Novell Identity Manager

3.0

13.12.05

www.novell.com

ADMINISTRATIONSHANDBUCH

Novell®

Rechtliche Hinweise

Novell Inc. übernimmt für Inhalt oder Verwendung dieser Dokumentation keine Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder Eignung für einen bestimmten Zweck aus. Novell Inc. behält sich weiterhin das Recht vor, dieses Dokument jederzeit und ohne vorherige Ankündigung teilweise oder vollständig zu überarbeiten.

Novell Inc., gibt ebenfalls keine Erklärungen oder Garantien in Bezug auf Novell-Software und schließt insbesondere jegliche ausdrückliche oder stillschweigende Garantie für handelsübliche Qualität oder Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell Inc. das Recht vor, Novell-Software jederzeit und ohne vorherige Ankündigung ganz oder teilweise zu ändern.

Gemäß dieser Vereinbarung zur Verfügung gestellte Produkte bzw. technische Informationen unterliegen den Ausfuhrkontrollbestimmungen der USA und 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 ferner damit einverstanden, nicht in Länder zu exportieren oder zu re-exportieren, die sich aktuell auf der Ausschlussliste für US-Exporte befinden, für die ein Embargo verhängt wurde oder die terroristischer Aktivitäten verdächtigt werden. Maßgeblich für diese Kategorisierungen sind die US-Exportgesetze. Sie dürfen die Bestandteile des Produkts nicht zur Herstellung von Raketen bzw. von Waffen nuklearer oder chemisch-biologischer Art einsetzen. Zusätzliche Informationen über den Export von Novell-Software finden Sie unter www.novell.com/info/exports/. Novell übernimmt keine Verantwortung für Ihr etwaiges Versäumnis in Bezug auf das Einholen der erforderlichen Exportgenehmigungen.

Novell Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
USA
www.novell.com

Online-Dokumentation: Zugriff auf die Online-Dokumentation für dieses und andere Novell-Produkte sowie auf Aktualisierungen erhalten Sie unter www.novell.com/documentation.

Novell-Marken

eDirectory ist eine Marke von Novell Inc.
exteNd ist eine Marke von Novell Inc.
exteNd Director ist eine Marke von Novell Inc.
GroupWise ist eine eingetragene Marke von Novell Inc. in den USA und in anderen Ländern.
NDS ist eine eingetragene Marke von Novell Inc. in den USA und in anderen Ländern.
NetWare ist eine eingetragene Marke von Novell Inc. in den USA und in anderen Ländern.
NMAS ist eine Marke von Novell Inc.
Novell ist eine eingetragene Marke von Novell Inc. in den USA und anderen Ländern.
Novell Certificate Server ist eine Marke von Novell Inc.
Novell Client ist eine Marke von Novell Inc.
SUSE ist eine eingetragene Marke von Novell Inc. in den USA und in anderen Ländern.

Materialien von Drittanbietern

Alle Marken von Drittanbietern sind Eigentum ihrer jeweiligen Inhaber.

Inhalt

Informationen zu diesem Handbuch

Novell® Identity Manager 3, vormals DirXML®, ist ein Service für die Datenfreigabe und -synchronisierung, mit dessen Hilfe Anwendungen, Verzeichnisse und Datenbanken Informationen gemeinsam nutzen können. Es verbindet über mehrere Verzeichnisse verstreute Informationen und ermöglicht Ihnen das Einrichten von Richtlinien für die automatische Aktualisierung designierter Systeme bei Identitätsänderungen. Identity Manager bietet die Grundlage für Kontenbereitstellung, Sicherheit, Benutzer-Self-Service (Selbstbedienung), Authentifizierung, Autorisierung, automatisierte Workflow- und Web-Services. Das Programm ermöglicht Ihnen, die verteilten Identitätsinformationen zu integrieren, zu verwalten und zu steuern, sodass Sie den richtigen Personen die richtigen Ressourcen auf sichere Weise zur Verfügung stellen können.

Dieses Handbuch enthält einen Überblick über die Identity Manager-Technologien und eine Beschreibung der Administrations- und Konfigurationsfunktionen.

Feedback

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation dieses Produkts. Bitte verwenden Sie die Funktion für Benutzerkommentare unten auf jeder Seite der Online-Dokumentation oder geben Sie Ihre Kommentare unter http://www.novell.com/documentation/feedback.html ein.

Aktualisierungen für Dokumentationen

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

Zusätzliche Dokumentation

Weitere Informationen zum Installieren und Aufrüsten von Identity Manager finden Sie im *Identity Manager 3.0 Installation Guide* (Identity Manager 3.0 Installationshandbuch).

Weitere Informationen und Dokumentationen zu Identity Manager-Richtlinien und -Filtern finden Sie im *Policy Builder and Driver Customization Guide* (Handbuch zum Richtlinien-Builder und zur Treiberanpassung).

Die Dokumentation zur Design- und Implementierungspraxis finden Sie im *Designer for Identity Manager 3: Administration Guide* (Designer für Identity Manager: Administrationshandbuch).

Weitere Informationen zu Passwortrichtlinien, zur Passwort-Selbstbedienung und zum Verwalten von Passwörtern finden Sie im Password Management Administration Guide (http://www.novell.com/documentation) (Administrationshandbuch zur Passwortverwaltung).

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

Konventionen in der Dokumentation

In dieser Dokumentation dient das Symbol „größer als“ (>) zur Trennung von Aktionen innerhalb eines Schritts sowie von Objekten in einem Querverweispfad.

Ein Markensymbol (®, ™ usw.) kennzeichnet eine Marke von Novell. Drittanbieter-Marken sind durch ein Sternchen (*) gekennzeichnet.

Überblick über die Identity Manager 3.0-Architektur

1

Identity Manager umfasst drei Hauptkomponenten.

- Abschnitt 1.2, „Identity Manager“, auf Seite 10
- Abschnitt 1.3, „Benutzeranwendung“, auf Seite 18
- Abschnitt 1.4, „Designer“, auf Seite 18

1.1 Terminologieänderungen im Vergleich zu früheren Versionen

Diesen Abschnitt müssen Sie nur lesen, wenn Sie bereits mit DirXML® 1.1a oder Identity Manager 2.0 gearbeitet haben.

In DirXML 1.1a wurde der Begriff „Regel“ verwendet, um je nach Kontext einen Regelsatz, die einzelnen Regeln in einem Satz und die Bedingungen und Aktionen innerhalb der einzelnen Regeln zu beschreiben. Diese Überschneidung führte bei fehlendem Kontext zu Verwechslungen.

In Identity Manager 2 wurde bei der Beschreibung der übergeordneten Transformation der Begriff „Regel“ durch den Begriff „Richtlinie“ ersetzt. Sie definieren nun einen Richtliniensatz, wobei jede Richtlinie eine oder mehrere Regeln enthält. Der Begriff „Regel“ wird jetzt nur zur Beschreibung einzelner Bedingungen und Aktionen verwendet.

Die folgende Tabelle enthält die Terminologieänderungen von DirXML 1.1a zu Identity Manager 2.x.

Tabelle 1-1 *Terminologieänderungen von DirXML 1.1a zu Identity Manager 2.x.*

Beschriebenes Element	DirXML 1.1a-Terminologie	Identity Manager 2.x-Terminologie
Transformationssatz	Regel	Richtliniensatz
Eine einzelne Transformation innerhalb eines Satzes	Regel	“Richtlinien”
Die Bedingungen und Aktionen innerhalb einer einzelnen Transformation	Regel	Regel

Die folgende Tabelle enthält die Terminologieänderungen von Identity Manager 2.x zu Identity Manager 3.0.

Tabelle 1-2 *Terminologieänderungen von Identity Manager 2.x zu Identity Manager 3.0*

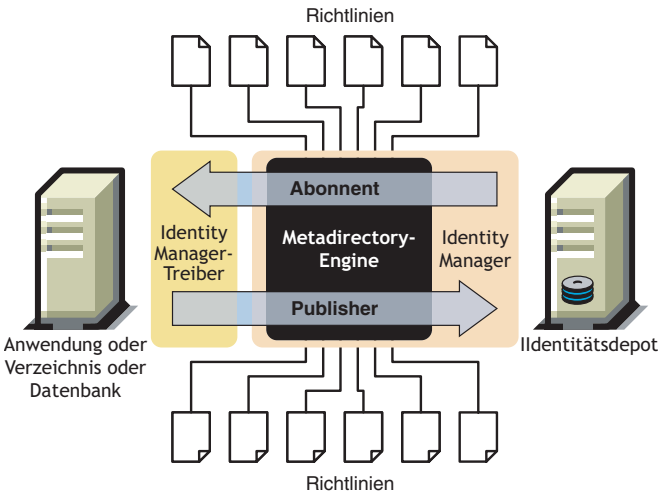
Beschriebenes Element	Identity Manager 2.x-Terminologie	Identity Manager 3-Terminologie
Das Produkt	DirXML	Identity Manager
Ein Server, auf dem das Produkt installiert ist	DirXML-Server	Metaverzeichnis-Server
Ein Server der Anwendung oder Datenbank, mit dem die Daten synchronisiert werden	Verbundener DirXML-System-server	Verbundener Systemserver
Speicherort der Objekte	eDirectory™	Identitätsdepot
Die Verarbeitungskomponente	DirXML-Engine	Metaverzeichnis-Engine

1.2 Identity Manager

Identity Manager ermöglicht die Synchronisierung von Daten zwischen dem Identitätsdepot und dem verbundenen System. Das verbundene System besteht aus Anwendungen, Verzeichnissen, Datenbanken oder Dateien.

Identity Manager umfasst mehrere Komponenten. In der folgenden Abbildung sind die grundlegenden Komponenten und ihre Beziehungen abgebildet:

Abbildung 1-1 *Identity Manager-Komponenten*



Die Metaverzeichnis-Engine ist das wichtigste Modul in der Identity Manager-Architektur. Sie stellt die Schnittstelle zur Verfügung, über die Identity Manager-Treiber Informationen mit dem Identitätsdepot synchronisieren und über die verschiedenartigen Datensysteme eine Verbindung herstellen und Daten gemeinsam nutzen können.

Die Metaverzeichnis-Engine verarbeitet Identitätsdepotdaten und -ereignisse unter Verwendung von XML. Die Metaverzeichnis-Engine verwendet zur Bearbeitung des Datenflusses zwischen zwei Systemen einen Regelprozessor und eine Datentransformations-Engine:

1. Sie liest den Filter für alle Identity Manager-Treiber.

2. Sie registriert die Treiber für die entsprechenden Identitätsdepot-Ereignisse.
3. Sie filtert die Daten gemäß den Spezifikationen der einzelnen Treiber.
4. Sie richtet einen Cache für die Identitätsdepot-Ereignisse ein, die von den einzelnen Treibern übergeben werden.

Bei der Initialisierung des Identitätsdepots führt die Engine Folgendes aus:

- Nachdem ein Ereignis im Cache gespeichert wurde, wird es von dem Treiber gelesen, der Eigentümer des Cache ist.
- Der Treiber empfängt die Identitätsdepotdaten im nativen eDirectory-Format, übersetzt sie in das XDS-Format (das von Identity Manager verwendete XML-Vokabular, das durch eine Richtlinie transformiert werden kann) und sendet das Ereignis an die Metaverzeichnis-Engine. Die Engine liest alle Richtlinien im verbundenen Systemtreiber und erstellt gemäß diesen Richtlinien XML-formatierte Daten, die sie anschließend an den verbundenen Systemtreiber sendet. Dann werden die Daten an das verbundene System gesendet. Weitere Informationen zu Richtlinien finden Sie unter "Introduction to Policies" (Einführung zu Richtlinien) im *Policy Builder and Driver Customization Guide* (Handbuch zum Richtlinien-Builder und zur Treiberanpassung).
- Das Erfassen und Senden von Aktualisierungen vom verbundenen System an das Identitätsdepot wird von der Herausgeberkomponente des Treibers ausgeführt. Wenn der Treiber des verbundenen Systems über Änderungen an den Informationen benachrichtigt wird, die die beiden Systeme gemeinsam nutzen, sammelt er diese Informationen und stellt sicher, dass sie in den richtigen Datensatz gefiltert wurden. Anschließend konvertiert er die Daten in das XDS-Format und sendet sie an die Engine.

