Novell Funktionsbasiertes Bereitstellungsmodul für Identity Manager

3.6

21. Januar 2008

www.novell.com

BENUTZERANWENDUNG:
INSTALLATIONSHANDBUCH

Novell®

Rechtliche Hinweise

Novell, Inc., leistet keinerlei Gewähr bezüglich des Inhalts oder Gebrauchs dieses Handbuchs. Insbesondere werden keine ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich der handelsüblichen Qualität oder Eignung für einen bestimmten Zweck übernommen. Novell, Inc., behält sich weiterhin das Recht vor, diese Dokumentation zu revidieren und ihren Inhalt jederzeit und ohne vorherige Ankündigung zu ändern.

Des Weiteren übernimmt Novell, Inc., für Software keinerlei Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder der Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc., das Recht vor, Novell-Software ganz oder teilweise jederzeit inhaltlich zu ändern, ohne dass für Novell, Inc., die Verpflichtung entsteht, Personen oder Organisationen von diesen Überarbeitungen oder Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie erkennen alle Ausfuhrkontrollbestimmungen an und erklären sich damit einverstanden, alle für anstehende Exporte, Re-Exporte oder Importe erforderlichen Lizenzen bzw. Klassifizierungen einzuholen. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen 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 Webseite Novell International Trade Services (http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Novell, Inc., besitzt Anrechte auf geistiges Eigentum für Technologie, die in das in dieser Dokumentation beschriebene Produkt integriert ist. Diese Rechte auf geistiges Eigentum umfassen möglicherweise insbesondere ein oder mehrere Patente in den USA, die auf der Webseite "Legal Patents" von Novell (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

Das funktionsbasierte Bereitstellungsmodul für Novell® Identity Manager 3.6 umfasst eine Identity Manager-Benutzeranwendung mit funktionsbasierter Bereitstellung. In diesem Handbuch wird die Installation des funktionsbasierten Bereitstellungsmoduls für Novell Identity Manager 3.6 beschrieben. Es behandelt folgende Themen:

Zielgruppe

Dieses Handbuch richtet sich an Administratoren und Berater, die für die Planung und Implementierung des funktionsbasierten Bereitstellungsmoduls für Identity Manager zuständig sind.

Rückmeldungen

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

Zusätzliche Dokumentation

Weitere Dokumentation zur Verwendung des funktionsbasierten Bereitstellungsmoduls für Identity Manager finden Sie auf der Website mit der Dokumentation zu Identity Manager (http://www.novell.com/documentation/lg/dirxmldrivers/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 (z. B. Linux* oder UNIX*), sollten die von der Software benötigten Schrägstriche verwenden.

Überblick

1

Dieser Abschnitt bietet einen Überblick über die Installation sowie eine Beschreibung der Systemanforderungen. Es werden u. a. folgende Themen erläutert:

1.1 Überblick über die Installation

Bei der Installation des funktionsbasierten Bereitstellungsmoduls für Novell® Identity Manager 3.6 werden sowohl eine Benutzeranwendung, die Funktionen unterstützt, als auch das funktionsbasierte Bereitstellungsmodul installiert. Bei der Installation werden die folgenden Schritte ausgeführt:

1. Bei einer Migration auf das funktionsbasierte Bereitstellungsmodul für Identity Manager lesen Sie bitte das *Identity Manager-Benutzeranwendung: Migrationshandbuch* (http://www.novell.com/documentation/idmrbpm36/pdfdoc/migration/migration.pdf).
2. Sicherstellen, dass die Systemanforderungen erfüllt werden. Weitere Informationen hierzu finden Sie unter Abschnitt 1.3, „Systemvoraussetzungen“, auf Seite 10.
3. Installation des Identity Manager-Metaverzeichnisses. Anleitungen finden Sie im *Identity Manager 3.5.1 Installationshandbuch* (http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf). Der Identity Manager-Metaverzeichnis-Server muss installiert sein, damit Sie die erforderlichen Treiber erstellen und die Benutzeranwendung sowie das funktionsbasierte Bereitstellungsmodul installieren können.
4. Erfüllen der Voraussetzungen für die Installation. Weitere Informationen hierzu finden Sie unter Kapitel 2, „Voraussetzungen für die Installation“, auf Seite 19.
5. Extrahieren der Datei `prerequisitefiles.zip` im Download-Verzeichnis. Manuelle Installation bzw. Anwendung der extrahierten Dateien.
6. Wenn Sie Designer zum Erstellen und Konfigurieren von Treibern verwenden möchten, installieren Sie Designer 2.1.1. Weitere Informationen hierzu finden Sie unter „Installing Designer“. (http://www.novell.com/documentation/designer21/admin_guide/index.html?page=/documentation/designer21/admin_guide/data/gsinstall.html).
7. Erstellen des Benutzeranwendungstreibers in iManager oder Designer 2.1.1. Anleitungen zum Erstellen des Treibers in iManager finden Sie in Abschnitt 3.1, „Erstellen des Benutzeranwendungstreibers in iManager“, auf Seite 33.

   Der Benutzeranwendungstreiber muss bereits vorhanden sein (aber nicht aktiviert), wenn Sie die Novell Identity Manager-Benutzeranwendung und das funktionsbasierte Bereitstellungsmodul installieren.
8. Erstellen des Funktionsservice-Treibers in iManager oder Designer 2.1.1. Anleitungen zum Erstellen des Treibers in iManager finden Sie in Abschnitt 3.2, „Erstellen des Funktionsservice-Treibers in iManager“, auf Seite 37.

   Der Funktionsservice-Treiber muss bereits vorhanden sein (aber nicht aktiviert), wenn Sie die Novell Identity Manager-Benutzeranwendung und das funktionsbasierte Bereitstellungsmodul installieren.

9 Installieren und Konfigurieren der Novell Identity Manager-Benutzeranwendung und des funktionsbasierten Bereitstellungsmoduls. Weitere Informationen hierzu finden Sie in:

- Kapitel 4, „Installation auf JBoss mithilfe einer GUI“, auf Seite 41
- Kapitel 5, „Installation von der Konsole aus oder mit einem einzigen Befehl“, auf Seite 73
- Kapitel 6, „Installation des WebSphere-Anwendungsservers“, auf Seite 83

Hinweis: Wenn Sie WebSphere* verwenden, müssen Sie die WAR-Datei manuell bereitstellen.

---

10 Ausführen der nach der Installation erforderlichen Aufgaben.

1.2 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*, DB2* 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. Unter WebSphere müssen Sie die WAR-Datei manuell bereitstellen.
- Aktivierung der Protokollierung von Novell Audit, sofern ausgewählt.
- Möglichkeit zum Importieren eines vorhandenen Master-Schlüssels zur Wiederherstellung einer bestimmten Installation des funktionsbasierten Bereitstellungsmoduls und zur Unterstützung von Clustern.

Das Installationsprogramm kann auf drei Arten gestartet werden:

- Über die grafische Benutzeroberfläche. Informationen finden Sie unter Kapitel 4, „Installation auf JBoss mithilfe einer GUI“, auf Seite 41 oder Kapitel 6, „Installation des WebSphere-Anwendungsservers“, auf Seite 83.
- Über die Konsolenschnittstelle (Befehlszeile). Weitere Informationen hierzu finden Sie unter Abschnitt 5.1, „Installation der Benutzeranwendung von der Konsole aus“, auf Seite 73.
- Automatische Installation. Siehe Abschnitt 5.2, „Installation der Benutzeranwendung mit einem einzigen Befehl“, auf Seite 73.

1.3 Systemvoraussetzungen

Für die Verwendung des funktionsbasierten Bereitstellungsmoduls für Novell Identity Manager 3.6 benötigen Sie jeweils eine der unter Tabelle 1-1 aufgeführten erforderlichen Komponenten.

Tabelle 1-1 *Systemvoraussetzungen*

Erforderliche Systemkomponente	Systemanforderungen	Hinweise
Metaverzeichnis-System (Identity Manager 3.5.1) ◆ Metaverzeichnis-Engine ◆ Novell Audit Agent ◆ Service-Treiber ◆ Identity Manager-Treiber ◆ Dienstprogramme (einschließlich Anwendungs-Dienstpro-grammen und dem Werkzeug für das Novell Audit-Setup)	Eines der folgenden Betriebssysteme: ◆ Netware® 6.5 SP6 ◆ Novell Open Enterprise Server (OES) 1.0 mit dem neuesten Support Pack ◆ Novell Open Enterprise Server (OES) 2.0 ◆ Windows* 2000 Server mit dem neuesten Service Pack (32 Bit) ◆ Windows Server 2003 mit dem neuesten Service Pack (32 Bit) ◆ Linux Red Hat 3.0, 4.0 oder 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 oder 5.3 Eine der folgenden Versionen von eDirectory™: ◆ eDirectory 8.7.3.10 ◆ eDirectory 8.8.1 oder 8.8.2 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=52670386&stateId=1%200%204926187)).

Erforderliche Systemkomponente	Systemanforderungen	Hinweise
Webbasierter Administrationsserver ◆ Passwortsynchronisierung ◆ iManager 2.6 und Plugins ◆ iManager 2.7 und Plugins ◆ Treiberkonfigurationen	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 oder 5.0 ES oder AS (32- und 64-Bit-Unterstützung) ◆ Solaris* 9 oder 10 mit dem neuesten Support Pack ◆ SUSE Linux Enterprise Server 9 oder 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 oder 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.

Erforderliche Systemkomponente	Systemanforderungen	Hinweise
Sicherer Protokollserver ◆ Der sichere Protokoll-server ◆ Der Plattform-agent (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 oder 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) ◆ Linux Red Hat 3.0, 4.0 oder 5.0 ES oder AS (32 Bit oder 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 mit dem neuesten Support Pack (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 oder ES (32 Bit oder 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 oder 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

Erforderliche Systemkomponente	Systemanforderungen	Hinweise
Anwendungsserver für die Benutzer-anwendung	Die Benutzeranwendung kann auf JBoss* und WebSphere ausgeführt werden, wie unten beschrieben. Folgende Server unterstützen JBoss 4.0.5 GA: ◆ Novell Open Enterprise Server (OES) 1.0 SP2 oder das neueste Support Pack – nur Linux ◆ SUSE Linux Enterprise Server 9 SP2 (in OES 1.0 SP2 enthalten) oder 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) ◆ Windows 2003 SP1 Die Benutzeranwendung erfordert JRE* 1.5.0_14.	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 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=52670386&stateId=1%200%204926187)).

Erforderliche Systemkomponente	Systemanforderungen	Hinweise
Benutzeranwendungsbrowser	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 SP1 wird in den folgenden Umgebungen unterstützt: ◆ Windows 2000 Professional mit SP4 ◆ Windows XP mit SP2	
Datenbankserver für die Benutzeranwendung ◆ MySQL ◆ Oracle ◆ MS SQL ◆ DB2	Die folgenden Datenbanken werden mit JBoss unterstützt: ◆ MySQL Version 5.0.27 ◆ Oracle 9i (9.2.0.1.4) ◆ Oracle 10g Release 2 (10.2.0.1.0) ◆ 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 eine Reihe bestimmter 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.

Erforderliche Systemkomponente	Systemanforderungen	Hinweise
Arbeitsstationen ◆ Designer 2.1.1 for Identity Manager 3.5.1 ◆ Webzugriff auf iManager	Designer wurde auf folgenden Plattformen getestet: Windows: ◆ Windows 2000 Professional mit dem neuesten Service Pack ◆ Windows XP SP2 ◆ Microsoft Windows Vista Linux: ◆ SUSE Linux Enterprise Server 10 (nur Designer) ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 ◆ Red Hat Enterprise LinuxWS 4.0 (nur für Designer), Gnome* Standard ◆ Red Hat Fedora Core 5 (nur für Designer), Gnome Standard ◆ Novell Linux Desktop 9, KDE Standard	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

Erforderliche Systemkomponente	Systemanforderungen	Hinweise
Server für verbundenes System (Host auf einem separaten Server, auf dem Remote Loader ausgeführt wird) ◆ Remote Loader ◆ Remote Loader-Konfigurationswerkzeug (nur Windows) ◆ Novell Audit Agent ◆ Passwortsynchronisierungs-Agent ◆ Treiberschnittstellenmodul 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/idm35drivers).	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 oder 5.0 ES oder AS ◆ SUSE Linux Enterprise Server 9 oder 10 ◆ AIX 5.2L, Version 5.2 oder 5.3 Java Remote Loader-System: ◆ HP-UX* 11i ◆ OS/400 ◆ xOS* ◆ Es sollte auf jedem System verwendet werden können, auf dem JVM 1.4.2 oder höher installiert ist
Audit	Novell Audit 2.0.2	
Benutzeranwendung - SSO-Integration	Erfordert Novell Access Manager 3.0.1.	Enthält eine Version von saslsaml.jar, die mit JDK*1.5 erstellt wurde.

Voraussetzungen für die Installation

2

In diesem Abschnitt werden die Voraussetzungen für die Installation des funktionsbasierten Bereitstellungsmoduls für Identity Manager beschrieben. Es werden u. a. folgende Themen erläutert:

2.1 Das Java Development Kit

JBoss, WebSphere und das Identitätsdepot haben individuelle Java Development Kit-Anforderungen.

JBoss-Anwendungsserver: Verwenden Sie auf JBoss-Anwendungsservern das Java 2 Platform Standard Edition Development Kit Version 1.5.0_14.

Verwenden Sie diese Version des Sun JDK, um das Installationsprogramm des funktionsbasierten Bereitstellungsmoduls wie folgt zu starten:

Linux/Solaris:

```
$ /opt/jdk1.5.0_10/bin/java -jar IdmUserApp.jar
```

Windows:

```
C:\Novell\InstallFiles\> "C:\Program
Files\Java\jdk1.5.0_10\bin\java.exe" -jar IdmUserApp.jar
```

Wenn bei der Installation nach dem vollständigen Pfad Ihrer Java-Installation gefragt wird, geben Sie den Stammpfad des Sun JDK an. Der Stammpfad unter Linux könnte beispielsweise wie folgt lauten:

```
/opt/jdk1.5.0_10
```

Hinweis: SLES-Benutzer: Verwenden Sie nicht das IBM JDK, das mit SLES mitgeliefert wird. Diese Version ist mit einigen Aspekten der Installation nicht kompatibel.

WebSphere-Anwendungsserver: Verwenden Sie auf WebSphere*-Anwendungsservern das IBM JDK, das mit WebSphere Application Server 6.1.0.9 mitgeliefert wird, und wenden Sie die uneingeschränkten Richtliniendateien an. Wenden Sie das WAS JDK-Fixpack für 6.1.0.9 an.

Installationsprogramm für das Identitätsdepot (Metaverzeichnis): Das Installationsprogramm für das Identitätsdepot (Metaverzeichnis) installiert seine eigene Kopie des JVM auf allen Plattformen außer NetWare®. Unter NetWare verwendet das Identitätsdepot die Version von Java, die auf dem System installiert ist.

2.2 Installation des Identity Manager-Metaverzeichnisses

Installation des Identity Manager 3.5.1-Metaverzeichnisses. Anleitungen finden Sie im *Novell Identity Manager 3.5.1 Installationshandbuch* (http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf).

Gewähren Sie einem Administrator des funktionsbasierten Bereitstellungsmoduls für Identity Manager Zugriff auf das Identitätsdepot. Geben Sie hierzu in iManager dem Administrator Zugriff auf den Kontext, in dem sich die Benutzer des funktionsbasierten Bereitstellungsmoduls für Identity Manager befinden.

2.3 Installation des JBoss-Anwendungsservers

Wenn Sie den JBoss*-Anwendungsserver installieren möchten, führen Sie einen der folgenden Schritte aus:

- Laden Sie den JBoss 4.2.0-Anwendungsserver herunter und installieren Sie ihn gemäß den Anweisungen des Herstellers.
- Verwenden Sie das JbossMysql-Dienstprogramm, das mit dem Download des funktionsbasierten Bereitstellungsmoduls bereitgestellt wurde, um den JBoss-Anwendungsserver (und optional MySQL) zu installieren. Anleitungen finden Sie in Abschnitt 2.3.1, „Installation des JBoss-Anwendungsservers und der MySQL-Datenbank“, auf Seite 21.

Starten Sie den JBoss-Server erst, nachdem Sie das funktionsbasierte Bereitstellungsmodul für Identity Manager installiert haben. Das Starten des JBoss-Servers gehört zu den nach der Installation durchzuführenden Aufgaben.

RAM: Für den JBoss-Anwendungsserver sollten mindestens 512 MB RAM zur Verfügung stehen, wenn das funktionsbasierte Bereitstellungsmodul für Identity Manager ausgeführt wird.

Port: Notieren Sie den von Ihrem Anwendungsserver verwendeten Port, da das Installationsprogramm für das funktionsbasierte Bereitstellungsmodul danach fragt. (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 das funktionsbasierte Bereitstellungsmodul für Identity Manager und die `IDMPwdMgt.war`-Datei bereitstellen. Eine Anleitung zur Aktivierung von SSL finden Sie in der JBoss-Dokumentation. Stellen Sie außerdem sicher, dass der SSL-Port über die Firewall geöffnet ist. Informationen zur `IDMPwdMgt.war-Datei` finden Sie in Abschnitt 7.5, „Zugriff auf die externe Passwort-WAR“, auf Seite 114 und im *Administrationshandbuch zur IDM Benutzeranwendung* (http://www.novell.com/documentation/idmrbpm36/index.html).

2.3.1 Installation des JBoss-Anwendungsservers und der MySQL-Datenbank

Zum Installieren eines JBoss-Anwendungsservers und von MySQL auf Ihrem System können Sie das Dienstprogramm JbossMysql verwenden.

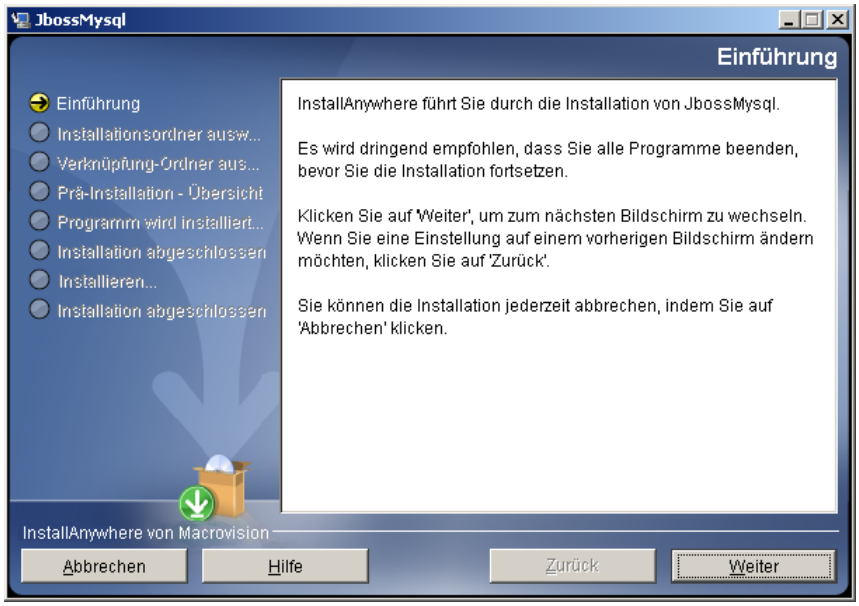
Hinweis: Das Dienstprogramm installiert den JBoss-Anwendungsserver jedoch nicht als Windows-Dienst. Informationen zur Installation des JBoss-Anwendungsservers als Dienst unter Windows finden Sie in Abschnitt 2.3.2, „Installation des JBoss-Anwendungsservers als Dienst“, auf Seite 23.

