite 185 fort.

5.8 Installation der Benutzeranwendung mit einem einzigen Befehl

In diesem Abschnitt wird erläutert, wie eine automatische Installation durchgeführt wird. Eine automatische Installation erfordert keine Benutzeraktion und kann Zeit einsparen, besonders, wenn die Installation auf mehreren Systemen erfolgt. Die automatische Installation wird unter Linux und Solaris unterstützt.

1 Rufen Sie die in Tabelle 5-2 auf Seite 113 beschriebenen Installationsdateien ab.

2 Melden Sie sich an und eröffnen Sie eine Terminalsitzung.

3 Suchen Sie die IDM-Eigenschaftsdatei, `silent.properties`, die Teil der Installationsdateien ist. Wenn Sie von einer CD aus arbeiten, machen Sie eine lokale Kopie dieser Datei.

4 Bearbeiten Sie die `silent.properties`-Datei, sodass sie Ihre Installationsparameter und die Konfigurationsparameter der Benutzeranwendung zur Verfügung stellt.

   In der `silent.properties`-Datei finden Sie ein Beispiel für die einzelnen Installationsparameter. Die Installationsparameter entsprechen den Installationsparametern, die Sie bei der Installation der GUI oder der Konsolenschnittstelle angegeben haben.

   Eine Beschreibung der einzelnen Benutzeranwendungs-Konfigurationsparameter finden Sie in Tabelle 5-8. Die Benutzeranwendungs-Konfigurationsparameter sind identisch mit den Parametern, die Sie bei der Installation der GUI oder der Konsolenschnittstelle bzw. mit dem configupdate-Dienstprogramm einrichten können.

5 Starten Sie die automatische Installation wie folgt:

   ```
   java -jar IdmUserApp.jar -i silent -f / IhrVerzeichnispfad/
   silent.properties
   ```

   Geben Sie den vollständigen Pfad zur Datei `silent.properties` ein, falls sich die Datei in einem anderen Verzeichnis befindet als das Skript des Installationsprogramms. Das Skript entpackt die notwendigen Dateien in ein temporärer Verzeichnis und startet die automatische Installation.

Tabelle 5-8 *Benutzeranwendungs-Konfigurationsparameter für die automatische Installation*

