Benutzeranwendung: Installationshandbuch

Novell®
Funktionsbasiertes Bereitstellungsmodul für Identity Manager

3.6.1

23. Juli 2008

www.novell.com

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

In diesem Handbuch wird die Installation des funktionsbasierten Bereitstellungsmoduls für Novell® Identity Manager 3.6.1 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.

1 Überblick über die Installation des funktionsbasierten Bereitstellungsmoduls

Dieser Abschnitt gibt einen Überblick über die einzelnen Schritte bei der Installation des funktionsbasierten Bereitstellungsmoduls. Außerdem erhalten Sie hier Hilfe für die zusätzliche Installation und Konfiguration der Standard Edition der Benutzeranwendung, die Teil der Metaverzeichnis-Serverinstallation ist. Es werden u. a. folgende Themen erläutert:

- Abschnitt 1.1, „Installations-Checkliste“, auf Seite 9
- Abschnitt 1.2, „Allgemeines zum Installationsprogramm“, auf Seite 11
- Abschnitt 1.3, „Systemanforderungen“, auf Seite 11

Wenn Sie von einer früheren Version der Benutzeranwendung oder des funktionsbasierten Bereitstellungsmoduls migrieren, lesen Sie das *Benutzeranwendung: Migrationshandbuch* (http://www.novell.com/documentation/idmrbpm361/index.html)

1.1 Installations-Checkliste

Führen Sie die folgenden Aufgaben durch, um das funktionsbasierte Bereitstellungsmodul für Novell® Identity Manager oder die Standard Edition der Benutzeranwendung zu installieren:

- ❑ Vergewissern Sie sich, dass Ihre Software die Systemanforderungen erfüllt. Weitere Informationen hierzu finden Sie unter Abschnitt 1.3, „Systemanforderungen“, auf Seite 11.
- ❑ Laden Sie das funktionsbasierte Bereitstellungsmodul für Identity Manager 3.6.1 herunter. Weitere Informationen hierzu finden Sie unter Abschnitt 2.2, „Herunterladen des funktionsbasierten Bereitstellungsmoduls“, auf Seite 17.
- ❑ Richten Sie die folgenden unterstützenden Komponenten ein:
  - ❑ Stellen Sie sicher, dass ein unterstütztes Identity Manager-Metaverzeichnis installiert ist. Weitere Informationen hierzu finden Sie unter Abschnitt 2.1, „Installation des Identity Manager-Metaverzeichnisses“, auf Seite 17.
  - ❑ Installieren und konfigurieren Sie einen Anwendungsserver. Weitere Informationen hierzu finden Sie unter Abschnitt 2.3, „Installation eines Anwendungsservers“, auf Seite 19.
  - ❑ Installieren und konfigurieren Sie eine Datenbank. Weitere Informationen hierzu finden Sie unter Abschnitt 2.4, „Installieren einer Datenbank“, auf Seite 22.
  - ❑ Wenn Sie von einer früheren Version der Benutzeranwendung migrieren und weiterhin das Identity Manager 3.5.1-Metaverzeichnis verwenden, führen Sie die folgenden Aufgaben durch:
    - ❑ Führen Sie das Installationsprogramm für den Funktionsservice und Benutzeranwendungstreiber aus, um das Identitätsdepot-Schema zu erweitern, installieren Sie die erforderlichen Konfigurationsdateien für den Funktionsservice und Benutzeranwendungstreiber, und kopieren Sie beliebige zusätzliche Dateien, soweit erforderlich. Weitere Informationen finden Sie unter Abschnitt 2.6, „Installieren zusätzlicher Dateien für Metaverzeichnis 3.5.1“, auf Seite 24.

Hinweis: Das Identity Manager 3.6-Metaverzeichnis führt das Installationsprogramm für den Funktionsservice und Benutzeranwendungstreiber im unbeaufsichtigten Modus aus. Hiermit wird sichergestellt, dass alle erforderlichen Dateien vorhanden sind.

- ❑ Kopieren Sie den Inhalt von `iManager_icons_for_roles.zip` an den korrekten iManager-Speicherort. Weitere Informationen hierzu finden Sie unter Abschnitt 2.6.3, „Kopieren der iManager-Symbole“, auf Seite 26.
- ❑ Kopieren Sie die Datei `afadmin.jar` an den korrekten Speicherort. Weitere Informationen hierzu finden Sie unter „Kopieren von afadmin.jar“ auf Seite 26.

- ❑ Erstellen Sie den Benutzeranwendungstreiber in iManager oder Designer für Identity Manager 3.0.
  - Für iManager: Abschnitt 3.1, „Erstellen des Benutzeranwendungstreibers in iManager“, auf Seite 27.
  - Für Designer: Benutzeranwendung: Designhandbuch (http://www.novell.com/documentation/idmrbpm361/index.html).
- ❑ Erstellen Sie den Funktionsservice-Treiber in iManager oder Designer für Identity Manager 3.0.
  - Für iManager: Abschnitt 3.2, „Erstellen des Funktionsservice-Treibers in iManager“, auf Seite 29.
  - Für Designer: Benutzeranwendung: Designhandbuch (http://www.novell.com/documentation/idmrbpm361).
- ❑ Installieren und konfigurieren Sie die Novell Identity Manager-Benutzeranwendung oder das funktionsbasierte Bereitstellungsmodul. (Sie müssen das korrekte JDK* installiert haben, bevor Sie das Installationsprogramm starten. Weitere Informationen hierzu finden Sie unter Abschnitt 2.5, „Installieren des Java Development Kit“, auf Seite 23.)

  Das Installationsprogramm kann auf drei Arten gestartet werden:
  - Über die grafische Benutzeroberfläche. Lesen Sie dazu Folgendes:
    - Kapitel 4, „Installieren auf JBoss mithilfe des GUI-Installationsprogramms“, auf Seite 33.
    - Kapitel 5, „Installation auf einem WebSphere-Anwendungsserver mithilfe des GUI-Installationsprogramms“, auf Seite 41.
    - Kapitel 6, „Installation auf einem WebLogic-Anwendungsserver mithilfe des GUI-Installationsprogramms“, auf Seite 51.
  - Über die Konsolenschnittstelle (Befehlszeile). Weitere Informationen hierzu finden Sie unter Abschnitt 7.1, „Installation der Benutzeranwendung von der Konsole aus“, auf Seite 59.
  - Automatische Installation. Siehe Abschnitt 7.2, „Installation der Benutzeranwendung mit einem einzigen Befehl“, auf Seite 60.
- ❑ Führen Sie die Aufgaben nach der Installation aus, wie in Kapitel 8, „Aufgaben nach Abschluss der Installation“, auf Seite 71 beschrieben.

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* und WebLogic* müssen Sie die WAR-Datei manuell bereitstellen.
- Aktiviert die Protokollierung von Novell Audit oder OpenXDAS, sofern ausgewählt.
- Ermöglicht das Importieren eines vorhandenen Master-Schlüssels zur Wiederherstellung einer bestimmten Installation des funktionsbasierten Bereitstellungsmoduls und zur Unterstützung von Clustern.
- Migriert vorhandene Daten von einem Bereitstellungsmodul der Version 3.5.1 oder einem funktionsbasierten Bereitstellungsmodul der Version 3.6 auf das erforderliche Datenformat für Version 3.6.2.

1.3 Systemanforderungen

Für die Verwendung des funktionsbasierten Bereitstellungsmoduls für Novell Identity Manager 3.6.1 benötigen Sie jeweils eine der unter Tabelle 1-1 aufgeführten erforderlichen Komponenten.

Tabelle 1-1 *Systemvoraussetzungen*

Erforderliche Systemkomponente	Systemanforderungen
Identity Manager 3.5.1 (Metaverzeichnissystem)	SUSE® Linux Enterprise Server (SLES) 10 mit dem neuesten Support Pack (32- und 64-Bit-Unterstützung) eDirectory™: 8.8.2 Security Services 2.0.5 (NMAS™ 3.1.3)
Identity Manager 3.6 (Metaverzeichnissystem)	Eines der folgenden Betriebssysteme: ◆ Windows Server* 2003 SP2 (32-Bit) ◆ Linux Red Hat 5.0 (32-Bit) mit dem neuesten Support Pack ◆ SLES* 10 SP2 (32-Bit) mit dem neuesten Support Pack ◆ Solaris* 10 (32-Bit) ◆ AIX* 5L v5.3 (32-Bit) eDirectory: 8.8.3

Erforderliche Systemkomponente	Systemanforderungen
Webbasierter Administrationsserver ◆ iManager 2.6 und Plugins (nur mit Metaverzeichnis 3.5.1) ◆ iManager 2.7 und Plugins	Eines der folgenden Betriebssysteme: ◆ Novell Open Enterprise Server (OES) 1.0 unter NetWare mit dem neuesten Support Pack ◆ Novell Open Enterprise Server 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* ◆ 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 ◆ Windows Vista Ultimate und Business Editionen (nur iManager 2.7) ◆ SUSE Linux Enterprise Desktop 10 ◆ SUSE Linux 10.1 ◆ openSUSE® 10.3 (nur iManager 2.7) Die folgende Software: ◆ Novell iManager 2.6 oder 2.7 mit dem neuesten Support Pack und den neuesten Plugins

Erforderliche Systemkomponente	Systemanforderungen
Sicherer Protokollserver ◆ Der sichere Protokollserver ◆ Der Plattformagent (Client-Komponente) ◆ Novell Audit 2.0.2 oder Sentinel™ 5.1.3 oder Sentinel 6.1 (nur Metaverzeichnis 3.6)	Eines der folgenden Betriebssysteme für den sicheren Protokollserver: ◆ Novell Open Enterprise Server 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 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

Erforderliche Systemkomponente	Systemanforderungen
Anwendungsserver für die Benutzeranwendung	Die Benutzeranwendung kann auf JBoss*, WebSphere* und WebLogic* ausgeführt werden, wie unten beschrieben. Die Benutzeranwendung mit JBoss 4.2.2 GA erfordert JRE* 1.5.0_15 und wird auf den folgenden Systemen unterstützt: ◆ 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 2003 Server mit SP1 (64 Bit) ◆ Solaris 10 Support Pack mit Datum 6/06 ◆ Red Hat Linux 5 (32-Bit) Die Benutzeranwendung auf WebSphere 6.1 erfordert das IBM JDK. Die minimale Fixpack-Ebene ist 6.1.0.9 mit angewendeten uneingeschränkten Richtliniendateien. Sie wird auf den folgenden Plattformen unterstützt: ◆ Solaris 10 (64-Bit) ◆ Windows 2003 SP1 (64 Bit) Die Benutzeranwendung auf WebLogic 10 erfordert JRockit* 1.5.0_06 und wird auf diesen Plattformen unterstützt. ◆ Solaris 10 (32-Bit oder 64-Bit) ◆ Windows 2003 SP1
Benutzeranwendungsbrowser	Die Benutzeranwendung unterstützt Firefox* und Internet Explorer*, wie nachfolgend beschrieben. Firefox* 2 wird in den folgenden Umgebungen unterstützt: ◆ Windows XP mit SP2 ◆ Windows Vista ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 ◆ openSUSE 10 Internet Explorer 7 wird in den folgenden Umgebungen unterstützt: ◆ Windows XP mit SP2 ◆ Windows Vista Enterprise Internet Explorer 6 SP1 wird in den folgenden Umgebungen unterstützt: ◆ Windows XP mit SP2

Erforderliche Systemkomponente	Systemanforderungen
Datenbankserver für die Benutzeranwendung	Die folgenden Datenbanken werden mit JBoss unterstützt: ◆ MySQL Version 5.0.51 ◆ 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 folgenden Datenbanken werden mit WebLogic unterstützt: ◆ Oracle 10g Release 2 (10.2.0) ◆ MS SQL 2005 SP1 Es werden folgende JDBC-Treiber unterstützt: Microsoft SQL Server Version 1.2.2828.100 Oracle Thin-Treiber: Oracle JDBC-Treiber Version 10.2.0.1.0 Oracle OCI-Treiber: Oracle JDBC-Treiber Version 10.2.0.2.0 MySQL Connector/J 5.0.8 DB2-Treiber Version 1.4.2
Arbeitsstationen ◆ Designer 3.0 for Identity Manager 3.6 ◆ Webzugriff auf iManager	Designer wurde auf folgenden Plattformen getestet: Windows: ◆ Windows XP SP2 ◆ Microsoft Windows Vista Linux: ◆ SUSE Linux Enterprise Server 10 (nur Designer) ◆ SUSE Linux Enterprise Desktop 10 ◆ openSUSE 10
Audit	Novell Audit 2.0.2
OpenXDAS	OpenXDAS Version 0.5.257
Benutzeranwendung - SSO-Integration	Erfordert Novell Access Manager 3.0.1

Voraussetzungen

2

In diesem Abschnitt werden die Software und die Komponenten beschrieben, die Sie installieren oder konfigurieren müssen, bevor Sie das funktionsbasierte Bereitstellungsmodul für Identity Manager oder die Standard Edition der Benutzeranwendung installieren können. Es werden u. a. folgende Themen erläutert:

2.1 Installation des Identity Manager-Metaverzeichnisses

Das funktionsbasierte Bereitstellungsmodul 3.6.1 kann mit dem Metaverzeichnis von Identity Manager 3.5.1 oder 3.6 verwendet werden.

Weitere Anweisungen zum Installieren des Identity Manager 3.6-Metaverzeichnisses finden Sie im *Novell Identity Manager 3.6 Installationshandbuch* (http://www.novell.com/documentation/idm36/).