---

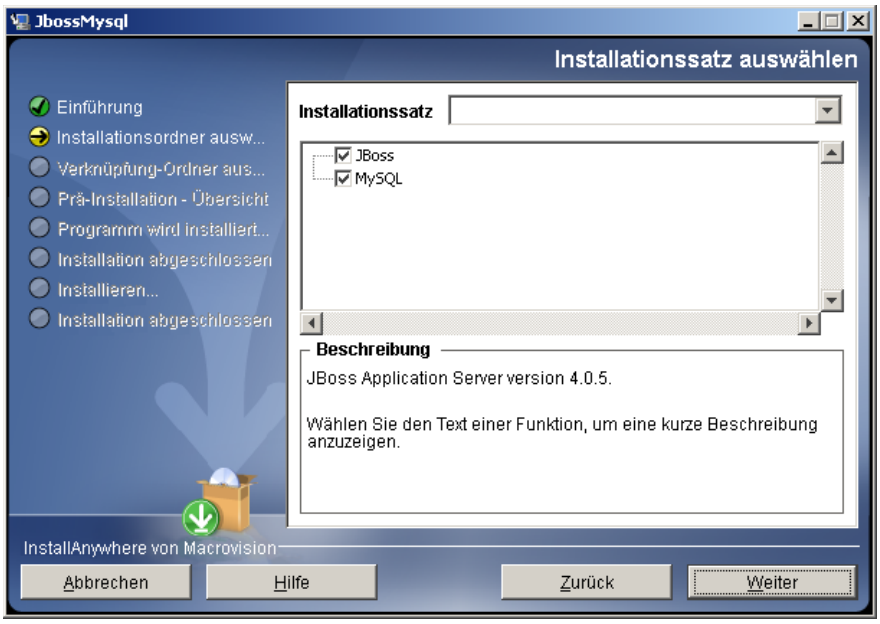
1. Führen Sie `JbossMysql.bin` oder `JbossMysql.exe` aus. Sie finden dieses Dienstprogramm mit dem Benutzeranwendungs-Installationsprogramm gebündelt unter

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

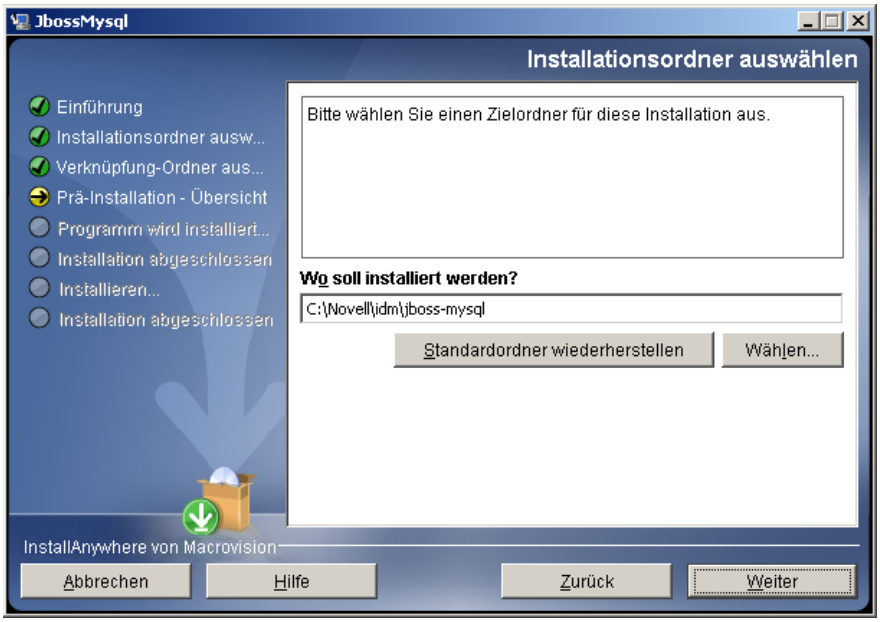
   Das Dienstprogramm ist für Solaris nicht verfügbar.
2. Wählen Sie Ihr Gebietsschema aus.
3. Lesen Sie die Einführung und klicken Sie anschließend auf *Weiter*.



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

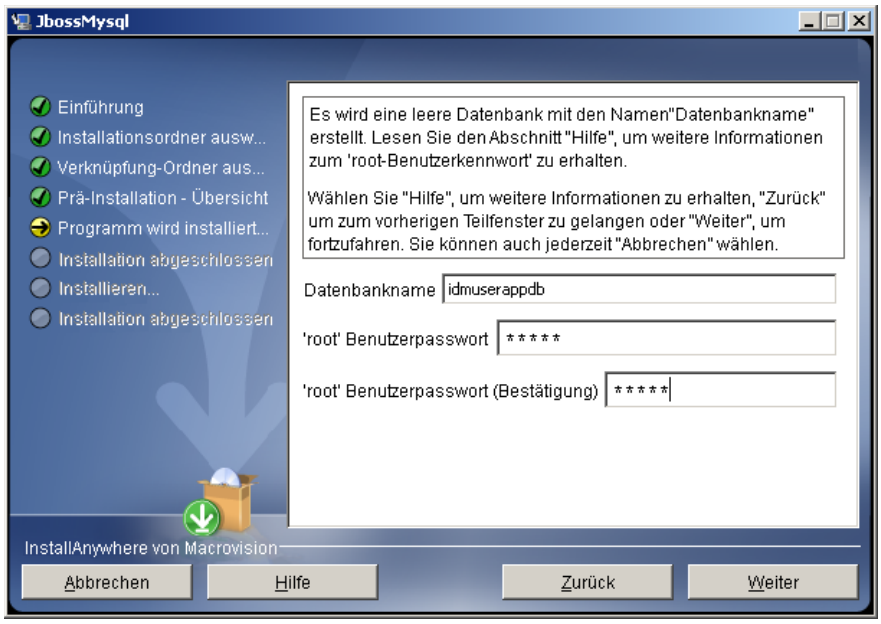


5 Klicken Sie zur Auswahl des Basisordners, in dem die ausgewählten Produkte installiert werden sollen, auf *Basisordner wählen* und anschließend auf *Weiter*.



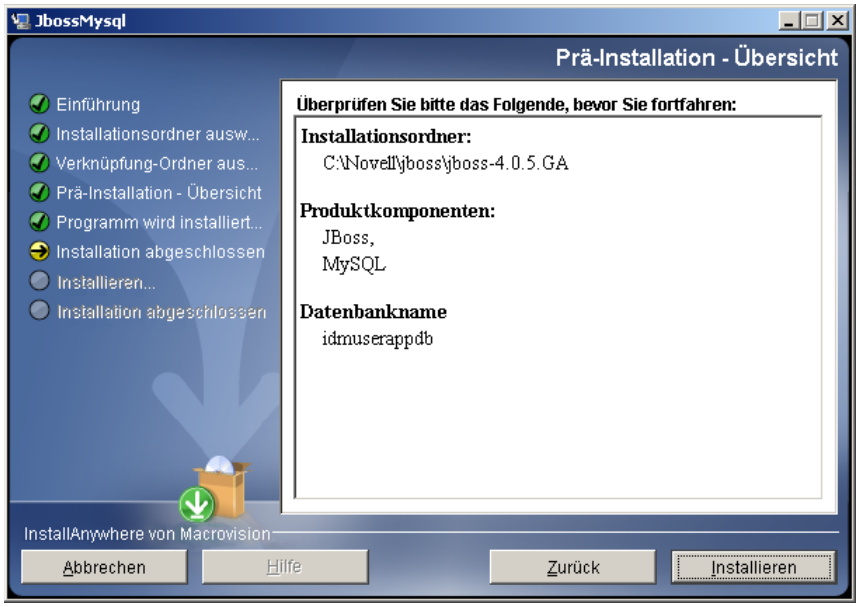
6 Legen Sie einen Namen für die Datenbank fest. Dieser Name ist bei der Installation der Benutzeranwendung erforderlich.

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 2.5.2, „Konfiguration der MySQL-Datenbank“, auf Seite 25 fort.

2.3.2 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).

Dieser Abschnitt umfasst folgende Themen:

- „Verwendung eines Java Service Wrapper“ auf Seite 24
- „Verwendung eines Dienstprogramms eines Drittanbieters“ auf Seite 24

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
```

Wichtig: 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.

Wichtig: 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).

2.4 Installation des WebSphere-Anwendungsservers

Wenn Sie planen, den WebSphere-Anwendungsserver zu verwenden, laden Sie den WebSphere 6.1.0.9-Anwendungsserver herunter und installieren Sie ihn. Wenden Sie das WAS JDK-Fixpack für 6.1.0.9 an.

2.5 Datenbanken

Installieren Sie Ihre Datenbank und den Datenbanktreiber und erstellen Sie eine Datenbank oder eine Datenbankinstanz. Notieren Sie die folgenden Datenbankparameter für die Installation des funktionsbasierten Bereitstellungsmoduls für Identity Manager:

- Host und Port
- Datenbankname, Benutzername und Benutzerpasswort

Eine Ursprungsdatei muss auf die Datenbank verweisen. Die Methode variiert je nach Anwendungsserver. Für JBoss erstellt das Installationsprogramm des funktionsbasierten Bereitstellungsmoduls für Identity Manager eine Anwendungsserver-Datenquelldatei, die auf die Datenbank verweist, und benennt die Datei anhand des Namens der WAR-Datei des funktionsbasierten Bereitstellungsmoduls für Identity Manager. Für WebSphere müssen Sie die Datenquelle vor der Installation manuell konfigurieren.

Datenbanken müssen UTF-8-fähig sein.

- Abschnitt 2.5.1, „Installation von MySQL“, auf Seite 25
- Abschnitt 2.5.2, „Konfiguration der MySQL-Datenbank“, auf Seite 25

2.5.1 Installation von MySQL

Lesen Sie Abschnitt 2.5.2, „Konfiguration der MySQL-Datenbank“, auf Seite 25, 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 des funktionsbasierten Bereitstellungsmoduls für Identity Manager nicht geöffnet sein. Starten Sie die Datenbank einfach, bevor Sie den Anwendungsserver starten.

2.5.2 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:

- „INNODB-Storage-Engine und Tabellentypen“ auf Seite 26
- „Zeichensatz“ auf Seite 26
- „Beachtung der Groß- und Kleinschreibung“ auf Seite 26

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.

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
```

Sie können auch den Zeichensatz für eine Datenbank bei ihrer Erstellung angeben, 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
```

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.

2.6 Sicherheitsvoraussetzungen

Sie können die gleichzeitige Abmeldung im funktionsbasierten Bereitstellungsmodul für Identity Manager ermöglichen, indem Sie die Option für die Cookieweiterleitung in Novell Access Manager™ oder iChain® aktivieren. Anleitungen hierzu finden Sie unter „Injecting into the Cookie Header“ (http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b5pqck8.html) im *Novell Access Manager 3.0 SP1 Administrationshandbuch*.

2.7 Herunterladen des Produkts

Sie können das funktionsbasierte Bereitstellungsmodul für Identity Manager 3.6 von der Website Novell Downloads (http://download.novell.com/index.jsp) herunterladen.

Laden Sie die richtige `.iso`-Image-Datei der Benutzeranwendung für Ihr System herunter: `Identity_Manager_3_6_0_User_Application_Provisioning.iso`

Die .iso-Datei enthält folgende Verzeichnisse:

`/linux/user_application` (für Linux)
`/nt/user_application` (für Windows)
`/solaris/user_application` (für Solaris)
`/36MetaDirSupport (enthält die erforderlichen Dateien für die Aktualisierung des IDM 3.5.1-Metaverzeichnisses zur Unterstützung der IDM 3.6-Benutzeranwendung)`

In Tabelle 2-1 sind alle Dateien und Skripts aufgeführt, die zur Installation des funktionsbasierten Bereitstellungsmoduls für Identity Manager 3.6 benötigt werden.

Tabelle 2-1 *Dateien und Skripts, die zur Installation der Identity Manager 3.6-Benutzeranwendung benötigt werden*

Datei	Beschreibung
`IDMProv.war`	Dies ist die WAR-Datei des funktionsbasierten Bereitstellungsmoduls. Sie enthält die Identity Manager 3.6-Benutzeranwendung mit Funktionen für die Identitätsselbstbedienung und das funktionsbasierte Bereitstellungsmodul.
`IDMUserApp.jar`	Dies ist das Installationsprogramm des funktionsbasierten Bereitstellungsmoduls.
`silent.properties`	Diese Datei enthält die Installationsparameter, die für eine automatische Installation erforderlich sind. Diese Parameter entsprechen den Installationsparametern, die Sie bei der Installation der GUI oder der Konsolenschnittstelle angegeben haben.
`prerequisitefiles.zip`	Diese ZIP-Datei enthält andere Dateien, die manuell installiert werden müssen.
`UserApplication_3_6_0-IDM3_5_1-V1.xml`	Dies ist die Konfigurationsdatei des Benutzeranwendungstreibers.

Datei	Beschreibung
iManager_icons_for_roles.zip	Diese Datei enthält die iManager-Symbole für Funktionsobjekte in eDirectory.

Tipp: Sie finden die Dateien iManager_icons_for_roles.zip und prerequisites.zip im Verzeichnis /36MetaDirSupport. Die anderen Dateien befinden sich im Verzeichnis < *Betriebssystem*> / user_application.

Das System, auf dem Sie das funktionsbasierte Bereitstellungsmodul für Identity Manager installieren, muss mindestens 320 MB verfügbaren Speicherplatz haben.

Der Standardinstallationsspeicherort lautet wie folgt:

- Linux oder Solaris: /opt/novell/idm
- Windows: C:\Novell\IDM

Sie können ein anderes Standardinstallationsverzeichnis während der Installation auswählen, es muss jedoch bereits vor Beginn der Installation vorhanden und beschreibbar sein (im Falle von Linux oder Solaris muss es außerdem von Nicht-Root-Benutzern beschreibbar sein).

2.8 Installation des Inhalts der prerequisitefiles.zip-Datei

Suchen Sie im heruntergeladenen .iso-Image die Datei prerequisitefiles.zip und extrahieren Sie diese. Sie enthält Dateien, die Sie manuell installieren müssen, wie in Tabelle 2-2 aufgeführt:

Tabelle 2-2 *Dateien, die manuell zu installieren sind*

Dateiname	Beschreibung	Anleitung
`nrf-extensions.sch`	eDirectory™-Schemadatei	Abschnitt 2.8.1, „Erweiterung des eDirectory-Schemas für das funktionsbasierte Bereitstellungsmodul Version 3.6“, auf Seite 29
`nrfdriver.jar`	Funktionsservice-Treiber-Jar-Datei	Abschnitt 2.8.2, „Kopieren der JAR-Datei für den Funktionsservice-Treiber“, auf Seite 30
`RoleService-IDM3_5_1-V1.xml`	Funktionsservice-Treiber-Konfigurationsdatei	Abschnitt 2.8.3, „Kopieren der Funktionsservice-Treiber-Konfigurationsdatei“, auf Seite 31
`UserApplicationn_3_6_0-IDM3_5_1-V1.xml`	Konfigurationsdatei für den Benutzeranwendungstreiber, die das funktionsbasierte Bereitstellungsmodul unterstützt	Abschnitt 2.8.4, „Kopieren der Benutzeranwendungstreiber-Konfigurationsdatei“, auf Seite 31
`dirxml.lsc`	Protokoll-Schemadatei der Protokollierungsanwendung	Abschnitt 2.8.5, „Kopieren der dirxml.lsc-Datei“, auf Seite 31

- Abschnitt 2.8.1, „Erweiterung des eDirectory-Schemas für das funktionsbasierte Bereitstellungsmodul Version 3.6“, auf Seite 29
- Abschnitt 2.8.2, „Kopieren der JAR-Datei für den Funktionsservice-Treiber“, auf Seite 30
- Abschnitt 2.8.3, „Kopieren der Funktionsservice-Treiber-Konfigurationsdatei“, auf Seite 31
- Abschnitt 2.8.4, „Kopieren der Benutzeranwendungstreiber-Konfigurationsdatei“, auf Seite 31
- Abschnitt 2.8.5, „Kopieren der dirxml.lsc-Datei“, auf Seite 31

2.8.1 Erweiterung des eDirectory-Schemas für das funktionsbasierte Bereitstellungsmodul Version 3.6

Erweitern Sie das eDirectory-Schema für das funktionsbasierte Bereitstellungsmodul, wie in den folgenden Abschnitten beschrieben:

- „Erweiterung des Schemas unter Windows“ auf Seite 29
- „Erweiterung des Schemas unter UNIX/Linux“ auf Seite 30
- „Erweiterung des Schemas unter NetWare“ auf Seite 30

Erweiterung des Schemas unter Windows

Erweitern Sie das Schema auf Windows-Servern mithilfe von `NDSCons.exe`. Mit eDirectory mitgelieferte Schemadateien (*.sch) werden standardmäßig im Verzeichnis `C:\Novell\NDS` installiert.

1 Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung* > *Novell eDirectory Services*.

2 Klicken Sie auf *install.dlm* und anschließend auf *Starten*.

3 Klicken Sie auf *Zusätzliche Schemadateien installieren* und dann auf *Weiter*.

4 Melden Sie sich als Benutzer mit Administratorrechten an und klicken Sie dann auf *OK*.

5 Geben Sie den Pfad und den Namen der Schemadatei an (zum Beispiel `c:\Novell\NDS\nrf-extensions.sch`).

6 Klicken Sie auf *Fertig stellen*.

Erweiterung des Schemas unter UNIX/Linux

Führen Sie zur Erweiterung des eDirectory-Schemas für das funktionsbasierte Bereitstellungsmodul auf einer UNIX/Linux-Plattform folgende Schritte aus:

1 Fügen Sie die Schemadatei des funktionsbasierten Bereitstellungsmoduls, `nrf-extensions.sch`, hinzu. Geben Sie hierzu den Befehl `ndssch` auf der Befehlszeile ein:

```
ndssch [-h Hostname[: Port]] [-t Baumname] admin-FDN
schemafilename.sch
```

Erweiterung des Schemas unter NetWare

Erweitern Sie das Schema auf NetWare-Servern mithilfe von `NWConfig.nlm`. Mit eDirectory mitgelieferte Schemadateien (*.sch) werden standardmäßig im Verzeichnis `sys:\system\schema` installiert.

1 Geben Sie `nwconfig` an der Serverkonsole ein.

2 Wählen Sie *Directory-Optionen* > *Schema erweitern*.

3 Melden Sie sich als Benutzer mit Administratorrechten an.

4 Drücken Sie F3, um einen anderen Pfad anzugeben, und geben Sie dann `sys:\system\schema` (oder den Pfad Ihrer *.sch-Datei) und die Schemadatei `nrf-extensions.sch` ein.

5 Drücken Sie die `Eingabetaste`.

2.8.2 Kopieren der JAR-Datei für den Funktionsservice-Treiber

Installieren Sie den Funktionsservice-Treiber manuell auf dem Metaverzeichnis-Server. Kopieren Sie hierzu die ausführbare Funktionsservice-JAR-Datei, `nrfdriver.jar`, aus dem extrahierten `prerequisitefiles.zip`-Archiv in das für Ihr System korrekte Verzeichnis:

Tabelle 2-3 *Speicherort der Funktionsservice-Treiber-JAR-Datei*

Betriebssystem	Verzeichnis
UNIX (eDirectory 8.7.x)	`/usr/lib/dirxml/classes`
UNIX (eDirectory 8.8.x)	`/opt/novell/eDirectory/lib/dirxml/classes`
Windows	`<Laufwerk>:\novell\nds\lib`
NetWare	`SYS:SYSTEM\LIB`

2.8.3 Kopieren der Funktionsservice-Treiber-Konfigurationsdatei

Installieren Sie die Funktionsservice-Treiber-Konfigurationsdatei, `RoleService_IDM3_5_1-V1.xml`, manuell in das für Ihr System korrekte Verzeichnis:

Tabelle 2-4 *Speicherort der Funktionsservice-Treiber-Konfigurationsdatei*

Betriebssystem	Verzeichnis
Linux (eDirectory 8.7.x)	`/usr/lib/dirxml/classes`
Linux (eDirectory 8.8)	`/var/opt/novell/iManager/nps/DirXML.Drivers`
Windows	`C:\Programme\Novell\tomcat\webapps\nps\Dirxml.Drivers`
NetWare	`SYS:\tomcat\4\webapps\nps\Dirxml.Drivers`

2.8.4 Kopieren der Benutzeranwendungstreiber-Konfigurationsdatei

Installieren Sie die Benutzeranwendungstreiber-Konfigurationsdatei, `UserApplication_3_6_0-IDM3_5_1-V1.xml`, manuell in das für Ihr System korrekte Verzeichnis:

Tabelle 2-5 *Speicherort der Benutzeranwendungstreiber-Konfigurationsdatei*

Betriebssystem	Verzeichnis
Linux (eDir 8.7.x)	`/usr/lib/dirxml/classes`
Linux (eDir 8.8)	`/var/opt/novell/iManager/nps/DirXML.Drivers`
Windows	`C:\Programme\Novell\tomcat\webapps\nps\Dirxml.Drivers`
NetWare	`SYS:\tomcat\4\webapps\nps\Dirxml.Drivers`

2.8.5 Kopieren der dirxml.lsc-Datei

Kopieren Sie die Datei `dirxml.lsc` auf den Audit-Server. Befolgen Sie hierbei die Anweisungen im Abschnitt zum Einrichten der Protokollierung im Identity Manager Benutzeranwendung: Administrationshandbuch (http://www.novell.com/documentation/idmrbpm36/pdfdoc/agpro/agpro.pdf).

2.9 Installation der iManager-Symbole für Funktionen

Suchen Sie im heruntergeladenen .iso-Image die Datei `iManager_icons_for_roles.zip` und extrahieren Sie sie. Kopieren Sie die extrahierten Symboldateien in das Verzeichnis `nps/portal/modules/dev/images/dir`. Starten Sie iManager neu, sodass es die neuen Symbole verwendet.

Erstellen von Treibern

3

In diesem Abschnitt wird beschrieben, wie die zur Verwendung des funktionsbasierten Bereitstellungsmoduls erforderlichen Treiber erstellt werden. Es werden u. a. folgende Themen erläutert:

Wichtig: Sie müssen zuerst den Benutzeranwendungstreiber und anschließend den Funktionsservice-Treiber erstellen. Der Benutzeranwendungstreiber muss zuerst erstellt werden, da der Funktionsservice-Treiber den Funktionsdepot-Container (RoleConfig.AppConfig) im Benutzeranwendungstreiber referenziert.

Die zulässige Treiberkonfiguration lautet wie folgt:

- Sie können einen Funktionsservice-Treiber pro Treibersatz in iManager hinzufügen.
- Sie können einen Benutzeranwendungstreiber mit einem Funktionsservice-Treiber verknüpfen.
- Sie können eine Benutzeranwendung mit einem Benutzeranwendungstreiber verknüpfen.

3.1 Erstellen des Benutzeranwendungstreibers in iManager

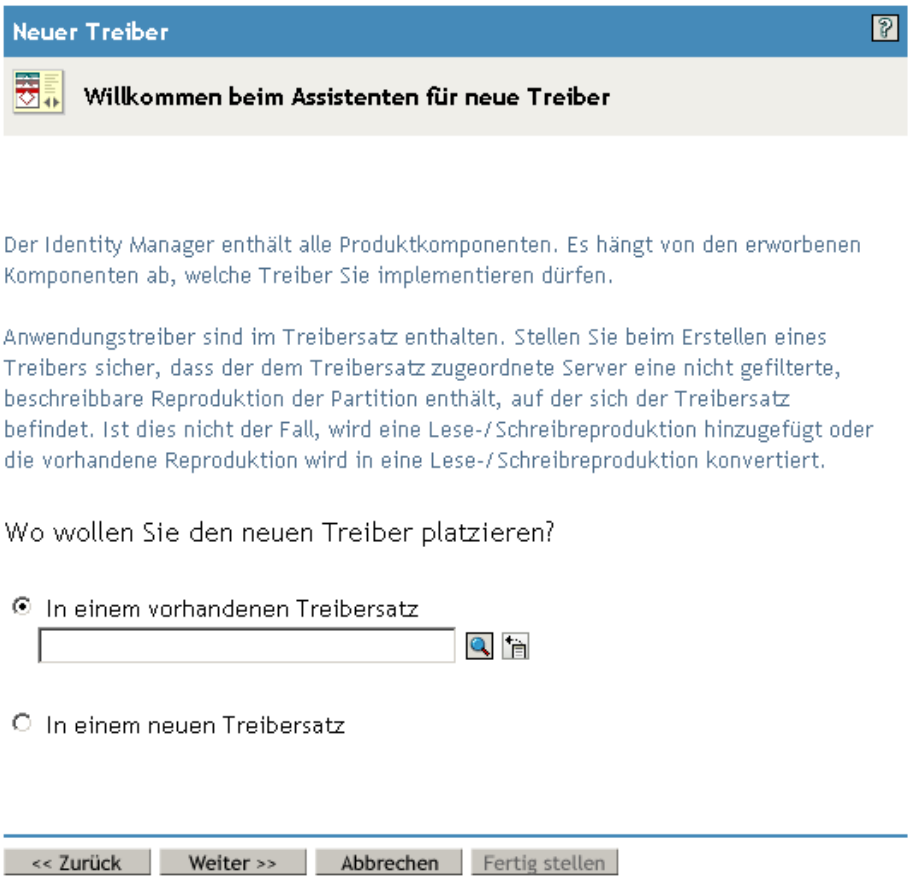
Sie müssen für jedes funktionsbasierte Bereitstellungsmodul für Identity Manager einen eigenen Benutzeranwendungstreiber erstellen, außer für funktionsbasierte Bereitstellungsmodule, die einem Cluster angehören. Funktionsbasierte Bereitstellungsmodule im selben Cluster müssen einen Benutzeranwendungstreiber gemeinsam verwenden. Weitere Informationen zum Ausführen des funktionsbasierten Bereitstellungsmoduls in einem Cluster finden Sie im *Administrationshandbuch zur Identity Manager -Benutzeranwendung* (http://www.novell.com/documentation/idmrbpm36/index.html).

Das funktionsbasierte Bereitstellungsmodul speichert anwendungsspezifische Daten im Benutzeranwendungstreiber, um die Anwendungsumgebung zu steuern und zu konfigurieren. Dazu gehören die Cluster-Informationen für den Anwendungsserver und die Workflow-Engine-Konfiguration.

Wichtig: Wird mehreren funktionsbasierten Bereitstellungsmodulen, die sich nicht in einem Cluster befinden, derselbe Treiber zugeordnet, führt dies bei einer oder mehreren Komponenten im funktionsbasierten Bereitstellungsmodul 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. Öffnen Sie iManager 2.6 oder höher in einem Webbrowser.
2. Wechseln Sie zu *Funktionen und Aufgaben* > *Identity Manager-Dienstprogramme* und wählen Sie *Neuer Treiber*, um den Assistenten zur Treibererstellung zu starten.

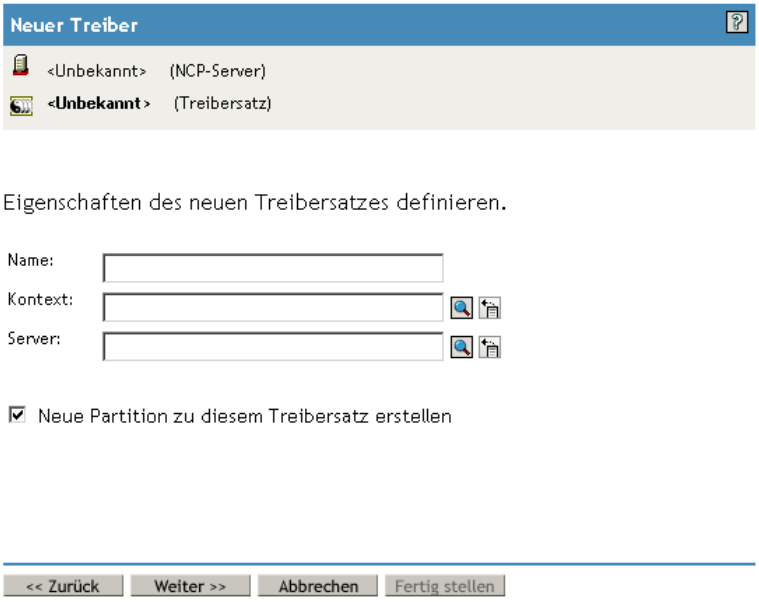


3 Wenn der Treiber in einem vorhandenen Treibersatz erstellt werden soll, wählen Sie die Option *In einem vorhandenen Treibersatz*. Klicken Sie anschließend auf das Symbol für die Objektauswahl, wählen Sie ein Treibersatzobjekt und klicken Sie auf *Weiter*. Fahren Sie dann mit Schritt 4 fort.

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. Beim Kontext handelt es sich um den eDirectory™-Kontext, in dem sich das Serverobjekt befindet.



3b Klicken Sie auf *Weiter*.

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

5 Wählen Sie *UserApplication_3_6_0-IDM3_5_1-V1.xml* aus der Dropdown-Liste aus. Hierbei handelt es sich um die Konfigurationsdatei für den Benutzeranwendungstreiber, die das funktionsbasierte Bereitstellungsmodul unterstützt.

Wenn *UserApplication_3_6_0-IDM3_5_1-V1.xml* nicht in dieser Dropdown-Liste enthalten ist, haben Sie die Datei nicht an den richtigen Speicherort kopiert. Lesen Sie hierzu bitte Abschnitt 2.8.4, „Kopieren der Benutzeranwendungstreiber-Konfigurationsdatei“, auf Seite 31.

6 Klicken Sie auf *Weiter*.

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 des funktionsbasierten Bereitstellungsmoduls 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. In diesem Feld muss eine Eingabe erfolgen.
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“.

Feld	Beschreibung
Host	Der Hostname oder die IP-Adresse des Anwendungsservers, auf dem die Identity Manager-Benutzeranwendung bereitgestellt wird. Wird die Benutzeranwendung 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*.

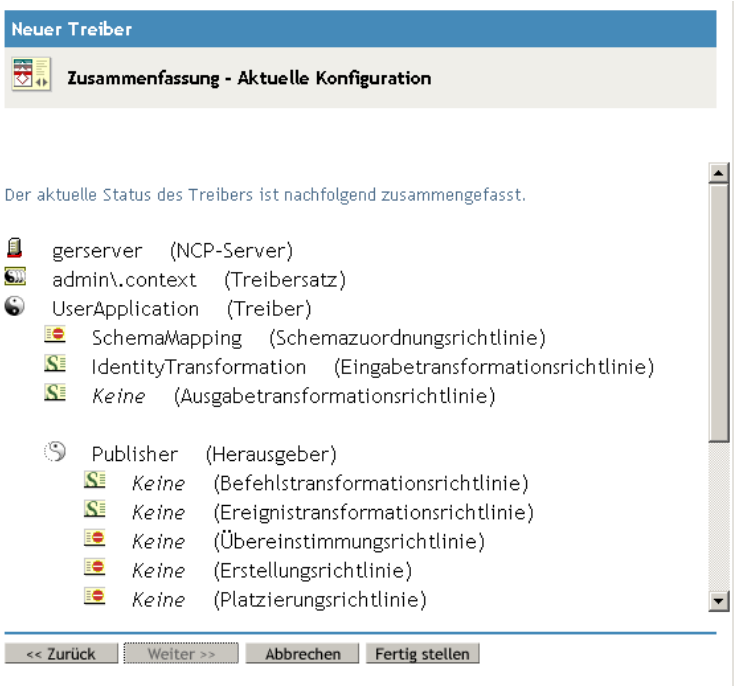
9 Klicken Sie zum Öffnen des Fensters „Sicherheitsäquivalenzen“ auf *Sicherheitsäquivalenzen definieren*. Wählen Sie einen Administrator oder ein anderes Supervisor-Objekt aus und klicken Sie auf *Hinzufügen*.

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*.

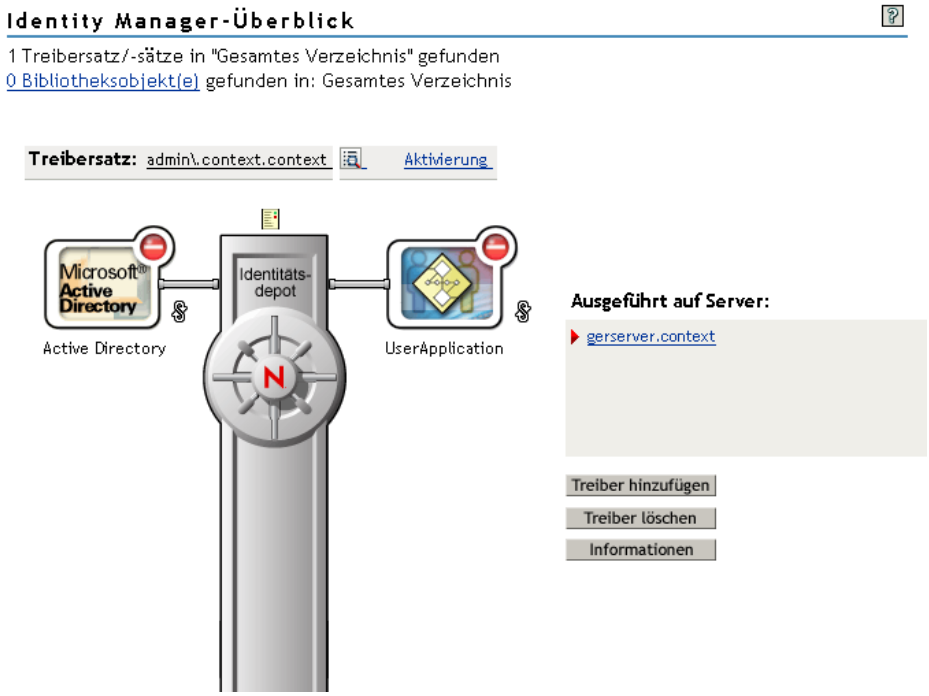
11 Klicken Sie auf *Hinzufügen*, wählen Sie die Benutzer aus, die von Treiberaktionen ausgeschlossen werden sollen (z. B. Verwaltungsfunktionen), klicken Sie zweimal auf *OK* und klicken Sie anschließend auf *Weiter*.

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



13 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 des funktionsbasierten Bereitstellungsmoduls.



3.2 Erstellen des Funktionsservice-Treibers in iManager

So erstellen und konfigurieren Sie den Funktionsservice-Treiber in iManager:

1 Öffnen Sie iManager 2.6 oder höher in einem Webbrowser.

2 Wählen Sie unter *Identity Manager* > *Identity Manager-Überblick* den Treibersatz aus, in dem Sie den Funktionsservice-Treiber installieren möchten.

   Installieren Sie den Benutzeranwendungstreiber, bevor Sie den Funktionsservice-Treiber installieren. Verwenden Sie Version 3.6 des Benutzeranwendungstreibers (`UserApplication_3_6_0-IDM3_5_1-V1.xml`) mit dem Funktionsservice-Treiber. Wenn Sie eine andere Version des Benutzeranwendungstreibers verwenden, ist der Funktionskatalog nicht verfügbar.

   Sie können nur einen Funktionsservice-Treiber pro Treibersatz verwenden.

3 Klicken Sie auf *Treiber hinzufügen*.

4 Übernehmen Sie im Assistenten für neue Treiber die Vorgabe *In einem vorhandenen Treibersatz*. Klicken Sie auf *Weiter*.

5 Wählen Sie *RoleService-IDM3_5_1-V1.xml* aus der Dropdown-Liste aus. Hierbei handelt es sich um die Konfigurationsdatei für den Funktionsservice-Treiber, die das funktionsbasierte Bereitstellungsmodul unterstützt.

Wenn *RoleService-IDM3_5_1-V1.xml* nicht in dieser Dropdown-Liste enthalten ist, haben Sie die Datei nicht an den richtigen Speicherort kopiert. Lesen Sie hierzu bitte Abschnitt 2.8.3, „Kopieren der Funktionsservice-Treiber-Konfigurationsdatei“, auf Seite 31.

Klicken Sie auf *Weiter*.

Es ist möglich, dass beim Erstellen des Treibers folgender Fehler angezeigt wird:

```
The following 'Namespace Exception' occurred while trying to access
the directory.  (CLASS_NOT_DEFINED)
```

In diesem Fall hat die iManager-Anwendung möglicherweise noch nicht Ihr neues Funktionsschema übernommen. Dieses neue Schema wird für den Funktionsservice-Treiber benötigt. Versuchen Sie, die iManager-Sitzung neu zu starten (schließen Sie alle Browser und melden Sie sich erneut bei iManager an). Sie können auch versuchen, den Server neu zu starten.

6 Machen Sie auf der Seite „Importinformationen angefordert“ die erforderlichen Angaben. Die erforderlichen Angaben sind in der folgenden Tabelle beschrieben.

Option	Beschreibung
Treibername	Geben Sie den Treibernamen an oder übernehmen Sie den vorgegebenen Namen, `Funktionsservice`, des Funktionsservice-Treibers. Wenn Sie einen neuen Treiber installieren, der denselben Namen wie ein vorhandener Treiber hat, überschreibt der neue Treiber die Konfiguration des vorhandenen Treibers. Mithilfe der Schaltfläche *Durchsuchen* können Sie die vorhandenen Treiber im ausgewählten Treibersatz anzeigen. In diesem Feld muss eine Eingabe erfolgen.
Benutzeranwendungstreiber-DN	Der eindeutige Name des Benutzeranwendungstreiberobjekts, das das Funktionssystem hostet. Verwenden Sie das eDirectory-Format (z. B. UserApplication.driverset.org) oder wählen Sie den Benutzer aus. In diesem Feld muss eine Eingabe erfolgen.
URL der Benutzeranwendung	Die URL, die zum Herstellen der Verbindung mit der Benutzeranwendung verwendet wird, um Genehmigungsworkflows zu starten. Die angegebene Beispiel-URL lautet *http://host:port/IDM*. In diesem Feld muss eine Eingabe erfolgen.

Option	Beschreibung
Benutzeranwendungsidentität	Der eindeutige Name des Objekts, das zum Authentifizieren der Benutzeranwendung verwendet wird, um Genehmigungsworkflows zu starten. Dies kann ein Benutzeranwendungsadministrator sein, dem Sie die erforderlichen Rechte zur Verwaltung des Benutzeranwendungsportals erteilen. Verwenden Sie das eDirectory-Format (z. B. admin.department.org) oder wählen Sie den Benutzer aus. In diesem Feld muss eine Eingabe erfolgen.
Benutzeranwendungspasswort	Geben Sie das Passwort für den in der Authentifizierungs-ID angegebenen Administrator der Benutzeranwendung ein. Das Passwort wird zum Authentifizieren der Benutzeranwendung verwendet, um Genehmigungsworkflows zu starten. In diesem Feld muss eine Eingabe erfolgen.
Wiederholen Sie das Passwort	Geben Sie das Passwort für den Benutzeranwendungsadministrator erneut ein.

7 Klicken Sie nach der Eingabe der Informationen auf *Fertig stellen*.

Installation auf JBoss mithilfe einer GUI

4

In diesem Abschnitt wird die Installation des funktionsbasierten Bereitstellungsmoduls für Identity Manager auf einem JBoss-Anwendungsserver über die grafische Benutzeroberfläche des Installationsprogramms erläutert. Wenn Sie das Modul lieber von der Konsole aus oder mithilfe eines einzelnen Befehls auf JBoss installieren möchten, lesen Sie Kapitel 5, „Installation von der Konsole aus oder mit einem einzigen Befehl“, auf Seite 73.

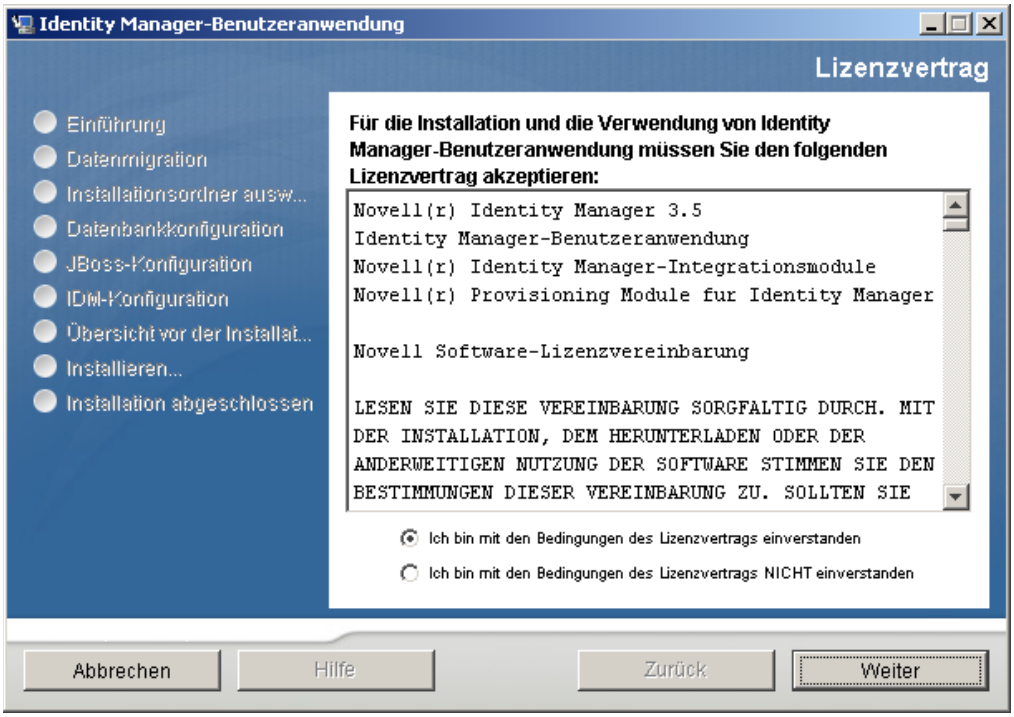
Wenn Sie die Installation lieber über die Befehlszeile durchführen möchten, lesen Sie Kapitel 5, „Installation von der Konsole aus oder mit einem einzigen Befehl“, auf Seite 73.

4.1 Starten der GUI des Installationsprogramms

1. Rufen Sie das Verzeichnis mit den in Tabelle 2-1 auf Seite 27 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 den Lizenzvertrag, klicken Sie zur Bestätigung auf die entsprechende Schaltfläche und klicken Sie anschließend auf *Weiter*.



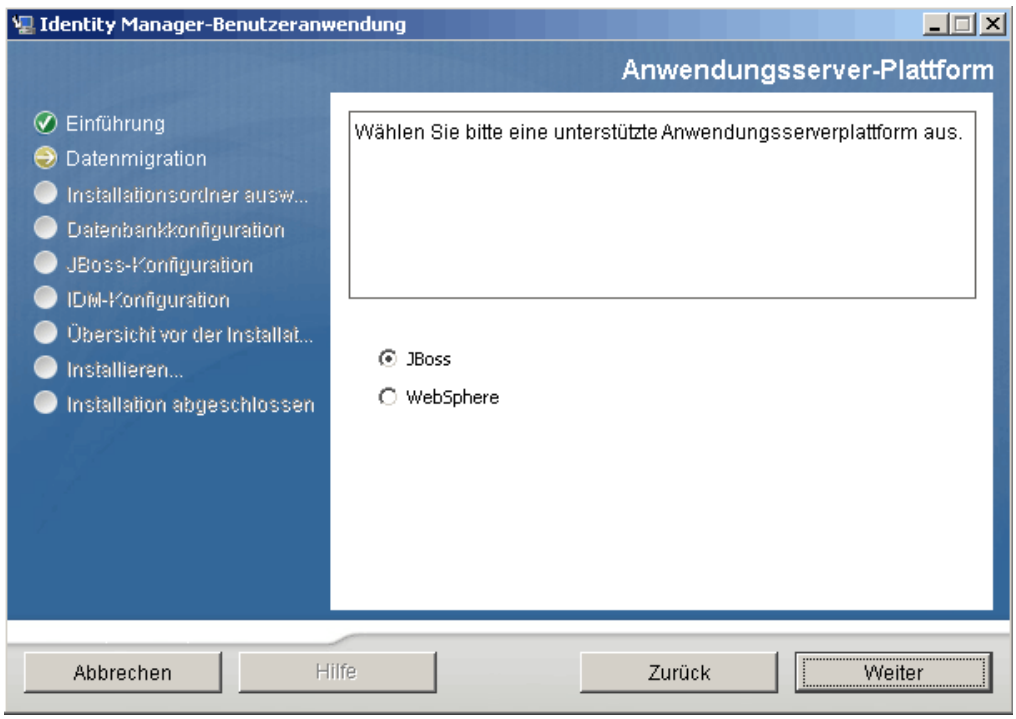
5 Lesen Sie die Einführungsseite des Installationsassistenten und klicken Sie anschließend auf *Weiter*.

6 Fahren Sie mit Abschnitt 4.2, „Auswahl einer Anwendungsserver-Plattform“, auf Seite 42 fort.

4.2 Auswahl einer Anwendungsserver-Plattform

Führen Sie den Vorgang aus, der in Abschnitt 4.1, „Starten der GUI des Installationsprogramms“, auf Seite 41 beschrieben ist, und fahren Sie dann mit den folgenden Schritten fort:

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



4.3 Migration einer Datenbank

1 Wenn Sie keine Datenbank migrieren möchten, klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 4.4, „Angabe des Speicherorts der WAR-Datei“, auf Seite 45 fort.

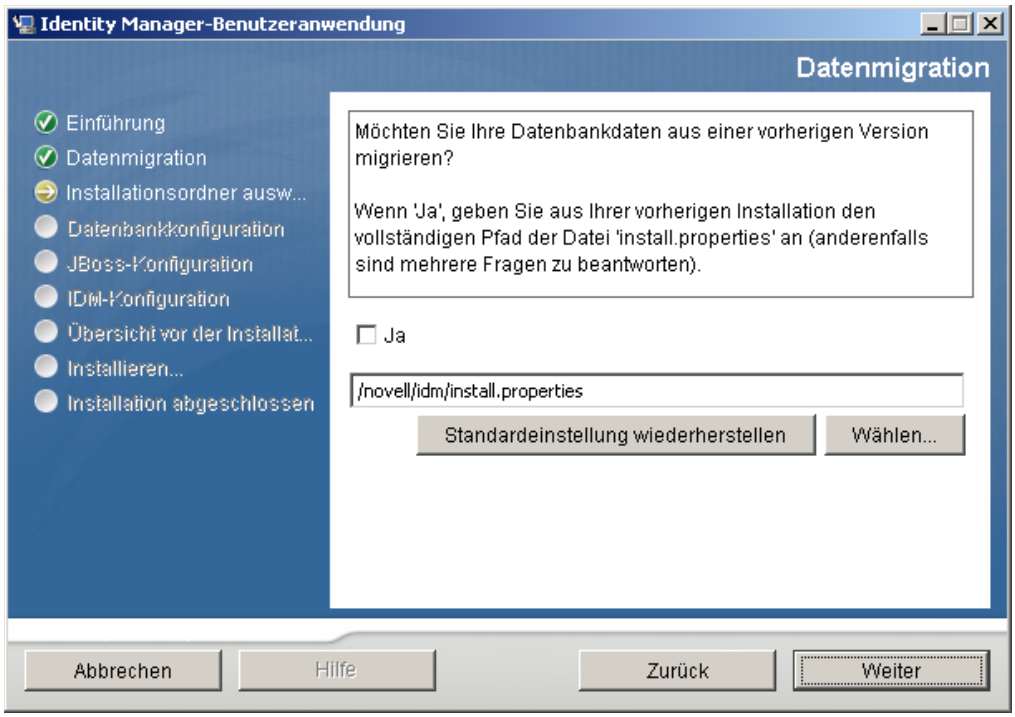
Wenn Sie weiterhin eine bestehende Datenbank der Version 3.0 oder 3.01 der Benutzeranwendung verwenden möchten, müssen Sie die Datenbank migrieren. Fahren Sie mit dem nächsten Schritt fort.

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

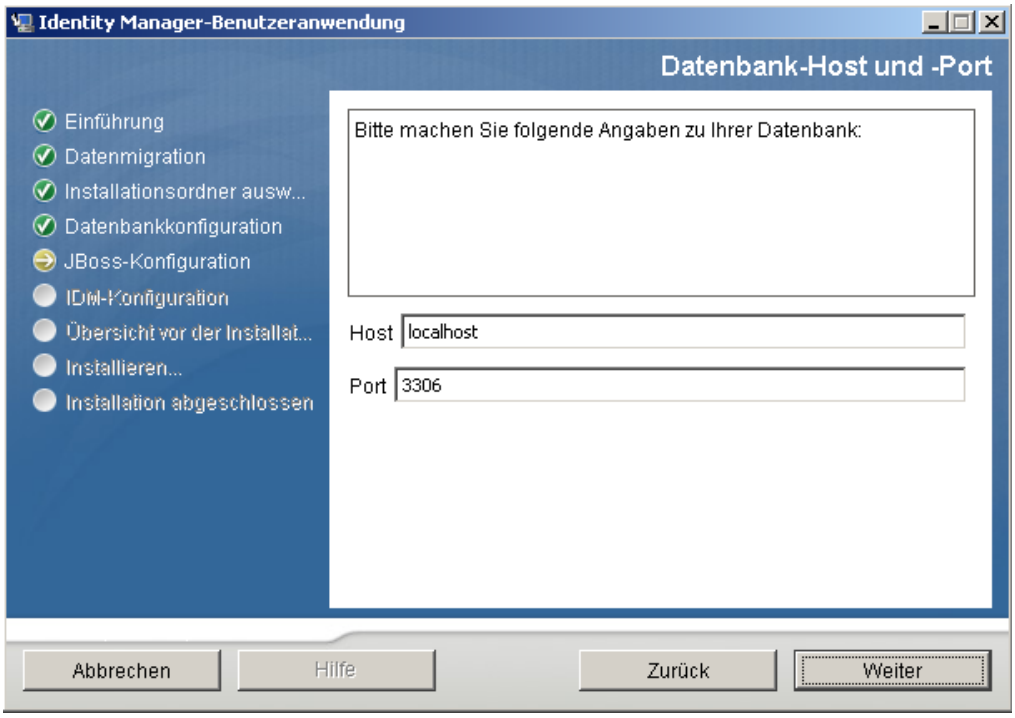
3 Klicken Sie auf der Seite „Datenmigration“ des Installationsprogramms auf *Ja*.

4 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.



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



6 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 4.4, „Angabe des Speicherorts der WAR-Datei“, auf Seite 45 oder Abschnitt 4.5, „Auswahl eines Installationsordners“, auf Seite 45 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/idmrbpm36/index.html).

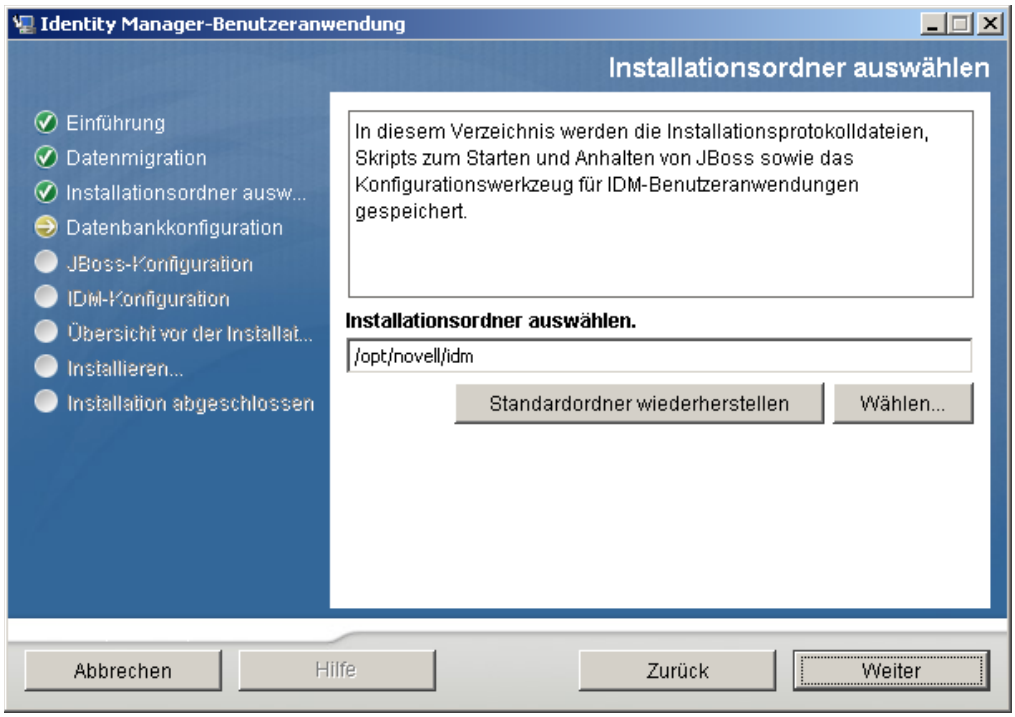
4.4 Angabe des Speicherorts der WAR-Datei

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 4.5, „Auswahl eines Installationsordners“, auf Seite 45 fort.

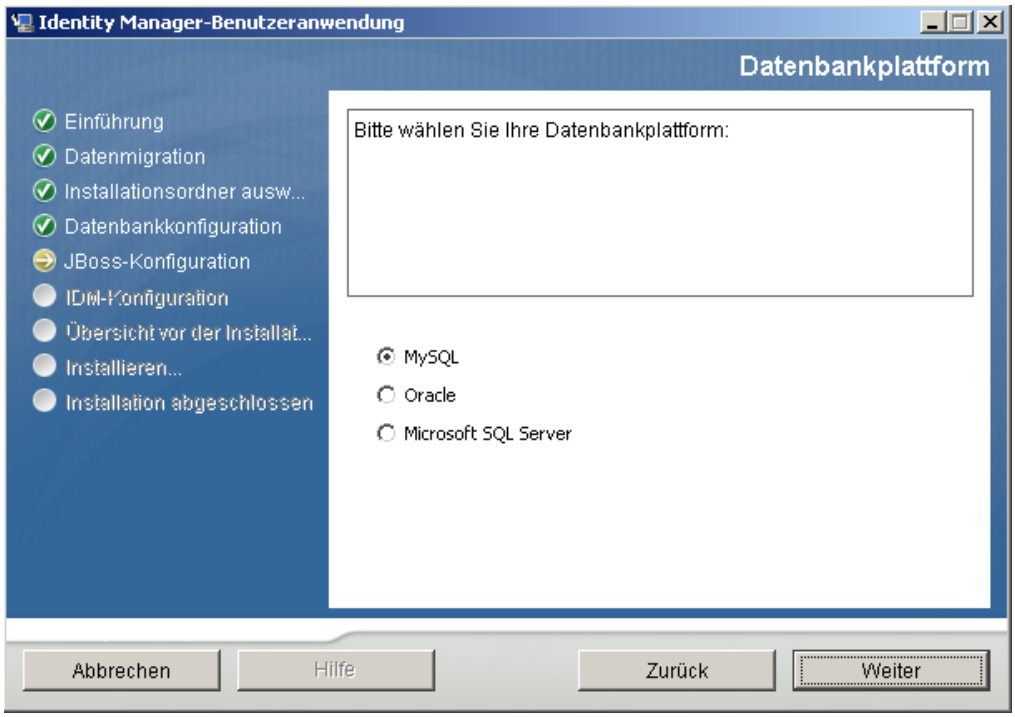
4.5 Auswahl eines Installationsordners

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 *Standardordner 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 4.6, „Auswahl einer Datenbankplattform“, auf Seite 46 fort.



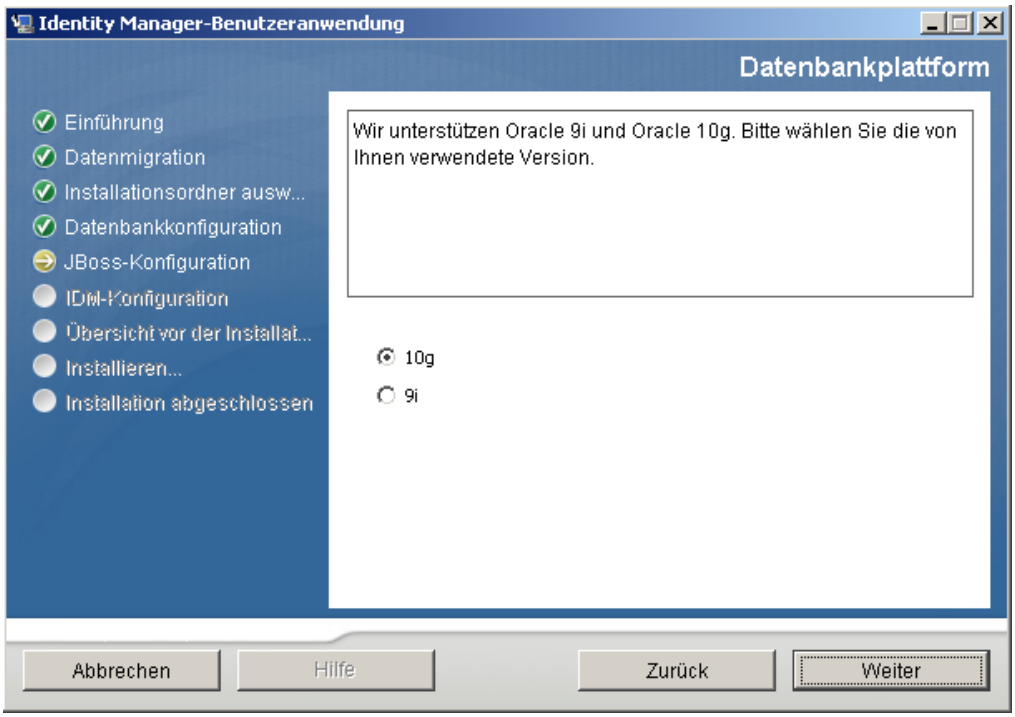
4.6 Auswahl einer Datenbankplattform

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.

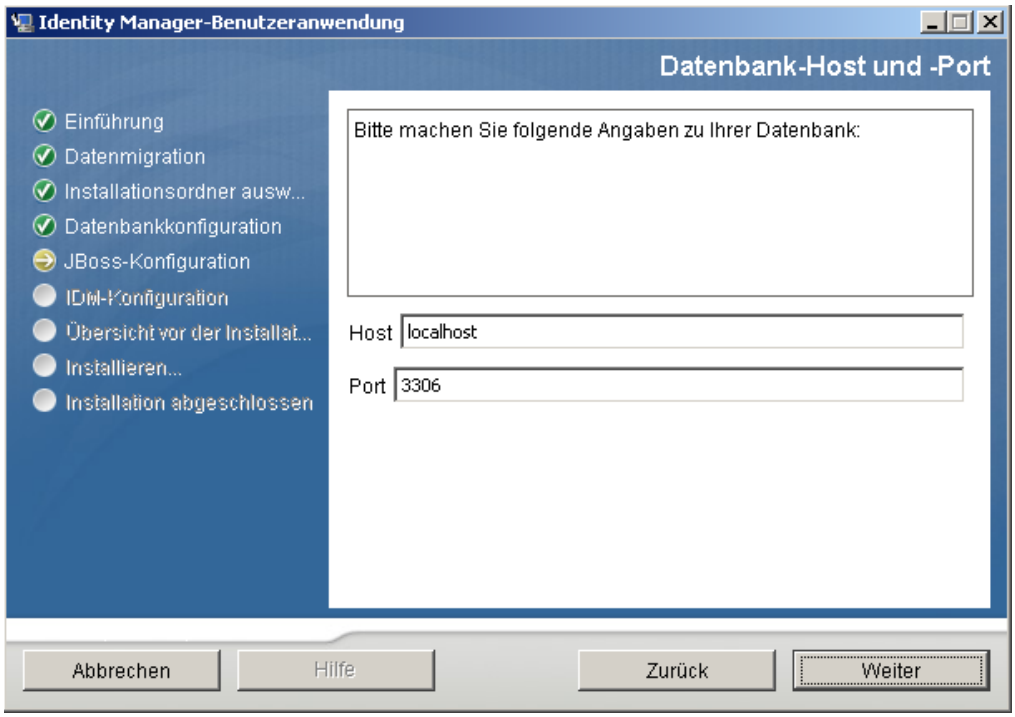
3 Bei Verwendung einer Oracle-Datenbank fragt Sie das Installationsprogramm nach deren Version. Wählen Sie die entsprechende Version aus.



4 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 4.7, „Angabe von Datenbank-Host und-Port“, auf Seite 47 fort.

4.7 Angabe von Datenbank-Host und-Port

1 Vervollständigen Sie die folgenden Felder:

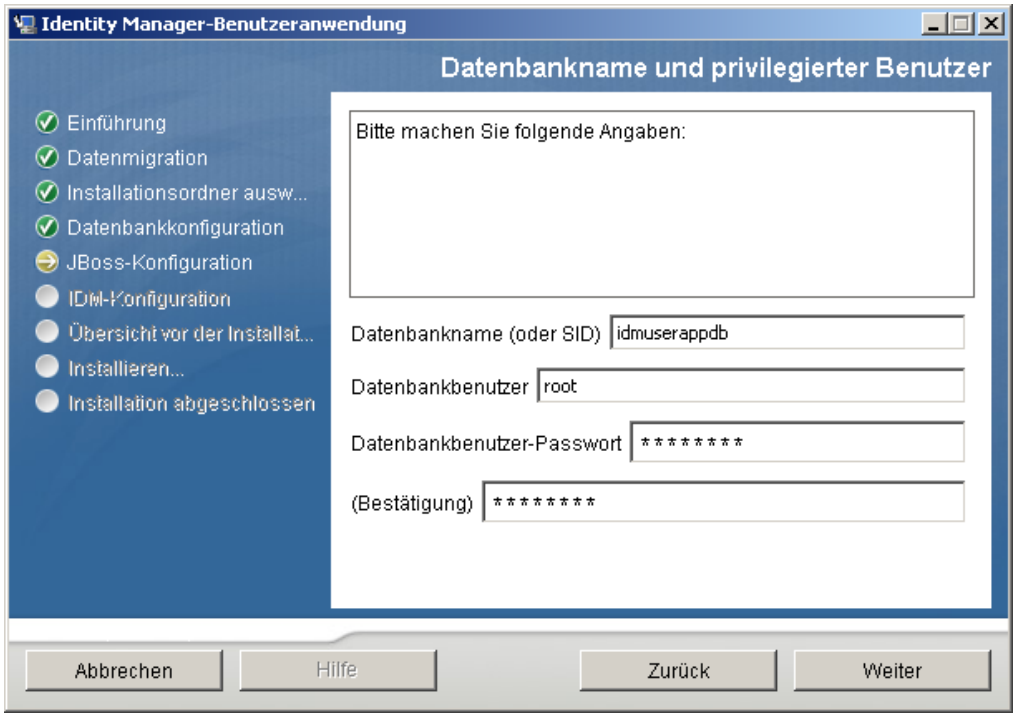


Feld	Beschreibung
Host	Geben Sie den Host oder die IP-Adresse des Datenbankservers an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Hostname bzw. dieselbe IP-Adresse angegeben werden.
Port	Geben Sie die Listener-Portnummer der Datenbank an. In einer Clusterkonfiguration muss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

2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 4.8, „Angabe des Datenbanknamens und des privilegiertes Benutzers“, auf Seite 48 fort.

4.8 Angabe des Datenbanknamens und des privilegiertes Benutzers

1 Vervollständigen Sie die folgenden Felder:

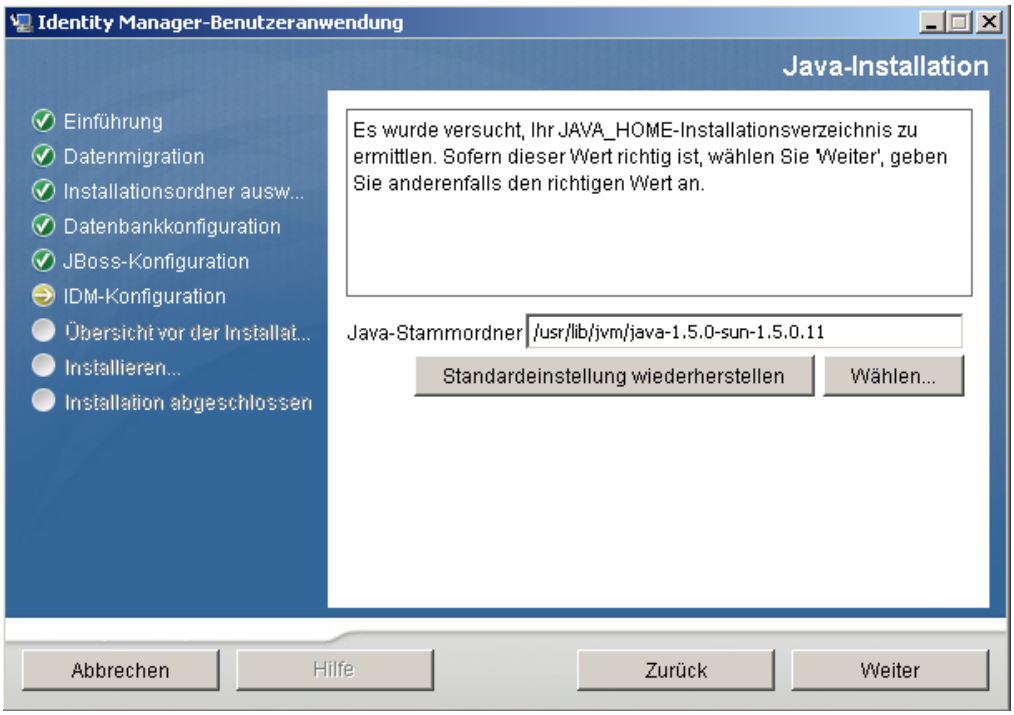


Feld	Beschreibung
Datenbankname (oder SID)	Geben Sie für MySQL oder MS SQL Server den Namen der vorkonfigurierten Datenbank an. Geben Sie für Oracle den zuvor erstellten Oracle System Identifier (SID) ein. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Datenbankname bzw. derselbe SID angegeben werden.
Datenbankbenutzer	Geben Sie den Datenbankbenutzer an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied dieselbe Datenbank angegeben werden.
Datenbankbenutzer-Passwort und Bestätigung	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 4.9, „Angabe des Java-Stammordners“, auf Seite 49 fort.

4.9 Angabe des Java-Stammordners

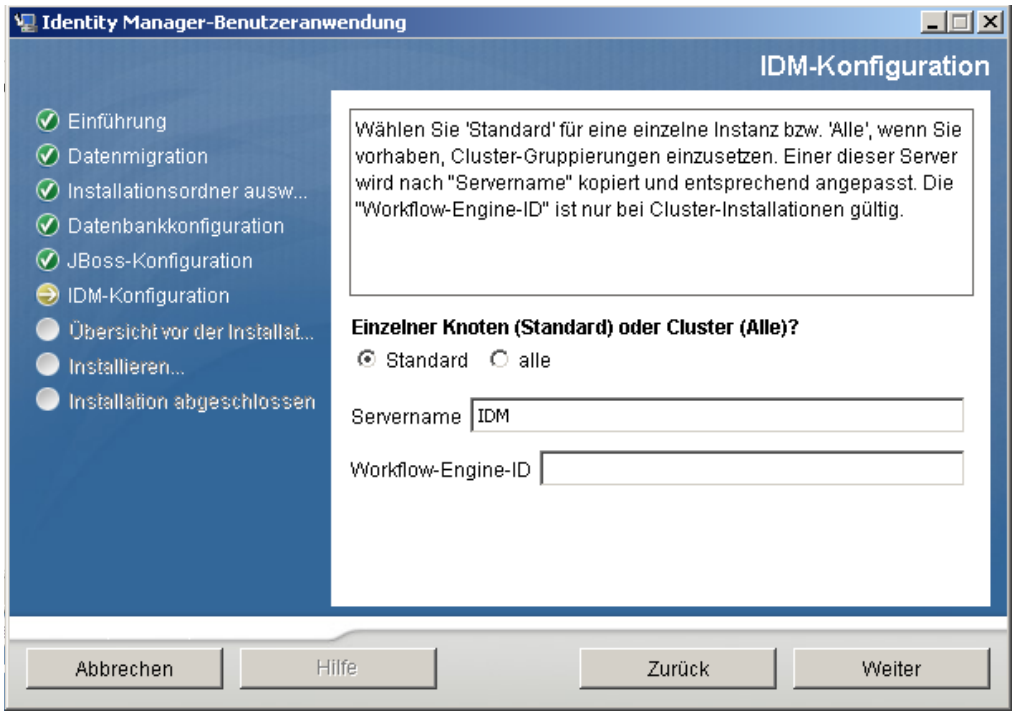
1 Klicken Sie zum Wechseln in den Java-Stammordner auf die Schaltfläche zum *Auswählen*. Wenn Sie den Standardspeicherort verwenden möchten, klicken Sie auf *Standardeinstellung wiederherstellen*.



2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 4.11, „Angabe der Einstellungen für den JBoss-Anwendungsserver“, auf Seite 52 fort.