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Konfigurationsparametern der Benutzeranwendung mit Beschreibung
NOVL_CONFIG_LDAPHOST=	eDirectory-Verbindungseinstellungen: LDAP-Host. Erforderlich. Geben Sie den Hostnamen oder die IP-Adresse des LDAP-Servers an.
NOVL_CONFIG_LDAPADMIN=	Erforderlich. Geben Sie die Berechtigungsnachweise für den LDAP-Administrator an. Dieser Benutzer muss bereits vorhanden sein. Die Benutzeranwendung verwendet dieses Konto für eine administrative Verbindung zum Identitätsdepot. Dieser Wert ist mit dem Master-Schlüssel verschlüsselt.
NOVL_CONFIG_LDAPADMINPASS=	eDirectory-Verbindungseinstellungen: LDAP-Administratorpasswort. Erforderlich. Geben Sie das LDAP-Administratorpasswort an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
NOVL_CONFIG_ROOTCONTAINERNAME=	eDirectory-DNs: Stammcontainer-DN. Erforderlich. Geben Sie den eindeutigen LDAP-Namen des Stammcontainers an. Diese Angabe wird als Standard-Suchstamm der Entitätsdefinition verwendet, sofern in der Verzeichnisabstraktionsschicht kein Suchstamm angegeben wurde.
NOVL_CONFIG_PROVISIONROOT=	eDirectory-DNs: Bereitstellungstreiber-DN. Erforderlich. Geben Sie den eindeutigen Namen des Benutzeranwendungstreibers an, den Sie zuvor in Abschnitt 5.3, „Erstellen des Benutzeranwendungstreibers“, auf Seite 107 erstellt haben. Wenn Ihr Treiber beispielsweise „UserApplicationDriver“ und der Treibersatz „myDriverSet“ ist und sich der Treibersatz in einem Kontext „o=myCompany“ befindet, geben Sie folgenden Wert ein: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Konfigurationsparametern der Benutzeranwendung mit Beschreibung
NOVL_CONFIG_LOCKSMITH=	eDirectory-DNs: Benutzeranwendung - Administrator. Erforderlich. Ein vorhandener Benutzer im Identitätsdepot mit den Rechten zum Ausführen von administrativen Tätigkeiten für den in der Benutzeranwendung angegebenen Benutzercontainer. Dieser Benutzer hat die Möglichkeit, über die Registerkarte *Administration* der Benutzeranwendung das Portal zu verwalten. Wenn der Benutzeranwendungsadministrator in iManager, Novell Designer für Identity Manager oder der Benutzeranwendung (Registerkarte *Anforderungen und Genehmigungen*) freigelegte Aufgaben zur Workflow-Administration bearbeitet, müssen Sie dem entsprechenden Administrator ausreichende Trustee-Rechte auf Objektinstanzen gewähren, die im Benutzeranwendungstreiber enthalten sind. Weitere Informationen finden Sie im *Administrationshandbuch zur IDM-Benutzeranwendung*. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration > Sicherheit* der Benutzeranwendung geändert werden.
NOVL_CONFIG_PROVLOCKSMITH=	eDirectory-DNs: Bereitstellungsanwendung - Administrator. Diese Funktion ist in der Bereitstellungsversion von Identity Manager 3.5.1 verfügbar. Der Administrator für die Bereitstellungsanwendung kann die Funktionen des Bereitstellungs-Workflows über die Registerkarte *Bereitstellung* (in der Registerkarte *Administration*) verwalten. Auf diese Funktionen können die Benutzer über die Registerkarte *Anforderungen und Genehmigungen* der Benutzeranwendung zugreifen. Dieser Benutzer muss im Identitätsdepot vorhanden sein, bevor ihm die Rolle des Administrators für die Bereitstellungsanwendung zugewiesen werden kann. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration > Sicherheit* der Benutzeranwendung geändert werden.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Konfigurationsparametern der Benutzeranwendung mit Beschreibung
NOVL_CONFIG_USERCONTAINERDN=	Benutzeridentität für Metaverzeichnis: Benutzercontainer-DN. Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Benutzercontainers an. Diese Angabe definiert den Suchbereich für Benutzer und Gruppen. Benutzer in diesem Container (und unterhalb) dürfen sich bei der Benutzeranwendung anmelden. **Wichtig:** Stellen Sie sicher, dass der bei der Installation des Benutzeranwendungstreibers angegebene Benutzeranwendungsadministrator in diesem Container vorhanden ist, wenn dieser Benutzer Workflows ausführen soll.
NOVL_CONFIG_GROUPCONTAINERDN=	Benutzergruppen für Metaverzeichnis: Gruppencontainer-DN. Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Gruppencontainers an. Wird von Entitätsdefinitionen innerhalb der Verzeichnisabstraktionsschicht verwendet.
NOVL_CONFIG_KEYSTOREPATH=	eDirectory-Zertifikate: Keystore-Pfad. Erforderlich. Geben Sie den vollständigen Pfad zur Keystore-Datei (`cacerts`) der JRE an, die der Anwendungsserver verwendet. Während der Installation der Benutzeranwendung wird die Keystore-Datei geändert. Unter Linux oder Solaris benötigt der Benutzer eine entsprechende Berechtigung zum Schreiben in diese Datei.
NOVL_CONFIG_KEYSTOREPASSWORD=	eDirectory-Zertifikate: Keystore-Passwort. Erforderlich. Geben Sie das `cacerts`-Passwort an. Die Vorgabe ist `changeit`.
NOVL_CONFIG_SECUREADMINCONNECTION=	eDirectory-Verbindungseinstellungen: Sichere Admin-Verbindung. Wählen Sie „True“, wenn die gesamte Kommunikation über das Admin-Konto über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung beeinträchtigen). Wählen Sie „False“, wenn die Kommunikation über das Admin-Konto nicht über eine SSL-Verbindung erfolgen soll.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Konfigurationsparametern der Benutzeranwendung mit Beschreibung
NOVL_CONFIG_SECUREUSERCONNECTION=	eDirectory-Verbindungseinstellungen: Sichere Benutzerverbindung. Wählen Sie „True“, wenn die gesamte Kommunikation über das Konto des angemeldeten Benutzers über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung stark beeinträchtigen). Wählen Sie „False“, wenn die Kommunikation über das Benutzerkonto nicht über eine SSL-Verbindung erfolgen soll.
NOVL_CONFIG_SESSIONTIMEOUT=	Sonstige: Sitzungszeitüberschreitung. Geben Sie für die Benutzeranwendung einen Zeitüberschreitungsintervall an.
NOVL_CONFIG_LDAPPLAINPORT=	eDirectory-Verbindungseinstellungen: Nicht sicherer LDAP-Port. Geben Sie den nicht sicheren Port des LDAP-Servers an, z. B. Port 389.
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory-Verbindungseinstellungen: Sicherer LDAP-Port. Geben Sie den sicheren Port des LDAP-Servers an, z. B. Port 636.
NOVL_CONFIG_ANONYMOUS=	eDirectory-Verbindungseinstellungen: Öffentliches anonymes Konto verwenden. Geben Sie „True“ an, damit nicht angemeldete Benutzer auf das öffentliche anonyme LDAP-Konto zugreifen können. Geben Sie „False“ an, um stattdessen NOVL_CONFIG_GUEST zu aktivieren.
NOVL_CONFIG_GUEST=	eDirectory-Verbindungseinstellungen: LDAP-Gast. Ermöglicht nicht angemeldeten Benutzern den Zugriff auf zulässige Portlets. Die Option *Öffentliches anonymes Konto verwenden* muss deaktiviert werden. Das Gast-Benutzer-Konto muss bereits im Identitätsdepot vorhanden sein. Aktivieren Sie zum Deaktivieren des Gast-Benutzers das Kontrollkästchen *Öffentliches anonymes Konto verwenden*.
NOVL_CONFIG_GUESTPASS=	eDirectory-Verbindungseinstellungen: LDAP-Gastpasswort.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Konfigurationsparametern der Benutzeranwendung mit Beschreibung