Wenn Sie das Identity Manager 3.5.1-Metaverzeichnis haben, müssen Sie verschiedene Dateien aktualisieren, damit das funktionsbasierte Bereitstellungsmodul 3.6.1 läuft. Weitere Informationen finden Sie unter Abschnitt 2.6, „Installieren zusätzlicher Dateien für Metaverzeichnis 3.5.1“, auf Seite 24. Beim Identity Manager 3.6-Metaverzeichnis ist dies nicht erforderlich, da die Dateien automatisch als Teil der Installation des Identity Manager 3.6-Metaverzeichnisses installiert werden.

2.2 Herunterladen des funktionsbasierten Bereitstellungsmoduls

Laden Sie das funktionsbasierte Bereitstellungsmodul für Identity Manager 3.6.1 von Novell Downloads (http://download.novell.com/index.jsp) herunter. Laden Sie die `.iso`-Image-Dateien für Ihr Produkt in Tabelle 2-1 herunter.

Tabelle 2-1 *Die .iso-Download-Dateien*

Für dieses Produkt	Diese .iso-Datei herunterladen
Funktionsbasiertes Bereitstellungsmodul für	`Identity_Manager_3_6_1_User_Application_ Provisioning.iso`
Standard Edition der Benutzeranwendung	`Identity_Manager_3_6_1_User_Application_NON_Provisioning.iso`

Wenn Sie das Identity Manager 3.5.1-Metaverzeichnis haben, müssen Sie außerdem `Roles_Driver_Install_Utility.iso` herunterladen. Sie müssen `Roles_Driver_Install_Utility.iso` nicht herunterladen, wenn Sie ein Identity Manager 3.6-Metaverzeichnis-Benutzer sind, da die in diesem `.iso` enthaltenen Dateien bereits Teil der Installation des Identity Manager 3.6-Metaverzeichnisses sind.

In Tabelle 2-2 werden die Installationsdateien des funktionsbasierten Bereitstellungsmoduls oder der `.iso`-Datei der Standard Edition der Benutzeranwendung beschrieben.

Tabelle 2-2 *In der .iso-Datei enthaltene Dateien und Skripte*

Datei	Beschreibung
`IDMProv.war`	Das WAR-Archiv des funktionsbasierten Bereitstellungsmoduls. Sie enthält die Identity Manager 3.6.1-Benutzeranwendung mit Funktionen für die Identitätsselbstbedienung und das funktionsbasierte Bereitstellungsmodul.
`IDM.war`	Das WAR-Archiv der Standard Edition der Benutzeranwendung. Es enthält die Identity Manager 3.6.1-Benutzeranwendung, die die Funktionen für die Identitätsselbstbedienung unterstützt.
`IDMUserApp.jar`	Das funktionsbasierte Bereitstellungsmodul und das Benutzeranwendungsinstallationsprogramm.
`silent.properties`	Eine Datei, die die für eine automatische Installation erforderlichen Parameter enthält. Diese Parameter entsprechen den Installationsparametern, die Sie bei der Installation der GUI oder der Konsolenschnittstelle angegeben haben. Sie sollten diese Datei kopieren und anschließend den Inhalt an Ihre Installationsumgebung anpassen.
`JBossMySQL.bin` oder `JBossMySQL.exe`	Ein praktisches Dienstprogramm zum Installieren des JBoss-Anwendungsservers und der MySQL-Datenbank.
`nmassaml.zip`	Enthält eine eDirectory-Methode zur Unterstützung von SAML. Nur erforderlich, wenn Sie Access Manager nicht verwenden.
`afadmin.jar`	Nur für das Identity Manager 3.5.1-Metaverzeichnis erforderlich.
`prerequisitefiles.zip`	Nur für das Identity Manager 3.5.1-Metaverzeichnis erforderlich. Enthält andere Dateien, die manuell an den korrekten Speicherort kopiert werden müssen.

Das System, auf dem Sie das funktionsbasierte Bereitstellungsmodul für Identity Manager oder Standard Edition der Benutzeranwendung installieren, benötigt mindestens 320 MB verfügbaren Speicherplatz sowie freien Speicher für die unterstützenden Anwendungen (Datenbank, Anwendungsserver usw.). Das System benötigt nach und nach zusätzlichen Speicherplatz für die Aufnahme weiterer Daten, z. B. Datenbanken oder Anwendungsserverprotokolle.

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).

2.3 Installation eines Anwendungsservers

- Abschnitt 2.3.1, „Installation des JBoss-Anwendungsservers“, auf Seite 19
- Abschnitt 2.3.2, „Installation des WebLogic-Anwendungsservers“, auf Seite 21
- Abschnitt 2.3.3, „Installation des WebSphere-Anwendungsservers“, auf Seite 22

2.3.1 Installation des JBoss-Anwendungsservers

Wenn Sie den JBoss-Anwendungsserver verwenden möchten, können Sie Folgendes tun:

- Laden Sie den JBoss-Anwendungsserver herunter und installieren Sie ihn gemäß den Anweisungen des Herstellers. Unter Abschnitt 1.3, „Systemanforderungen“, auf Seite 11 finden Sie die unterstützte Version.
- 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 „Installation des JBoss-Anwendungsservers und der MySQL-Datenbank“ auf Seite 20.

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.

Tabelle 2-3 *Empfohlene Mindestanforderungen für JBoss-Anwendungsserver*

Komponente	Empfehlung
RAM	Für den JBoss-Anwendungsserver sollten mindestens 512 MB RAM zur Verfügung stehen, wenn das funktionsbasierte Bereitstellungsmodul für Identity Manager ausgeführt wird.
Port	8080 ist der Standardport für den Anwendungsserver. Notieren Sie den Port, den Ihr Anwendungsserver verwendet.

Komponente	Empfehlung
SSL	Aktivieren Sie SSL, wenn Sie beabsichtigen, eine externe Passwortverwaltung zu verwenden: ◆ Aktivieren Sie SSL für die JBoss-Server, auf denen Sie das funktionsbasierte Bereitstellungsmodul für Identity Manager und die Datei `IDMPwdMgt.war` bereitstellen möchten. ◆ Stellen Sie sicher, dass der SSL-Port in Ihrer Firewall offen ist. Weitere Informationen zum Aktivieren von SSL finden Sie in Ihrer JBoss-Dokumentation. Informationen zur `IDMPwdMgt.war-Datei` finden Sie in Abschnitt 8.5, „Konfigurieren der externen Passwortverwaltung“, auf Seite 74 und im *Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idmrbpm361/index.html).

Installation des JBoss-Anwendungsservers und der MySQL-Datenbank

Das JBossMysql-Dienstprogramm installiert den JBoss-Anwendungsserver und MySQL auf Ihrem System. Dieses Dienstprogramm unterstützt keinen Konsolenmodus, sondern erfordert eine grafische Benutzeroberflächenumgebung. Linux/Unix-Benutzern wird empfohlen, die Installation als Nicht-root-Benutzer durchzuführen.

1 Suchen Sie die Datei `JBossMySQL.bin` oder `JBossMySQL.exe` in der .iso-Datei und führen Sie sie aus.

`/linux/jboss/JBossMySQL.bin` (für Linux)
`/nt/jboss/JBossMySQL.exe` (für Windows)

Das Dienstprogramm ist für Solaris nicht verfügbar.

2 Führen Sie zur Bedienung des Dienstprogramms die Anweisungen auf dem Bildschirm aus. Weitere Informationen hierzu finden Sie in der folgenden Tabelle.

Installationsbildschirm	Beschreibung
Auswählen des Installationssets	Wählen Sie die zu installierenden Produkte aus. ◆ *JBoss*: Installiert den JBoss-Anwendungsserver in das Verzeichnis, das Sie zusammen mit den Skripts zum Starten und Beenden angeben. **Hinweis:** Dieses Dienstprogramm installiert den JBoss-Anwendungsserver nicht als Windows-Dienst. Anleitungen finden Sie unter „Installation des JBoss-Anwendungsservers als Dienst oder als Daemon“ auf Seite 21. ◆ *MySQL*: Installiert MySQL und erstellt eine MySQL-Datenbank in dem Verzeichnis, das Sie zusammen mit den Skripts zum Starten und Beenden angeben.
Auswählen des übergeordneten JBoss-Ordners	Klicken Sie auf *Auswählen*, um einen anderen Installationsordner als den Standardordner auszuwählen.

Installationsbildschirm	Beschreibung
Auswählen des übergeordneten MySQL-Ordners	Klicken Sie auf *Auswählen*, um einen anderen Installationsordner als den Standardordner auszuwählen.
MySQL-Info	Geben Sie hierzu Folgendes an: ◆ *Datenbankname*: Geben Sie den Namen der Datenbank für das zu erstellende Installationsprogramm an. Das Benutzeranwendungsinstallationsprogramm fragt Sie nach diesem Namen, daher sollten Sie sich den Namen und den Speicherort notieren. ◆ *Root-Benutzer-Passwort* (und Passwort bestätigen): Geben Sie das Root-Benutzer-Passwort für diese Datenbank ein (und bestätigen Sie es).
Zusammenfassung vor der Installation	Überprüfen Sie die Seite „Zusammenfassung“. Wenn die Spezifikationen korrekt sind, klicken Sie 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 2.4.1, „Konfiguration einer MySQL-Datenbank“, auf Seite 22 fort.

Installation des JBoss-Anwendungsservers als Dienst oder als Daemon

Wenn Sie die JBoss-Anwendung als Daemon starten möchten, lesen Sie die Anweisungen unter JBoss (http://wiki.jboss.org/wiki/Wiki.jsp?page=StartJBossOnBootWithLinux).

Verwendung eines JavaServiceWrapper Sie können mithilfe eines JavaServiceWrapper den JBoss-Anwendungsserver als Windows-Dienst installieren, starten und anhalten. 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). 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)).

Wichtig: 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, aber JBoss empfiehlt nicht mehr die Verwendung von JavaService. Einzelheiten finden Sie unter http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService (http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService).

2.3.2 Installation des WebLogic-Anwendungsservers

Wenn Sie den WebLogic-Anwendungsserver 10 verwenden möchten, laden Sie ihn herunter und installieren Sie ihn. Unter Abschnitt 1.3, „Systemanforderungen“, auf Seite 11 finden Sie weitere Informationen zu den unterstützten Versionen.

2.3.3 Installation des WebSphere-Anwendungsservers

Wenn Sie den WebSphere Anwendungsserver 6.1 verwenden möchten, laden Sie ihn herunter und installieren Sie ihn. Unter Abschnitt 1.3, „Systemanforderungen“, auf Seite 11 finden Sie weitere Informationen zu den unterstützten Versionen.

2.4 Installieren einer Datenbank

Die Benutzeranwendung verwendet eine Datenbank für eine Reihe bestimmter Aufgaben, z. B. zum Speichern von Konfigurationsdaten und von Daten aus Workflow-Aktivitäten. Bevor Sie das funktionsbasierte Bereitstellungsmodul oder die Benutzeranwendung installieren können, müssen Sie eine der unterstützten Datenbanken für Ihre Plattform installiert und konfiguriert haben. Dies beinhaltet:

- ❑ Installieren Ihrer Datenbank und des Datenbanktreibers.
- ❑ Erstellen einer Datenbank oder einer Datenbankinstanz.
- ❑ Aufzeichnen der folgenden Datenbankparameter für die Installation des funktionsbasierten Bereitstellungsmoduls für Identity Manager:
  - Host und Port
  - Datenbankname, Benutzername und Benutzerpasswort
- ❑ Erstellen einer Datenquelldatei, die auf die Datenbank zeigt.

  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 und WebLogic müssen Sie die Datenquelle vor der Installation manuell konfigurieren.
- ❑ Datenbanken müssen UTF-8-fähig sein.

Hinweis: Wenn Sie auf eine neue Version des funktionsbasierten Bereitstellungsmoduls migrieren, müssen Sie die gleiche Benutzeranwendungsdatenbank verwenden, die Sie für die vorherige Installation verwendet haben (d. h. die Installation, von der aus Sie migrieren.)