4.10 Auswahl des Anwendungsserver-Konfigurationstyps

1 Füllen Sie die folgenden Felder aus:



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.
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.

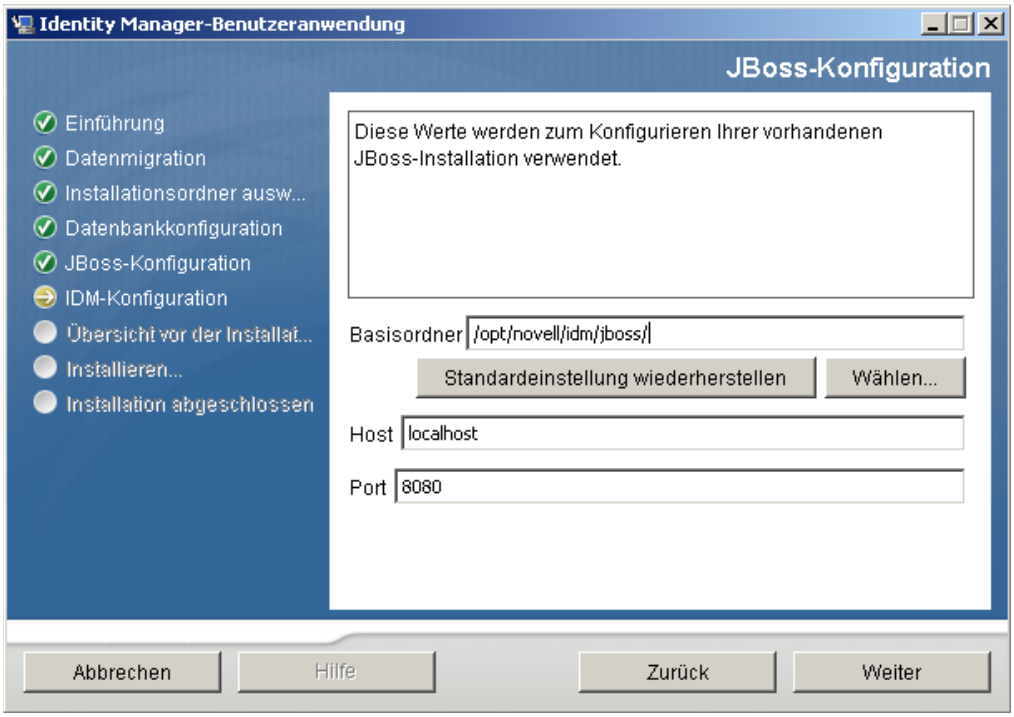
2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 4.12, „Aktivieren der Novell Audit-Protokollierung“, auf Seite 52 fort.

4.11 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 2.3.1, „Installation des JBoss-Anwendungsservers und der MySQL-Datenbank“, auf Seite 21.

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



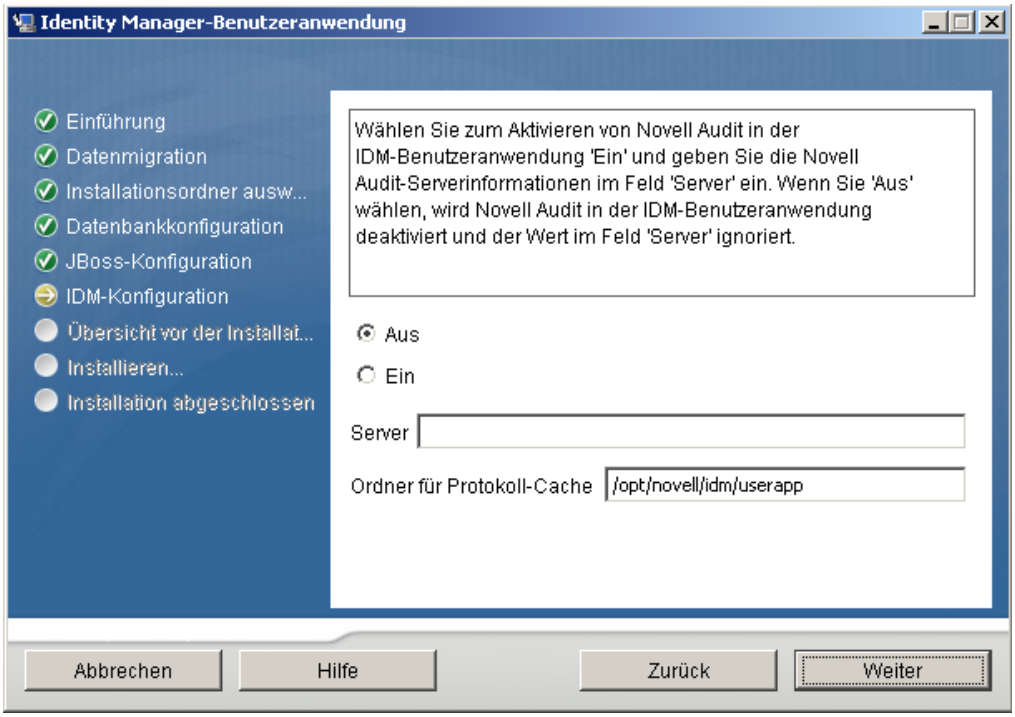
Feld	Beschreibung
Basisordner	Geben Sie den Speicherort des Anwendungsservers an.
Host	Geben Sie den Hostnamen oder die IP-Adresse des Anwendungsservers an.
Port	Geben Sie die Listener-Portnummer des Anwendungsservers an. Der JBoss-Standardport ist 8080.

2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 4.10, „Auswahl des Anwendungsserver-Konfigurationstyps“, auf Seite 50 fort.

4.12 Aktivieren der Novell Audit-Protokollierung

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

1 Füllen Sie die folgenden Felder aus:



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 den Karteireiter *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 4.14, „Konfiguration der Benutzeranwendung“, auf Seite 55 fort.

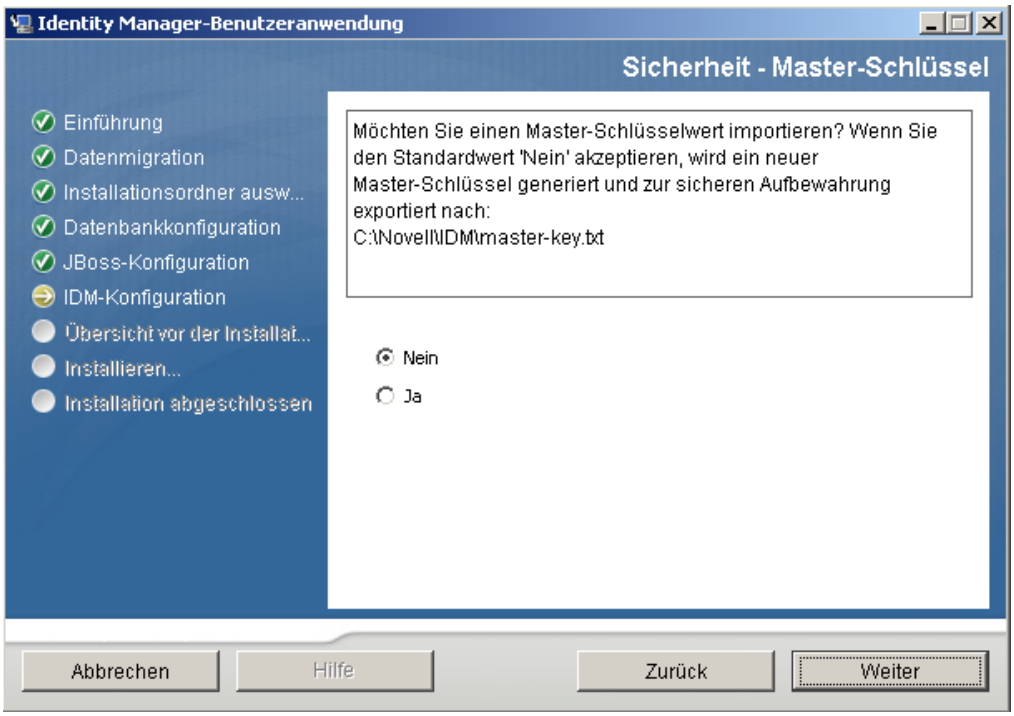
4.13 Angabe eines Master-Schlüssels

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 4.14, „Konfiguration der Benutzeranwendung“, auf Seite 55 fort. Nach Abschluss der Installation müssen Sie den Master-Schlüssel manuell speichern, wie in Abschnitt 7.1, „Aufzeichnen des Master-Schlüssels“, auf Seite 113 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*.

4.14 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 4-1 beschrieben an und fahren Sie dann mit Schritt 2 fort.

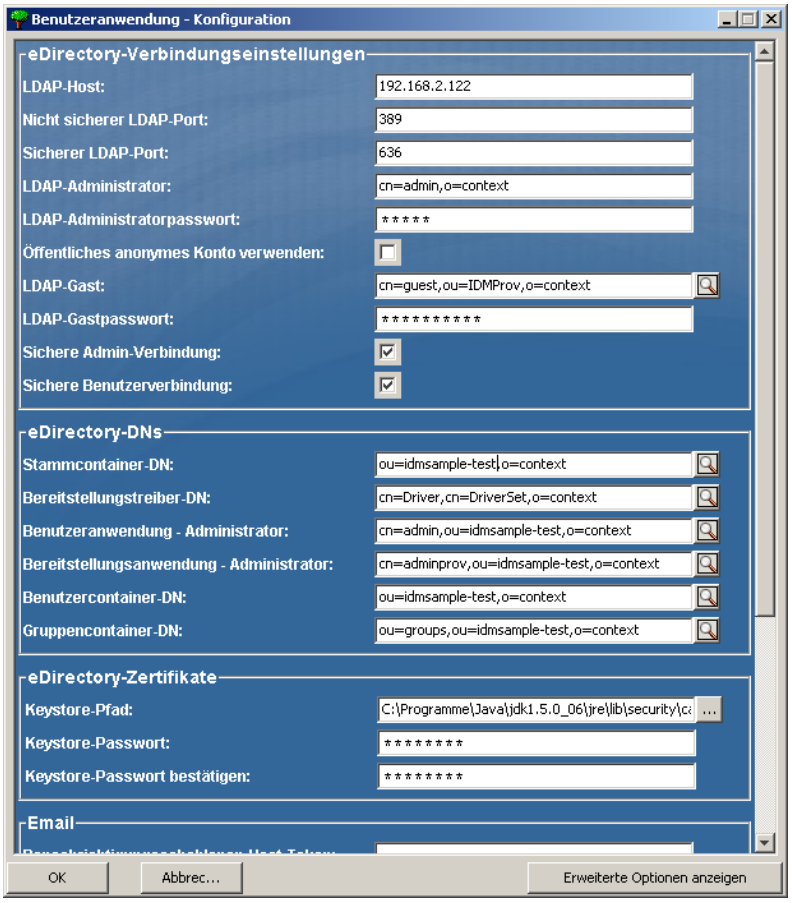

Benutzeranwendung - Konfiguration
eDirectory-Verbindungseinstellungen
LDAP-Host:
192.168.2.122
Nicht sicherer LDAP-Port:
389
Sicherer LDAP-Port:
636
LDAP-Administrator:
cn=admin,o=context
LDAP-Administratorpasswort:
*****
Öffentliches anonymes Konto verwenden:
LDAP-Gast:
cn=guest,ou=IDMProv,o=context
LDAP-Gastpasswort:
****
Sichere Admin-Verbindung:
Sichere Benutzerverbindung:
eDirectory-DNs
Stammcontainer-DN:
ou=idmsample-test,o=context
Bereitstellungstreiber-DN:
cn=Driver,cn=DriverSet,o=context
Benutzeranwendung - Administrator:
cn=admin,ou=idmsample-test,o=context
Bereitstellungsanwendung - Administrator:
cn=adminprov,ou=idmsample-test,o=context
Benutzercontainer-DN:
ou=idmsample-test,o=context
Gruppencontainer-DN:
ou=groups,ou=idmsample-test,o=context
eDirectory-Zertifikate
Keystore-Pfad:
C:\Programme\Java\jdk1.5.0_06\jre\lib\security\ca
Keystore-Passwort:
****
Keystore-Passwort bestätigen:
****
Email
OK
Abbrec...
Erweiterte Optionen anzeigen

Tabelle 4-1 *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 zum Deaktivieren des Gast-Benutzers das Kontrollkästchen *Öffentliches anonymes Konto verwenden*.
	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). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können.
	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). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können.

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 3.1, „Erstellen des Benutzeranwendungstreibers in iManager“, auf Seite 33 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 den Karteireiter *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	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 den Karteireiter *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)	*Funktionsadministrator*	Diese Funktion ist im funktionsbasierten Bereitstellungsmodul für Novell Identity Manager verfügbar. Mit dieser Funktion können Mitglieder alle Funktionen erstellen, entfernen oder modifizieren und Benutzern, Gruppen oder Containern Funktionen zuweisen oder entziehen. Außerdem können die Funktionsmitglieder damit einen Bericht für einen beliebigen Benutzer ausführen. Standardmäßig wird diese Funktion dem Benutzeranwendungsadministrator zugewiesen. Sie können die Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Funktionen* > *Funktionszuweisungen* in der Benutzeranwendung ändern.
	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	*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-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.
	'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 69.

Einstellungstyp	Feld	Beschreibung
	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 4-2 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 4-2 *Konfiguration der Benutzeranwendung: Alle Parameter*

Einstellungstyp	Feld	Beschreibung
eDirectory-Verbindungseinstellungen	*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). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können.
	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). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können.

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 3.1, „Erstellen des Benutzeranwendungstreibers in iManager“, auf Seite 33 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 den Karteireiter *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	Der Bereitstellungsanwendungsadministrator verwaltet die Bereitstellungs-Workflow-Funktionen, die in der Registerkarte *Anforderungen und Genehmigungen* der Benutzeranwendung zur Verfügung stehen. 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.
	Funktions-administrator	Diese Funktion ist im funktionsbasierten Bereitstellungsmodul für Novell Identity Manager verfügbar. Mit dieser Funktion können Mitglieder alle Funktionen erstellen, entfernen oder modifizieren und Benutzern, Gruppen oder Containern Funktionen zuweisen oder entziehen. Außerdem können die Funktionsmitglieder damit einen Bericht für einen beliebigen Benutzer ausführen. Standardmäßig wird diese Funktion dem Benutzeranwendungsadministrator zugewiesen. Sie können diese Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Funktionen* > *Funktionszuweisungen* in der Benutzeranwendung ändern.

Einstellungstyp	Feld	Beschreibung
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).
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.

Einstellungstyp	Feld	Beschreibung
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.
	Passwort für Herkunftsverbürgungsspeicher	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.
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.
Access Manager- und iChain-Einstellungen	*Gleichzeitige Abmeldung aktiviert*	Bei Auswahl dieser Option unterstützt die Benutzeranwendung die gleichzeitige Abmeldung von der Benutzeranwendung und dem Novell Access Manager bzw. iChain. Bei der Abmeldung leitet die Benutzeranwendung den Benutzer bei Vorhandensein eines Novell Access Manager™- oder iChain®-Cookies zur Seite für die gleichzeitige Abmeldung um.
	Seite 'Gleichzeitige Abmeldung'	Die URL für die Abmeldeseite von Novell Access Manager oder iChain, wobei die URL ein Hostname ist, den Novell Access Manager oder iChain erwartet. Wenn die gleichzeitige Abmeldung aktiviert ist und sich ein Benutzer von der Benutzeranwendung abmeldet, wird der Benutzer auf diese Seite umgeleitet. Eine der folgenden beiden URLs sollte die Funktion zum gleichzeitigen Abmelden abhängig von Ihrer Umgebung auf die richtige Seite umleiten: Access Manager: `https://IhrAccessGatewayServer/AGLogout` iChain: `https://IhriChainServer/cmd/ICSLogout`

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 69.
	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 *Novell iManager 2.6 Administrationshandbuch (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 4.16, „Überprüfen und Installieren der Einstellungen“, auf Seite 71 fort.