NOVL_CONFIG_EMAILNOTIFYHOST=	Email: Benachrichtigungsschablonen-Host-Token. Geben Sie den Anwendungsserver an, der die Identity Manager-Benutzeranwendung hostet. Beispiel: `myapplication serverServer` Dieser Wert ersetzt das $HOST$-Token in Email-Schablonen. Die erstellte URL ist eine Verknüpfung zu Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen.
NOVL_CONFIG_EMAILNOTIFYPORT=	Email: Benachrichtigungsschablonen-Port-Token. Ersetzt das $PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	Email: Token für den sicheren Port der Benachrichtigungsschablone. Ersetzt das $SECURE_PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden
NOVL_CONFIG_NOTFSMTPEMAILFROM=	Benachrichtigungs-SMTP-Email-Von. Geben Sie Emails an, die von einem Benutzer in der Bereitstellungs-Email stammen.
NOVL_CONFIG_NOTFSMTPEMAILHOST=	Email: Benachrichtigungs-SMTP-Email-Host. Geben Sie den SMTP-Email-Host an, der für die Bereitstellungs-Emails verwendet wird. Dies kann eine IP-Adresse oder ein DNS-Name sein.
NOVL_CONFIG_USEEXTPWDWAR=	Passwortverwaltung: Externe WAR-Datei für Passwort verwenden. Geben Sie „True“ an, falls Sie eine externe WAR-Datei für die Passwortverwaltung verwenden. Wenn Sie „True“ angeben, müssen auch Werte für *NOVL_CONFIG_EXTPWDWARPTH* und *NOVL_CONFIG_EXTPWDWARRTNPATH* angegeben werden. Geben Sie „False“ an, um die interne Standardfunktion für die Passwortverwaltung `/jsps/pwdmgt/ForgotPassword.jsf` (ohne http(s) am Anfang) zu verwenden. Hierdurch wird der Benutzer nicht zu einer externen WAR-Datei, sondern zur in der Benutzeranwendung integrierten Funktionalität „Passwort vergessen“ umgeleitet.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Konfigurationsparametern der Benutzeranwendung mit Beschreibung
NOVL_CONFIG_EXTPWDWARPATH=	Passwortverwaltung: 'Passwort vergessen'-Link. Geben Sie die URL für die Seite „Passwort vergessen“, `ForgotPassword.jsf`, in einer externen oder internen WAR-Datei für die Passwortverwaltung ein. Alternativ können Sie auch die vorgegebene WAR-Datei für die Passwortverwaltung übernehmen. Weitere Informationen finden Sie in „Verwendung von Passwort-WAR-Dateien“ auf Seite 145.
NOVL_CONFIG_EXTPWDWARRTNPATH=	Passwortverwaltung: Link zurück zu 'Passwort vergessen'. Bei Verwendung einer externen WAR-Datei für die Passwortverwaltung müssen Sie den Pfad angeben, den diese WAR-Datei für den Rückruf der Benutzeranwendung über die Web-Services verwendet. Beispiel: `https://idmhost:sslport/idm`.
NOVL_CONFIG_USEROBJECTATTRIBUTE=	Benutzeridentität für Metaverzeichnis: Benutzerobjektklasse. Die LDAP-Benutzerobjektklasse (in der Regel inetOrgPerson).
NOVL_CONFIG_LOGINATTRIBUTE=	Benutzeridentität für Metaverzeichnis: Anmeldeattribut. Das LDAP-Attribut (z. B. CN), das den Anmeldenamen des Benutzers repräsentiert.
NOVL_CONFIG_NAMINGATTRIBUTE=	Benutzeridentität für Metaverzeichnis: Benennungsattribut. Das als ID verwendete LDAP-Attribut beim Nachschlagen von Benutzern oder Gruppen. Dieses Attribut ist nicht identisch mit dem Anmeldeattribut, das nur für die Anmeldung, nicht aber bei der Suche nach Benutzern oder Gruppen verwendet wird.
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	Benutzeridentität für Metaverzeichnis: Benutzermitgliedschaftsattribut. Optional. Das LDAP-Attribut, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	Benutzergruppen für Metaverzeichnis: Gruppenobjektklasse. Die Objektklasse für die LDAP-Gruppen (in der Regel groupofNames).
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	Benutzergruppen für Metaverzeichnis: Gruppenmitgliedschaftsattribut. Geben Sie das Attribut an, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.
NOVL_CONFIG_USEDYNAMICGROUPS=	Benutzergruppen für Metaverzeichnis: Dynamische Gruppen verwenden. Geben Sie „True“ an, um dynamische Gruppen zu verwenden. Geben Sie anderenfalls „False“ an.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Konfigurationsparametern der Benutzeranwendung mit Beschreibung
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	Benutzergruppen für Metaverzeichnis: Klasse für dynamisches Gruppenobjekt. Geben Sie die Objektklasse für die dynamische Gruppe an (in der Regel dynamicGroup).
NOVL_CONFIG_PRIVATESTOREPATH=	Speicher für privaten Schlüssel: Pfad für privaten Keystore. Geben Sie den Pfad zum privaten Keystore an, der den privaten Schlüssel und die Zertifikate der Benutzeranwendung enthält. Reserviert. Wenn Sie keine Eingabe vornehmen, lautet der Standardpfad `/jre/lib/security/cacerts`.
NOVL_CONFIG_PRIVATESTOREPASSWORD=	Speicher für privaten Schlüssel: Passwort für privaten Keystore.
NOVL_CONFIG_PRIVATEKEYALIAS=	Speicher für privaten Schlüssel: Alias für privaten Schlüssel. Dieser Alias lautet `novellIDMUserApp`, sofern Sie keinen anderen Namen festgelegt haben.
NOVL_CONFIG_PRIVATEKEYPASSWORD=	Speicher für privaten Schlüssel: Passwort für privaten Schlüssel.
NOVL_CONFIG_TRUSTEDSTOREPATH=	Speicher für Herkunftsverbürgungsschlüssel: Pfad für Herkunftsverbürgungsspeicher. Der Speicher für Herkunftsverbürgungsschlüssel enthält alle verbürgten Zertifikate der Signierer, die zum Validieren digitaler Signaturen verwendet werden. Wurde kein Pfad angegeben, ruft die Benutzeranwendung den Pfad von der Systemeigenschaft `javax.net.ssl.trustStore` ab. Wurde kein Pfad angegeben, wird `jre/lib/security/cacerts` verwendet.
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	Speicher für Herkunftsverbürgungsschlüssel: Passwort für Herkunftsverbürgungsspeicher.
NOVL_CONFIG_AUDITCERT=	Novell Audit-Digitalsignatur-Zertifikat
NOVL_CONFIG_AUDITKEYFILEPATH=	Schlüsseldateipfad für Novell Audit-Digitalsignatur.
NOVL_CONFIG_ICSLOGOUTENABLED=	iChain-Einstellungen: ICS-Abmeldung aktiviert. Geben Sie „True“ an, um die gleichzeitige Abmeldung von der Benutzeranwendung und iChain bzw. Novell Access Manager zu aktivieren. Bei der Abmeldung leitet die Benutzeranwendung den Benutzer bei Vorhandensein des iChain- oder Novell Access Manager-Cookies zur ICS-Abmeldungsseite um. Geben Sie „False“ an, um die gleichzeitige Abmeldung zu deaktivieren.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Konfigurationsparametern der Benutzeranwendung mit Beschreibung
NOVL_CONFIG_ICSLOGOUTPAGE=	iChain-Einstellungen: ICS-Abmeldungsseite. Geben Sie die URL zur iChain- oder Novell Access Manager-Abmeldungsseite an, wobei die URL ein von iChain oder Novell Access Manager erwarteter Hostname ist. Wenn die ICS-Protokollierung aktiviert ist und sich ein Benutzer von der Benutzeranwendung abmeldet, wird der Benutzer auf diese Seite umgeleitet.
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	Email: Benachrichtigungsschablonen-Protokoll-Token. Bezieht sich auf ein nicht sicheres Protokoll, HTTP. Ersetzt das $PROTOCOL$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	Email: Token für den sicheren Port der Benachrichtigungsschablone.
NOVL_CONFIG_OCSPURI=	Sonstige: OCSP-URI. Wenn für die Client-Installation das OSCP (On-Line Certificate Status Protocol) verwendet wird, stellen Sie eine URI (Uniform Resource Identifier) bereit. Beispiel für das Format: http://hstport/ocspLocal. Die OCSP-URI aktualisiert den Status der verbürgten Zertifikate online.
NOVL_CONFIG_AUTHCONFIGPATH=	Sonstige: Konfigurationspfad für Autorisierung. Der vollständig qualifizierte Name der Konfigurationsdatei für die Autorisierung.