1.2.1 Metaverzeichnis-Engine

Die Metaverzeichnis-Engine kann in zwei Komponenten aufgeteilt werden: die eDirectory-Schnittstelle und die Synchronisierungs-Engine.

eDirectory-Schnittstelle

Die in der Metaverzeichnis-Engine integrierte eDirectory-Schnittstelle wird zum Erkennen von Ereignissen verwendet, die in eDirectory auftreten. Diese Schnittstelle garantiert durch die Verwendung des Ereignis-Cache die Zustellung der Ereignisse an Identity Manager. Die eDirectory-Schnittstelle unterstützt das Laden mehrerer Treiber. Dies bedeutet, dass nur eine Instanz von Identity Manager für diesen eDirectory-Server ausgeführt wird, dieser aber mit mehreren verbundenen Systemen kommunizieren kann. Um Ereignis-Loops zwischen dem Identitätsdepot und dem verbundenen System zu verhindern, wurde die Loopback-Erkennung in diese Schnittstelle integriert. Obwohl die Schnittstelle mit einem Loopback-Schutz ausgestattet ist, sollten Entwickler die Loopback-Erkennung dennoch in die einzelnen Treiber der angeschlossenen Systeme integrieren.

Synchronisierungs-Engine

Die Synchronisierungs-Engine wendet die Identity Manager-Richtlinien auf alle Ereignisse an, die ihr präsentiert werden. Die Richtlinien werden unter Verwendung des DirXML-Skripts im Richtlinien-Builder erstellt. Mit dem Richtlinien-Builder können Sie Richtlinien über die GUI-Schnittstelle erstellen und müssen nicht XML-Dokumente oder XSLT-Formatvorlagen verwenden. Sie können diese Formatvorlagen zwar weiterhin nutzen, aber der Richtlinien-Builder ist einfacher zu verwenden. Weitere Informationen zum Richtlinien-Builder oder zum DirXML-Skript finden Sie

im *Policy Builder and Driver Customization Guide* (Handbuch zum Richtlinien-Builder und zur Treiberanpassung).

Die Synchronisierungs-Engine wendet alle Richtlinientypen auf das Quelldokument an. Die Fähigkeit, diese Transformationen auszuführen, ist eine der leistungsstärksten Funktionen von Identity Manager. Die Transformation der Daten erfolgt in Echtzeit, während sie vom Identitätsdepot und den verbundenen Systemen gemeinsam genutzt werden.

1.2.2 Treiberkonfigurationsdateien

Bei den Treiberkonfigurationen handelt es sich um vorkonfigurierte XML-Dateien, die in Identity Manager enthalten sind. Sie können diese Konfigurationsdateien über die Assistenten in iManager und in Designer importieren.

Diese Treiberkonfigurationen enthalten Beispielrichtlinien. Sie sind nicht für die Verwendung in einer Produktionsumgebung vorgesehen, sondern dienen als Schablonen, die Sie ändern können.

1.2.3 Ereignis-Cache von Identity Manager

Alle über eDirectory generierten Ereignisse werden bis zu ihrer erfolgreichen Verarbeitung in einem Ereignis-Cache gespeichert. Dadurch ist gewährleistet, dass bei einer schlechten Verbindung, einem Verlust der Systemressourcen, der Nichtverfügbarkeit eines Treibers oder bei anderen Netzwerkfehlern keine Daten verloren gehen.

1.2.4 Treiberschnittstellenmodul

Das Treiberschnittstellenmodul dient als Kanal für den Austausch von Informationen zwischen dem verbundenen System und dem Identitätsdepot. Es wird in Java, C oder C++ programmiert.

Die Kommunikation zwischen der Metaverzeichnis-Engine und dem Treiberschnittstellenmodul erfolgt über XML-Dokumente, die Ereignisse, Abfragen und Ergebnisse beschreiben. Das Treiberschnittstellenmodul wird in der Regel als Treiber bezeichnet. Die Informationen zwischen dem verbundenen System und dem Identitätsdepot werden über diesen Kanal übermittelt.

Das Treiberschnittstellenmodul unterstützt folgende Objektereignisse:

- Hinzufügen (Erstellung)
- Ändern
- Löschen
- Umbenennen
- Verschieben
- Abfragen

Zusätzlich muss das Treiberschnittstellenmodul eine definierte Abfragefunktion unterstützen, sodass Identity Manager das verbundene System abfragen kann.

Wenn im Identitätsdepot ein Ereignis auftritt, das im verbundenen System eine Aktion auslöst, erstellt Identity Manager ein XML-Dokument mit einer Beschreibung des Identitätsdepot-Ereignisses und sendet es dann über den Abonnentenkanal an das Treiberschnittstellenmodul.

Wenn ein Ereignis im verbundenen System auftritt, generiert das Treiberschnittstellenmodul ein XML-Dokument mit einer Beschreibung dieses Ereignisses. Das Treiberschnittstellenmodul sendet das XML-Dokument anschließend über den Herausgeberkanal an Identity Manager. Im Anschluss an die Verarbeitung des Ereignisses durch bestimmte Herausgeberrichtlinien weist Identity Manager das Identitätsdepot an, die entsprechende Aktion auszuführen.

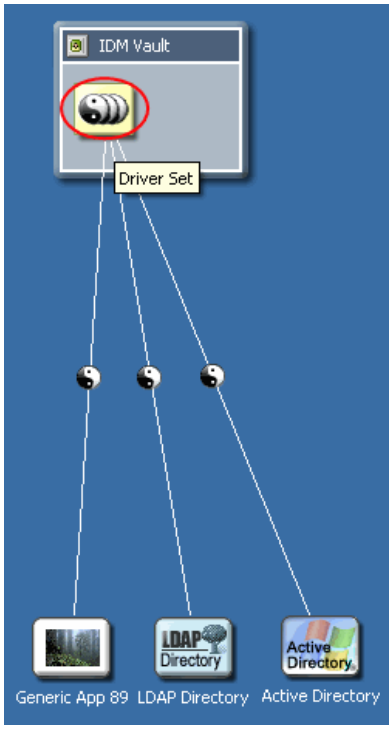
1.2.5 Treibersatz

Ein Treibersatz ist ein Containerobjekt, das Identity Manager-Treiber enthält. Ein Treibersatz kann immer nur einem Server zugeordnet sein. Aus diesem Grund müssen alle laufenden Treiber im selben Treibersatz zusammengefasst werden.

Da sich das Treibersatzobjekt auf jedem Server, der es verwendet, in einer vollwertigen Lese-/Schreibreproduktion befinden muss, wird empfohlen, den Treibersatz in einer separaten Partition abzulegen. Dies wird empfohlen, damit beim Verschieben von Benutzerreproduktionen auf einen anderen Server die Treiberobjekte nicht mit verschoben werden.

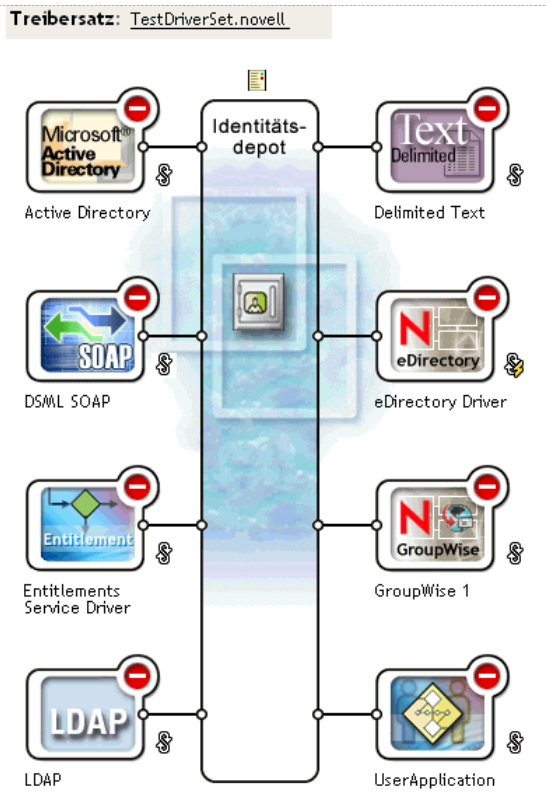
Die folgende Abbildung zeigt, wie der Treibersatz in Designer angezeigt wird.

Abbildung 1-2 *Treibersatz in Designer*



Die folgende Abbildung zeigt, wie der Treibersatz in iManager angezeigt wird.

Abbildung 1-3 *Treibersatz in iManager*



Im Modeler in Designer (siehe Abbildung 1-2 auf Seite 13) oder auf der Seite „Überblick“ in iManager (siehe Abbildung 1-3 auf Seite 14) können Sie Folgendes ausführen:

- Den Treibersatz und seine Eigenschaften anzeigen und ändern
- Die Treiber innerhalb des Treibersatzes anzeigen
- Den Status eines Treibers ändern
- Einen Treibersatz einem Server zuordnen
- Treiber hinzufügen oder entfernen
- Aktivierungsinformationen für den Treibersatz anzeigen
- Das Statusprotokoll für den Treibersatz anzeigen

1.2.6 Treiberobjekt

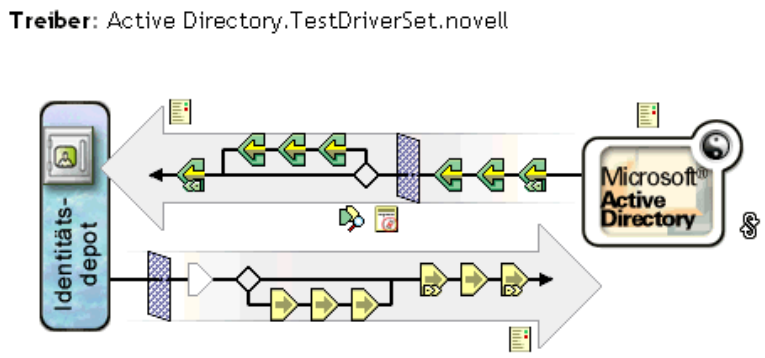
Ein Treiberobjekt stellt einen Treiber dar, der die Verbindung zu dem verbundenen System herstellt, das in das Identitätsdepot integriert wird. Das Treiberobjekt und seine Konfigurationsparameter bestehen aus folgenden Komponenten:

- Ein Treiberobjekt in der eDirectory-Baumstruktur, das in einem Treibersatzobjekt enthalten ist.
- Ein Abonnentenkanalobjekt, das im Treiberobjekt enthalten ist.
- Ein Herausgeberobjekt, das im Treiberobjekt enthalten ist.