2.4.1 Konfiguration einer MySQL-Datenbank

Die Benutzeranwendung erfordert einige Konfigurationsoptionen für MySQL. Wenn Sie MySQL selbst installieren, müssen Sie diese Einstellungen konfigurieren. 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 23
- „Zeichensatz“ auf Seite 23
- „Beachtung der Groß- und Kleinschreibung“ auf Seite 23

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=utf8&amp;connectionCollation=ut
f8_bin</connection-url>
```

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.

2.5 Installieren des Java Development Kit

Die Installationsprogramme für das funktionsbasierte Bereitstellungsmodul und die Standard Edition der Benutzeranwendung erfordern, dass Sie mindestens das Java 2 Platform Standard Edition Development Kit in Version 1.5 verwenden.

Setzen Sie die Umgebungsvariable JAVA_HOME so, dass sie auf das JDK* verweist, das mit der Benutzeranwendung verwendet werden soll. Alternativ können Sie den Pfad während der Installation der Benutzeranwendung manuell eingeben, um JAVA_HOME zu überschreiben.

Hinweis: Für Benutzer von SUSE Linux Enterprise Server (SLES): Verwenden Sie nicht das mit SLES mitgelieferte IBM* JDK. Diese Version ist mit einigen Aspekten der Installation nicht kompatibel. Sie müssen das Sun JDK verwenden.

2.6 Installieren zusätzlicher Dateien für Metaverzeichnis 3.5.1

Wenn Sie das Identity Manager 3.5.1-Metaverzeichnis verwenden, müssen Sie die zusätzlichen Schritte ausführen, die in diesen Abschnitten beschrieben werden:

- Abschnitt 2.6.1, „Installieren des Funktionsservice-Treibers mithilfe der GUI“, auf Seite 24
- Abschnitt 2.6.2, „Installieren des Funktionsservice-Treibers über die Konsole“, auf Seite 26
- Abschnitt 2.6.3, „Kopieren der iManager-Symbole“, auf Seite 26
- Abschnitt 2.6.4, „Kopieren von afadmin.jar“, auf Seite 26

Linux/Unix-Benutzer müssen die Installation als Nicht-root-Benutzer durchführen.

2.6.1 Installieren des Funktionsservice-Treibers mithilfe der GUI

Dies ist nur erforderlich, wenn Sie Idas dentity Manager 3.5.1-Metaverzeichnis verwenden. Wenn Sie das Identity Manager 3.6-Metaverzeichnis installiert haben, sind diese Dateien bereits installiert.

Das Installationsprogramm für den Funktionsservice- und Benutzeranwendungstreiber bietet Optionen für die folgenden Aktionen:

- Erweitern des Identitätsdepot-Schemas, um die Benutzeranwendung und das funktionsbasierte Bereitstellungsmodul zu unterstützen
- Installieren der Konfigurationsdateien für den Funktionsservice-Treiber und den Benutzeranwendungstreiber auf dem Metaverzeichnis-Server.
- Installieren der Konfigurationsdateien für den Funktionsservice-Treiber und den Benutzeranwendungstreiber in iManager.

Sie müssen dieses Installationsprogramm auf den Metaverzeichnis- und iManager-Computern ausführen.

Hinweis: Ihr Metaverzeichnis muss am Standardspeicherort installiert sein, damit Sie dieses Installationsprogramm verwenden können.

Zugriff auf `Roles_Driver_Install_Utility.iso`

1 Suchen Sie das Installationsprogramm für Ihr Betriebssystem und führen Sie es aus:

Betriebssystem	Installationsprogramm für den Funktionsservice-Treiber:
AIX	`roles_driver_install.aix.bin`
Linux	`roles_driver_install.linux.bin`
Solaris	`roles_driver_install.solaris.bin`
Windows	`roles_dirver_install.exe`

2 Mithilfe der folgenden Informationen wird die Installation ausgeführt:

Installationsbildschirm	Beschreibung
Lizenzvereinbarung	Lesen Sie die Lizenzvereinbarung und klicken Sie auf *Lizenzvertrag zustimmen*.
Auswählen der Komponenten	*Treiber*: Installiert den Funktionsservice-Treiber und den Benutzeranwendungstreiber auf dem Metaverzeichnis-Server und aktualisiert die unterstützenden Bibliothek-JARs. *Schema*: Aktualisiert das Metaverzeichnisschema, um die für das funktionsbasierte Bereitstellungsmodul und die Standard Edition der Benutzeranwendung benötigten Objekte einzuschließen. Es installiert die Dateien `nrf-extensions.sch` und srvprv.sch und führt den Befehl (`NdsCons.exe` für Windows und `ndssch` für UNIX/Linux) der aktuellen Plattform aus. *Treiberkonfigurationsdateien*: Installiert die Funktionsservice-Treiber und die Konfigurationsdateien für den Benutzeranwendungstreiber. Diese Dateien werden verwendet, wenn Sie die neuen Treiber in iManager erstellen. Sie müssen dies auf dem iManager-Computer ausführen.
Authentifizierung	Wenn Sie *Schemaerweiterungen* auswählen, müssen Sie einen Benutzernamen und ein Passwort angeben. Dieser Benutzer benötigt Administratorrechte für das Identitätsdepot. Beispiel: *cn=admin,o=novell*.
Auswählen des Speicherortes für den Treiber	Wenn Sie den Funktionsservice und den Benutzeranwendungstreiber zur Installation ausgewählt haben, werden Sie nach dem Speicherort auf dem eDirectory-Server gefragt. In der Regel werden sie im Verzeichnis „/lib/dirxml/classes“ vom Metaverzeichnis installiert.
Installationsverzeichnis für Treiberkonfigurationsdateien	Geben Sie an, wo das Installationsprogramm die Treiberkonfigurationsdateien auf dem iManager-Computer speichern soll. In der Regel werden sie im Verzeichnis „/nps/Dirxml.Drivers“ vom iManager installiert.
Zusammenfassung vor der Installation	Überprüfen Sie auf der Seite „Zusammenfassung vor der Installation“ die Einstellungen der Installationsparameter und schließen Sie die Installation ab.

2.6.2 Installieren des Funktionsservice-Treibers über die Konsole

Führen Sie den folgenden Befehl aus, um das Installationsprogramm im Konsolenmodus (Textmodus) auszuführen:

```
roles_driver_install_<operatingsystemfile> -i console
```

Führen Sie die gleichen Schritte für die grafische Benutzeroberfläche aus, wie unter Abschnitt 2.6.1, „Installieren des Funktionsservice-Treibers mithilfe der GUI“, auf Seite 24 beschrieben, lesen Sie die Eingabeaufforderungen und geben Sie die Antworten auf der Befehlszeile ein.

2.6.3 Kopieren der iManager-Symbole

Hinweis: Dieses Verfahren ist nicht erforderlich, wenn Sie iManager 2.7 zusammen mit den neuesten Plugins installiert haben.

1. Suchen Sie in Ihrem heruntergeladenen `.iso`-Image die Datei `prerequisites.zip`.
2. Entpacken Sie sie und suchen Sie die Datei `iManager_icons_for_roles.zip`.

   Diese Datei enthält die iManager-Symbole für Funktionsobjekte in eDirectory.
3. Entpacken Sie sie und kopieren Sie anschließend die extrahierten Symbole ins Verzeichnis `nps/portal/modules/dev/images/dir`.
4. Starten Sie iManager neu, sodass es die neuen Symbole verwendet.

2.6.4 Kopieren von afadmin.jar

Hinweis: Dieses Verfahren ist nicht erforderlich, wenn Sie iManager 2.7 zusammen mit den neuesten Plugins installiert haben.

1. Suchen Sie in Ihrem heruntergeladenen `.iso`-Image die Datei `prerequisites.zip`.

   Sie finden Sie im Verzeichnis `/36MetaDirSupport`.
2. Entpacken Sie die Datei und suchen Sie die Datei `afadmin.jar`.
3. Kopieren Sie `afadmin.jar` ins Verzeichnis `/iManager/nps/WEB-INF/lib`.

Erstellen von Treibern

3

In diesem Abschnitt wird beschrieben, wie die Treiber zur Verwendung des funktionsbasierten Bereitstellungsmoduls 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.

Mit der Treiberkonfigurationsunterstützung können Sie Folgendes ausführen:

- Verknüpfen eines Benutzeranwendungstreibers mit einem Funktionsservice-Treiber
- Verknüpfen einer Benutzeranwendung mit einem Benutzeranwendungstreiber

3.1 Erstellen des Benutzeranwendungstreibers in iManager

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.

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 *Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idmrbpm361/index.html).

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 in einem Webbrowser.

   Verwenden von iManager 2.6 (für Identity Manager 3.5.1) oder iManager 2.7 (für Identity Manager 3.6).

2. Gehen Sie zu *Funktionen und Aufgaben* > *Identity Manager-Dienstprogramme* und wählen Sie *Neuer Treiber* oder *Konfiguration importieren* (abhängig von der Version des von Ihnen verwendeten Plugins).

   Für Identity Manager 3.5.1 verwenden Sie den Link *Neuer Treiber*.

Für Identity Manager 3.6 verwenden Sie den Link *Konfiguration importieren*.

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 die Konfigurationsdatei für den Benutzeranwendungstreiber aus der Dropdown-Liste aus. Der Dateiname lautet:

   UserApplication_3_6_1-IDM3_5_1-V1.xml

   Wenn sich diese Datei nicht in der Liste befindet, ist der Funktionsservice-Treiber möglicherweise nicht ordnungsgemäß installiert. Weitere Informationen finden Sie unter Abschnitt 2.6.1, „Installieren des Funktionsservice-Treibers mithilfe der GUI“, auf Seite 24.

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. Der Standard 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:	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. Klicken Sie anschließend auf *Weiter*, um die Zusammenfassungsseite 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

Hinweis: Sie brauchen die Schritte in diesem Abschnitt nicht durchzuführen, wenn Sie die Standard Edition der Benutzeranwendung verwenden.

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

1 Öffnen Sie iManager in einem Webbrowser.

Verwenden Sie 2.6 (für Identity Manager 3.5.1) oder iManager 2.7 (für Identity Manager 3.6).

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 3.6.1 des Benutzeranwendungstreibers (`UserApplication_3_6_1-IDM3_5_1-V1.xml`) mit dem Funktionsservice-Treiber. Wenn Sie eine andere Version des Benutzeranwendungstreibers verwenden, ist der Funktionskatalog nicht verfügbar.

3 Klicken Sie auf *Treiber hinzufügen*.

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

5 Wählen Sie *RoleService_3_6_1-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 sie nicht in dieser Dropdown-Liste enthalten ist, haben Sie die Datei nicht an den richtigen Speicherort kopiert. Weitere Informationen finden Sie unter Abschnitt 2.6.1, „Installieren des Funktionsservice-Treibers mithilfe der GUI“, auf Seite 24.

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. Starten Sie iManager und eDirectory neu, um sicherzustellen, dass alle neuen Schemaänderungen ordnungsgemäß übernommen wurden.

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.
DN des Benutzergruppen-Basiscontainers	Der Treiber wirkt sich nur auf Benutzer, Container und Gruppe in diesem Basiscontainer aus. Wenn es Gruppenfunktionszuweisungen gibt, erteilt bzw. entzieht der Funktionstreiber nur Funktionen von Mitgliedern innerhalb der Domäne des Containers.

Option	Beschreibung
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.
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 *Weiter*.
8. 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.
9. (Optional, aber empfohlen) Klicken Sie auf *Verwaltungsfunktionen ausschließen*.
10. 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*.
11. Klicken Sie auf *OK*, um das Fenster „Sicherheitsäquivalenzen“ zu schließen. Klicken Sie anschließend auf *Weiter*, um die Zusammenfassungsseite anzuzeigen.
12. Wenn die Informationen korrekt sind, klicken Sie auf *Fertig stellen*.

Installieren auf JBoss mithilfe des GUI-Installationsprogramms

4

In diesem Abschnitt wird die Installation des funktionsbasierten Bereitstellungsmoduls für Identity Manager auf einem JBoss-Anwendungsserver über die grafische Benutzeroberfläche des Installationsprogramms erläutert. Es werden folgende Themen behandelt:

- Abschnitt 4.1, „Installieren und Konfigurieren der Benutzeranwendungs-WAR“, auf Seite 33
- Abschnitt 4.2, „Testen der Installation“, auf Seite 39

Wenn Sie die Installation lieber über die Befehlszeile durchführen möchten, lesen Sie Kapitel 7, „Installation von der Konsole aus oder mit einem einzigen Befehl“, auf Seite 59.

Führen Sie das Installationsprogramm als Nicht-root-Benutzer aus.

4.1 Installieren und Konfigurieren der Benutzeranwendungs-WAR

Hinweis: Das Installationsprogramm erfordert mindestens das Java 2 Platform Standard Edition Development Kit Version 1.5. Wenn Sie eine frühere Version verwenden, wird die WAR-Datei der Benutzeranwendung bei der Installation nicht richtig konfiguriert. Die Installation scheint erfolgreich zu verlaufen, Sie erhalten aber Fehlermeldungen, wenn Sie die Benutzeranwendung starten.

1 Starten Sie das Installationsprogramm für Ihre Plattform über die Befehlszeile:

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

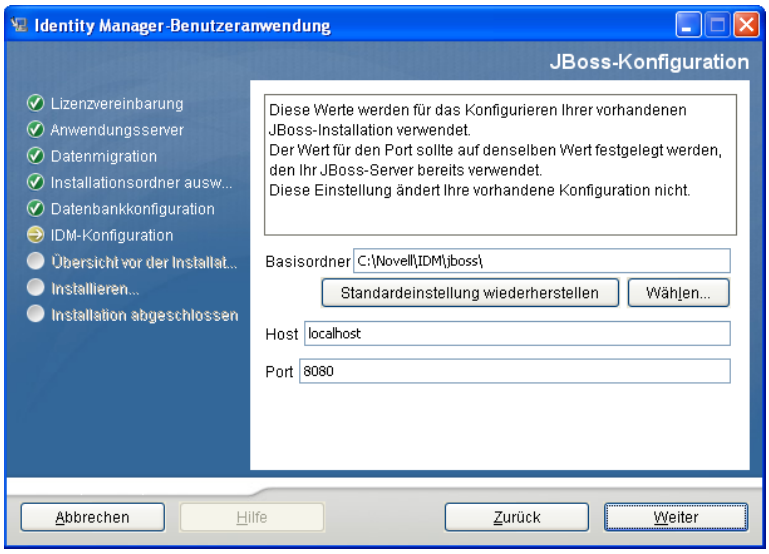
Wenn das Installationsprogramm startet, werden Sie nach der Sprache gefragt.

2 Verwenden Sie die folgenden Informationen zusammen mit den Anweisungen in jedem Installationsteilfenster, um die Installation abzuschließen:

Installationsbildschirm	Beschreibung
Novell Identity Manager	Wählen Sie die Sprache für das Installationsprogramm. Die Standardeinstellung ist „Englisch“.
Lizenzvereinbarung	Lesen Sie die Lizenzvereinbarung und klicken Sie auf *Lizenzvertrag zustimmen*.
Anwendungsserverplattform	Wählen Sie *JBoss*.
Standard oder Bereitstellung	*Standard*: Wählen Sie diese Option, wenn Sie die Standard Edition der Benutzeranwendung installieren. *Funktionsbasierte Bereitstellung*: Wählen Sie diese Option, wenn Sie das funktionsbasierte Bereitstellungsmodul installieren.
Datenmigration	Akzeptieren Sie den Standardwert (stellen Sie sicher, dass *Ja* nicht ausgewählt ist). **Warnung:** Wählen Sie nicht *Ja*. Wenn "Ja" ausgewählt wird, treten beim Starten der Benutzeranwendung Probleme auf. Weitere Informationen zur Migration finden Sie im *Benutzeranwendung: Migrationshandbuch* (http://www.novell.com/documentation/idmrbpm361/index.html).
Wo ist die WAR-Datei abgelegt?	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.
Installationsordner auswählen	Geben Sie an, wo das Installationsprogramm die Dateien speichern soll.
Datenbankplattform	Wählen Sie die Datenbankplattform. Die Datenbank- und JDBC-Treiber müssen bereits installiert sein. Die gültigen Optionen sind: ◆ MySQL ◆ Oracle (Sie werden nach der Oracle-Version gefragt) ◆ Microsoft SQL Server
Datenbank-Host und Port	*Host*: Geben Sie den Hostnamen 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.

Installationsbildschirm	Beschreibung
Datenbankname und privilegierter Benutzer	*Datenbankname (oder SID)*: Geben Sie für MySQL oder Microsoft SQL Server den Namen Ihrer 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. *Datenbankpasswort/Passwort bestätigen*: Geben Sie das Datenbankpasswort an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied dasselbe Passwort angegeben werden.
Java-Installation	Geben Sie den Java-Stamminstallationsordner an.

Sie werden gefragt, wo Ihr JBoss-Anwendungsserver installiert ist.

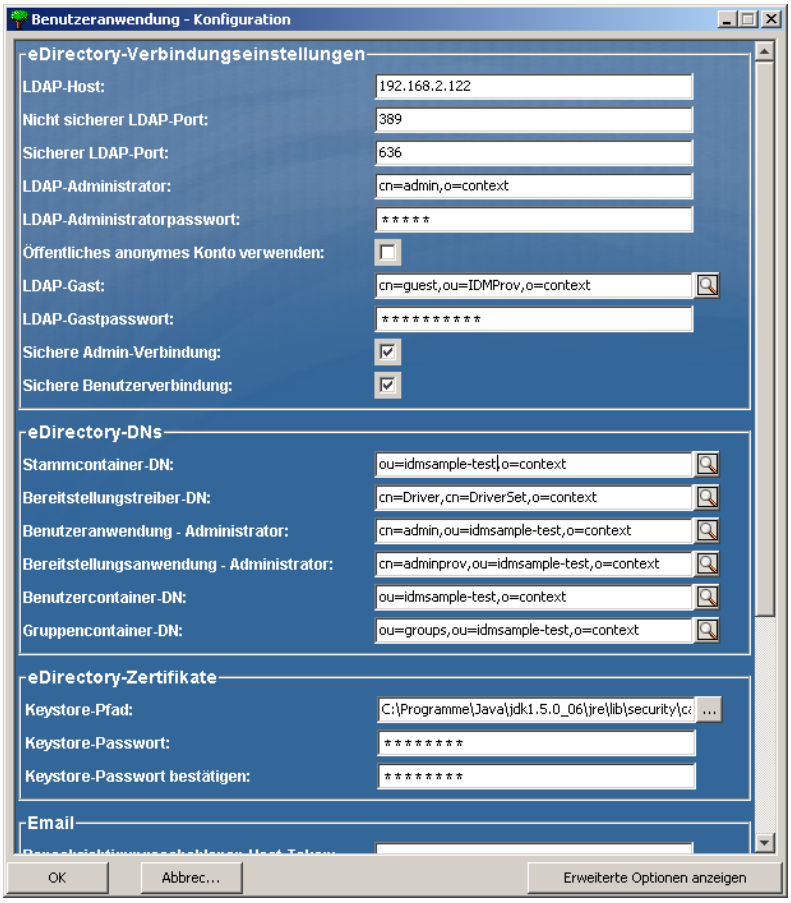


3 Verwenden Sie die folgenden Informationen, um dieses Teilfenster fertigzustellen und mit der Installation fortzufahren.

Installationsbildschirm	Beschreibung
JBoss-Konfiguration	Teilt der Benutzeranwendung mit, wo sich der JBoss-Anwendungsserver befindet. Bei diesem Installationsvorgang wird der JBoss-Anwendungsserver nicht installiert. Eine Anleitung für die Installation des JBoss-Anwendungsservers finden Sie in „Installation des JBoss-Anwendungsservers und der MySQL-Datenbank“ auf Seite 20. *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.
IDM-Konfiguration	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. Wenn Sie *Standard* auswählen und zu einem späteren Zeitpunkt einen Cluster benötigen, müssen Sie die Benutzeranwendung erneut installieren. *Anwendungsname*: Der Name der Anwendungsserver-Konfiguration, 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 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 *Benutzeranwendung: Administrationshandbuch* in Abschnitt 3.5.4 zur Konfiguration von Workflows für das Clustering.
Audit-Protokollierung	Klicken Sie auf *Ja*, um die Protokollierung zu aktivieren. Im nächsten Teilfenster werden Sie aufgefordert, den Typ für die Protokollierung anzugeben. Treffen Sie eine Auswahl aus den folgenden Optionen: ◆ *Novell Audit*: Aktiviert die Novell® Audit-Protokollierung für die Benutzeranwendung. ◆ *OpenXDAS*: Ereignisse werden auf Ihrem OpenXDAS-Protokollierungsserver protokolliert. Weitere Informationen zum Einrichten der Novell Audit- oder OpenXDAS-Protokollierung finden Sie im *Benutzeranwendung: Administrationshandbuch*.
Novell Audit	*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 Cache-Protokoll*: Geben Sie das Verzeichnis für den Protokollierungs-Cache-Speicher an.

Installationsbildschirm	Beschreibung
Sicherheit - Master-Schlüssel	*Ja*: Erlaubt den Import eines vorhandenen Master-Schlüssels. Wenn ein vorhandener verschlüsselter Master-Schlüssel importiert werden soll, kopieren Sie den Schlüssel und fügen Sie ihn in das Fenster des Installationsvorgangs ein. *Nein*: Erstellt einen neuen Master-Schlüssel. Nach Abschluss der Installation müssen Sie den Master-Schlüssel manuell speichern, wie in Abschnitt 8.1, „Aufzeichnen des Master-Schlüssels“, auf Seite 71 beschrieben. Bei der Installation wird der verschlüsselte Master-Schlüssel im Installationsverzeichnis in die Datei `master-key.txt` geschrieben. 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.

4 Sie werden zur Eingabe der Informationen aufgefordert, die das Installationsprogramm zum Konfigurieren der Benutzeranwendungs-WAR-Datei verwendet. (Wenn Sie nicht zur Eingabe dieser Informationen aufgefordert werden, haben Sie möglicherweise die in Abschnitt 2.5, „Installieren des Java Development Kit“, auf Seite 23 aufgeführten Schritte nicht ausgeführt.



5 Verwenden Sie die folgenden Informationen, um das Teilfenster auszufüllen und mit der Installation fortzufahren.

Installationsbildschirm	Beschreibung
Benutzeranwendung - Konfiguration	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. Unter Anhang A, „IDM Benutzeranwendung - Konfigurationsreferenz“, auf Seite 79 finden Sie eine Beschreibung für jede Option.

Installationsbildschirm	Beschreibung
Zusammenfassung vor der Installation	Überprüfen Sie auf der Seite „Zusammenfassung vor der Installation“ die Einstellungen der Installationsparameter. 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. 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*.
Installation abgeschlossen	Zeigt an, dass die Installation abgeschlossen ist.

4.1.1 Anzeigen der Installations- und Protokolldateien

Wenn die Installation ohne Fehler abgeschlossen wurde, fahren Sie mit Testen der Installation 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.

4.2 Testen der Installation

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` oder `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 wird angezeigt.

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 8.7, „Fehlersuche“, auf Seite 76 nach.

5 Installation auf einem WebSphere-Anwendungsserver mithilfe des GUI-Installationsprogramms

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

Führen Sie das Installationsprogramm als Nicht-root-Benutzer aus.

5.1 Installieren und Konfigurieren der Benutzeranwendungs-WAR

Hinweis: Das Installationsprogramm erfordert mindestens das Java 2 Platform Standard Edition Development Kit Version 1.5. Wenn Sie eine frühere Version verwenden, wird die WAR-Datei der Benutzeranwendung bei der Installation nicht richtig konfiguriert. Die Installation scheint erfolgreich zu verlaufen, Sie erhalten aber Fehlermeldungen, wenn Sie die Benutzeranwendung starten.

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

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

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

   Wenn das Installationsprogramm startet, werden Sie nach der Sprache gefragt.

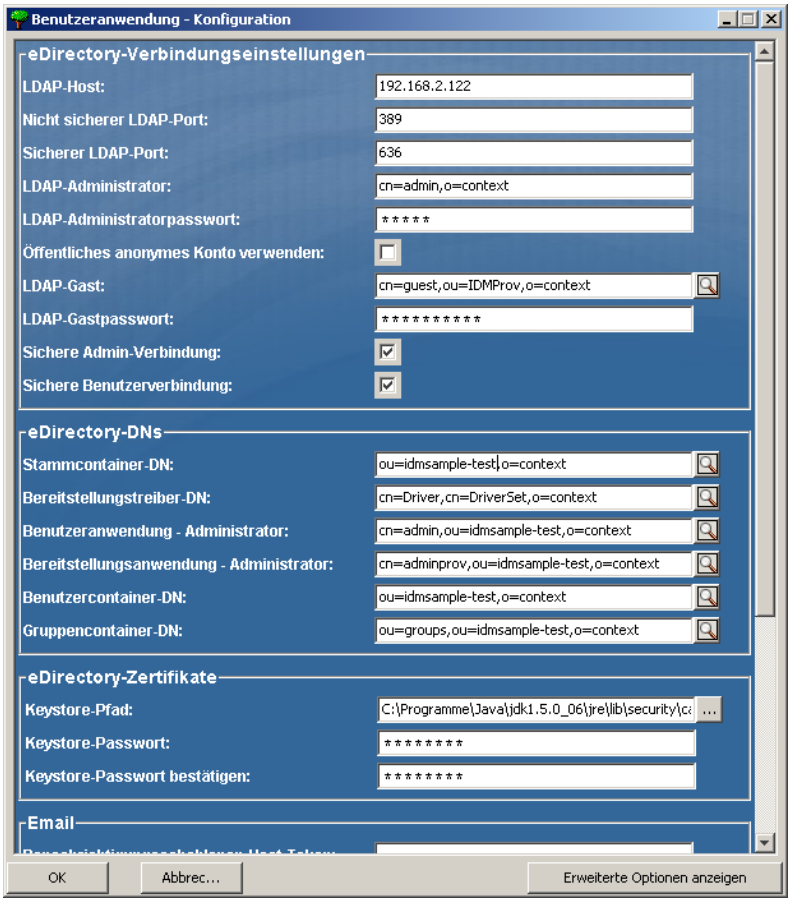
3 Verwenden Sie die folgenden Informationen zusammen mit den Anweisungen in jedem Installationsteilfenster, um die Installation abzuschließen:

Installationsbildschirm	Beschreibung
Novell Identity Manager	Wählen Sie die Sprache für das Installationsprogramm. Die Standardeinstellung ist „Englisch“.
Lizenzvereinbarung	Lesen Sie die Lizenzvereinbarung und klicken Sie auf *Lizenzvertrag zustimmen*.