5.9 Aufgaben nach der Installation

Nach der Installation und Konfiguration der Benutzeranwendung müssen Sie sich um die folgenden Aufgaben kümmern.

5.9.1 Aufzeichnen des Master-Schlüssels

Kopieren Sie direkt nach der Installation den verschlüsselten Master-Schlüssel und speichern Sie ihn an einem sicheren Ort.

1. Öffnen Sie die Datei `master-key.txt`, die sich im Installationsverzeichnis befindet.
2. Kopieren Sie den verschlüsselten Master-Schlüssel an einen sicheren Speicherort, auf den Sie bei einem Systemfehler zugreifen können.

Warnung: Bewahren Sie immer eine Kopie des verschlüsselten Master-Schlüssels auf. Der verschlüsselte Master-Schlüssel wird benötigt, um Zugriff auf verschlüsselte Daten zu erlangen, falls der Master-Schlüssel z. B. durch einen Gerätefehler verloren geht.

Erfolgt die Installation auf dem ersten Mitglied eines Clusters, müssen Sie diesen verschlüsselten Master-Schlüssel verwenden, wenn Sie die Benutzeranwendung auf anderen Cluster-Mitgliedern installieren.

Weitere Informationen zum Master-Schlüssel finden Sie im *Identity Manager-Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idm35/index.html) in den Abschnitten zur *Verschlüsselung von vertraulichen Daten der Benutzeranwendung* und zu *JBoss-Clustern*.