- Mehrere Richtlinienobjekte, die von den Treiber-, Abonnenten- und Herausgeberobjekten referenziert werden.
- Ein ausführbares Treiberschnittstellenmodul, das vom Treiberobjekt referenziert wird.
- Schnittstellenmodulspezifische Parameter, die vom Administrator konfiguriert werden.
- Ein eDirectory-Passwort für das Treiberobjekt. Das Passwort kann vom Schnittstellenmodul zur Authentifizierung eines entfernten Teils des Schnittstellenmoduls verwendet werden.
- Authentifizierungsparameter, die verwendet werden, um eine Verbindung zum verbundenen System herzustellen und dieses zu authentifizieren.
- Berechtigungen, obwohl diese nicht in allen Treibern enthalten sind. Berechtigungen können beim Erstellen des Treibers oder zu einem späteren Zeitpunkt aktiviert werden.
- Eine Startoption für den Treiber, die folgende Auswahlmöglichkeiten bietet:
  - Deaktiviert: Der Treiber wird nicht ausgeführt.
  - Manuell: Der Treiber muss manuell über iManager gestartet werden.
  - Autom. starten: Der Treiber wird beim Starten des Identitätsdepots automatisch gestartet.
- Eine Referenz auf eine Schemazuordnungsrichtlinie.
- Eine XML-Darstellung des verbundenen Systemschemas. Diese wird in der Regel automatisch vom verbundenen System über das Schnittstellenmodul zur Verfügung gestellt.

In iManager können Sie auf „Identity Manager - Treiberüberblick“ zugreifen und Parameter, Richtlinien, Formatvorlagen und Berechtigungen eines vorhandenen Treibers ändern. Der Identity Manager-Treiberüberblick ist im Folgenden dargestellt.

Abbildung 1-4 *Identity Manager - Treiberüberblick*



Das Treiberobjekt wird zudem für das Überprüfen von eDirectory-Rechten verwendet. Das Treiberobjekt muss ausreichende eDirectory-Rechte für alle Objekte besitzen, die es lesen bzw. schreiben muss. Diese Rechte können Sie gewähren, indem Sie das Treiberobjekt zu einem Trustee der eDirectory-Objekte machen, mit denen der Treiber synchronisiert wird, oder indem Sie dem Treiberobjekt Sicherheitsäquivalenzen gewähren.

Weitere Informationen zu Zugriffsrechten finden Sie unter eDirectory Rights (http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbachifb.html) (eDirectory-Rechte) im *Novell eDirectory 8.8 Administration Guide* (Novell eDirectory 8.8 Administrationshandbuch).

1.2.7 Herausgeber- und Abonnentenkanäle

Identity Manager-Treiber enthalten zwei Kanäle für die Verarbeitung von Daten: den Herausgeberkanal und den Abonnentenkanal. Der Herausgeberkanal sendet Ereignisse vom verbundenen System an das Identitätsdepot. Der Abonnentenkanal sendet Ereignisse vom Identitätsdepot an das verbundene System. Jeder Kanal enthält eigene Richtlinien für die Verarbeitung und Transformation von Daten.

Abbildung 1-5 *Herausgeber- und Abonnentenkanäle in Designer*

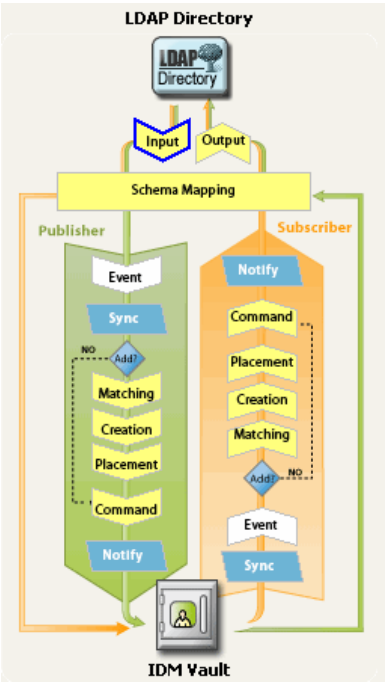
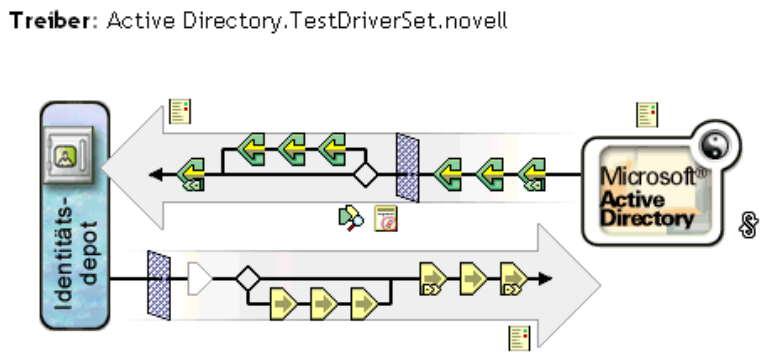


Abbildung 1-6 *Herausgeber- und Abonnentenkanäle in iManager*



1.2.8 Ereignisse und Befehle

Die Unterscheidung von Ereignissen und Befehlen in Identity Manager ist wichtig. Wenn ein Ereignis an einen Treiber gesendet wird, handelt es sich um einen Befehl. Wenn das Ereignis an Identity Manager gesendet wird, handelt es sich um eine Benachrichtigung. Wenn der Treiber eine Ereignisbenachrichtigung an Identity Manager sendet, informiert er Identity Manager über eine

Änderung, die im verbundenen System aufgetreten ist. Die Metaverzeichnis-Engine ermittelt anschließend anhand konfigurierbarer Regeln, welche Befehle, sofern erforderlich, an das Identitätsdepot gesendet werden müssen.

Wenn Identity Manager einen Befehl an den Treiber sendet, hat Identity Manager bereits ein Identitätsdepot-Ereignis als Input verarbeitet, die entsprechenden Richtlinien angewendet und festgelegt, dass die durch den Befehl dargestellte Änderung im verbundenen System erforderlich ist.

1.2.9 Richtlinien und Filter

Mit Richtlinien und Filtern können Sie den Datenfluss von einem System zu einem anderen steuern. Über die Regeln in den Richtlinien legen Sie fest, wie verwaltungsrelevante Identitätsdepot-Klassen, -Attribute und -Ereignisse für die Verwendung im verbundenen System übersetzt werden (und umgekehrt) . Weitere Informationen zu Richtlinien und Filtern finden Sie im *Policy Builder and Driver Customization Guide* (Handbuch zum Richtlinien-Builder und zur Treiberanpassung).

1.2.10 Verknüpfungen

Die meisten anderen Identity Management-Produkte erfordern, dass das verbundene System eine ID beliebigen Typs speichert, um Objekte eines verbundenen Systems dem Verzeichnis zuzuordnen. Bei Identity Manager sind keine Änderungen des verbundenen Systems erforderlich. Jedes Objekt im Identitätsdepot enthält eine Verknüpfungstabelle, die das Identitätsdepot-Objekt einer eindeutigen ID in den verbundenen Systemen zuordnet. Die Tabelle ist umgekehrt indiziert, sodass das verbundene System bei der Aktualisierung des Identitätsdepots dem Treiber keine Identitätsdepot-ID (z. B. einen eindeutigen Namen) zur Verfügung stellen muss.

Das Erstellen einer Verknüpfung zwischen zwei Objekten erfolgt, wenn ein Ereignis für ein Objekt auftritt, das noch keinem anderen Objekt im Identitätsdepot zugeordnet ist. Damit eine Verknüpfung erstellt werden kann, muss eine Mindestanzahl definierbarer Kriterien zwischen den einzelnen Objekten übereinstimmen. Sie können beispielsweise eine Richtlinie erstellen, die besagt, dass, wenn bei zwei von vier Attributen eine Übereinstimmung von mehr als 90% vorliegt (Vollständiger Name, Telefonnummer, Mitarbeiter-ID und Email-Adresse), das Objekt zugeordnet wird.

In Übereinstimmungsrichtlinien sind die Kriterien definiert, die festlegen, ob zwei Objekte identisch sind. Wenn für das geänderte Objekt keine Übereinstimmung gefunden wird, kann ein neues Objekt erstellt werden. Hier müssen jedoch die Mindestkriterien für die Objekterstellung erfüllt sein. Diese Kriterien werden in einer Erstellungsrichtlinie definiert. In der Platzierungsrichtlinie wird schließlich definiert, an welcher Stelle das neue Objekt in der Benennungshierarchie erstellt werden soll.

Es gibt zwei Möglichkeiten, Verknüpfungen zu erstellen:

- Als Entsprechung zwischen Objekten
- Als neu erstelltes Objekt an einem bestimmten Speicherort

Nachdem eine Verknüpfung zwischen Objekten hergestellt wurde, bleibt diese gültig, bis die Objekte gelöscht werden oder die Verknüpfung von einem Administrator gelöscht wird.

Verknüpfungstabelle

Verknüpfungen in Identity Manager beziehen sich auf die Übereinstimmung von Objekten in eDirectory mit Objekten, die sich in verbundenen Systemen befinden. Bei der Erstinstallation von Identity Manager wird das eDirectory-Schema erweitert. Teil dieser Erweiterung ist ein neues

Attribut, das an die Basisklasse aller eDirectory-Objekte gebunden wird. Dieses Attribut ist eine Verknüpfungstabelle. In Verknüpfungstabellen werden alle Objekte des verbundenen Systems protokolliert, mit denen ein eDirectory-Objekt verknüpft ist. Diese Tabelle wird automatisch erzeugt und gepflegt, sodass es selten notwendig ist, diese Informationen manuell zu bearbeiten. Es ist jedoch häufig hilfreich, sich diese Informationen anzusehen.

Das Verknüpfungsattribut des Objekts kann in iManager angezeigt werden.

1. Wählen Sie in der iManager-Symbolleiste das Symbol *Objekte anzeigen*.

2. Wählen Sie ein Objekt aus und klicken Sie anschließend auf *Objekt bearbeiten*.
3. Wählen Sie die Registerkarte „Identity Manager“.

Das Verknüpfungsattribut wird in der Registerkarte „Identity Manager“ angezeigt.

1.3 Benutzeranwendung

Die Benutzeranwendung ist eine Bereitstellungslösung. Sie ist ein Zusatzprodukt für Identity Manager 3. Die Benutzeranwendung integriert einen leistungsstarken Genehmigungs-Workflow in Identity Manager. Dies ermöglicht Unternehmen, Bereitstellungsentscheidungen anhand von Benutzereingaben und automatisierten Regeln zu treffen, wobei kein manuelles Eingreifen erforderlich ist. Weitere Informationen hierzu finden Sie in der Dokumentation der Benutzeranwendung (http://www.novell.com/documentation/idm).

1.4 Designer

Designer ist eine eigenständige Client-Anwendung. Die Anwendung besteht aus einem Modeler-Bereich, einer Palette, Ansichten, einem Richtlinien-Builder, einem Dokumentengenerator und anderen Funktionen, sodass Sie Identity Manager-basierte Lösungen in einer hoch produktiven Umgebung entwerfen, testen, dokumentieren und bereitstellen können. Weitere Informationen zu Designer finden Sie im *Designer for Identity Manager 3: Administration Guide* (Designer für Identity Manager 3: Administrationshandbuch).

Verwalten von Identity Manager-Treibern

2

In diesem Abschnitt wird beschrieben, wie Sie Identity Manager-Treiber erstellen und verwalten. Es werden u. a. folgende Themen erläutert:

2.1 Erstellen und Konfigurieren von Treibern

Für jeden Identity Manager-Treiber, den Sie verwenden möchten, sollten Sie ein Treiberobjekt erstellen und eine Treiberkonfiguration importieren. Das Treiberobjekt enthält Konfigurationsparameter und Richtlinien für diesen Treiber. Beim Erstellen eines Treiberobjekts importieren Sie eine treiberspezifische Konfigurationsdatei. Treiberkonfigurationen enthalten mehrere standardmäßige Richtlinien. Diese Richtlinien unterstützen Sie beim Implementieren Ihres Datenfreigabemodells. In den meisten Fällen richten Sie einen Treiber unter Verwendung der zum Lieferumfang gehörenden Standardkonfiguration ein und ändern anschließend die Treiberkonfiguration gemäß den Anforderungen Ihrer Umgebung.

Es gibt zwei Möglichkeiten zum Erstellen von Treiberobjekten.