Anwendungsserverplattform	Wählen Sie *WebSphere.* Wenn sich die WAR-Datei der Benutzeranwendung nicht im selben Verzeichnis befindet wie das Installationsprogramm, werden Sie aufgefordert, den Pfad zur WAR-Datei einzugeben. 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.
Standard oder Bereitstellung	*Standard*: Wählen Sie diese Option, wenn Sie die Standard Edition der Benutzeranwendung installieren. *Funktionsbasierte Bereitstellung*: Wählen Sie diese Option, wenn Sie das funktionsbasierte Bereitstellungsmodul installieren.
Datenmigration	Akzeptieren Sie den Standardwert (stellen Sie sicher, dass *Ja* nicht ausgewählt ist). **Warnung:** Wählen Sie nicht *Ja*. Wenn "Ja" ausgewählt wird, treten beim Starten der Benutzeranwendung Probleme auf. Weitere Informationen zur Migration finden Sie im *Benutzeranwendung: Migrationshandbuch* (http://www.novell.com/documentation/idmrbpm361/index.html).
Wo ist die WAR-Datei abgelegt?	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.
Auswählen des Installationsordners	Geben Sie an, wo das Installationsprogramm die Dateien speichern soll.
Datenbankplattform	Wählen Sie die Datenbankplattform. Die Datenbank- und JDBC-Treiber müssen bereits installiert sein. Die gültigen Optionen sind: ◆ Oracle (Sie werden nach der Oracle-Version gefragt) ◆ Microsoft SQL Server ◆ DB2

Installationsbildschirm	Beschreibung
Java-Installation	Geben Sie den Java-Stamminstallationsordner an. **Hinweis:** Mit WebSphere müssen Sie das IBM JDK mit den unbeschränkten Richtliniendateien verwenden.
IDM-Konfiguration	Angeben des Anwendungskontexts
Audit-Protokollierung	Klicken Sie auf *Ja*, um die Protokollierung zu aktivieren. Im nächsten Teilfenster werden Sie aufgefordert, den Typ für die Protokollierung anzugeben. Treffen Sie eine Auswahl aus den folgenden Optionen: ◆ *Novell Audit*: Aktiviert die Novell Audit-Protokollierung für die Benutzeranwendung. Weitere Informationen zum Einrichten der Novell Audit-Protokollierung finden Sie im *Identity Manager-Benutzeranwendung: Administrationshandbuch*. ◆ *OpenXDAS*: Ereignisse werden auf Ihrem OpenXDAS-Protokollierungsserver protokolliert. Weitere Informationen zum Einrichten der Novell Audit- oder OpenXDAS-Protokollierung finden Sie im *Benutzeranwendung: Administrationshandbuch*.
Novell Audit	*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 Cache-Protokoll*: Geben Sie das Verzeichnis für den Protokollierungs-Cache-Speicher an.

Installationsbildschirm	Beschreibung
Sicherheit - Master-Schlüssel	*Ja*: Erlaubt den Import eines vorhandenen Master-Schlüssels. Wenn ein vorhandener verschlüsselter Master-Schlüssel importiert werden soll, kopieren Sie den Schlüssel und fügen Sie ihn in das Fenster des Installationsvorgangs ein. *Nein*: Erstellt einen neuen Master-Schlüssel. Nach Abschluss der Installation müssen Sie den Master-Schlüssel manuell aufzeichnen. Bei der Installation wird der verschlüsselte Master-Schlüssel im Installationsverzeichnis in die Datei `master-key.txt` geschrieben. 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.

4 Sie werden zur Eingabe der Informationen aufgefordert, die das Installationsprogramm zum Konfigurieren der Benutzeranwendungs-WAR-Datei verwendet. (Wenn Sie nicht zur Eingabe dieser Informationen aufgefordert werden, haben Sie möglicherweise die in Abschnitt 2.5, „Installieren des Java Development Kit“, auf Seite 23 aufgeführten Schritte nicht ausgeführt.



5 Verwenden Sie die folgenden Informationen, um das Teilfenster auszufüllen und mit der Installation fortzufahren.

Installationsbildschirm	Beschreibung
Benutzeranwendung - Konfiguration	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. Weitere Informationen finden Sie unter Anhang A, „IDM Benutzeranwendung - Konfigurationsreferenz“, auf Seite 79.

Installationsbildschirm	Beschreibung
Zusammenfassung vor der Installation	Überprüfen Sie auf der Seite „Zusammenfassung vor der Installation“ die Einstellungen der Installationsparameter. 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. 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*.
Installation abgeschlossen	Zeigt an, dass die Installation abgeschlossen ist.

5.1.1 Anzeigen der Installationsprotokolldateien

Wenn die Installation ohne Fehler abgeschlossen wurde, fahren Sie mit Abschnitt 5.2.1, „Hinzufügen von Benutzeranwendungs-Konfigurationsdateien und JVM-Systemeigenschaften“, auf Seite 46 fort.

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

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

5.2 Konfigurieren der WebSphere-Umgebung

5.2.1 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.

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

5.2.2 Importieren der eDirectory-Herkunftsverbürgung in den WebSphere-Keystore

1 Kopieren Sie die eDirectory™ Herkunftsverbürgungszertifikate auf den WebSphere-Server.

Bei der Installation der Benutzeranwendung werden die Zertifikate in das Verzeichnis exportiert, in dem Sie die Benutzeranwendung installieren.

2 Importieren Sie die Zertifikate in den WebSphere-Keystore. Sie können dies mithilfe der WebSphere-Administrationskonsole („Zertifikate mit der WebSphere-Administrationskonsole importieren“ auf Seite 48) oder über die Befehlszeile („Zertifikate über die Befehlszeile importieren“ auf Seite 48) tun.

3 Fahren Sie nach dem Importieren der Zertifikate mit Abschnitt 5.3, „Bereitstellung der WAR-Datei“, auf Seite 48 fort.

Zertifikate mit der WebSphere-Administrationskonsole importieren

1. Melden Sie sich bei der Administrationskonsole von WebSphere als Admin-Benutzer an.
2. Rufen Sie in der linken Kontrollleiste *Security* > *SSL Certificate and Key Management* auf.
3. Rufen Sie in der Liste der Einstellungen auf der rechten Seite unter *Additional Properties* die Option *Key stores and certificates* auf.
4. Wählen Sie *NodeDefaultTrustStore* (oder den Verbürgungsspeicher, den Sie verwenden).
5. Wählen Sie rechts unter *Additional Properties* die Option *Signer Certificates* aus.
6. Klicken Sie auf *Add*.
7. Geben Sie den Aliasnamen und den vollständigen Pfad zur Zertifikatsdatei ein.
8. Ändern Sie den Datentyp in der Dropdown-Liste in *Binary DER data*.
9. Klicken Sie auf *OK*. Jetzt sollte das Zertifikat in der Liste der Signierzertifikate angezeigt werden.

Zertifikate über die Befehlszeile importieren

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.

5.3 Bereitstellung der WAR-Datei

Stellen Sie die WAR-Datei mithilfe der WebSphere-Bereitstellungswerkzeuge bereit.

5.4 Starten der und Zugriff auf die Benutzeranwendung

So starten Sie die Benutzeranwendung:

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.

So greifen Sie auf die Benutzeranwendung zu:

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`

Installation auf einem WebLogic-Anwendungsserver mithilfe des GUI-Installationsprogramms

6

Das WebLogic-Installationsprogramm konfiguriert die Benutzeranwendungs-WAR-Datei basierend auf Ihrer Eingabe. In diesem Abschnitt finden Sie Details zu folgenden Themen:

Informationen zum Installieren mithilfe einer nicht-grafischen Benutzeroberfläche finden Sie unter Kapitel 7, „Installation von der Konsole aus oder mit einem einzigen Befehl“, auf Seite 59.

Führen Sie das Installationsprogramm als Nicht-root-Benutzer aus.

6.1 WebLogic-Installations-Checkliste

- ❑ Erstellen Sie eine WebLogic-fähige WAR-Datei.

  Führen Sie diese Aufgabe mithilfe des Installationsprogramms der Identity Manager-Benutzeranwendung durch. Weitere Informationen hierzu finden Sie unter Abschnitt 6.2, „Installieren und Konfigurieren der Benutzeranwendungs-WAR“, auf Seite 51.

- ❑ Bereiten Sie die WebLogic-Umgebung für die WAR-Bereitstellung vor, indem Sie die Konfigurationsdateien an die entsprechenden WebLogic-Speicherorte kopieren.

  Weitere Informationen hierzu finden Sie unter Abschnitt 6.3, „Vorbereiten der WebLogic-Umgebung“, auf Seite 56.

- ❑ Stellen Sie die WAR-Datei bereit.

  Weitere Informationen hierzu finden Sie unter Abschnitt 6.4, „Bereitstellen der Benutzeranwendungs-WAR-Datei“, auf Seite 58.

6.2 Installieren und Konfigurieren der Benutzeranwendungs-WAR

Hinweis: Das Installationsprogramm erfordert mindestens das Java 2 Platform Standard Edition Development Kit Version 1.5. Wenn Sie eine frühere Version verwenden, wird die WAR-Datei der Benutzeranwendung bei der Installation nicht richtig konfiguriert. Die Installation scheint erfolgreich zu verlaufen, Sie erhalten aber Fehlermeldungen, wenn Sie die Benutzeranwendung starten.

---

1 Rufen Sie das Verzeichnis mit den Installationsdateien auf.

2 Starten Sie das Installationsprogramm für Ihre Plattform über die Befehlszeile:

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

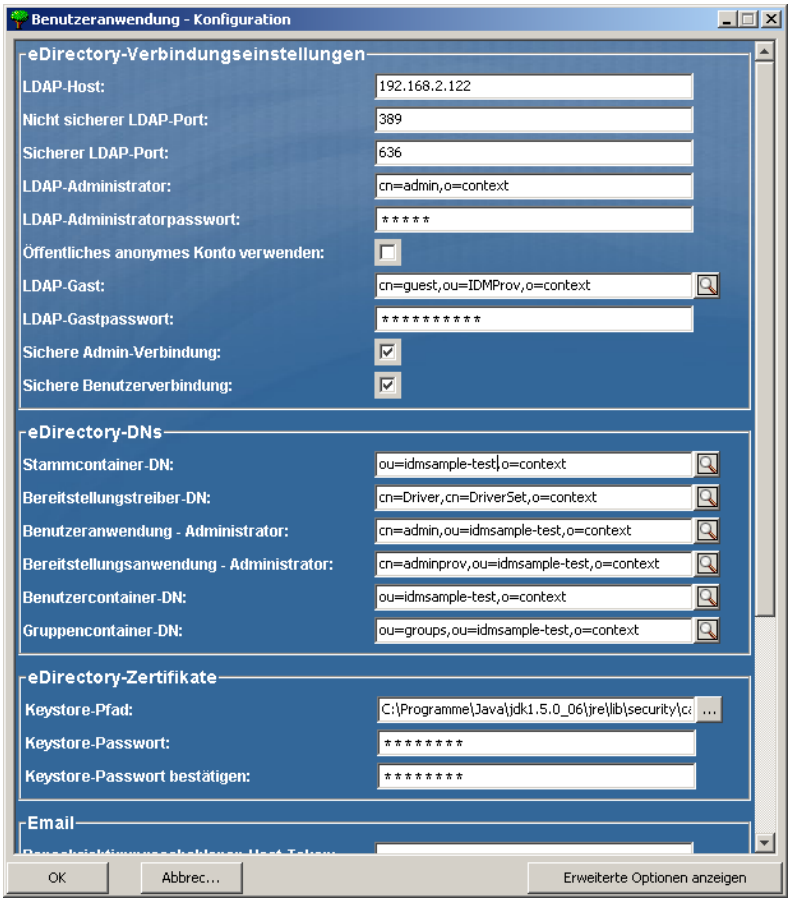
Wenn das Installationsprogramm startet, werden Sie nach der Sprache gefragt.

3 Verwenden Sie die folgenden Informationen zusammen mit den Anweisungen in jedem Installationsteilfenster, um die Installation abzuschließen:

Installationsbildschirm	Beschreibung
Novell Identity Manager	Wählen Sie die Sprache für das Installationsprogramm. Die Standardeinstellung ist „Englisch“.
Lizenzvereinbarung	Lesen Sie die Lizenzvereinbarung und klicken Sie auf *Lizenzvertrag zustimmen*.
Anwendungsserverplattform	Wählen Sie *WebLogic* für den Anwendungsserver aus.
Standard oder Bereitstellung	*Standard*: Wählen Sie diese Option, wenn Sie die Standard Edition der Benutzeranwendung installieren. *Funktionsbasierte Bereitstellung*: Wählen Sie diese Option, wenn Sie das funktionsbasierte Bereitstellungsmodul installieren.
Datenmigration	Akzeptieren Sie den Standardwert (stellen Sie sicher, dass *Ja* nicht ausgewählt ist). **Warnung:** Wählen Sie nicht *Ja*. Wenn "Ja" ausgewählt wird, treten beim Starten der Benutzeranwendung Probleme auf. Weitere Informationen zur Migration finden Sie im *Benutzeranwendung: Migrationshandbuch* (http://www.novell.com/documentation/idmrbpm361/index.html).
Wo ist die WAR-Datei abgelegt?	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.
Installationsordner auswählen	Geben Sie an, wo das Installationsprogramm die Dateien speichern soll.
Datenbankplattform	Wählen Sie die Datenbankplattform. Die Datenbank- und JDBC-Treiber müssen bereits installiert sein. Die gültigen Optionen sind: ◆ Oracle (Sie werden nach der Oracle-Version gefragt) ◆ Microsoft SQL Server
Java-Installation	Geben Sie den Java-Stamminstallationsordner an.
IDM-Konfiguration	Geben Sie den Anwendungskontext an. Dies wird ein Teil der URL sein, wenn Sie die Benutzeranwendung in einem Browser starten.
Audit-Protokollierung	Klicken Sie auf *Ja*, um die Protokollierung zu aktivieren. Im nächsten Teilfenster werden Sie aufgefordert, den Typ für die Protokollierung anzugeben. Treffen Sie eine Auswahl aus den folgenden Optionen: ◆ *Novell Audit*: Aktiviert die Novell Audit-Protokollierung für die Benutzeranwendung. ◆ *OpenXDAS*: Ereignisse werden auf Ihrem OpenXDAS-Protokollierungsserver protokolliert. Weitere Informationen zum Einrichten der Novell Audit- oder OpenXDAS-Protokollierung finden Sie im *Benutzeranwendung: Administrationshandbuch*.

Installationsbildschirm	Beschreibung
Novell Audit	*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 Cache-Protokoll*: Geben Sie das Verzeichnis für den Protokollierungs-Cache-Speicher an.
Sicherheit - Master-Schlüssel	*Ja*: Erlaubt den Import eines vorhandenen Master-Schlüssels. Wenn ein vorhandener verschlüsselter Master-Schlüssel importiert werden soll, kopieren Sie den Schlüssel und fügen Sie ihn in das Fenster des Installationsvorgangs ein. *Nein*: Erstellt einen neuen Master-Schlüssel. Nach Abschluss der Installation müssen Sie den Master-Schlüssel manuell speichern, wie in Abschnitt 8.1, „Aufzeichnen des Master-Schlüssels“, auf Seite 71 beschrieben. Bei der Installation wird der verschlüsselte Master-Schlüssel im Installationsverzeichnis in die Datei `master-key.txt` geschrieben. 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.

4 Sie werden zur Eingabe der Informationen aufgefordert, die das Installationsprogramm zum Konfigurieren der Benutzeranwendungs-WAR-Datei verwendet. (Wenn Sie nicht zur Eingabe dieser Informationen aufgefordert werden, haben Sie möglicherweise die in Abschnitt 2.5, „Installieren des Java Development Kit“, auf Seite 23 aufgeführten Schritte nicht ausgeführt.



Installationsbildschirm	Beschreibung
Benutzeranwendung - Konfiguration	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. Weitere Informationen finden Sie unter Anhang A, „IDM Benutzeranwendung - Konfigurationsreferenz“, auf Seite 79.
Zusammenfassung vor der Installation	Überprüfen Sie auf der Seite „Zusammenfassung vor der Installation“ die Einstellungen der Installationsparameter. 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. 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*.

Installationsbildschirm	Beschreibung
Installation abgeschlossen	Zeigt an, dass die Installation abgeschlossen ist.

6.2.1 Anzeigen der Installations- und Protokolldateien

Wenn die Installation ohne Fehler abgeschlossen wurde, fahren Sie mit Vorbereiten der WebLogic-Umgebung 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.

6.3 Vorbereiten der WebLogic-Umgebung

- Abschnitt 6.3.1, „Konfigurieren des Verbindungs-Pools“, auf Seite 56
- Abschnitt 6.3.2, „Angeben des Speicherortes der Benutzeranwendungskonfigurationsdateien“, auf Seite 56
- Abschnitt 6.3.3, „Workflow-Plugin und WebLogic-Setup“, auf Seite 58

6.3.1 Konfigurieren des Verbindungs-Pools

- ❑ Kopieren Sie die JAR-Dateien des Datenbanktreibers in die Domäne, auf der Sie die Benutzeranwendung bereitstellen möchten.
- ❑ Erstellen Ihrer Datenquelle

  Befolgen Sie die Anweisungen zum Erstellen einer Datenquelle in der WebLogic-Dokumentation.

  Der JNDI-Name für die Datenquelle muss dem Namen der Datenbank entsprechen, die Sie beim Erstellen der Benutzeranwendungs-WAR-Datei angegeben haben, zum Beispiel `jdbc/IDMUADataSource`.
- ❑ Kopieren Sie `antlr-2.7.6.jar` aus dem Benutzeranwendungs-Installationsverzeichnis in den lib-Ordner der Domäne.

6.3.2 Angeben des Speicherortes der Benutzeranwendungskonfigurationsdateien

Die WebLogic-Benutzeranwendung benötigt Informationen zum Auffinden der Dateien `sys-configuration-xmldata.xml` und `idmuserapp_logging.xml`. Hierzu können Sie den Speicherort der Dateien in die Datei `setDomainEnv.cmd` eintragen.

Wenn Sie den Speicherort in der Datei `setDomainEnv.cmd` oder `setDomainEnv.sh` angeben, werden diese Informationen dem Anwendungsserver zur Verfügung gestellt:

1. Öffnen Sie `setDomainEnv.cmd` oder `setDomainEnv.sh`.
2. Suchen Sie die Zeile, die wie folgt aussieht:

```
set JAVA_PROPERTIES

export JAVA_PROPERTIES
```

3 Fügen Sie unter dem Eintrag JAVA_PROPERTIES Einträge für Folgendes hinzu:

- `-Dextend.local.config.dir`: Geben Sie den Ordner (nicht die Datei selbst) an, der die Datei `sys-configuration.xml` enthält.
- `-Didmuserapp.logging.config.dir`: Geben Sie den Ordner (nicht die Datei selbst) an, der die Datei `idmuserapp_logging.xml` enthält.

Zum Beispiel unter Windows:

```
set JAVA_OPTIONS=-Dextend.local.config.dir=c:/bea/user_projects/domains/
base_domain/idm.local.config.dir
-Didmuserapp.logging.config.dir=c:/bea/user_projects/domains/base_domain/
idm.local.config.dir
```

4 Definieren Sie die Umgebungsvariable `EXT_PRE_CLASSPATH` so, dass sie auf `antlr.jar` zeigt.

4a Suchen Sie diese Zeile:

```
ADD EXTENSIONS TO CLASSPATH
```

4b Fügen Sie `EXT_PRE_CLASSPATH` unterhalb der Zeile hinzu. Zum Beispiel unter Windows:

```
set EXT_PRE_CLASSPATH=C:\bea\user_projects\domains\base_domain\lib\antlr-
2.7.6.jar
```

Zum Beispiel unter Linux:

```
export EXT_PRE_CLASSPATH=/opt/bea/user_projects/domains/base_domain/lib/
antlr-2.7.6.jar
```

5 Speichern und schließen Sie die Datei.

Die XML-Dateien werden auch vom Dienstprogramm „ConfigUpdate“ verwendet. Daher müssen Sie die Datei `configupdate.bat` oder `configupdate.sh` folgendermaßen bearbeiten:

1 Öffnen Sie `configupdate.bat` oder `configupdate.sh`.

2 Suchen Sie die folgende Zeile:

```
-Duser.language=en -Duser.region="
```

3 Fügen Sie den folgenden Eintrag darunter ein:

```
Add -Dextend.local.config.dir=<directory-path>\extend.local.config.dir
```

4 Speichern und schließen Sie die Datei.

5 Führen Sie das Dienstprogramm „ConfigUpdate“ aus, um das Zertifikat in den Keystore des JDK unter BEA_HOME zu installieren.

Wenn Sie `ConfigUpdate` ausführen, werden Sie nach der Datei `cacerts` unter dem von Ihnen verwendeten JDK gefragt. Wenn Sie nicht das gleiche JDK verwenden, das während der Installation angegeben wurde, müssen Sie `ConfigUpdate` für die WAR-Datei ausführen. Achten Sie auf das angegebene JDK, da dieser Eintrag auf das von WebLogic verwendete JDK zeigen muss. Hiermit wird eine Zertifikatsdatei für die Verbindung zum Identitätsdepot importiert. Der Zweck besteht darin, eine Zertifikatsdatei für die Verbindung mit eDirectory zu importieren.

6.3.3 Workflow-Plugin und WebLogic-Setup

Das Workflow-Administration-Plugin für iManager kann keine Verbindung zum Benutzeranwendungstreiber herstellen, der auf WebLogic ausgeführt wird, wenn das `enforce-valid-basic-auth-credentials`-Flag auf „true“ gesetzt ist. Damit diese Verbindung erfolgreich ist, müssen Sie dieses Flag deaktivieren.

Führen Sie zur Deaktivierung des enforce-valid-basic-auth-credentials-Flags folgende Schritte durch:

1. Öffnen Sie die Datei `Config.xml` im Ordner *<WLHome>*`/user_projects/domains/base_domain/config/` .
2. Fügen Sie die folgende Zeile zum Abschnitt `<security-configuration>` hinzu:

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
   ```
3. Speichern Sie die Datei und starten Sie den Server neu.

Nachdem Sie diese Änderung durchgeführt haben, sollten Sie sich im Workflow-Administration-Plugin anmelden können.

6.4 Bereitstellen der Benutzeranwendungs-WAR-Datei

- ❑ Stellen Sie die Datei jsf-ri-1.1.1.war als Bibliothek bereit.
- ❑ Kopieren Sie die aktualisierte Benutzeranwendungs-WAR-Datei aus dem Installationsverzeichnis (üblicherweise `Novell\IDM`) in die Anwendungsdomäne. Beispiel:

  ```
  bea\user_projects\domains\base_domain\servers\AdminServer\upload
  ```
- ❑ Stellen Sie die Benutzeranwendungs-WAR-Datei mithilfe des standardmäßigen WebLogic-Bereitstellungsverfahrens bereit.

6.5 Zugriff auf die Benutzeranwendung

- ❑ Navigieren Sie zur Benutzeranwendungs-URL:

  ```
  http://application-server-host:port/application-context
  ```

  Beispiel:

  ```
  http://localhost:8080/IDMProv
  ```

Installation von der Konsole aus oder mit einem einzigen Befehl

7

In diesem Abschnitt werden die Installationsmethoden beschrieben, die Sie statt der Installation über eine grafische Benutzeroberfläche (siehe Kapitel 4, „Installieren auf JBoss mithilfe des GUI-Installationsprogramms“, auf Seite 33) verwenden können. Es werden u. a. folgende Themen erläutert:

7.1 Installation der Benutzeranwendung von der Konsole aus

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

Hinweis: Das Installationsprogramm erfordert mindestens das Java 2 Platform Standard Edition Development Kit Version 1.5. Wenn Sie eine frühere Version verwenden, wird die WAR-Datei der Benutzeranwendung bei der Installation nicht richtig konfiguriert. Die Installation scheint erfolgreich zu verlaufen, Sie erhalten aber Fehlermeldungen, wenn Sie die Benutzeranwendung starten.

---

1. Sobald Sie die entsprechenden Installationsdateien erhalten haben, die in Tabelle 2-2 auf Seite 18 beschrieben werden, melden Sie sich an und öffnen Sie eine Terminal-Sitzung.
2. Starten Sie das Installationsprogramm für Ihre Plattform mit Java und gehen Sie wie folgt vor:

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

3. Befolgen Sie die unter Kapitel 4, „Installieren auf JBoss mithilfe des GUI-Installationsprogramms“, auf Seite 33 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.
4. Starten Sie das Dienstprogramm „ConfigUpdate“, 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 A.1, „Benutzeranwendung - Konfiguration: Standardparameter“, auf Seite 79 beschrieben, ein.
5. 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.
6. Fahren Sie mit Kapitel 8, „Aufgaben nach Abschluss der Installation“, auf Seite 71 fort.

7.2 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 2-2 auf Seite 18 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 7-1. Die Benutzeranwendungs-Konfigurationsparameter sind identisch mit den Parametern, die Sie bei der Installation der GUI oder der Konsolenschnittstelle bzw. mit dem Dienstprogramm „ConfigUpdate“ 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 7-1 *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. Geben Sie den Hostnamen oder die IP-Adresse des LDAP-Servers an.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_LDAPADMIN=	eDirectory-Verbindungseinstellungen: LDAP-Administrator. 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. Geben Sie das LDAP-Administratorpasswort an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
NOVL_CONFIG_ROOTCONTAINERNAME=	eDirectory-DNs: Stammcontainer-DN. 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. Geben Sie den eindeutigen Namen des Benutzeranwendungstreibers an, den Sie zuvor in Abschnitt 3.1, „Erstellen des Benutzeranwendungstreibers in iManager“, auf Seite 27 erstellt haben. Wenn Ihr Treiber beispielsweise „UserApplicationDriver“ und der Treibersatz „myDriverSet“ ist und sich der Treibersatz in einem Kontext „o=myCompany“ befindet, geben Sie folgenden Wert ein: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_LOCKSMITH=	eDirectory-DNs: Benutzeranwendung - Administrator. 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 *Benutzeranwendung: Administrationshandbuch*. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden.
NOVL_CONFIG_PROVLOCKSMITH=	eDirectory-DNs: Bereitstellungsanwendung - Administrator. Diese Funktion ist in der Bereitstellungsversion von Identity Manager 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.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
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 die Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Funktionen* > *Funktionszuweisungen* in der Benutzeranwendung ändern.
NOVL_CONFIG_COMPLIANCECONTAINERDN	Der Konformitätsmoduladministrator ist eine Systemfunktion, die es Mitgliedern ermöglicht, alle Funktionen der Registerkarte *Konformität* durchzuführen. Dieser Benutzer muss im Identitätsdepot vorhanden sein, damit ihm die Rolle des Konformitätsmoduladministrators zugewiesen werden kann.
NOVL_CONFIG_USERCONTAINERDN=	Benutzeridentität für Metaverzeichnis: Benutzercontainer-DN. 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 können soll.
NOVL_CONFIG_GROUPCONTAINERDN=	Benutzergruppen für Metaverzeichnis: Gruppencontainer-DN. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Gruppencontainers an. Wird von Entitätsdefinitionen innerhalb der Verzeichnisabstraktionsschicht verwendet.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
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. Geben Sie das `cacerts`-Passwort an. Die Vorgabe ist `changeit`.
NOVL_CONFIG_SECUREADMINCONNECTION=	eDirectory-Verbindungseinstellungen: Sichere Admin-Verbindung. Erforderlich. 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. Erforderlich. 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.
NOVL_CONFIG_SESSIONTIMEOUT=	Sonstige: Sitzungszeitüberschreitung. Erforderlich. Geben Sie für die Benutzeranwendung einen Zeitüberschreitungsintervall an.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_LDAPPLAINPORT=	eDirectory-Verbindungseinstellungen: Nicht sicherer LDAP-Port. Erforderlich. Geben Sie den nicht sicheren Port des LDAP-Servers an, z. B. Port 389.
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory-Verbindungseinstellungen: Sicherer LDAP-Port. Erforderlich. Geben Sie den sicheren Port des LDAP-Servers an, z. B. Port 636.
NOVL_CONFIG_ANONYMOUS=	eDirectory-Verbindungseinstellungen: Öffentliches anonymes Konto verwenden. Erforderlich. 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 Bereitstellungsanforderungsaufgaben 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. Erforderlich. Geben Sie Emails an, die von einem Benutzer in der Bereitstellungs-Email stammen.
NOVL_CONFIG_NOTFSMTPEMAILHOST=	Email: Benachrichtigungs-SMTP-Email-Host. Erforderlich. 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.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
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 „Konfigurieren der externen Passwortverwaltung“ auf Seite 74.
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. Erforderlich. Die LDAP-Benutzerobjektklasse (in der Regel inetOrgPerson).
NOVL_CONFIG_LOGINATTRIBUTE=	Benutzeridentität für Metaverzeichnis: Anmeldeattribut. Erforderlich. Das LDAP-Attribut (z. B. CN), das den Anmeldenamen des Benutzers repräsentiert.
NOVL_CONFIG_NAMINGATTRIBUTE=	Benutzeridentität für Metaverzeichnis: Benennungsattribut. Erforderlich. 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. Erforderlich. Das LDAP-Attribut, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	Benutzergruppen für Metaverzeichnis: Gruppenobjektklasse. Erforderlich. Die Objektklasse für die LDAP-Gruppen (in der Regel groupofNames).