5.9.2 Überprüfen der Cluster-Installationen

Überprüfen Sie Ihre Cluster-Installationen. Stellen Sie sicher, dass jeder JBoss-Server des Clusters Folgendes hat:

- einen eindeutigen Partitionsnamen (partition name)
- ein eindeutiges Partitions-UDP (partition.udpGroup)
- eine eindeutige Workflow-Engine-ID
- Dieselbe (identische) WAR-Datei. Die WAR-Datei wird während der Installation standardmäßig in das Verzeichnis `jboss\server\IDM\deploy` geschrieben.

Stellen Sie sicher, dass jeder Server in einem WebSphere-Cluster eine eindeutige Workflow-Engine-ID besitzt.

Weitere Informationen hierzu finden Sie im Abschnitt „Clustering“ in Kapitel 4 des Handbuchs *Identity Manager-Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idm35/index.html).

5.9.3 Konfiguration der SSL-Kommunikation zwischen JBoss-Servern

Wenn Sie während der Installation *Externe WAR-Datei für Passwort verwenden* in der Benutzeranwendungskonfigurationsdatei auswählen, müssen Sie die SSL-Kommunikation zwischen den JBoss-Servern konfigurieren, auf denen die Benutzeranwendungs-WAR und die `IDMPwdMgt.war`-Datei bereitgestellt werden. Eine Anleitung hierzu finden Sie in der JBoss-Dokumentation.

5.9.4 Zugriff auf die externe Passwort-WAR

Wenn Sie eine externe Passwort-WAR verwenden und die „Passwort vergessen“-Funktion testen möchten, können Sie an zwei Orten auf sie zugreifen:

- In einem Browser. Rufen Sie die Seite „Passwort vergessen“ in der externen Passwort-WAR auf, z. B. `http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`.
- Klicken Sie auf der Anmeldeseite der Benutzeranwendung auf den Link *Passwort vergessen*.

5.9.5 Aktualisierung der Einstellungen für „Passwort vergessen“

Die Werte von *'Passwort vergessen'-Link* und *Link zurück zu 'Passwort vergessen'* können nach der Installation über das configupdate-Dienstprogramm oder die Benutzeranwendung geändert werden.

So verwenden Sie das Dienstprogramm „configupdate“: Wechseln Sie in der Befehlszeile zum Installationsverzeichnis und geben Sie `configupdate.sh` (Linux oder Solaris) bzw. `configupdate.bat` (Windows) ein. Wenn Sie eine externe WAR-Datei für die Passwortverwaltung erstellen oder bearbeiten, müssen Sie die WAR-Datei manuell umbenennen, bevor Sie sie auf den Remote-JBoss-Server kopieren.

So verwenden Sie die Benutzeranwendung: Melden Sie sich als Administrator der Benutzeranwendung an und wechseln Sie zu *Administration* > *Anwendungskonfiguration* > *Passwortmodul - Setup* > *Anmeldung*. Bearbeiten Sie die folgenden Felder:

- *'Passwort vergessen'-Link* (z. B. `http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`)
- *Link zurück zu 'Passwort vergessen'* (z. B. `https://idmhost:sslport/idm`)

5.9.6 Einrichten der Email-Benachrichtigung

So implementieren Sie Email-Benachrichtigungsfunktionen für Workflows und bei vergessenem Passwort:

1. Wählen Sie in iManager unter „Funktionen und Aufgaben“ die Option *Workflow-Administration* und anschließend *Email-Serveroptionen*.
2. Geben Sie unter *Hostname* den Namen des SMTP-Servers an.
3. Geben Sie unter *Von* eine Email-Adresse an (z. B. *noreply@novell.com*) und klicken Sie anschließend auf *OK*.

5.9.7 Testen der Installation auf dem JBoss-Anwendungsserver

1. Starten Sie die Datenbank. Eine Anleitung hierzu finden Sie in der Dokumentation zur Datenbank.
2. Starten Sie den Benutzeranwendungsserver (JBoss). Wechseln Sie an der Befehlszeile zum Installationsverzeichnis und führen Sie das folgende Skript aus (bereitgestellt von der Benutzeranwendungs-Installation):

   `start-jboss.sh` (Linux und Solaris)

   `start-jboss.bat` (Windows)

   Sie können den Anwendungsserver anhalten, indem Sie den Befehl `stop-jboss.sh` oder `stop-jboss.bat` eingeben oder das Fenster schließen, in dem `start-jboss.sh` bzw. `start-jboss.bat` läuft.
3. Starten Sie den Benutzeranwendungstreiber. So wird die Kommunikation mit dem Benutzeranwendungstreiber ermöglicht.
   - **3a** Melden Sie sich bei iManager an.
   - **3b** Wählen Sie in der Anzeige der Funktionen und Aufgaben im linken Navigationsrahmen unter *Identity Manager* die Option *Identity Manager-Überblick*.
   - **3c** Geben Sie im angezeigten Inhaltsrahmen den Treibersatz ein, der den Benutzeranwendungstreiber enthält, und klicken Sie auf *Suchen*. Es wird eine Grafik aufgerufen, in der der Treibersatz mit seinen verknüpften Treibern angezeigt wird.
   - **3d** Klicken Sie auf dem Treiber auf das rot-weiße Symbol.
   - **3e** Wählen Sie *Treiber starten*. Der Treiberstatus ändert sich in das Yin-Yang-Symbol, das anzeigt, das der Treiber gestartet wurde.