- Mit der Aufgabe „Treiber erstellen“ können Sie einen einzelnen Treiber erstellen und dessen Treiberkonfiguration importieren. Weitere Informationen hierzu finden Sie unter „Erstellen von Treiberobjekten“ auf Seite 20.
- Mit der Aufgabe „Treiber importieren“ können Sie mehrere Treiber gleichzeitig erstellen und deren Konfigurationen importieren. Weitere Informationen hierzu finden Sie in Abschnitt 2.1.2, „Erstellen mehrerer Treiber“, auf Seite 20.

2.1.1 Erstellen von Treiberobjekten

Die für die ordnungsgemäße Funktion eines Treibers erforderlichen Objekte werden in einer Treiberkonfigurationsdatei (XML) erstellt und konfiguriert. Diese Datei enthält zudem Beispielrichtlinien, die Sie für Ihre Implementierung ändern können.

1. Wählen Sie in iManager *Identity Manager-Dienstprogramme* > *Neuer Treiber*.
2. Wählen Sie einen Treibersatz, in dem der Treiber erstellt werden soll, und klicken Sie anschließend auf *Weiter*.

   Wenn Sie diesen Treiber in einem neuen Treibersatz erstellen, müssen Sie für den Treibersatz einen Namen, einen Kontext und den zugeordneten Server angeben.
3. Aktivieren Sie die Option *Treiberkonfiguration vom Server importieren (.XML-Datei)*, wählen Sie die XML-Datei aus und klicken Sie auf *Weiter*.

   Die Treiberkonfigurationsdatei wird beim Einrichten von iManager auf dem Webserver installiert.
4. Führen Sie die Anweisungen aus, um das Importieren der Treiberkonfiguration abzuschließen.

Die erforderlichen Identity Manager-Objekte werden erstellt. Wenn Sie während des Importvorgangs keine Sicherheitsäquivalenzen definiert oder verwaltungsbefugte Benutzer ausgeschlossen haben, können Sie diese Aufgaben durchführen, indem Sie die Eigenschaften des Treiberobjekts ändern.

Hinweis: Wenn Sie während des Importvorgangs keine Berechtigungen aktiviert haben, werden keine Berechtigungsrichtlinien erstellt. Wenn Sie zu einem späteren Zeitpunkt Berechtigungen verwenden möchten, müssen Sie einen neuen Treiber erstellen und die Berechtigungen aktivieren.

2.1.2 Erstellen mehrerer Treiber

In Identity Manager haben Sie die Möglichkeit, mehrere Treiber gleichzeitig zu erstellen. Dieser Prozess ist mit dem Erstellen eines einzelnen Treibers vergleichbar, da auch hier die für die ordnungsgemäße Funktion des Treibers erforderlichen Objekte in Treiberkonfigurationsdateien (XML) erstellt werden.

So importieren Sie mehrere Treiber gleichzeitig:

1. Wählen Sie in iManager *Identity Manager-Dienstprogramme* > *Treiber importieren*.
2. Wählen Sie einen Treibersatz, in dem die neuen Treiber erstellt werden sollen, und klicken Sie anschließend auf *Weiter*.

   Wenn Sie diese Treiber in einem neuen Treibersatz erstellen, müssen Sie für den Treibersatz einen Namen, einen Kontext und den zugeordneten Server angeben.
3. Wählen Sie die dem Treibersatz hinzuzufügenden Anwendungskonfigurationen aus und klicken Sie auf *Weiter*.
4. Führen Sie die Anweisungen aus, geben Sie die angeforderten Daten ein und klicken Sie auf *Weiter*.

   Wenn Sie mehrere Konfigurationen gleichzeitig für den Import auswählen, werden die Konfigurationsseiten der Anwendung nacheinander angezeigt.

Die erforderlichen Identity Manager-Objekte für die einzelnen Treiber werden erstellt. Wenn Sie während des Importvorgangs keine Sicherheitsäquivalenzen definiert oder verwaltungsbefugte

Benutzer ausgeschlossen haben, können Sie diese Aufgaben durchführen, indem Sie die Eigenschaften des Treiberobjekts ändern.

2.2 Verwalten von DirXML 1.1a-Treibern in einer Identity Manager-Umgebung

Vorhandene Treiber, die für DirXML 1.1a erstellt wurden, funktionieren auch in Identity Manager.

Die zum Lieferumfang von Identity Manager 3.0 gehörende Metaverzeichnis-Engine ist abwärtskompatibel mit älteren Treibern (sofern die älteren Treiberschnittstellenmodule und Konfigurationen mit den neuesten Produktaktualisierungen und Patches aktualisiert wurden). Da die Engine abwärtskompatibel ist, können Sie DirXML 1.1a-Treiber auf den Identity Manager-Servern beliebig lange ausführen, ohne Änderungen vornehmen zu müssen.

Die iManager-Plugins verfügen jedoch nur über eine eingeschränkte Abwärtskompatibilität. Ältere Treiber können im Treibersatz-Überblick angezeigt werden, die Treiberkonfiguration kann jedoch ohne Konvertierung des Treibers weder angezeigt noch bearbeitet werden. Wenn Sie im Treibersatz-Überblick auf einen DirXML 1.1a-Treiber klicken, erkennen die Identity Manager-Plugins, dass der Treiber im DirXML 1.1a-Format vorliegt. Anschließend werden Sie aufgefordert, den Treiber unter Verwendung eines Assistenten in das 3.0-Format zu konvertieren.

Wenn Sie keine Änderungen an einem vorhandenen Treiber vornehmen möchten, können Sie den Assistenten abbrechen.

Zum Bearbeiten eines 1.1a-Treibers im 1.1a-Format müssen Sie die DirXML 1.1a-Plugins verwenden. Hierzu müssen Sie einen separaten iManager-Webserver verwenden, auf dem die 1.1a-Plugins installiert sind. Sie können die mit Identity Manager gelieferten Plugins nicht zum Bearbeiten einer Treiberkonfiguration verwenden, ohne den Treiber zuvor in das Identity Manager 3.0-Format zu konvertieren.

2.3 Upgrade einer Treiberkonfiguration von DirXML 1.1 auf ein Identity Manager-Format

Beim Upgrade von DirXML 1.1a auf Identity Manager 3 erfolgt zunächst das Upgrade auf Identity Manager 2. Die Identity Manager 2-Installation installiert neue Treiberschnittstellenmodule, nimmt jedoch keine Änderungen an vorhandenen Treiberobjekten oder Treiberkonfigurationen vor.

Vorhandene Treiberkonfigurationen, die für DirXML 1.1a erstellt wurden, funktionieren auch in Identity Manager. Mit den Identity Manager-Plugins können Sie jedoch nur Treiber bearbeiten, die im Identity Manager-Format vorliegen.

Wichtig: Das Ausführen eines Identity Manager-Treiberschnittstellenmoduls oder einer Treiberkonfiguration mit einer DirXML 1.1a-Engine wird nicht unterstützt.

Ein Assistent hilft Ihnen beim Konvertieren von DirXML 1.1a-Treibern in das Identity Manager-Format.

So starten Sie den Assistenten:

1. Klicken Sie in iManager auf *Identity Manager > Identity Manager-Überblick*.
2. Wählen Sie den Treibersatz aus, der den zu konvertierenden Treiber enthält, und klicken Sie anschließend auf *Suchen*.

3 Klicken Sie auf das Symbol für den zu konvertierenden Treiber.

   Sie werden aufgefordert, den Treiber in das neue Format zu konvertieren.

4 Führen Sie die Schritte des Assistenten aus, um die Konvertierung abzuschließen.

2.4 Starten, Stoppen oder Neustart eines Treibers

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

2 Wechseln Sie zu dem Treibersatz, der den Treiber enthält, und klicken Sie auf *Suchen*.

3 Klicken Sie auf die obere rechte Ecke des Treibersymbols, dessen Status Sie ändern möchten, und klicken Sie dann auf *Treiber starten*, wenn der Treiber angehalten ist, oder auf *Treiber anhalten*, wenn er ausgeführt wird.

2.5 Treiberparameter

Die Eigenschaften der einzelnen Treiber enthalten Treiberparameter. In diesen Parametern werden treiberspezifische Informationen gespeichert. In diesen Parametern werden Informationen wie das Polling-Intervall, die Authentifizierungsmethode, die Verwendung von SSL oder das Einrichten eines Heartbeats für den Treiber gespeichert.

2.6 Globalkonfigurationswerte

Globalkonfigurationswerte (Global configuration values, abgekürzt GCVs) sind mit Treiberparametern vergleichbare Einstellungen. Globalkonfigurationswerte können sowohl für einen Treibersatz als auch für einzelne Treiber festgelegt werden. Wenn ein Treiber keinen GCV-Wert hat, übernimmt er den Wert für diesen GCV aus dem Treibersatz.

Mit GCVs können Sie Einstellungen für Identity Manager-Funktionen wie die Passwortsynchronisierung und den Treiber-Heartbeat sowie Einstellungen angeben, die für die Funktion einer einzelnen Treiberkonfiguration spezifisch sind. Einige GCVs gehören bereits zum Lieferumfang des Treibers, Sie können aber auch eigene GCVs hinzufügen. Zum Anpassen der Treiberkonfiguration können Sie diese Werte auch in einer Richtlinie angeben.

Wichtig: Die Einstellungen für die Passwortsynchronisierung sind ebenfalls GCVs. Sie sollten diese jedoch auf der Seite „Passwortsynchronisierung“ der Registerkarte „Server-Variablen“ bearbeiten und nicht auf der GCV-Seite. Die Seite „Server-Variablen“, auf der die Einstellungen für die Passwortsynchronisierung angezeigt werden, steht wie die anderen Treiberparameter als Registerkarte zur Verfügung. Sie können auch auf *Passwortverwaltung* > *Passwortsynchronisierung* klicken, nach dem Treiber suchen und auf den Treibernamen klicken. Auf der Seite ist zudem für die einzelnen Einstellungen der Passwortsynchronisierung eine Online-Hilfe verfügbar.

So können Sie GCVs hinzufügen, entfernen oder bearbeiten, die nicht mit der Passwortsynchronisierung in Identity Manager in Zusammenhang stehen:

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

2 Wechseln Sie zum gewünschten Treibersatz oder -objekt und klicken Sie anschließend auf *Suchen*.

3 Klicken Sie auf die obere rechte Ecke des Treibers und klicken Sie anschließend auf *Eigenschaften bearbeiten*.

4 Wählen Sie *Globalkonfigurationswerte*.

5 Ändern Sie die beim Erstellen des Treibers festgelegten Standardwerte.

6 Wenn Sie weitere Informationen hinzufügen möchten, klicken Sie auf *XML bearbeiten*.

7 Klicken Sie auf *XML-Bearbeitung aktivieren*.

8 Fügen Sie die XML-Daten hinzu, entfernen oder bearbeiten Sie sie und klicken Sie anschließend auf *OK*, um die Änderungen zu übernehmen.

2.7 Verwenden des DirXML-Befehlszeilenprogramms

Das DirXML-Befehlszeilenprogramm bietet Zugriff auf Identity Manager-spezifische eDirectory-Verben. Dieses Dienstprogramm ist nicht als Ersatz für iManager oder Designer vorgesehen. Dieses Dienstprogramm wird primär zum Generieren von Skripts verwendet. Weitere Informationen zum DirXML-Befehlszeilenprogramm finden Sie in Anhang A, „DirXML-Befehlszeilenprogramm“, auf Seite 265. Verwenden Sie für tägliche Aufgaben iManager oder Designer.