4.15 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.

- Abschnitt 4.15.1, „Angabe einer externen WAR-Datei für die Passwortverwaltung“, auf Seite 69
- Abschnitt 4.15.2, „Angeben einer internen Passwort-WAR-Datei“, auf Seite 70

4.15.1 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 7.4, „Konfiguration der SSL-Kommunikation zwischen JBoss-Servern“, auf Seite 114.

5 Führen Sie einen der folgenden Vorgänge aus:

   - Wenn Sie das Installationsprogramm verwenden, lesen Sie die Informationen in diesem Schritt und fahren Sie dann mit Schritt 6 auf Seite 70 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 auf Seite 70 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.

4.15.2 Angeben einer internen Passwort-WAR-Datei

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

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'*.

4.16 Überprüfen und Installieren der Einstellungen

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*.

4.17 Anzeigen der Protokolldateien

1. Wenn die Installation ohne Fehler abgeschlossen wurde, fahren Sie mit Kapitel 7, „Aufgaben nach Abschluss der Installation“, auf Seite 113 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 7.12, „Fehlersuche“, auf Seite 117.

Installation von der Konsole aus oder mit einem einzigen Befehl

5

In diesem Abschnitt werden die Installationsmethoden beschrieben, die Sie statt der Installation über eine grafische Benutzeroberfläche (siehe Kapitel 4, „Installation auf JBoss mithilfe einer GUI“, auf Seite 41) verwenden können. Es werden u. a. folgende Themen erläutert:

5.1 Installation der Benutzeranwendung von der Konsole aus

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

1. Rufen Sie die in Tabelle 2-1 auf Seite 27 beschriebenen Installationsdateien ab.
2. Melden Sie sich an und eröffnen Sie eine Terminalsitzung.
3. Starten Sie das Installationsprogramm für Ihre Plattform mit Java und gehen Sie wie folgt vor:

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

4. Befolgen Sie die unter Kapitel 4, „Installation auf JBoss mithilfe einer GUI“, auf Seite 41 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 4.14, „Konfiguration der Benutzeranwendung“, auf Seite 55 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 Kapitel 7, „Aufgaben nach Abschluss der Installation“, auf Seite 113 fort.

5.2 Installation der Benutzeranwendung mit einem einzigen Befehl

In diesem Abschnitt wird die Durchführung einer automatischen Installation beschrieben. 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 2-1 auf Seite 27 beschriebenen Installationsdateien ab.
2. Melden Sie sich an und eröffnen Sie eine Terminalsitzung.

3 Suchen Sie die Identity Manager-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 5-1. 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 5-1 *Benutzeranwendungs-Konfigurationsparameter für eine automatische Installation*

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_LDAPHOST=	eDirectory-Verbindungseinstellungen: LDAP-Host. Erforderlich. Geben Sie den Hostnamen oder die IP-Adresse des LDAP-Servers an.
NOVL_CONFIG_LDAPADMIN=	eDirectory-Verbindungseinstellungen: 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.
NOVL_CONFIG_LDAPADMINPASS=	eDirectory-Verbindungseinstellungen: LDAP-Administratorpasswort. Erforderlich. Geben Sie das LDAP-Administratorpasswort an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
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 3.1, „Erstellen des Benutzeranwendungstreibers in iManager“, auf Seite 33 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`
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 den Karteireiter *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.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_PROVLOCKSMITH=	eDirectory-DNs: Bereitstellungsanwendung - Administrator. Diese Funktion ist in der Bereitstellungsversion von Identity Manager 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 den Karteireiter *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.
NOVL_CONFIG_ROLECONTAINERDN=	Diese Funktion ist im funktionsbasierten Bereitstellungsmodul für Novell Identity Manager verfügbar. Mit dieser Funktion können Mitglieder alle Funktionen erstellen, entfernen oder modifizieren und Benutzern, Gruppen oder Containern Funktionen zuweisen oder entziehen. Außerdem können die Funktionsmitglieder damit einen Bericht für einen beliebigen Benutzer ausführen. Standardmäßig wird diese Funktion dem Benutzeranwendungsadministrator zugewiesen. Sie können diese Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Funktionen* > *Funktionszuweisungen* in der Benutzeranwendung ändern.
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.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
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). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können. Wählen Sie *False*, wenn die Kommunikation über das Admin-Konto nicht über eine SSL-Verbindung erfolgen soll.
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). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können. Wählen Sie *False*, wenn die Kommunikation über das Benutzerkonto nicht über eine SSL-Verbindung erfolgen soll.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
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. Wählen Sie *True*, damit nicht angemeldete Benutzer auf das öffentliche anonyme LDAP-Konto zugreifen können. Wählen Sie *False*, 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.
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.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
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 für die Bereitstellungs-Email an. Dies kann eine IP-Adresse oder ein DNS-Name sein.
NOVL_CONFIG_USEEXTPWDWAR=	Passwortverwaltung: Externe WAR-Datei für Passwort verwenden. Wählen Sie *True*, 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. Wählen Sie *False*, um die interne Standardfunktion für die Passwortverwaltung zu verwenden. `/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.
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 69

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
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. Wählen Sie *True*, um dynamische Gruppen zu verwenden. Anderenfalls wählen Sie *False*.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
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.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_ICSLOGOUTENABLED=	Access Manager- und iChain-Einstellungen: Gleichzeitige Abmeldung aktiviert. Wählen Sie *True*, um die gleichzeitige Abmeldung von der Benutzeranwendung und iChain® bzw. dem 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. Wählen Sie *False*, um die gleichzeitige Abmeldung zu deaktivieren.
NOVL_CONFIG_ICSLOGOUTPAGE=	Access Manager- und iChain-Einstellungen: Seite 'Gleichzeitige Abmeldung'. Geben Sie die URL zur iChain- oder Novell Access Manager-Abmeldungsseite an, wobei die URL ein von iChain oder vom 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.

Installation des WebSphere-Anwendungsservers

6

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

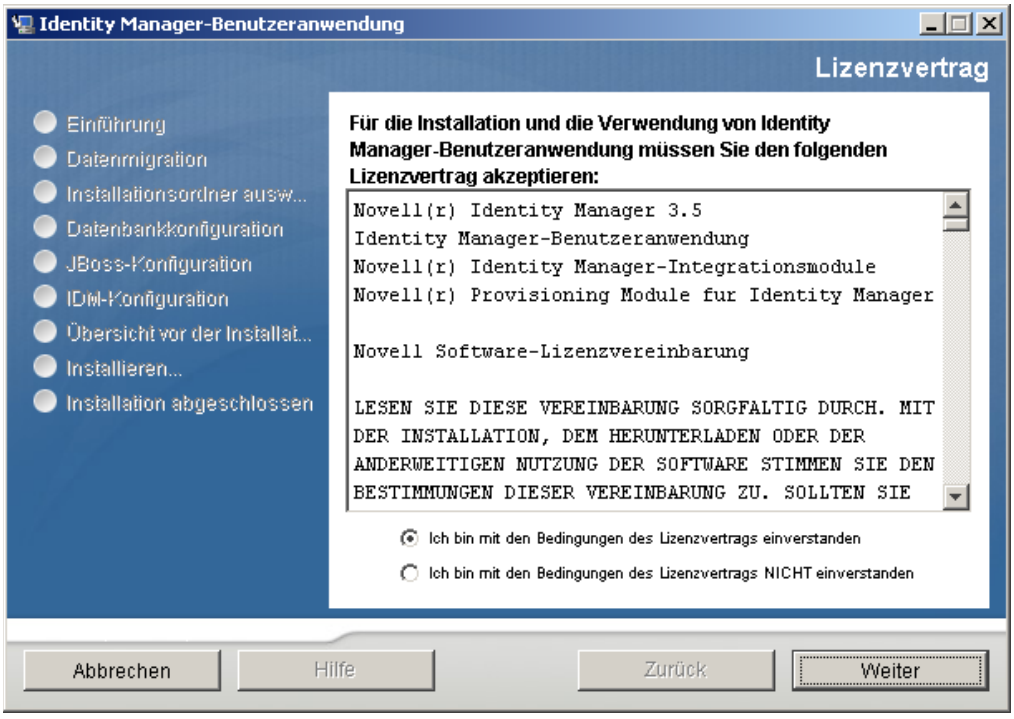
6.1 Starten der GUI des Installationsprogramms

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

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

   Hinweis: Mit WebSphere müssen Sie das IBM JDK mit den unbeschränkten Richtliniendateien verwenden.
3. Wählen Sie im Dropdown-Menü eine Sprache aus und klicken Sie anschließend auf OK.

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

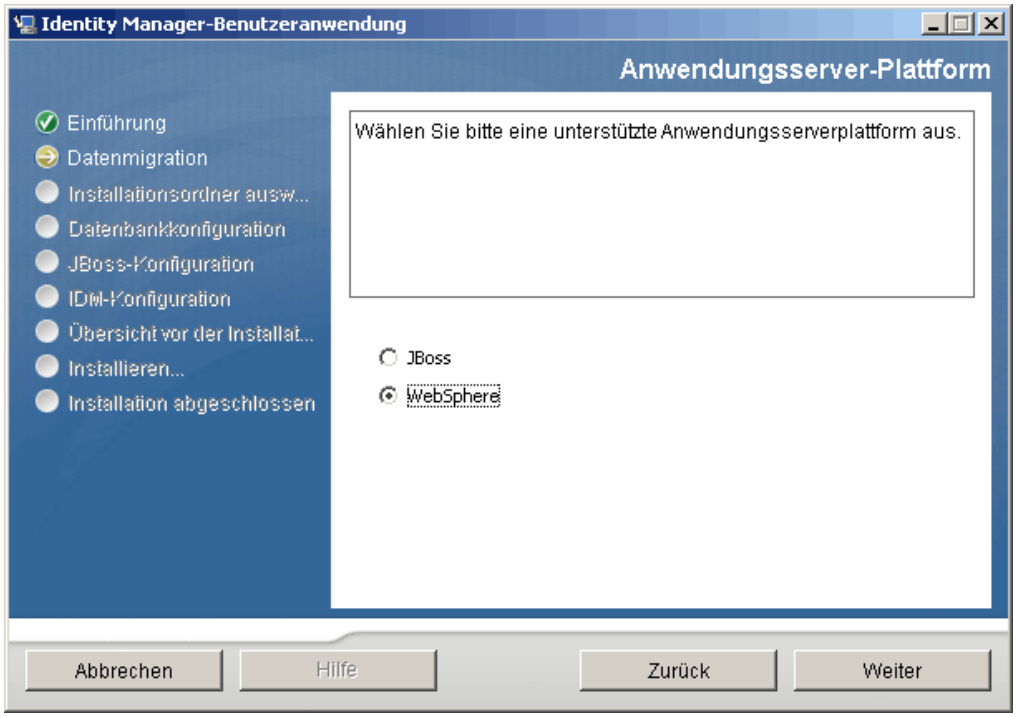