     Beim Start versucht der Treiber mit der Benutzeranwendung einen „Handshake“ durchzuführen. Wenn die Benutzeranwendung nicht läuft oder die WAR-Datei nicht erfolgreich bereitgestellt wurde, gibt der Treiber einen Fehler zurück.

4 Sie können die Benutzeranwendung starten und sich bei ihr anmelden, indem Sie im Adressfeld Ihres Webbrowsers

   http://*Hostname*:*Port*/*Anwendungsname* eingeben.

   Hostname:*Port* entspricht dem Hostnamen des Anwendungsservers (z. B. MeinServer.Domäne.com) und der Port ist der Port des Anwendungsservers (der Standard-Port auf JBoss ist beispielsweise Port 8080). *Anwendungsname* ist standardmäßig IDM. Der Anwendungsname wurde während der Installation bei der Eingabe der Konfigurationsinformationen für den Anwendungsserver angegeben.

   Die Standard-Portalseiteder Novell Identity Manager-Benutzeranwendung sollte angezeigt werden.

5 Klicken Sie am oberen rechten Seitenrand auf *Anmelden*, um sich bei der Benutzeranwendung anzumelden.

Wird nach Ausführung dieser Schritte die Seite „Identity Manager-Benutzeranwendung“ nicht im Browser angezeigt, überprüfen Sie die Terminal-Konsole auf Fehlermeldungen und lesen Sie in Abschnitt 5.11, „Fehlersuche“, auf Seite 191 nach.

5.9.8 Einrichten von Bereitstellungsteams und Anforderungen

Richten Sie zum Aktivieren von Workflow-Aufgaben Bereitstellungsteams und Bereitstellungsteamanforderungen ein. Eine entsprechende Anleitung hierzu finden Sie im *Identity Manager 3.5.1 Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idm35/index.html).

5.9.9 Erstellen von Indizes in eDirectory

Für eine verbesserte Leistung der IDM-Benutzeranwendung muss der eDirectory-Administrator Indizes für die manager-, ismanager- und srvprvUUID-Attribute erstellen. Sind für diese Attribute keine Indizes vorhanden, kann dies insbesondere in einer Cluster-Umgebung eine eingeschränkte Leistung der Benutzeranwendung zur Folge haben. Im *Administrationshandbuch zu Novell eDirectory* (http://www.novell.com/documentation) finden Sie eine Anleitung zum Erstellen von Indizes mithilfe von Index Manager.

5.10 Neukonfiguration der IDM WAR-Datei nach der Installation

1. Führen Sie das Dienstprogramm „ConfigUpdate“ im Installationsverzeichnis der Benutzeranwendung aus, indem Sie `configupdate.sh` oder `configupdate.bat` ausführen. Dadurch können Sie die WAR-Datei im Installationsverzeichnis aktualisieren.

   Weitere Informationen zu den Parametern des Dienstprogramms „ConfigUpdate“ finden Sie unter Abschnitt 5.5.14, „Konfiguration der Benutzeranwendung“, auf Seite 131 oder Abschnitt 5.6.9, „Konfiguration der Benutzeranwendung“, auf Seite 157.
2. Stellen Sie die neue WAR-Datei auf Ihrem Anwendungsserver bereit.

5.11 Fehlersuche

Ein Mitarbeiter von Novell unterstützt Sie bei der Behebung von Einrichtungs- und Konfigurationsproblemen. Unterdessen finden Sie in diesem Abschnitt einige Lösungsansätze zur Behebung von Problemen.

Tabelle 5-9 *Fehlersuche bei der Benutzeranwendung*

Problem	Empfohlene Vorgehensweise

Sie möchten die Benutzeranwendungs-Konfigurationseinstellungen ändern, die Sie während der Installation vorgenommen haben. Hierzu gehören folgende Konfigurationseinstellungen:
◆ Identitätsdepot-Verbindungen und -Zertifikate
◆ Email-Einstellungen
◆ Benutzeridentität für Metaverzeichnis, Benutzergruppen
◆ iChain-Einstellungen
	Das Dienstprogramm für die Konfiguration kann unabhängig vom Installationsprogramm ausgeführt werden.
	Führen Sie unter Linux und Solaris im Installationsverzeichnis (standardmäßig `\opt\novell\idm`) den folgenden Befehl aus:
	`configupdate.sh`
	Führen Sie unter Windows im Installationsverzeichnis (standardmäßig `c:\opt\novell\idm`) den folgenden Befehl aus:
	`configupdate.bat`