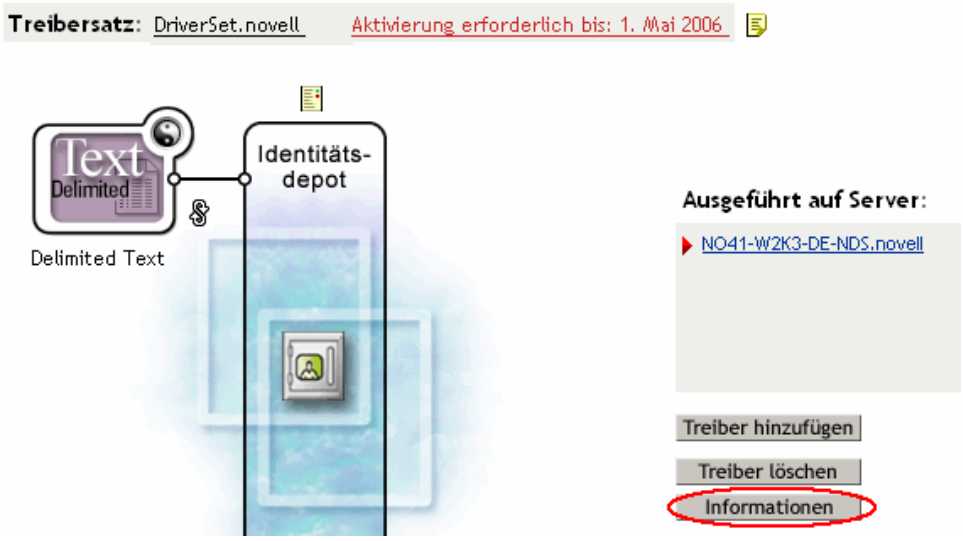
2.8 Anzeigen von Versionsinformationen

Mit dem Versionsermittlungswerkzeug können Sie Folgendes ausführen:

2.8.1 Anzeigen einer hierarchischen Struktur der Versionsinformationen

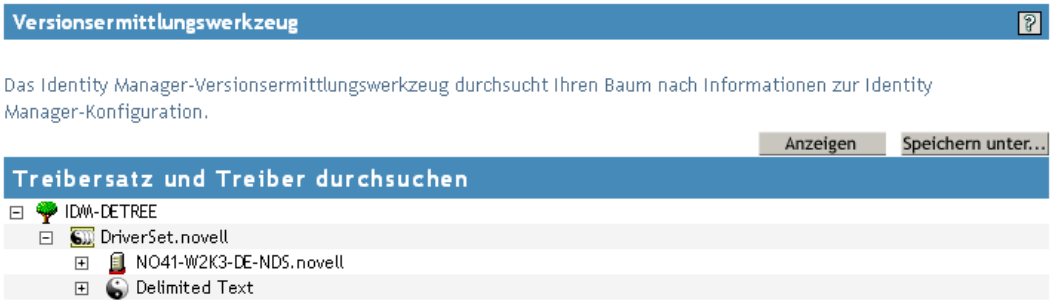
1 Klicken Sie in iManager auf *Identity Manager* > *Identity Manager-Überblick* und anschließend auf *Suchen*, um zum gewünschten Treibersatz zu wechseln.

2 Klicken Sie im Bildschirm „Identity Manager-Überblick“ auf *Informationen*.



Sie können auch *Identity Manager-Dienstprogramme* > *Versionsermittlung* wählen, den gewünschten Treibersatz auswählen und anschließend auf *OK* klicken.

3 Zeigen Sie die Versionsinformationen auf oberster Ebene oder in komprimierter Form an.

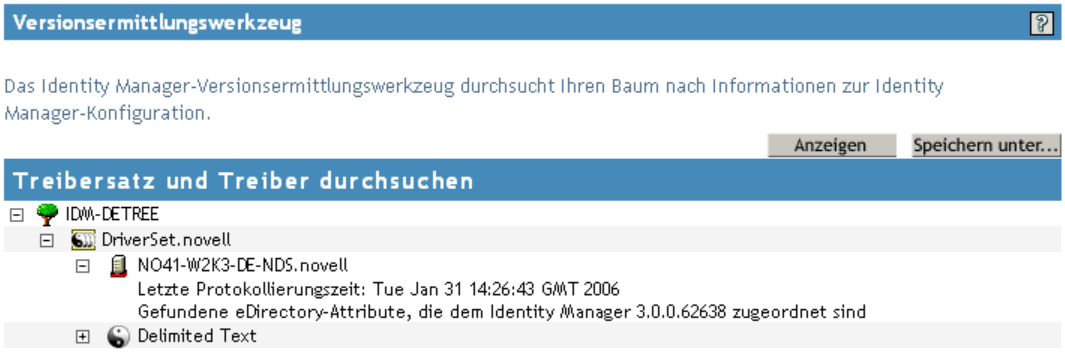


In der komprimierten hierarchischen Ansicht wird Folgendes angezeigt:

- Die eDirectory-Baumstruktur, für die Sie authentifiziert sind
- Der ausgewählte Treibersatz
- Server, die dem Treibersatz zugeordnet sind

  Wenn der Treibersatz zwei oder mehreren Servern zugeordnet ist, können Sie die Identity Manager-Informationen auf jedem Server anzeigen.
- Treiber

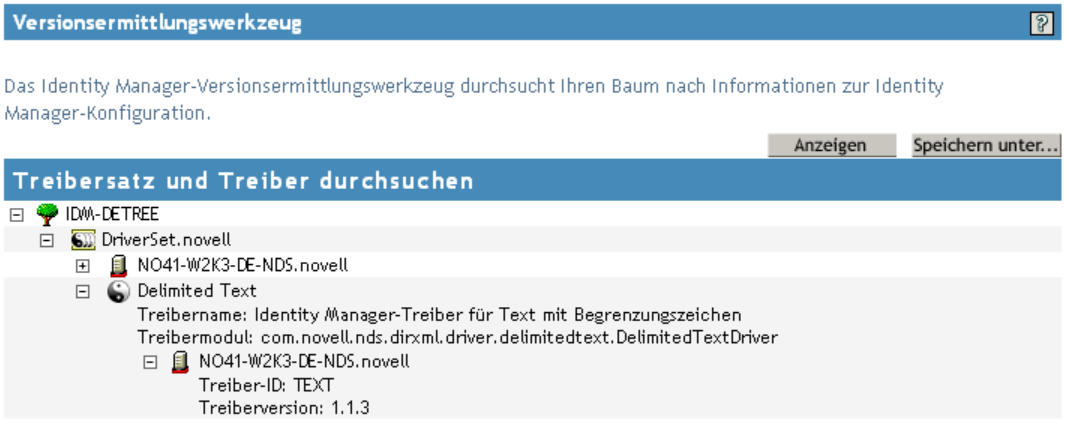
4 Zeigen Sie die mit den Servern in Zusammenhang stehenden Versionsinformationen an, indem Sie das Serversymbol erweitern.



Die erweiterte Ansicht eines Serversymbols der obersten Ebene enthält Folgendes:

- Letzte Protokollierungszeit
- Die auf dem Server ausgeführte Version von Identity Manager

5 Zeigen Sie die mit den Treibern in Zusammenhang stehenden Versionsinformationen an, indem Sie das Treibersymbol erweitern.



Die erweiterte Ansicht eines Treibersymbols der obersten Ebene enthält Folgendes:

- Treibername
- Treibermodul (z. B. com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver)

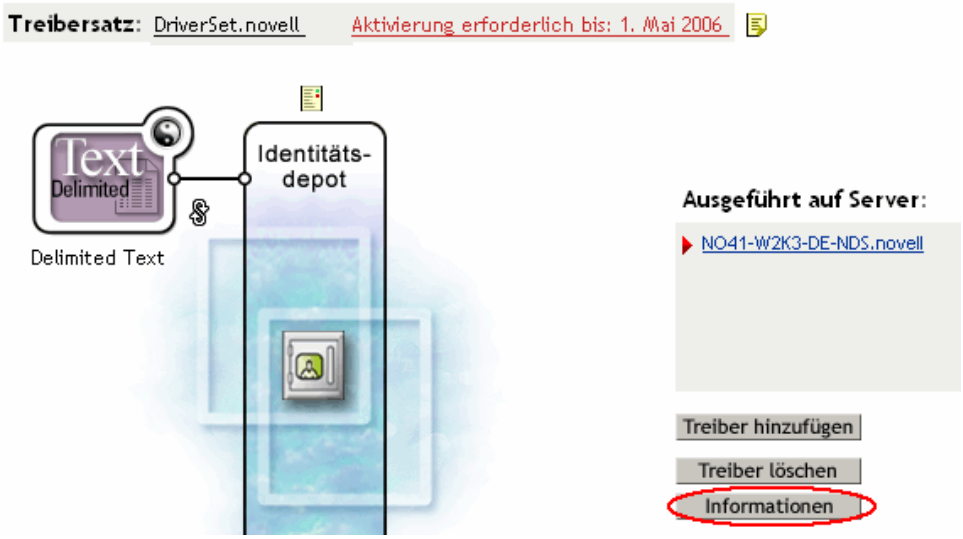
Die erweiterte Ansicht eines Servers unter einem Treibersymbol enthält Folgendes:

- Treiber-ID
- Version der auf diesem Server ausgeführten Treiberinstanz

2.8.2 Anzeigen der Versionsinformationen als Textdatei

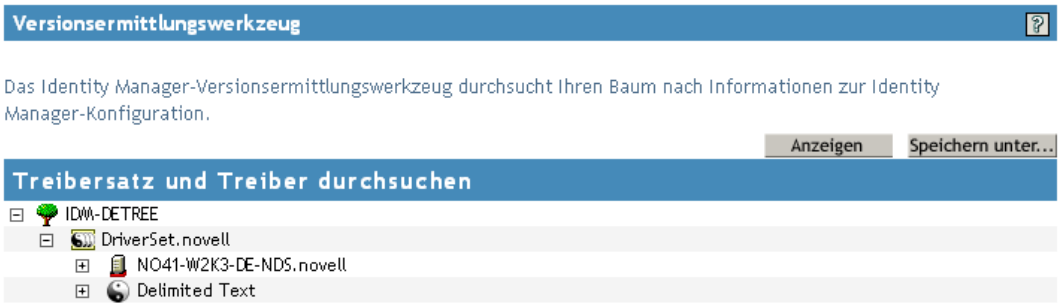
Identity Manager veröffentlicht Versionsinformationen in einer Datei. Sie können diese Informationen im Textformat anzeigen. Die Textdarstellung enthält dieselben Informationen wie die hierarchische Ansicht.

1. Klicken Sie in iManager auf *Identity Manager* > *Identity Manager-Überblick* und anschließend auf *Suchen*, um zum gewünschten Treibersatz zu wechseln.
2. Klicken Sie im Bildschirm „Identity Manager-Überblick“ auf *Informationen*.