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	Benutzergruppen für Metaverzeichnis: Gruppenmitgliedschaftsattribut. Erforderlich. 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. Erforderlich. Wählen Sie *True*, um dynamische Gruppen zu verwenden. Anderenfalls wählen Sie *False*.
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	Benutzergruppen für Metaverzeichnis: Klasse für dynamisches Gruppenobjekt. Erforderlich. 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.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	Speicher für Herkunftsverbürgungsschlüssel: Passwort für Herkunftsverbürgungsspeicher.
NOVL_CONFIG_AUDITCERT=	Novell Audit-Digitalsignatur-Zertifikat
NOVL_CONFIG_AUDITKEYFILEPATH=	Schlüsseldateipfad für Novell Audit-Digitalsignatur.
NOVL_CONFIG_ICSLOGOUTENABLED=	Access Manager- und iChain-Einstellungen: Gleichzeitige Abmeldung aktiviert. Geben Sie *True* an, um die gleichzeitige Abmeldung von der Benutzeranwendung und von 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.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
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.
NOVL_CONFIG_CREATEDIRECTORYINDEX	Sonstiges: eDirectory-Index erstellen Geben Sie „true“ an, wenn das automatische Installationsprogramm Indizes für die Attribute „manager“, „ismanager“ und „srvprvUUID“ auf dem eDirectory-Server erstellen soll, der in NOVL_CONFIG_SERVERDN angegeben wurde. Wenn dieser Parameter auf „true“ gesetzt ist, kann NOVL_CONFIG_REMOVEEDIRECTORYINDEX nicht auf „true“ gesetzt werden. Zur Erzielung einer optimalen Leistung sollte die Erstellung des Index abgeschlossen sein. Die Indizes sollten sich im Online-Modus befinden, bevor Sie die Benutzeranwendung verfügbar machen.
NOVL_CONFIG_REMOVEDIRECTORYINDEX	Sonstiges: eDirectory-Index entfernen Geben Sie „true“ an, wenn das automatische Installationsprogramm Indizes vom Server entfernen soll, der in NOVL_CONFIG_SERVERDN angegeben wurde. IWenn dieser Parameter auf „true“ gesetzt ist, kann NOVL_CONFIG_CREATEEDIRECTORYINDEX nicht den Wert „true“ haben.
NOVL_CONFIG_SERVERDN	Sonstiges: Server-DN: Geben Sie den eDirectory-Server an, auf dem Indizes erstellt oder entfernt werden sollen.

Aufgaben nach Abschluss der Installation

8

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

8.1 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.

8.2 Konfiguration der Benutzeranwendung

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 3.6.1* im Abschnitt zur Konfiguration der Benutzeranwendungsumgebung.
- Im *Designhandbuch zum funktionsbasierten Bereitstellungsmodul für Novell IDM 3.6.1*.

8.2.1 Einrichten von Novell Audit

Kopieren Sie die Datei `dirxml.lsc` (sie befindet sich in der Datei prerequisites.zip) auf den Audit-Server. Befolgen Sie hierbei die Anweisungen im Abschnitt zum Einrichten der Protokollierung im Benutzeranwendung: Administrationshandbuch (http://www.novell.com/documentation/idmrbpm361/index.html).

8.3 Konfiguration von eDirectory

8.3.1 Erstellen von Indizes in eDirectory

Um die Leistung der Benutzeranwendung zu verbessern, sollte der Administrator von eDirectory™ Indizes für die Attribute „manager“, „ismanager“ und „srvprvUUID“ erstellen. Sind für diese Attribute keine Indizes vorhanden, kann dies insbesondere in einer Cluster-Umgebung eine eingeschränkte Leistung zur Folge haben.

Diese Indizes können automatisch während der Installation erstellt werden, wenn Sie *Index für eDirectory erstellen* auf der Registerkarte *Erweitert* des Teilfensters „Benutzeranwendung - Konfiguration“ auswählen (beschrieben in Tabelle A-2 auf Seite 86). Alternativ erhalten Sie im *Novell eDirectory-Administrationshandbuch* weitere Anweisungen zur Verwendung des Index-Managers zum Erstellen von Indizes. (http://www.novell.com/documentation)

8.3.2 Installieren und Konfigurieren der SAML-Beglaubigungsmethode

Diese Konfiguration ist nur dann erforderlich, wenn Sie die SAML-Beglaubigungsmethode verwenden möchten, jedoch nicht den Access Manager verwenden. Wenn Sie den Access Manager verwenden, enthält Ihre eDirectory-Baumstruktur bereits die Methode. Das Verfahren umfasst folgende Schritte:

- ❑ Installieren der SAML-Methode in Ihrer eDirectory-Baumstruktur
- ❑ Bearbeiten der eDirectory-Attribute mithilfe von iManager

Installieren der SAML-Methode in Ihrer eDirectory-Baumstruktur

1. Suchen Sie im `.iso`-Image die Datei `nmassaml.zip` und entpacken Sie sie.
2. Installieren Sie die SAML-Methode in Ihre eDirectory-Baumstruktur.
   - **2a** Erweitern Sie das in `authsaml.sch` gespeicherte Schema.

     Im folgenden Beispiel wird die Durchführung unter Linux gezeigt:

     ```
     ndssch -h <edir_ip> <edir_admin> authsaml.sch
     ```
   - **2b** Installieren Sie die SAML-Methode.

     Im folgenden Beispiel wird die Durchführung unter Linux gezeigt:

     ```
     nmasinst   -addmethod <edir_admin> <tree> ./config.txt
     ```

Bearbeiten der eDirectory-Attribute

1. Öffnen Sie iManager und wechseln Sie zu *Funktionen und Aufgaben* > *Verzeichnisadministration* > *Objekt erstellen*.
2. Wählen Sie *Alle Objektklassen anzeigen*.
3. Erstellen Sie ein neues Objekt der Klasse `authsamlAffiliate`.
4. Wählen Sie `authsamlAffiliate` und klicken Sie auf *OK*. (Sie können diesem Objekt einen beliebigen gültigen Namen geben.)
5. Wählen Sie das Containerobjekt *SAML Assertion.Authorized Login Methods.Security* in der Baumstruktur aus, um den Kontext anzugeben, und klicken Sie anschließend auf *OK*.
6. Sie müssen Attribute zum Klassenobjekt `authsamlAffiliate` hinzufügen.
   - **6a** Wechseln Sie zur iManager-Registerkarte *Objekte anzeigen* > *Durchsuchen* und suchen Sie Ihr neues affiliate-Objekt im Container „SAML Assertion.Authorized Login Methods.Security“.
   - **6b** Wählen Sie das neue affiliate-Objekt und wählen Sie anschließend *Objekt ändern* aus.
   - **6c** Fügen Sie ein *authsamlProviderID*-Attribut zum neuen affiliate-Objekt hinzu. Dieses Attribut dient der Übereinstimmung einer Assertion mit ihrem Partner. Der Inhalt dieses Attributs muss exakt mit dem Ausstellerattribut übereinstimmen, das von der SAML-Assertion gesendet wurde.
   - **6d** Klicken Sie auf *OK*.
   - **6e** Fügen Sie die Attribute *authsamlValidBefore* und *authsamlValidAfter* zum affiliate-Objekt hinzu. Diese Attribute definieren die Zeit in Sekunden um ein *IssueInstant* in einer Assertion, wenn die Assertion als gültig angesehen wird. Der übliche Standardwert ist 180 Sekunden.
   - **6f** Klicken Sie auf *OK*.
7. Wählen Sie den Sicherheitscontainer und anschließend *Objekt erstellen* aus, um einen *Herkunftsverbürgungscontainer* in Ihrem Sicherheitscontainer zu erstellen.
8. Erstellen Sie ein *Herkunftsverbürgung*sobjekt im Herkunftsverbürgungscontainer.
   - **8a** Kehren Sie zurück zu *Funktionen und Aufgaben* > *Verzeichnisadministration* und wählen Sie anschließend *Objekt erstellen*.
   - **8b** Wählen Sie erneut *Alle Objektklassen anzeigen*.
   - **8c** So erstellen Sie ein *Herkunftsverbürgung*sobjekt für das Zertifikat, das Ihr Partner zum Signieren von Assertions verwendet. Sie benötigen hierzu eine verschlüsselte Kopie des Zertifikats.
   - **8d** Erstellen Sie neue Herkunftsverbürgungsobjekte für jedes Zertifikat in der Kette der unterzeichnenden Zertifikate bis zum Stamm-CA-Zertifikat.
   - **8e** Legen Sie den Kontext auf den zuvor erstellen Herkunftsverbürgungs-Container fest und klicken Sie anschließend auf *OK*.
9. Kehren Sie zum Objekt-Viewer zurück.
10. Fügen Sie ein *authsamlTrustedCertDN*-Attribut zum affiliate-Objekt hinzu und klicken Sie anschließend auf *OK*.

Dieses Attribut sollte auf das „Herkunftsverbürgungsobjekt“ für das unterzeichnende Zertifikat zeigen, das Sie im vorherigen Schritt erstellt haben. (Alle Assertions für den Partner müssen von Zertifikaten unterzeichnet werden, auf die dieses Attribut zeigt, sonst werden sie abgewiesen.)

11 Fügen Sie ein *authsamlCertContainerDN*-Attribut zum affiliate-Objekt hinzu und klicken Sie anschließend auf *OK*.

Dieses Attribut sollte auf den „Herkunftsverbürgungscontainer“ zeigen, den Sie bereits erstellt haben. (Dieses Attribut dient zur Überprüfung der Zertifikatskette des unterzeichnenden Zertifikats.)

8.4 Neukonfiguration der Benutzeranwendungs-WAR-Datei nach der Installation

Zum Aktualisieren Ihrer WAR-Datei können Sie das Dienstprogramm „ConfigUpdate“ folgendermaßen ausführen:

1 Führen Sie das Dienstprogramm „ConfigUpdate“ im Installationsverzeichnis der Benutzeranwendung aus, indem Sie `configupdate.sh` oder `configupdate.bat` ausführen. Dadurch können Sie die WAR-Datei im Installationsverzeichnis aktualisieren.

Weitere Informationen zu den Parametern des Dienstprogramms „ConfigUpdate“ finden Sie unter Abschnitt A.1, „Benutzeranwendung - Konfiguration: Standardparameter“, auf Seite 79, Tabelle 7-1 auf Seite 60.

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

Verlagern Sie bei WebLogic und WebSphere die WAR-Datei auf den Anwendungsserver. Bei einem JBoss-Einzelserver werden die Änderungen auf die bereitgestellte WAR-Datei angewendet. Wenn Sie einen JBoss-Cluster ausführen, muss die WAR-Datei auf jedem JBoss-Server im Cluster aktualisiert werden.

8.5 Konfigurieren der externen Passwortverwaltung

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.

8.5.1 Angabe einer externen WAR-Datei für die Passwortverwaltung

1 Sie können die externe WAR-Datei während des Installationsvorgangs oder über das Dienstprogramm „ConfigUpdate“ 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 8.5.4, „Konfiguration der SSL-Kommunikation zwischen JBoss-Servern“, auf Seite 76.

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

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

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

8.5.2 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'*.

8.5.3 Testen der externen Passwort-WAR-Konfiguration

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*.

8.5.4 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.

8.6 Aktualisierung der Einstellungen für „Passwort vergessen“

Die Werte von *'Passwort vergessen'-Link* und *Link zurück zu 'Passwort vergessen'* können nach der Installation über das Dienstprogramm „ConfigUpdate“ oder die Benutzeranwendung geändert werden.

Verwendung des Dienstprogramms „ConfigUpdate“ . Wechseln Sie in der Befehlszeile zum Installationsverzeichnis und geben Sie `configupdate.sh` (Linux oder Solaris) bzw. `configupdate.bat` (Windows) ein. Wenn Sie eine externe WAR-Datei für die Passwortverwaltung erstellen oder bearbeiten, müssen Sie die WAR-Datei manuell umbenennen, bevor Sie sie auf den Remote-JBoss-Server kopieren.

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`)

8.7 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.
Sie können sich nicht auf der Seite „Portaladministration“ anmelden.	Stellen Sie sicher, dass ein Konto für den Benutzeranwendungsadministrator vorhanden ist. Verwechseln Sie dieses Konto nicht mit Ihrem iManager-Administratorkonto. Dies sind zwei unterschiedliche Administratorobjekte (oder sollten es sein).
Sie können sich als Administrator anmelden, aber keine neuen Benutzer erstellen.	Der Administrator der Benutzeranwendung muss ein Trustee des Containers der obersten Ebene sein und über Supervisor-Rechte verfügen. Zur Überbrückung können Sie die Rechte des Administrators der Benutzeranwendung mit denen des LDAP-Administrators gleichsetzen (mithilfe von iManager).

Problem	Empfohlene Vorgehensweise
Beim Start des Anwendungsservers treten MySQL-Verbindungsfehler auf.	Führen Sie MySQL nicht als `root` aus. (Dieses Problem tritt normalerweise nicht auf, wenn Sie die MySQL-Version ausführen, die mit 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).

Es wurde keine Email-Benachrichtigung gesendet.	Führen Sie das Dienstprogramm „ConfigUpdate“ 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`

IDM Benutzeranwendung - Konfigurationsreferenz

A

In diesem Abschnitt werden die Optionen beschrieben, mit denen Werte während der Benutzeranwendungsinstallation oder einer Konfigurationsaktualisierung übergeben werden.