5 Lesen Sie die Einführungsseite des Installationsassistenten und klicken Sie anschließend auf *Weiter*.

6.2 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 6.3, „Angabe des Speicherorts der WAR-Datei“, auf Seite 85 fort.



6.3 Angabe des Speicherorts der WAR-Datei

Führen Sie den Vorgang aus, der in Abschnitt 6.1, „Starten der GUI des Installationsprogramms“, auf Seite 83 beschrieben ist, und fahren Sie dann mit den folgenden Schritten fort:

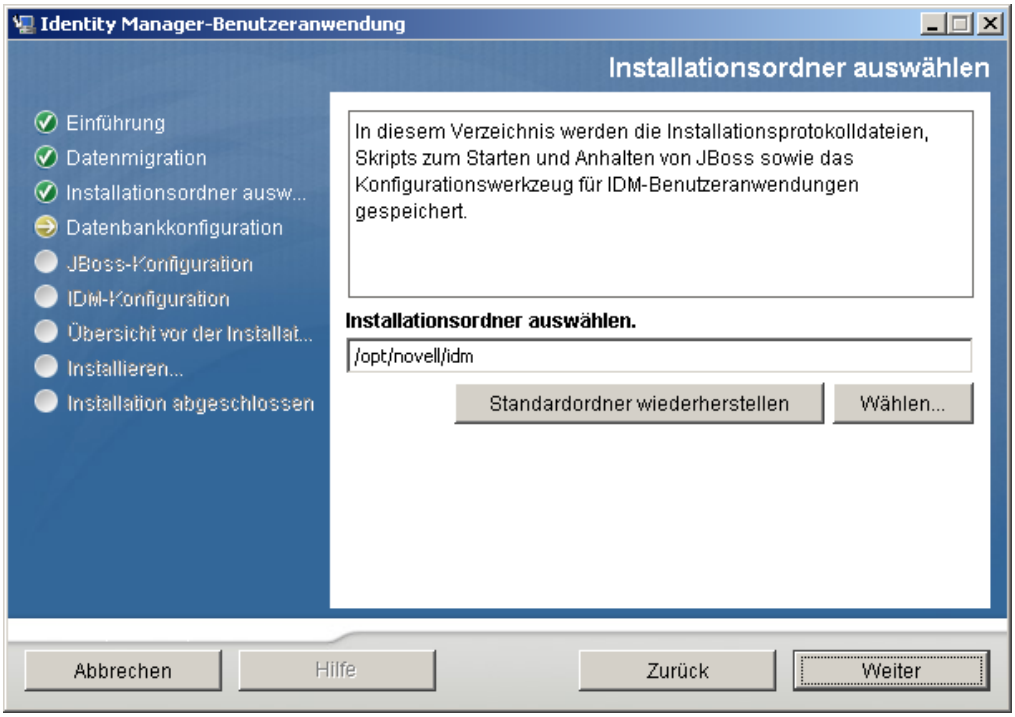
Wenn sich die WAR-Datei der Identity Manager-Benutzeranwendung nicht im selben Verzeichnis befindet wie das Installationsprogramm, werden Sie aufgefordert, den Pfad zur WAR-Datei einzugeben.

1 Wenn sich die WAR-Datei am Standardspeicherort befindet, können Sie auf *Standarddatei 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 6.4, „Auswahl eines Installationsordners“, auf Seite 86 fort.

6.4 Auswahl eines Installationsordners

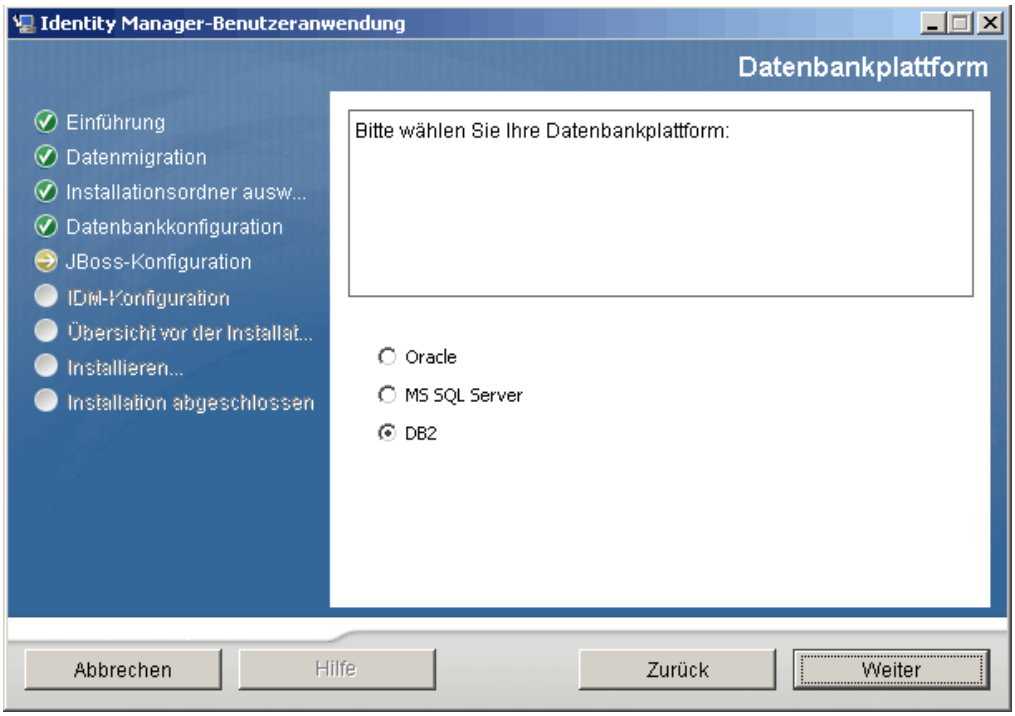
1 Geben Sie auf der Seite „Installationsordner auswählen“ die Stelle an, an der die Benutzeranwendung installiert werden soll. Wenn Sie den Standardspeicherort verwenden möchten, klicken Sie auf *Standardordner wiederherstellen* oder klicken Sie auf die Schaltfläche zum *Auswählen*, um einen anderen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



2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 6.5, „Auswahl einer Datenbankplattform“, auf Seite 87 fort.

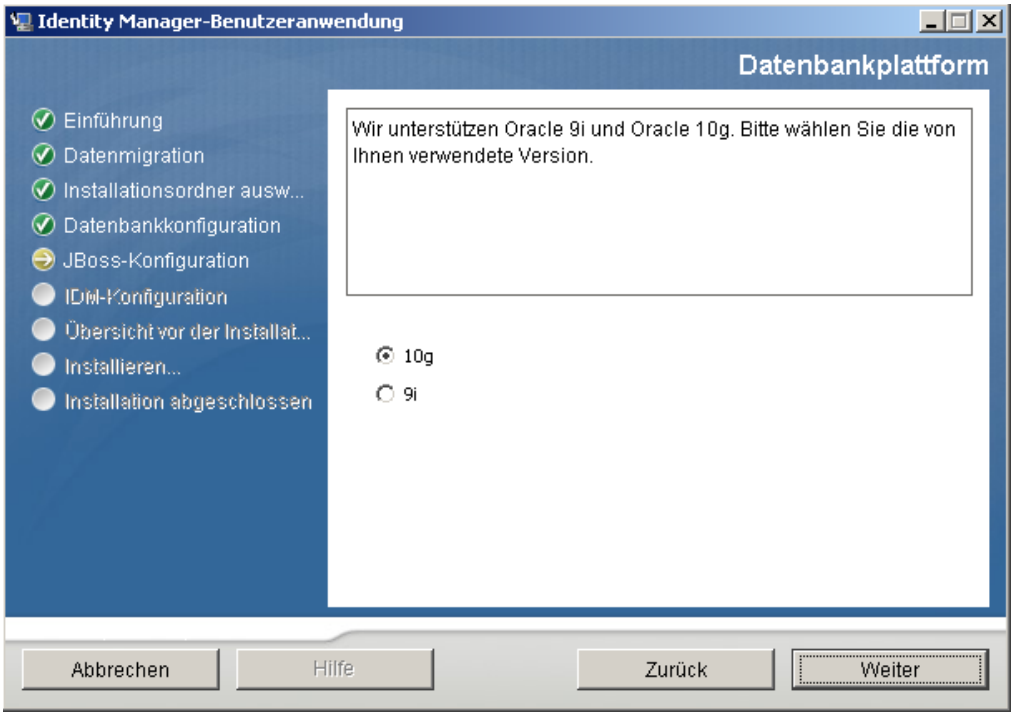
6.5 Auswahl einer Datenbankplattform

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.

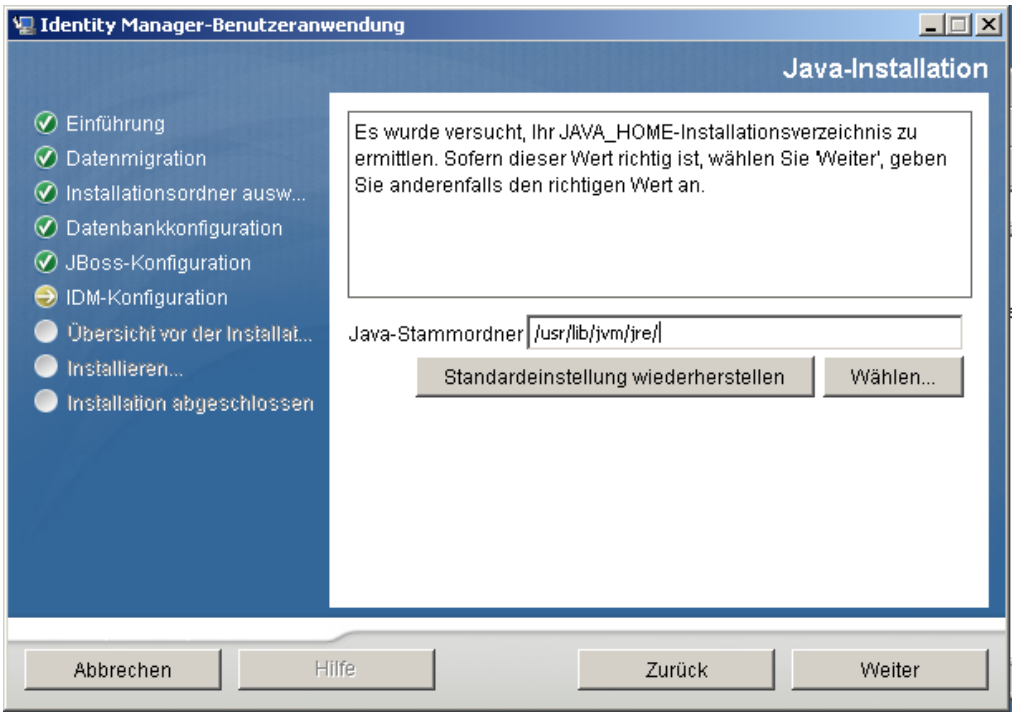


4 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 6.6, „Angabe des Java-Stammordners“, auf Seite 88 fort.

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*.

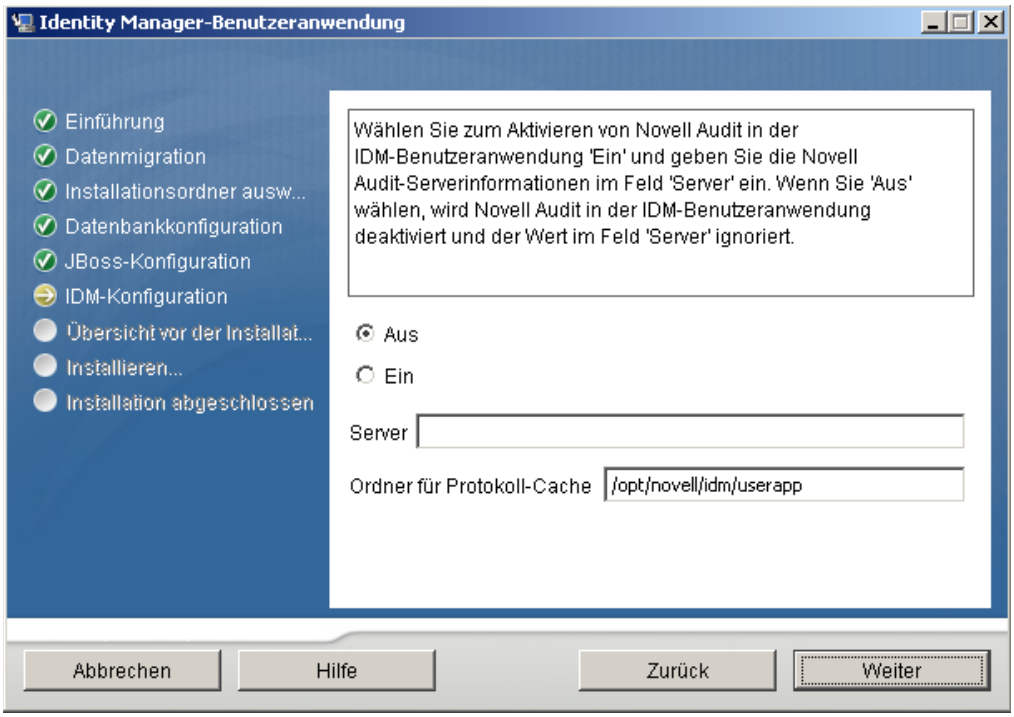


2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 6.7, „Aktivieren der Novell Audit-Protokollierung“, auf Seite 89 fort.

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.

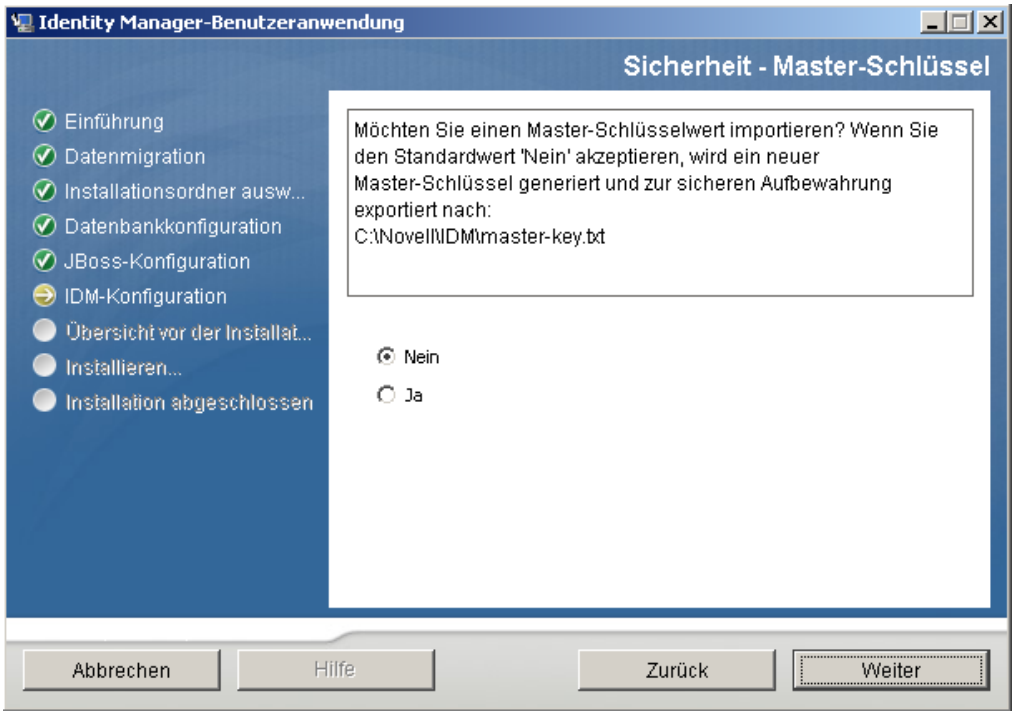
2 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 6.8, „Angabe eines Master-Schlüssels“, auf Seite 91 fort.

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 6.9, „Konfiguration der Benutzeranwendung“, auf Seite 92 fort. Nach Abschluss der Installation müssen Sie den Master-Schlüssel manuell speichern. Wenn Sie *Ja* gewählt haben, fahren Sie mit Schritt 3 auf Seite 91 fort.

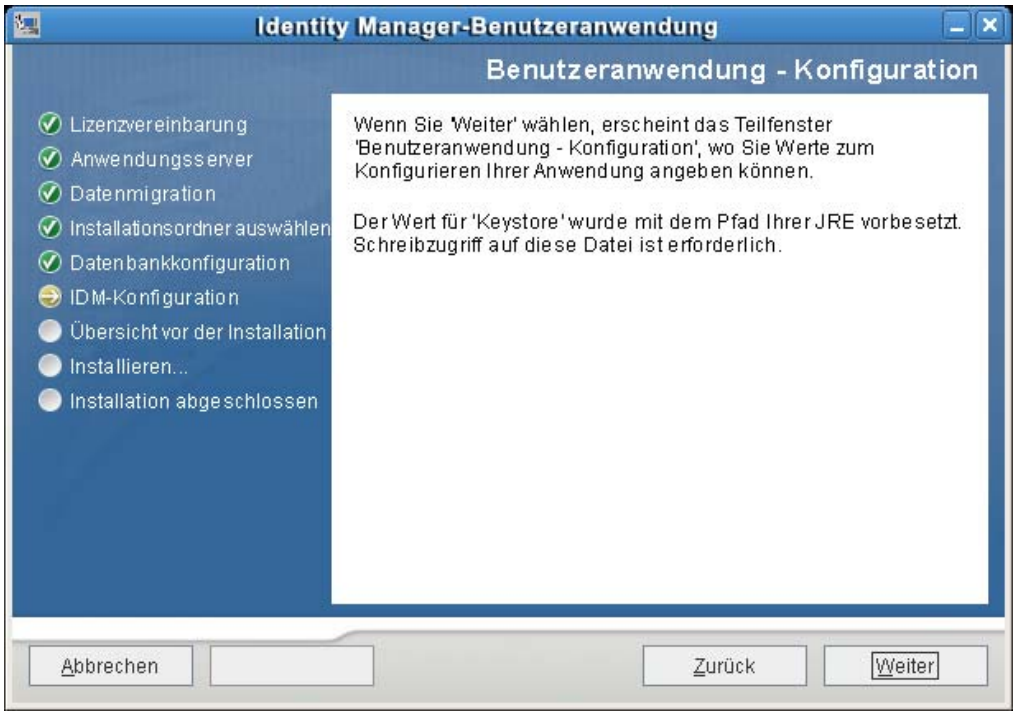
3 Wenn ein vorhandener verschlüsselter Master-Schlüssel importiert werden soll, kopieren Sie den Schlüssel und fügen Sie ihn in das Fenster des Installationsvorgangs ein.

4 Klicken Sie auf *Weiter* und fahren Sie mit Abschnitt 6.9, „Konfiguration der Benutzeranwendung“, auf Seite 92 fort.

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 6-1 auf Seite 95 beschrieben an und fahren Sie dann mit Schritt 3 fort.

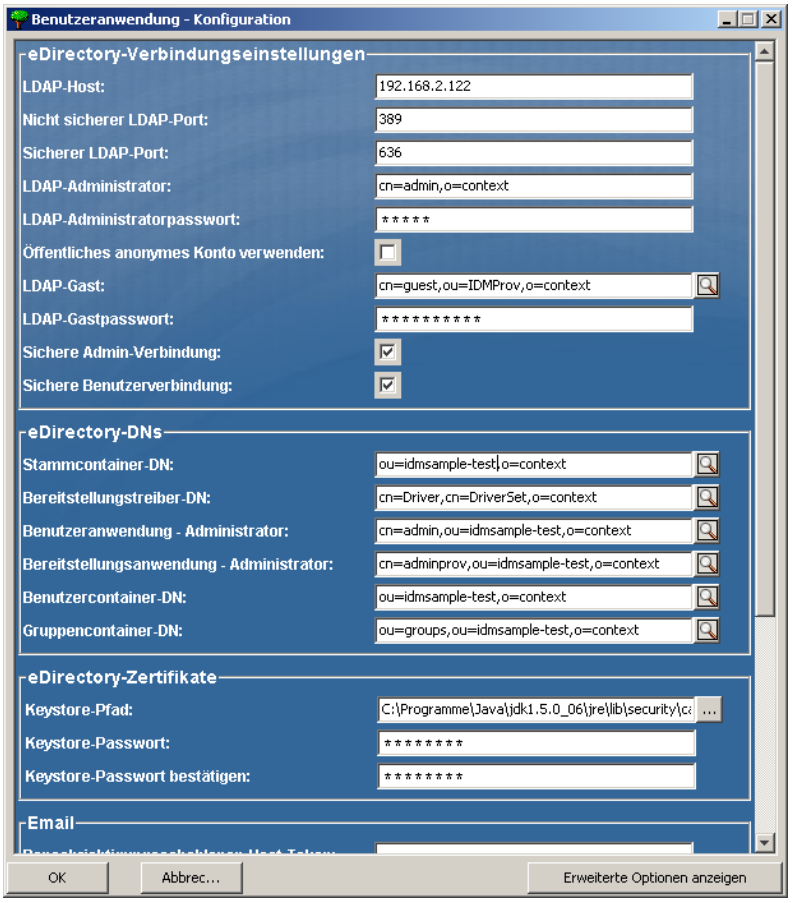

Benutzeranwendung - Konfiguration
eDirectory-Verbindungseinstellungen
LDAP-Host:
192.168.2.122
Nicht sicherer LDAP-Port:
389
Sicherer LDAP-Port:
636
LDAP-Administrator:
cn=admin,o=context
LDAP-Administratorpasswort:
*****
Öffentliches anonymes Konto verwenden:
LDAP-Gast:
cn=guest,ou=IDMProv,o=context
LDAP-Gastpasswort:
****
Sichere Admin-Verbindung:
Sichere Benutzerverbindung:
eDirectory-DNs
Stammcontainer-DN:
ou=idmsample-test,o=context
Bereitstellungstreiber-DN:
cn=Driver,cn=DriverSet,o=context
Benutzeranwendung - Administrator:
cn=admin,ou=idmsample-test,o=context
Bereitstellungsanwendung - Administrator:
cn=adminprov,ou=idmsample-test,o=context
Benutzercontainer-DN:
ou=idmsample-test,o=context
Gruppencontainer-DN:
ou=groups,ou=idmsample-test,o=context
eDirectory-Zertifikate
Keystore-Pfad:
C:\Programme\Java\jdk1.5.0_06\jre\lib\security\ca
Keystore-Passwort:
****
Keystore-Passwort bestätigen:
****
Email
OK
Abbrec...
Erweiterte Optionen anzeigen

Tabelle 6-1 *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 zum Deaktivieren des Gast-Benutzers das Kontrollkästchen *Öffentliches anonymes Konto verwenden*.
	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). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können.
	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). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können.

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 den Karteireiter *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	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 den Karteireiter *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)	*Funktionsadministrator*	Diese Funktion ist im funktionsbasierten Bereitstellungsmodul für Novell Identity Manager verfügbar. Mit dieser Funktion können Mitglieder alle Funktionen erstellen, entfernen oder modifizieren und Benutzern, Gruppen oder Containern Funktionen zuweisen oder entziehen. Außerdem können die Funktionsmitglieder damit einen Bericht für einen beliebigen Benutzer ausführen. Standardmäßig wird diese Funktion dem Benutzeranwendungsadministrator zugewiesen. Sie können die Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Funktionen* > *Funktionszuweisungen* in der Benutzeranwendung ändern.
	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	*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-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.
	'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`.

Einstellungstyp	Feld	Beschreibung
	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 6-2 auf Seite 100 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 6-2 *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). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können.
	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). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können.

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 den Karteireiter *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	Der Bereitstellungsanwendungsadministrator verwaltet die Bereitstellungs-Workflow-Funktionen, die in der Registerkarte *Anforderungen und Genehmigungen* der Benutzeranwendung zur Verfügung stehen. 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.
	Funktionsadministrator	Diese Funktion ist im funktionsbasierten Bereitstellungsmodul für Novell Identity Manager verfügbar. Mit dieser Funktion können Mitglieder alle Funktionen erstellen, entfernen oder modifizieren und Benutzern, Gruppen oder Containern Funktionen zuweisen oder entziehen. Außerdem können die Funktionsmitglieder damit einen Bericht für einen beliebigen Benutzer ausführen. Standardmäßig wird diese Funktion dem Benutzeranwendungsadministrator zugewiesen. Sie können diese Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Funktionen* > *Funktionszuweisungen* in der Benutzeranwendung ändern.

Einstellungstyp	Feld	Beschreibung
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).
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.

Einstellungstyp	Feld	Beschreibung
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.
	Passwort für Herkunftsverbürgungsspeicher	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.
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.
Access Manager- und iChain-Einstellungen	*Gleichzeitige Abmeldung aktiviert*	Bei Auswahl dieser Option unterstützt die Benutzeranwendung die gleichzeitige Abmeldung von der Benutzeranwendung und dem Novell Access Manager bzw. iChain. Bei der Abmeldung leitet die Benutzeranwendung den Benutzer bei Vorhandensein des iChain- oder Novell Access Manager-Cookies zur ICS-Abmeldungsseite um.