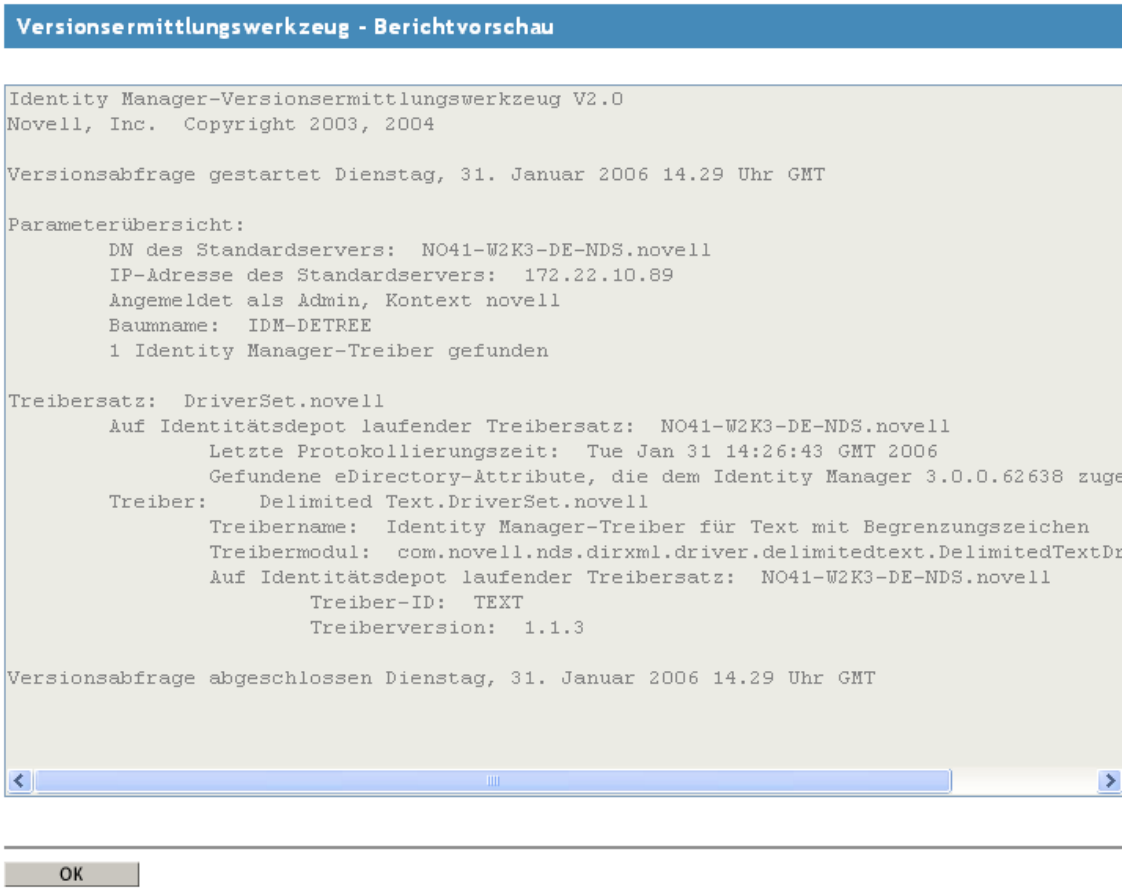


Sie können auch *Identity Manager-Dienstprogramme* > *Versionsermittlung* wählen, den gewünschten Treibersatz auswählen und anschließend auf *Informationen* klicken.

3. Klicken Sie im Dialogfeld „Versionsermittlungswerkzeug“ auf *Anzeigen*.



Die Informationen werden im Fenster „Berichtvorschau“ als Textdatei angezeigt.

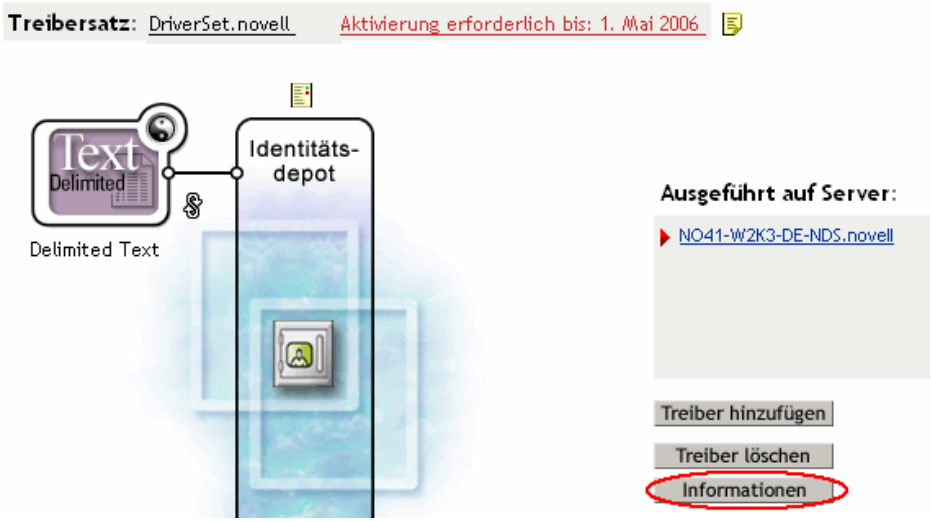


2.8.3 Speichern von Versionsinformationen

Sie können Versionsinformationen in einer Textdatei auf einem lokalen oder auf einem Netzlaufwerk speichern.

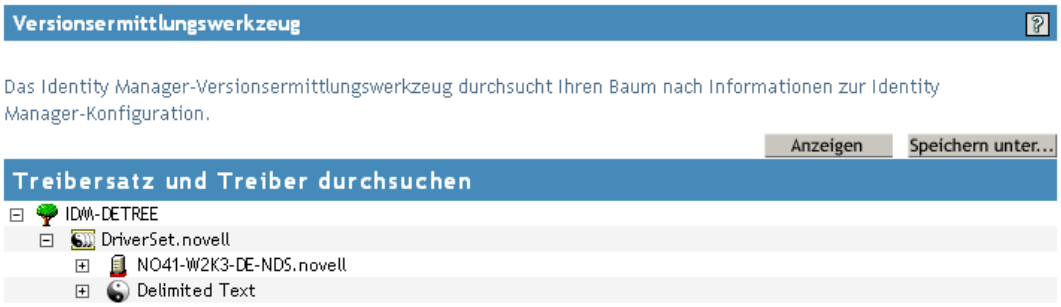
1 Klicken Sie in iManager auf *Identity Manager* > *Identity Manager-Überblick* und anschließend auf *Suchen*, um zum gewünschten Treibersatz zu wechseln.

2 Klicken Sie im Bildschirm „Identity Manager-Überblick“ auf *Informationen*.



Sie können auch *Identity Manager-Dienstprogramme* > *Versionsermittlung* wählen, den gewünschten Treibersatz auswählen und anschließend auf *Informationen* klicken.

3 Klicken Sie im Dialogfeld „Versionsermittlungswerkzeug“ auf *Speichern unter*.



4 Klicken Sie im Dialogfeld zum Herunterladen von Dateien auf *Speichern*.

5 Navigieren Sie zum gewünschten Verzeichnis, geben Sie einen Dateinamen ein und klicken Sie auf *Speichern*.

Identity Manager speichert die Daten in einer Textdatei.

2.9 Verwenden benannter Passwörter

In Identity Manager können Sie für einen bestimmten Treiber mehrere Passwörter sicher speichern. Diese Funktionalität wird als „Benannte Passwörter“ bezeichnet. Der Zugriff auf die einzelnen Passwörter erfolgt über einen Schlüssel oder Namen.

Mit der Funktion „Benannte Passwörter“ können Sie auch andere Informationen, z. B. den Benutzernamen, sicher speichern.

Wenn Sie ein benanntes Passwort in einer Treiberrichtlinie verwenden möchten, verweisen Sie mit dem Namen des Passworts darauf, anstatt das eigentliche Passwort zu verwenden. Das Passwort wird dann über die Metaverzeichnis-Engine an den Treiber gesendet. Die in diesem Abschnitt

beschriebene Methode zum Speichern und Abrufen von benannten Passwörtern kann für alle Treiber verwendet werden, ohne dass Änderungen am Treiberschnittstellenmodul erforderlich sind.

Hinweis: Die für den Identity Manager-Treiber für Lotus Notes verfügbaren Beispielkonfigurationen enthalten ein Beispiel für benannte Passwörter, die auf diese Weise verwendet werden. Das Notes-Treiberschnittstellenmodul wurde zudem so angepasst, dass es zusätzliche Methoden der Verwendung von benannten Passwörtern unterstützt. Beispiele dieser Methoden sind ebenfalls enthalten. Weitere Informationen hierzu finden Sie im Abschnitt zu den benannten Passwörtern im *Identity Manager Driver for Lotus Notes: Implementation Guide* (Identity Manager-Treiber für Lotus Notes: Implementierungshandbuch).

Dieser Abschnitt umfasst:

2.9.1 Konfigurieren benannter Passwörter in Designer

1. Klicken Sie mit der rechten Maustaste auf das gewünschte Treiberobjekt und wählen Sie *Eigenschaften*.
2. Wählen Sie *Benanntes Passwort* und klicken Sie auf *Neu*.

3. Geben Sie unter *Name* den Namen des benannten Passworts an.
4. Geben Sie unter *Display Name* (Anzeigename) den Anzeigenamen des benannten Passworts an.

5 Geben Sie das benannte Passwort ein und bestätigen Sie es durch eine erneute Eingabe.

6 Klicken Sie zweimal auf *OK*.

2.9.2 Konfigurieren benannter Passwörter in iManager

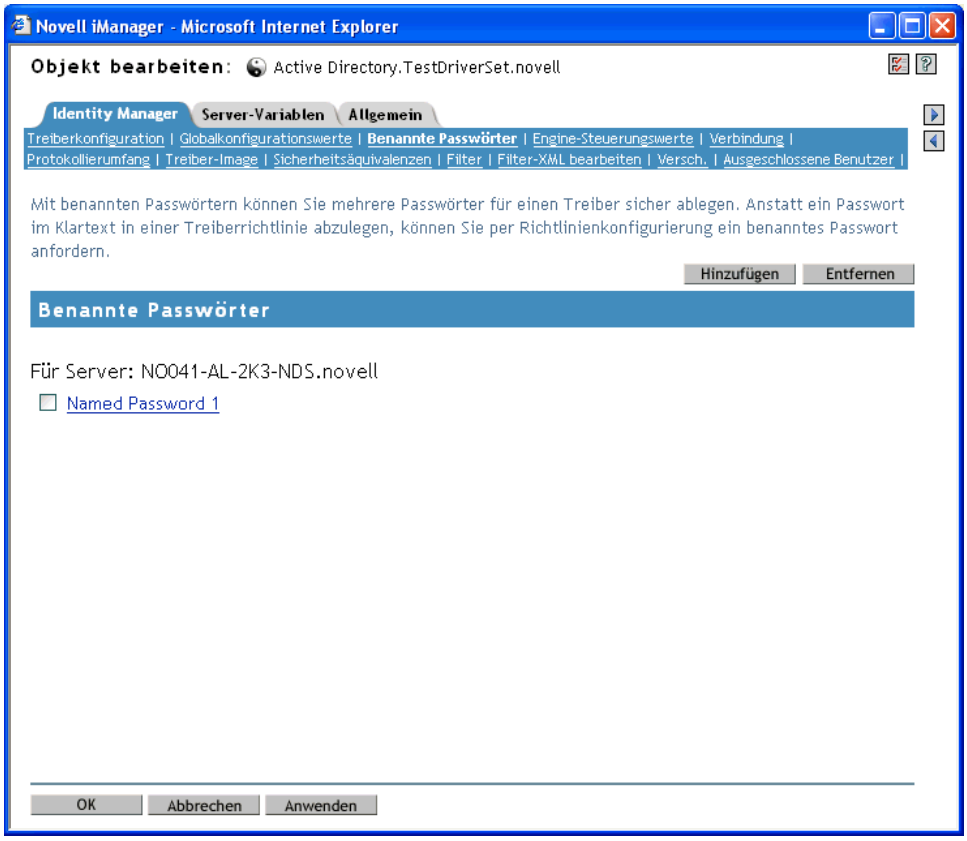
1 Klicken Sie in iManager auf *Identity Manager > Identity Manager-Überblick*.

2 Suchen Sie den gewünschten Treibersatz oder wählen Sie einen Container aus, der den Treibersatz enthält. Es wird eine grafische Darstellung des Treibersatzes angezeigt.