A.1 Benutzeranwendung - Konfiguration: Standardparameter

Abbildung A-1 *Standardoptionen für die Konfiguration der Benutzeranwendung*

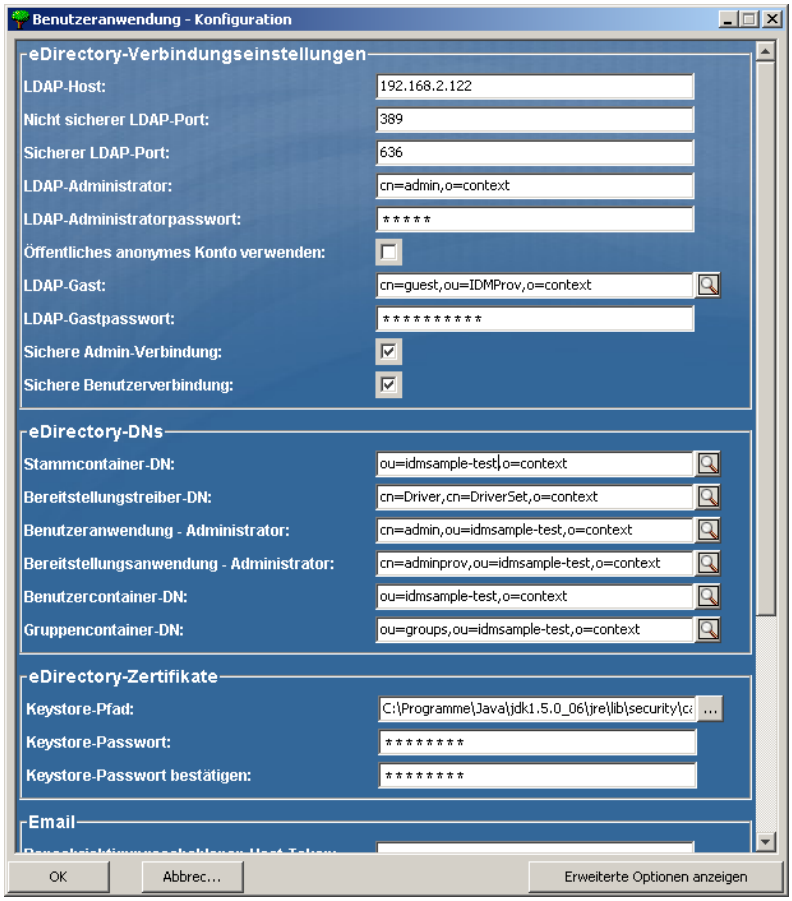


Tabelle A-1 *Benutzeranwendung - Konfiguration: Standardoptionen*

Einstellungstyp	Option	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. Sie können das Dienstprogramm „ConfigUpdate“ zum Bearbeiten dieser Einstellung verwenden, solange Sie sie nicht über die Registerkarte „Administration“ der Benutzeranwendung geändert haben.
	LDAP-Administrator-passwort	Erforderlich. Geben Sie das LDAP-Administratorpasswort an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt. Sie können das Dienstprogramm „ConfigUpdate“ zum Bearbeiten dieser Einstellung verwenden, solange Sie sie nicht über die Registerkarte „Administration“ der Benutzeranwendung geändert haben.
	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.

Einstellungstyp	Option	Beschreibung
eDirectory®-Verbindungseinstellungen. (Fortsetzung)	*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	Option	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.
	Bereitstellungs-treiber-DN	Erforderlich. Geben Sie den eindeutigen Namen des Benutzeranwendungstreibers an (beschrieben in Abschnitt 3.1, „Erstellen des Benutzeranwendungstreibers in iManager“, auf Seite 27). 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`
	Benutzer anwendung - 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 *Benutzeranwendung: Administrationshandbuch*. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden. Sie können diese Einstellung nicht über „ConfigUpdate“ ändern, wenn Sie den Anwendungsserver gestartet haben, auf dem die Benutzeranwendung installiert ist.
	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	Option	Beschreibung
	Konformitäts-administrator	Der Konformitätsmoduladministrator ist eine Systemfunktion, die es Mitgliedern ermöglicht, alle Funktionen der Registerkarte *Konformität* durchzuführen. Dieser Benutzer muss im Identitätsdepot vorhanden sein, damit ihm die Rolle des Konformitätsmoduladministrators zugewiesen werden kann. Während der Ausführung von „ConfigUpdate“ treten Änderungen an diesem Wert nur dann in Kraft, wenn Sie keinen gültigen Konformitätsmoduladministrator beauftragt haben. Wenn ein gültiger Konformitätsmoduladministrator existiert, werden Ihre Änderungen nicht gespeichert. Sie können die Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Funktionen* > *Funktionszuweisungen* in der Benutzeranwendung ändern.
eDirectory-DNs (Fortsetzung)	*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 die Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Funktionen* > *Funktionszuweisungen* in der Benutzeranwendung ändern. Während der Ausführung von „ConfigUpdate“ treten Änderungen an diesem Wert nur dann in Kraft, wenn Sie keinen gültigen Funktionsadministrator beauftragt haben. Wenn ein gültiger Funktionsadministrator existiert, werden Ihre Änderungen nicht gespeichert.
	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 können soll. Sie können diese Einstellung nicht über „ConfigUpdate“ ändern, wenn Sie den Anwendungsserver gestartet haben, auf dem die Benutzeranwendung installiert ist.

Einstellungstyp	Option	Beschreibung
	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. Sie können diese Einstellung nicht über „ConfigUpdate“ ändern, wenn Sie den Anwendungsserver gestartet haben, auf dem die Benutzeranwendung installiert ist.
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`.
Email	*Benachrichtigungsschablonen-Host-Token*	Geben Sie den Anwendungsserver an, der die Identity Manager-Benutzeranwendung hostet. Beispiel: `myapplication serverServer` Dieser Wert ersetzt das $HOST$-Token in Email-Schablonen. Die erstellte URL ist eine Verknüpfung zu Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen.
	Benachrichtigungsschablonen-Port-Token	Ersetzt das $PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungsaufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Token für den sicheren Port der 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.
	Benachrichti-gungs-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	Option	Beschreibung
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 internen WAR-Datei für die Passwortverwaltung eine Datei namens `ForgotPassword.jsf`. Weitere Informationen finden Sie in „Konfigurieren der externen Passwortverwaltung“ auf Seite 74.
	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`.

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.

A.2 Konfiguration der Benutzeranwendung: Alle Parameter

Diese Tabelle enthält die verfügbaren Konfigurationsparameter, wenn Sie auf *Erweiterte Optionen anzeigen* klicken.

Tabelle A-2 *Benutzeranwendung - Konfiguration: Alle Optionen*

Einstellungstyp	Option	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-Administrator-passwort	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 Benutzer-verbindung	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	Option	Beschreibung
eDirectory-DNs	*Stamm-container-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.
	Bereitstellungs-treiber-DN	Erforderlich. Geben Sie den eindeutigen Namen des Benutzeranwendungstreibers an (beschrieben in Abschnitt 3.1, „Erstellen des Benutzeranwendungstreibers in iManager“, auf Seite 27). 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`
	Benutzer-anwendung - 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 *Benutzeranwendung: Administrationshandbuch*. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden. Sie können diese Einstellung nicht über „ConfigUpdate“ ändern, wenn Sie den Anwendungsserver gestartet haben, auf dem die Benutzeranwendung installiert ist.
	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	Option	Beschreibung
	Konformitäts-administrator	Der Konformitätsmoduladministrator ist eine Systemfunktion, die es Mitgliedern ermöglicht, alle Funktionen der Registerkarte *Konformität* durchzuführen. Dieser Benutzer muss im Identitätsdepot vorhanden sein, damit ihm die Rolle des Konformitätsmoduladministrators zugewiesen werden kann. Während der Ausführung von „ConfigUpdate“ treten Änderungen an diesem Wert nur dann in Kraft, wenn Sie keinen gültigen Konformitätsmoduladministrator beauftragt haben. Wenn ein gültiger Konformitätsmoduladministrator existiert, werden Ihre Änderungen nicht gespeichert. Sie können die Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Funktionen* > *Funktionszuweisungen* in der Benutzeranwendung ändern.
	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 die Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Funktionen* > *Funktionszuweisungen* in der Benutzeranwendung ändern. Während der Ausführung von „ConfigUpdate“ treten Änderungen an diesem Wert nur dann in Kraft, wenn Sie keinen gültigen Funktionsadministrator beauftragt haben. Wenn ein gültiger Funktionsadministrator existiert, werden Ihre Änderungen nicht gespeichert.

Einstellungstyp	Option	Beschreibung
Benutzeridentität für Metaverzeichnis	*Benutzer-container-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Benutzercontainers an. Benutzer in diesem Container (und unterhalb) dürfen sich bei der Benutzeranwendung anmelden. Sie können diese Einstellung nicht über „ConfigUpdate“ ändern, wenn Sie den Anwendungsserver gestartet haben, auf dem die Benutzeranwendung installiert ist. **Wichtig:** Stellen Sie sicher, dass der bei der Installation des Benutzeranwendungstreibers angegebene Benutzeranwendungsadministrator in diesem Container vorhanden ist, wenn dieser Benutzer Workflows ausführen können soll.
	Benutzercon-tainerbereich	Diese Angabe definiert den Suchbereich für Benutzer.
	Benutzerobjekt-klasse	Die LDAP-Benutzerobjektklasse (in der Regel inetOrgPerson).
	Anmeldeattribut	Das LDAP-Attribut (z. B. CN), das den Anmeldenamen des Benutzers repräsentiert.
	Benennungs-attribut	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.
	Benutzermit-gliedschafts-attribut	Optional. Das LDAP-Attribut, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.

Einstellungstyp	Option	Beschreibung
Benutzergruppen für Metaverzeichnis	*Gruppen-container-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Gruppencontainers an. Wird von Entitätsdefinitionen innerhalb der Verzeichnisabstraktionsschicht verwendet. Sie können diese Einstellung nicht über „ConfigUpdate“ ändern, wenn Sie den Anwendungsserver gestartet haben, auf dem die Benutzeranwendung installiert ist.
	Gruppencon-tainerbereich	Diese Angabe definiert den Suchbereich für Gruppen.
	Gruppenobjekt-klasse	Die Objektklasse für die LDAP-Gruppen (in der Regel groupofNames).
	Gruppenmit-gliedschafts-attribut	Das Attribut, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.
	Dynamische Gruppen verwenden	Wählen Sie diese Option, wenn Sie dynamische Gruppen verwenden möchten.
	Klasse für dynamisches Gruppenobjekt	Die Objektklasse für die dynamische Gruppe (in der Regel dynamicGroup).
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	Erforderlich. Geben Sie das `cacerts`-Passwort an. Die Vorgabe ist `changeit`.
	Keystore-Passwort bestätigen	
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	Option	Beschreibung
Speicher für Herkunftsverbürgungsschlüssel	*Pfad für Herkunfts-verbürgungs-speicher*	Der Speicher für Herkunftsverbürgungsschlüssel enthält alle verbürgten Zertifikate der Signierer, die zum Validieren digitaler Signaturen verwendet werden. Wurde kein Pfad angegeben, ruft die Benutzeranwendung den Pfad von der Systemeigenschaft `javax.net.ssl.trustStore` ab. Wurde kein Pfad angegeben, wird `jre/lib/security/cacerts` verwendet.
	Passwort für Herkunfts-verbürgungs-speicher	Wurde kein Passwort angegeben, ruft die Benutzeranwendung das Passwort von der Systemeigenschaft `javax.net.ssl.trustStorePassword` ab. Ist dort kein Wert angegeben, lautet das Passwort `changeit`. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
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	Option	Beschreibung
Email	*Benachrichtigungsschablonen-Host-Token*	Geben Sie den Anwendungsserver an, der die Identity Manager-Benutzeranwendung hostet. Beispiel: `myapplication serverServer` Dieser Wert ersetzt das $HOST$-Token in Email-Schablonen. Die erstellte URL ist eine Verknüpfung zu Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen.
	Benachrichtigungsschablonen-Port-Token	Ersetzt das $PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungsaufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Token für den sicheren Port der Benachrichtigungsschablone	Ersetzt das $SECURE_PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	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.
	Token für das sichere Protokoll der Benachrichtigungsschablone	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	Option	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 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	*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.
	Konfigurations-pfad für Autorisierung	Vollständig qualifizierter Name der Konfigurationsdatei für die Autorisierung.

Einstellungstyp	Option	Beschreibung
	eDirectory-Index erstellen	Wählen Sie dieses Kontrollkästchen aus, wenn das Installationsprogramm Indizes für die Attribute „manager“, „ismanager“ und „srvprvUUID“ erstellen soll. Sind für diese Attribute keine Indizes vorhanden, kann dies insbesondere in einer Cluster-Umgebung eine eingeschränkte Leistung der Benutzeranwendung zur Folge haben. Sie können diese Indizes manuell mithilfe des iManager erstellen, nachdem Sie die Benutzeranwendung installiert haben. Weitere Informationen hierzu finden Sie unter Abschnitt 8.3.1, „Erstellen von Indizes in eDirectory“, auf Seite 72. Zur Erzielung einer optimalen Leistung sollte die Erstellung des Index abgeschlossen sein. Die Indizes sollten sich im Online-Modus befinden, bevor Sie die Benutzeranwendung verfügbar machen.
	Index für eDirectory entfernen	Entfernt Indizes von den Attributen „manager“, „ismanager“ und „srvprvUUID“.
	Server-DN	Wählen Sie den eDirectory-Server aus, auf dem die Indizes erstellt oder entfernt werden sollen. **Hinweis:** Zum Konfigurieren der Indizes auf mehreren eDirectory-Servern müssen Sie das Dienstprogramm „ConfigUpdate“ mehrmals aufrufen. Es kann jeweils nur ein Server angegeben werden.
Containerobjekt	*Ausgewählt*	Wählen Sie alle zu verwendenden Containerobjekttypen aus.
	Container-objekttyp	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.
	Container-attributname	Listet den mit dem Containerobjekttyp verknüpften Attributnamen auf.
	Neues Containerobjekt hinzufügen: Container-objekttyp	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: Container-attributname	Geben Sie den Attributnamen des Containerobjekts an.