Beim Start des Anwendungsserver werden Ausnahmen sowie die Protokollmeldung `port 8080 already in use` ausgegeben.	Schließen Sie alle Instanzen von Tomcat (oder anderer Server-Software), die möglicherweise bereits laufen. Wenn Sie den Anwendungsserver neu konfigurieren und einen anderen Port als Port 8080 festlegen möchten, müssen Sie die `config`-Einstellungen für den Benutzeranwendungstreiber in iManager bearbeiten.
Beim Start des Anwendungsservers wird angezeigt, dass keine verbürgten Zertifikate gefunden wurden.	Stellen Sie sicher, dass Sie den Anwendungsserver mithilfe des JDK starten, das bei der Installation der Benutzeranwendung angegeben wurde.
Sie können sich nicht auf der Seite „Portaladministration“ anmelden.	Stellen Sie sicher, dass ein Konto für den Benutzeranwendungsadministrator vorhanden ist. Verwechseln Sie dieses Konto nicht mit Ihrem iManager-Administratorkonto. Dies sind zwei unterschiedliche Administratorobjekte (oder sollten es sein).
Sie können sich als Administrator anmelden, aber keine neuen Benutzer erstellen.	Der Administrator der Benutzeranwendung muss ein Trustee des Containers der obersten Ebene sein und über Supervisor-Rechte verfügen. Zur Überbrückung können Sie die Rechte des Administrators der Benutzeranwendung mit denen des LDAP-Administrators gleichsetzen (mithilfe von iManager).

Problem	Empfohlene Vorgehensweise
Beim Start des Anwendungsservers treten MySQL-Verbindungsfehler auf.	Führen Sie MySQL nicht als `root` aus. (Dieses Problem tritt normalerweise nicht auf, wenn Sie die MySQL-Version ausführen, die mit IDM geliefert wurde.) Stellen Sie sicher, dass MySQL läuft und die richtige Version verwendet wird. Beenden Sie alle anderen Instanzen von MySQL. Führen Sie zunächst den Befehl `/idm/mysql/start-mysql.sh` und anschließend `/idm/start-jboss.sh` aus. Prüfen Sie `/idm/mysql/setup-mysql.sh` in einem Texteditor und berichtigen Sie alle Werte, die Ihnen verdächtig vorkommen. Führen Sie anschließen das Skript und den Befehl `/idm/start-jboss.sh` aus.
Beim Starten des Anwendungsservers treten Keystore-Fehler auf.	Ihr Anwendungsserver verwendet nicht das bei der Installation der Benutzeranwendung angegebene JDK. Importieren Sie die Zertifikatsdatei mithilfe des Befehls `keytool`: `keytool -import -trustcacerts -alias` *`aliasName`* `-file` *`certFile`* `-keystore ..\lib\security\cacerts -storepass changeit` ◆ Ersetzen Sie *aliasName* durch einen beliebigen eindeutigen Namen für dieses Zertifikat. ◆ Ersetzen Sie *certFile* durch den vollständigen Pfad und Namen der Zertifikatsdatei. ◆ Das Keystore-Standardpasswort lautet `changeit` (falls Sie ein anderes Passwort festgelegt haben, geben Sie es an).

Es wurde keine Email-Benachrichtigung gesendet.	Führen Sie das configupdate-Dienstprogramm aus, um zu überprüfen, ob Sie Werte für die Benutzeranwendungs-Konfigurationsparameter „Email-Von“ und „Email-Host“ angegeben haben.
	
	Führen Sie unter Linux und Solaris im Installationsverzeichnis (standardmäßig `\opt\novell\idm`) den folgenden Befehl aus:
	`configupdate.sh`
	
	Führen Sie unter Windows im Installationsverzeichnis (standardmäßig `c:\opt\novell\idm`) den folgenden Befehl aus:
	`configupdate.bat`

Aktivieren von Novell Identity Manager-Produkten

6

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:

- Erwerb einer Produktlizenz für Identity Manager
- Aktivieren von Novell Identity Manager-Produkten mithilfe eines Berechtigungsnachweises
- Installation einer Produktaktivierungsberechtigung
- Anzeigen der Produktaktivierungen für Identity Manager und Identity Manager-Treiber

6.1 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.

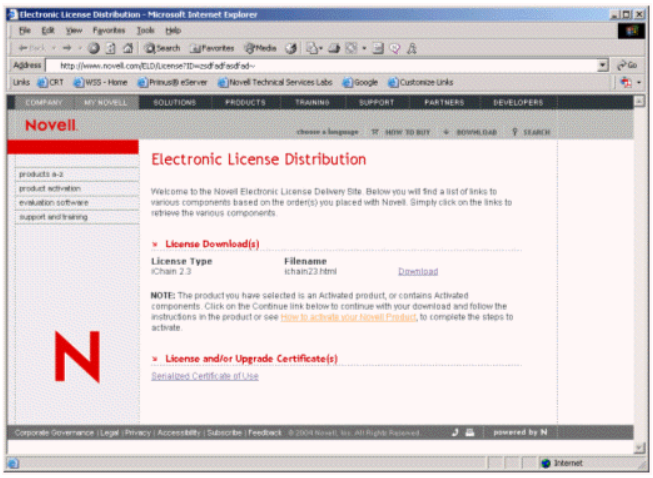
Wenn Sie eine Produktlizenz erworben haben, wird Ihnen von Novell die Kunden-ID per Email zugesendet. Die Email enthält außerdem die URL der Website, auf der Sie einen Berechtigungsnachweis erhalten. Wenn Sie Ihre Kunden-ID vergessen oder sie keine erhalten haben, rufen Sie bitte beim Novell Activation Center unter +1-800-418-8373 in den USA an. An allen anderen Standorten rufen Sie bitte unter +1-801-861-8373 an.