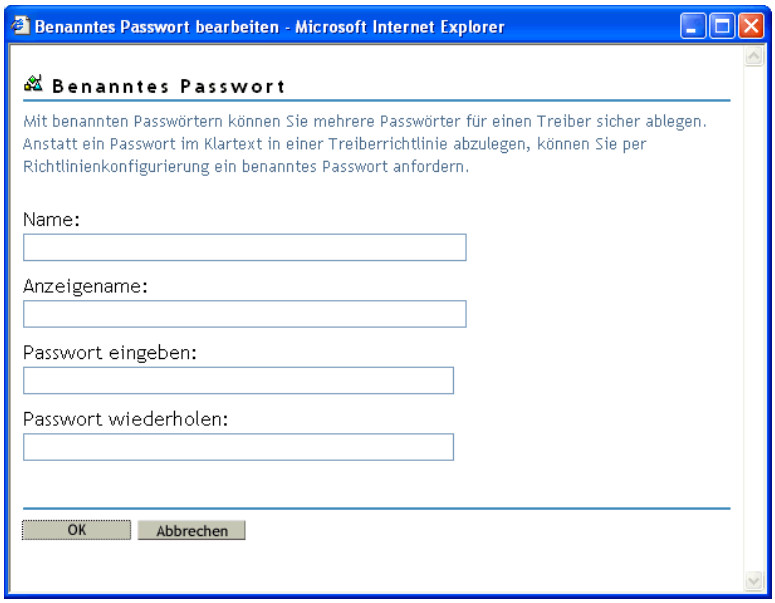
3 Klicken Sie im Bildschirm „Identity Manager-Überblick“ auf die obere rechte Ecke des Treibersymbols und anschließend auf *Eigenschaften bearbeiten*.

4 Klicken Sie auf der Seite „Objekt bearbeiten“ der Registerkarte „Identity Manager“ auf *Benannte Passwörter*.

Die Seite „Benannte Passwörter“ wird angezeigt, auf der die aktuellen benannten Passwörter für diesen Treiber aufgeführt sind. Wenn Sie noch keine benannten Passwörter festgelegt haben, ist diese Liste leer.



5 Klicken Sie zum Hinzufügen eines benannten Passworts auf *Hinzufügen*, füllen Sie die Felder aus und klicken Sie auf *OK*.



6 Geben Sie einen Namen, einen Anzeigenamen und ein Passwort ein und klicken Sie zweimal auf *OK*.

Beachten Sie, dass Sie mithilfe dieser Funktion auch andere Informationen, z. B. den Benutzernamen, sicher speichern können.

7 Es wird folgende Meldung angezeigt: „Möchten Sie den Treiber neu starten, damit Ihre Änderungen wirksam werden?“ (OK=Ja, Abbrechen=Nein) Klicken Sie auf *OK*.

8 Klicken Sie zum Entfernen eines benannten Passworts auf *Entfernen*. Das Passwort wird entfernt, ohne dass Sie diesen Vorgang bestätigen müssen.

2.9.3 Verwenden benannter Passwörter in Treiberrichtlinien

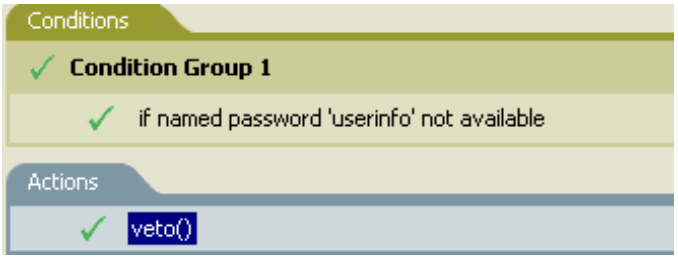
- „Verwenden des Richtlinien-Builder“ auf Seite 31
- „Verwenden von XSLT“ auf Seite 32

Verwenden des Richtlinien-Builder

Mit dem Richtlinien-Builder können Sie ein benanntes Passwort aufrufen. Erstellen Sie eine neue Regel und wählen Sie „Benanntes Passwort“ als Bedingung. Sie legen eine Aktion abhängig davon fest, ob das benannte Passwort verfügbar ist oder nicht. Das folgende Beispiel zeigt, dass, wenn die

Benutzerinformationen für das benannte Passwort nicht verfügbar sind, gegen das Ereignis ein Veto eingelegt wird.

Abbildung 2-1 *Eine Richtlinie, die ein benanntes Passwort verwendet*



Verwenden von XSLT

Das folgende Beispiel zeigt, wie ein benanntes Passwort in XSLT in einer Treiberrichtlinie auf dem Abonnentenkanal referenziert wird:

```
<xsl:value-of
select="query:getNamedPassword($srcQueryProcessor,'mynamedpassword')"
xmlns:query="http://www.novell.com/java/
com.novell.nds.dirxml.driver.XdsQueryProcessor/>
```

2.9.4 Konfigurieren benannter Passwörter mit dem DirXML-Befehlszeilenprogramm

- „Erstellen eines benannten Passworts mit dem DirXML-Befehlszeilenprogramm“ auf Seite 32
- „Entfernen eines benannten Passworts mit dem DirXML-Befehlszeilenprogramm“ auf Seite 34

Erstellen eines benannten Passworts mit dem DirXML-Befehlszeilenprogramm

1. Starten Sie das DirXML-Befehlszeilenprogramm.

   Weitere Informationen hierzu finden Sie in Anhang A, „DirXML-Befehlszeilenprogramm“, auf Seite 265.

2. Geben Sie Ihren Benutzernamen und das Passwort ein.

   Es wird eine Liste mit folgenden Optionen angezeigt.

```
DirXML commands

 1: Start driver
 2: Stop driver
 3: Driver operations...
 4: Driver set operations...
 5: Log events operations...
 6: Get DirXML version
99: Quit

Enter choice:
```

3 Geben Sie „3“ für Treibervorgänge ein.

Es wird eine nummerierte Liste mit Treibern angezeigt.

4 Geben Sie die Nummer des Treibers ein, dem Sie ein benanntes Passwort hinzufügen möchten.

Es wird eine Liste mit folgenden Optionen angezeigt.

```
Select a driver operation for:driver_name

 1: Start driver
 2: Stop driver
 3: Get driver state
 4: Get driver start option
 5: Set driver start option
 6: Resync driver
 7: Migrate from application into DirXML
 8: Submit XDS command document to driver
 9: Check object password
10: Initialize new driver object
11: Passwords operations
12: Cache operations
99: Exit

Enter choice:
```

5 Geben Sie „11“ für Passwortvorgänge ein.

Es wird eine Liste mit folgenden Optionen angezeigt.

```
Select a password operation

 1: Set shim password
 2: Reset shim password
 3: Set named password
 4: Clear named password(s)
 5: List named passwords
99: Exit

Enter choice:
```

6 Geben Sie „3“ ein, um ein neues benanntes Passwort festzulegen.

Es wird die folgende Eingabeaufforderung angezeigt:

```
Enter password name:
```

7 Geben Sie den Namen des benannten Passworts ein.

8 Geben Sie das eigentliche Passwort, das Sie schützen möchten, an der folgenden Eingabeaufforderung ein:

```
Enter password:
```

Die Zeichen, die Sie für das Passwort eingeben, werden nicht angezeigt.

9 Bestätigen Sie das Passwort, indem Sie es an der folgenden Eingabeaufforderung erneut eingeben:

```
Confirm password:
```

10 Wenn Sie das Passwort eingegeben und bestätigt haben, wird wieder das Menü für Passwortvorgänge angezeigt.

Wählen Sie nach Abschluss dieses Vorgangs zweimal die Option „99“, um das Menü zu verlassen und das DirXML-Befehlszeilenprogramm zu beenden.

Entfernen eines benannten Passworts mit dem DirXML-Befehlszeilenprogramm

Diese Option ist hilfreich, wenn Sie zuvor erstellte benannte Passwörter nicht länger benötigen.

1 Starten Sie das DirXML-Befehlszeilenprogramm.

Weitere Informationen hierzu finden Sie in Anhang A, „DirXML-Befehlszeilenprogramm“, auf Seite 265.

2 Geben Sie Ihren Benutzernamen und das Passwort ein.

Es wird eine Liste mit folgenden Optionen angezeigt.

```
DirXML commands

 1: Start driver
 2: Stop driver
 3: Driver operations...
 4: Driver set operations...
 5: Log events operations...
 6: Get DirXML version
99: Quit

Enter choice:
```

3 Geben Sie „3“ für Treibervorgänge ein.

Es wird eine nummerierte Liste mit Treibern angezeigt.

4 Geben Sie die Nummer des Treibers ein, aus dem Sie ein benanntes Passwort entfernen möchten.

Es wird eine Liste mit folgenden Optionen angezeigt.

```
Select a driver operation for:driver_name

 1: Start driver
 2: Stop driver
 3: Get driver state
 4: Get driver start option
 5: Set driver start option
 6: Resync driver
 7: Migrate from application into DirXML
 8: Submit XDS command document to driver
 9: Check object password
```

```
10: Initialize new driver object
11: Passwords operations
12: Cache operations
99: Exit

Enter choice:
```

5 Geben Sie „11“ für Passwortvorgänge ein.

Es wird eine Liste mit folgenden Optionen angezeigt.

```
Select a password operation

 1: Set shim password
 2: Reset shim password
 3: Set named password
 4: Clear named password(s)
 5: List named passwords
99: Exit

Enter choice:
```

6 (Optional) Geben Sie „5“ ein, um die Liste der vorhandenen benannten Passwörter anzuzeigen.

Die Liste der vorhandenen benannten Passwörter wird angezeigt.

In diesem Schritt können Sie sicherstellen, dass Sie das richtige Passwort entfernen.

7 Geben Sie „4“ ein, um ein oder mehrere benannte Passwörter zu entfernen.

8 Geben Sie an der folgenden Eingabeaufforderung „No“ ein, um ein einzelnes benanntes Passwort zu entfernen:

```
Do you want to clear all named passwords? (yes/no):
```

9 Geben Sie den Namen des zu löschenden benannten Passworts an der folgenden Eingabeaufforderung ein:

```
Enter password name:
```

Wenn Sie den Namen des zu löschenden Passworts eingegeben haben, wird wieder das Menü für Passwortvorgänge angezeigt:

```
Select a password operation

 1: Set shim password
 2: Reset shim password
 3: Set named password
 4: Clear named password(s)
 5: List named passwords
99: Exit

Enter choice:
```

10 (Optional) Geben Sie „5“ ein, um die Liste der vorhandenen benannten Passwörter anzuzeigen.

Die Liste der vorhandenen benannten Passwörter wird angezeigt.

In diesem Schritt können Sie verifizieren, dass Sie das richtige Passwort entfernt haben.

Wählen Sie nach Abschluss dieses Vorgangs zweimal die Option „99“, um das Menü zu verlassen und das DirXML-Befehlszeilenprogramm zu beenden.

2.10 Treiberobjekt einem Server erneut zuordnen

Ein Treiberobjekt ist einem Server zugeordnet.

Wenn diese Verknüpfung aus einem bestimmten Grund ungültig wird, wird dies durch eine der folgenden Aktionen angezeigt:

- Beim Aufrüsten von eDirectory auf dem Identity Manager-Server wird die Fehlermeldung „UniqueSPIException error -783“ angezeigt.
- Im Bildschirm „Identity Manager-Überblick“ wird neben dem Treiber kein Server angezeigt.
- Im Bildschirm „Identity Manager-Überblick“ wird neben dem Treiber ein Server angezeigt, aber sein Name erscheint als verstümmelter Text.

Wenn Sie dieses Problem beheben möchten, müssen Sie die Zuordnung zwischen dem Treiberobjekt und dem Server aufheben und anschließend eine erneute Zuordnung vornehmen.

Melden Sie sich bei iManager an und wechseln Sie im Bildschirm „Identity Manager-Überblick“ zum gewünschten Treiberobjekt. Entfernen Sie mithilfe der dafür vorgesehenen Symbole den Server aus der Servernamenliste neben dem Treibersymbol und fügen Sie ihn anschließend erneut hinzu. Durch das Entfernen und erneute Hinzufügen wird der Server dem Treiberobjekt wieder zugeordnet.