	Seite 'Gleichzeitige Abmeldung'	Die URL für die Abmeldeseite von Novell Access Manager oder iChain, wobei die URL ein Hostname ist, den Novell Access Manager oder iChain erwartet. 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	*Sitzungszeitüberschreitung*	Die Sitzungszeit-überschreitung 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 *Novell iManager 2.6 Administrationshandbuch (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 6.10, „Überprüfen und Installieren der Einstellungen“, auf Seite 107 fort.

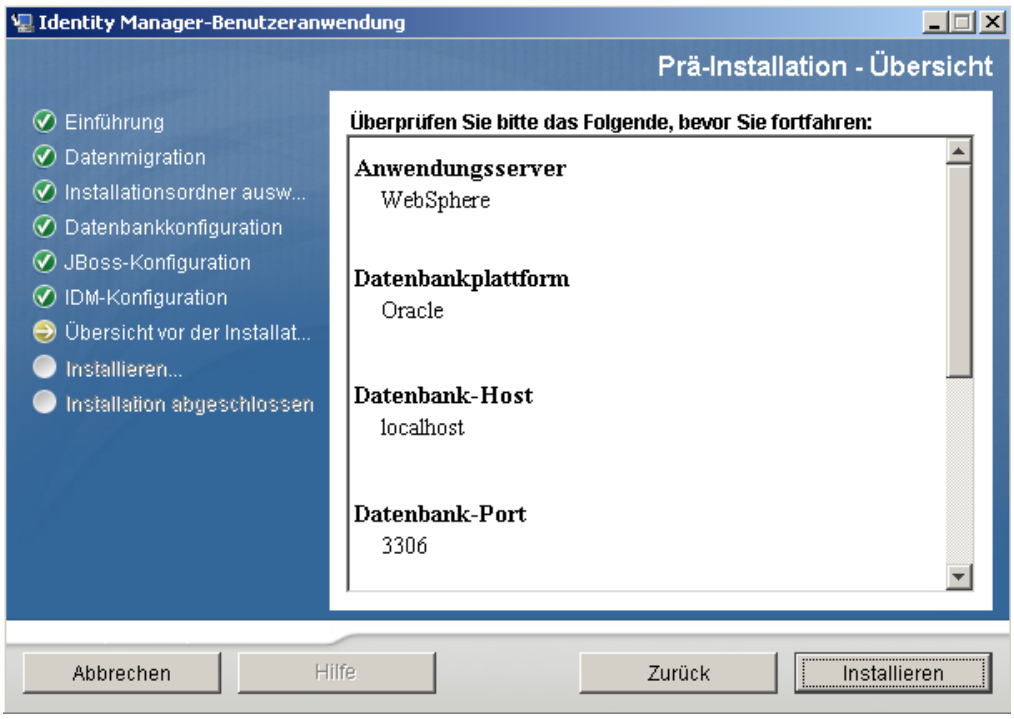
6.10 Überprüfen und Installieren der Einstellungen

1 Überprüfen Sie auf der Seite „Prä-Installation - Übersicht“ 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 „Prä-Installation - Übersicht“ zurück und klicken Sie auf *Installieren*.



6.11 Anzeigen der Protokolldateien

Wenn die Installation ohne Fehler abgeschlossen wurde, fahren Sie mit Abschnitt 6.12, „Hinzufügen von Benutzeranwendungs-Konfigurationsdateien und JVM-Systemeigenschaften“, auf Seite 108 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.

6.12 Hinzufügen von Benutzeranwendungs-Konfigurationsdateien und JVM-Systemeigenschaften

Für eine erfolgreiche WebSphere-Installation sind folgende Schritte erforderlich:

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* den Namen des Installationsordners (Verzeichnis) ein, den Sie während der Installation angegeben haben.

Das Installationsprogramm hat in diesem Ordner die Datei `sys-configuration-xmldata.xml` erstellt.

9c Geben Sie unter *Beschreibung* eine Beschreibung der Eigenschaft ein, 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* den Namen des Installationsordners (Verzeichnis) ein, den Sie während der Installation angegeben haben.

10c Geben Sie unter *Beschreibung* eine Beschreibung der Eigenschaft ein, beispielsweise `Pfad zu idmuserapp_logging.xml`.

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

Hinweis: Die Datei `idmuserapp-logging.xml` wird erst dann erstellt, wenn Sie die Änderungen über *Benutzeranwendung* > *Administration* > *Anwendungskonfiguration* > *Protokollierung* permanent gespeichert haben.

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 110) oder über die Befehlszeile („Zertifikate über die Befehlszeile importieren“ auf Seite 110) tun.

3 Fahren Sie nach dem Importieren der Zertifikate mit Abschnitt 6.14, „Bereitstellung der IDM WAR-Datei“, auf Seite 110 fort.

6.13.1 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.

6.13.2 Zertifikate über die Befehlszeile importieren

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`.

Im Folgenden finden Sie ein 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.

6.14 Bereitstellung der IDM WAR-Datei

1 Melden Sie sich bei der Administrationskonsole von WebSphere als Admin-Benutzer an.
2 Wählen Sie im linken Teilfenster *Applications* > *Install New Application*.
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 Lassen Sie die Optionsschaltfläche für *Prompt me only when additional information is required* ausgewählt. Klicken Sie anschließend auf *Weiter*, um die Seite für die Auswahl der Installationsoptionen anzuzeigen.

6 Übernehmen Sie die Standardeinstellungen für diese Seite und klicken Sie auf *Weiter*, um zur Seite „Map modules to servers“ zu wechseln.

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

8 Wählen Sie für die Authentifizierungsmethode die Option *Use 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 *Weiter*, um zur Seite *Map virtual hosts for Web modules* zu wechseln.

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

12 Wählen Sie *Fertig stellen*, um die Bereitstellung abzuschließen.

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

14 Fahren Sie mit Abschnitt 6.15, „Anwendung starten“, auf Seite 111 fort.

6.15 Anwendung starten

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

2 Wählen Sie in der linken Navigationsleiste *Applications* > *Enterprise Applications*.

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.

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`

Aufgaben nach Abschluss der Installation

7

In diesem Abschnitt werden die nach der Installation durchzuführenden Aufgaben erläutert. Es werden u. a. folgende Themen erläutert:

7.1 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.

7.2 Konfiguration nach der Installation

Anleitungen zur Konfiguration der Identity Manager-Benutzeranwendung und dem Funktionssubsystem nach der Installation finden Sie in folgenden Quellen:

- Im *Administrationshandbuch zum funktionsbasierten Bereitstellungsmodul für Novell IDM 3.6* im Abschnitt zur Konfiguration der Benutzeranwendungsumgebung.
- Im *Designhandbuch zum funktionsbasierten Bereitstellungsmodul für Novell IDM 3.6*.

7.3 Überprüfen der Cluster-Installationen

Stellen Sie bei JBoss-Clustern sicher, dass jeder Anwendungsserver im Cluster über folgende Elemente verfügt:

- 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 bei WebSphere-Clustern sicher, dass jeder Anwendungsserver im Cluster über eine eindeutige Workflow-Engine-ID verfügt.

Weitere Informationen hierzu finden Sie im Abschnitt „Clustering“ in Kapitel 4 des Handbuchs *Identity Manager-Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idmrbpm36/index.html).

7.4 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.

7.5 Zugriff auf die externe Passwort-WAR

Wenn Sie eine externe Passwort-WAR verwenden und die „Passwort vergessen“-Funktion testen möchten, können Sie wie folgt auf sie zugreifen:

- Direkt, 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*.

7.6 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.

Verwendung des configupdate-Dienstprogramms. 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.

Verwendung der Benutzeranwendung. Melden Sie sich als Administrator der Benutzeranwendung an und wechseln Sie zu *Administration* > *Anwendungskonfiguration* > *Passwortmodul - Setup* > *Anmeldung*. Bearbeiten Sie folgende 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`)

7.7 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*.

7.8 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.

   Wenn Sie den Anwendungsserver nicht auf einem X11 Window System ausführen, müssen Sie das Flag - `Djava.awt.headless=true` in Ihr Server-Startskript einfügen. Dies ist nicht für das Ausführen von Berichten erforderlich. Sie können beispielsweise folgende Zeile zu Ihrem Skript hinzufügen:

```
JAVA_OPTS="-Djava.awt.headless=true -server -Xms256M -Xmx256M-
XX:MaxPermSize=256m"
```

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 folgende URL angeben:

   http://*Hostname*:*Port*/*Anwendungsname* eingeben.

   In dieser URL entspricht *Hostname*:*Port* dem Hostnamen des Anwendungsservers (z. B. MeinServer.Domäne.com) und dem 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 7.12, „Fehlersuche“, auf Seite 117 nach.

7.9 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 Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idmrbpm36/index.html).

7.10 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 Identity Manager.

7.11 Neukonfiguration der IDM WAR-Datei nach der Installation

So aktualisieren Sie Ihre IDM-WAR-Datei:

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 in Tabelle 4-2 auf Seite 62, Tabelle 5-1 auf Seite 74 oder Tabelle 6-2 auf Seite 100.

2. Stellen Sie die neue WAR-Datei auf Ihrem Anwendungsserver bereit.

7.12 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.

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
◆ Access Manager- oder 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.

Problem	Empfohlene Vorgehensweise
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).
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 Identity Manager 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).

Problem	Empfohlene Vorgehensweise

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`