6.2 Aktivieren von Novell Identity Manager-Produkten mithilfe eines Berechtigungsnachweises

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.

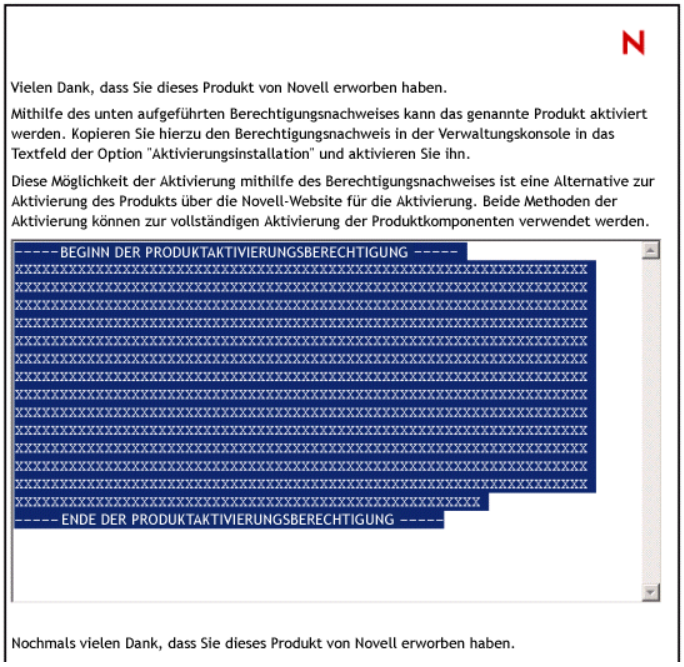
Wichtig: Zur Aktivierung des Produkts ist die Email nicht erforderlich. Wenn die Email an eine andere Person innerhalb Ihres Unternehmens gesendet wurde, erhalten Sie weitere Informationen vom Novell Activation Center.

Wenn Sie auf den Link geklickt haben, wird eine Website aufgerufen, die der folgenden Abbildung ähnelt:



2 Klicken Sie auf den Link zum Herunterladen der Lizenz und speichern oder öffnen Sie die `html`-Datei.

Der Inhalt der geöffneten Datei sollte der folgenden Abbildung ähneln:



3 Eine Anleitung zur Aktivierung der Identity Manager-Komponenten finden Sie in Abschnitt 6.3, „Installation einer Produktaktivierungsberechtigung“, auf Seite 195.

6.3 Installation einer Produktaktivierungsberechtigung

Die Produktaktivierungsberechtigung sollte über iManager installiert werden.

1. Öffnen Sie die Novell-Email mit der Produktaktivierungsberechtigung.
2. Führen Sie einen der folgenden Vorgänge 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. Wählen Sie den gewünschten Treibersatz aus und klicken Sie auf *Weiter*.
6. Wählen Sie auf der Seite „Identity Manager-Überblick“ den gewünschten Treibersatz aus, klicken Sie auf den roten Link *Aktivierung erforderlich bis* und anschließend auf *Aktivierung installieren*.
7. Wählen Sie den Treibersatz aus, in dem Sie die Identity Manager-Komponente aktivieren möchten.
8. Führen Sie einen der folgenden Vorgänge aus:
   - Geben Sie an, wo Sie den Identity Manager-Berechtigungsnachweis gespeichert haben, und klicken Sie auf *Weiter*.

     oder
   - Kopieren Sie den Inhalt der Datei in den Textbereich und klicken Sie auf *Weiter*.
9. Klicken Sie auf *Fertig stellen*.

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

6.4 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. So zeigen Sie die Produktaktivierungsberechtigungen an:

1. Öffnen Sie iManager.
2. Klicken Sie auf *Identity Manager* > *Identity Manager-Überblick*.
3. Geben Sie im Feld „Objektname“ den Namen des Treibersatzes oder des Treibers an, dessen Aktivierungsinformationen Sie anzeigen möchten.

oder

Navigieren Sie zu dem Treibersatz oder dem Treiber, dessen Aktivierungsinformationen Sie anzeigen möchten.

4. Wählen Sie den Treibersatz aus, dessen Aktivierungsinformationen Sie anzeigen möchten, und klicken Sie auf den Treibersatznamen.
5. Wählen Sie die Registerkarte *Aktivierung*.

   Sie können den Text des Berechtigungsnachweises anzeigen oder bei einer Fehlermeldung einen Berechtigungsnachweis entfernen.

Hinweis: Nach der Installation einer gültigen Produktaktivierungsberechtigung wird neben dem Treibernamen möglicherweise noch immer „Aktivierung erforderlich“ angezeigt. Starten Sie in diesem Fall den Treiber neu. Die Meldung sollte dann nicht mehr angezeigt werden.