2.11 Verwenden des Treiber-Heartbeats

Der Treiber-Heartbeat ist eine Funktion der Identity Manager-Treiber, die zum Lieferumfang von Identity Manager 2 und höher gehören. Seine Verwendung ist optional. Der Treiber-Heartbeat wird unter Verwendung eines Treiberparameters mit dem angegebenen Zeitintervall konfiguriert. Wenn ein Heartbeat-Parameter vorhanden ist und über einen Intervallwert größer 0 verfügt, sendet der Treiber ein Heartbeat-Dokument an die Metaverzeichnis-Engine, wenn während des angegebenen Zeitintervalls keine Kommunikation auf dem Herausgeberkanal stattfindet.

Der Treiber-Heartbeat soll als Auslöser für eine Aktion dienen, die in regelmäßigen Intervallen ausgeführt wird, wenn der Treiber nicht so häufig auf dem Herausgeberkanal kommuniziert, wie die Aktion stattfinden soll. Um die Vorteile des Heartbeats nutzen zu können, müssen Sie die Treiberkonfiguration und weitere Werkzeuge anpassen. Die Metaverzeichnis-Engine akzeptiert das Heartbeat-Dokument, führt aber aufgrund dessen keine Aktion aus.

Bei den meisten Treibern wird in den Beispielkonfigurationen kein Treiberparameter für den Heartbeat verwendet. Sie können diesen jedoch hinzufügen.

Ein benutzerdefinierter Treiber, der nicht zum Lieferumfang von Identity Manager gehört, kann auch ein Heartbeat-Dokument zur Verfügung stellen, wenn der Treiberentwickler den dafür erforderlichen Treiber programmiert hat.

Sie konfigurieren den Heartbeat wie folgt:

1. Klicken Sie in iManager auf *Identity Manager* > *Identity Manager-Überblick*.
2. Wählen Sie den gewünschten Treibersatz aus und klicken Sie auf *Suchen*.

3. Klicken Sie im Bildschirm „Identity Manager-Überblick“ auf die obere rechte Ecke des Treibersymbols und klicken Sie anschließend auf *Eigenschaften bearbeiten*.
4. Klicken Sie in der Registerkarte „Identity Manager“ auf *Treiberkonfiguration*, blättern Sie zu den Treiberparametern und suchen Sie nach „Heartbeat“ oder einem ähnlichen Anzeigenamen.

   Wenn für den Heartbeat bereits ein Treiberparameter vorhanden ist, können Sie das Intervall ändern und die Änderungen speichern. Die Konfiguration ist damit abgeschlossen.

   Der Wert des Intervalls darf nicht kleiner als 1 sein. Ein Wert von 0 bedeutet, dass die Funktion deaktiviert ist.

   Die Zeit wird in der Regel in Minuten angegeben. Bei einigen Treibern kann z. B. aber auch eine Angabe in Sekunden erforderlich sein.
5. Wenn für einen Heartbeat kein Treiberparameter vorhanden ist, klicken Sie auf „XML bearbeiten“.
6. Fügen Sie, wie im folgenden Beispiel dargestellt, einen Treiberparametereintrag als untergeordneten Eintrag von <publisher-options> hinzu. (Fügen Sie ihn bei einem AD-Treiber als untergeordneten Eintrag von <driver-options> hinzu.)

   ```
   <pub-heartbeat-interval display-name="Heart Beat">10</pub-
   heartbeat-interval>
   ```

   Tipp: Wenn der Treiber nach dem Neustart kein Heartbeat-Dokument generiert, prüfen Sie die Position des Treiberparameters in der XML-Datei.
7. Speichern Sie die Änderungen und stellen Sie sicher, dass der Treiber angehalten und neu gestartet wird.

Wenn Sie den Treiberparameter hinzugefügt haben, können Sie das Zeitintervall in der grafischen Ansicht bearbeiten. Sie können für das Zeitintervall aber auch eine Referenz auf einen Globalkonfigurationswert (GCV) erstellen. Der Treiber-Heartbeat kann wie andere Globalkonfigurationswerte auf Treibersatzebene festgelegt werden, d. h., es ist in diesem Fall nicht nötig, ihn für jedes einzelne Treiberobjekt festzulegen. Wenn ein Treiber keinen bestimmten Globalkonfigurationswert hat, aber der Treibersatz hat einen solchen Wert, übernimmt der Treiber den entsprechenden Wert aus dem Treibersatz.

Im Folgenden finden Sie ein Beispiel für ein Heartbeat-Statusdokument, das vom Notes-Treiber gesendet wurde:

```
<nds dtdversion="2.0" ndsversion="8.x">
  <source>
    <product build="20031112_1037" instance="blackcap"
version="2.0">DirXML Driver for Lotus Notes</product>
    <contact>Novell, Inc.</contact>
  </source>
  <input>
    <status level="success" type="heartbeat"/>
  </input>
</nds>
```

2.12 Anzeigen von Identity Manager-Prozessen

Verwenden Sie DSTRACE zum Anzeigen von Identity Manager-Prozessereignissen. Dies ist jedoch nur bei Tests und bei der Fehlerbehebung in Identity Manager möglich. Wenn DSTRACE ausgeführt wird, während die Treiber in Produktion sind, wird die Nutzlast der Identity Manager-Server erhöht . Dies kann dazu führen, dass Ereignisse nur sehr langsam ausgeführt werden.

Zum Anzeigen von Identity Manager-Prozessen in DSTRACE werden dem Treibersatz und den Treiberobjekten Werte hinzugefügt. Dies erfolgt in Designer oder in iManager.

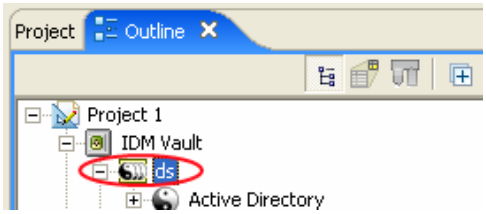
- Abschnitt 2.12.1, „Hinzufügen von Trace-Stufen in Designer“, auf Seite 38
- Abschnitt 2.12.2, „Hinzufügen von Trace-Stufen in iManager“, auf Seite 40
- Abschnitt 2.12.3, „Erfassen von Identity Manager-Prozessen in einer Datei“, auf Seite 41

2.12.1 Hinzufügen von Trace-Stufen in Designer

Sie können dem Treibersatzobjekt oder einzelnen Treiberobjekten Trace-Stufen hinzufügen.

Treibersatz

1 Wählen Sie in Designer in einem geöffneten Projekt das Treibersatzobjekt in der Überblicksansicht aus.



2 Klicken Sie mit der rechten Maustaste, wählen Sie *Properties* (Eigenschaften) und klicken Sie dann auf *5. Trace*.

3 Legen Sie die Parameter für das Tracing fest und klicken Sie auf *OK*. Weitere Informationen zu den Treibersatz-Trace-Parametern finden Sie in Tabelle 2-1 auf Seite 38.

Wenn Sie die Trace-Stufe für das Treibersatzobjekt festgelegt haben, werden alle Treiber in den DSTRACE-Protokollen angezeigt.

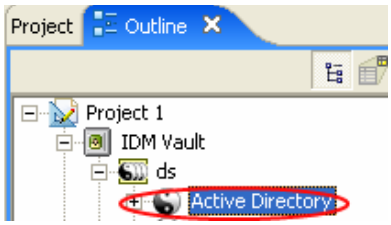
Tabelle 2-1 *Treibersatz-Trace-Parameter*

Parameter	Beschreibung
Treiber-Trace-Stufe	Je höher die Trace-Stufe des Treiberobjekts, desto mehr Informationen werden in DSTRACE angezeigt. Trace-Stufe 1 zeigt Fehler, aber nicht die Ursache für die Fehler an. Wenn Sie Informationen zur Passwortsynchronisierung anzeigen möchten, setzen Sie die Trace-Stufe auf 5.

Parameter	Beschreibung
XSL-Trace-Stufe	DSTRACE zeigt XSL-Ereignisse an. Diese Trace-Stufe wird nur bei der Fehlerbehebung in XSL-Formatvorlagen verwendet. Wenn keine XSL-Informationen angezeigt werden sollen, setzen Sie die Stufe auf 0.
Port für die Java-Fehlersuche	Ermöglicht Entwicklern den Einsatz eines Java-Fehlersuchprogramms (Debugger).
Java-Trace-Datei	Wenn dieses Feld einen Wert enthält, werden alle Java-Informationen für das Treibersatzobjekt in eine Datei geschrieben. Der Wert für dieses Feld ist der Patch für diese Datei. Solange die Datei angegeben wird, werden Java-Informationen in sie geschrieben. Wenn eine Fehlersuche in Java nicht erforderlich ist, lassen Sie dieses Feld leer.
Größenlimit der Trace-Datei	Ermöglicht Ihnen das Festlegen eines Größenlimits für die Java-Trace-Datei. Wenn Sie die Dateigröße auf „Unbegrenzt“ setzen, nimmt die Datei so lange an Größe zu, bis kein Festplattenplatz mehr vorhanden ist.

Treiber

1 Wählen Sie in Designer in einem geöffneten Projekt das Treiberobjekt in der Überblicksansicht aus.



2 Klicken Sie mit der rechten Maustaste, wählen Sie *Properties* (Eigenschaften) und klicken Sie dann auf *8. Trace*.

3 Legen Sie die Parameter für das Tracing fest und klicken Sie auf *OK*. Weitere Informationen zu diesen Parametern finden Sie in Tabelle 2-2 auf Seite 40.

Wenn Sie nur für das Treiberobjekt die Parameter festlegen, werden nur Informationen für diesen Treiber im DSTRACE-Protokoll angezeigt.

Tabelle 2-2 *Treiber-Trace-Parameter*

Parameter	Beschreibung
Trace-Stufe	Je höher die Trace-Stufe des Treiberobjekts, desto mehr Informationen werden in DSTRACE angezeigt. Trace-Stufe 1 zeigt Fehler, aber nicht die Ursache für die Fehler an. Wenn Sie Informationen zur Passwortsynchronisierung anzeigen möchten, setzen Sie die Trace-Stufe auf 5. Wenn Sie *Use setting from Driver Set* (Einstellung aus Treibersatz übernehmen) wählen, wird der Wert aus dem Treibersatzobjekt übernommen.
Trace-Datei	Geben Sie den Namen einer Datei an, in die die Identity Manager-Informationen für den ausgewählten Treiber geschrieben werden. Wenn Sie *Use setting from Driver Set* (Einstellung aus Treibersatz übernehmen) wählen, wird der Wert aus dem Treibersatzobjekt übernommen.
Größenlimit der Trace-Datei	Ermöglicht Ihnen das Festlegen eines Größenlimits für die Java-Trace-Datei. Wenn Sie die Dateigröße auf „Unbegrenzt“ setzen, nimmt die Datei so lange an Größe zu, bis kein Festplattenplatz mehr vorhanden ist. Wenn Sie *Use setting from Driver Set* (Einstellung aus Treibersatz übernehmen) wählen, wird der Wert aus dem Treibersatzobjekt übernommen.
Trace-Name	Anstelle des Treibernamens wird Treiber-Trace-Meldungen der eingegebene Wert vorangestellt. Verwenden Sie diesen Parameter, wenn der Treibername sehr lang ist.

2.12.2 Hinzufügen von Trace-Stufen in iManager

Sie können dem Treibersatzobjekt oder einzelnen Treiberobjekten Trace-Stufen hinzufügen.

Treibersatz

1. Klicken Sie in iManager auf *Identity Manager > Identity Manager-Überblick*.
2. Wählen Sie das gewünschte Treibersatzobjekt aus und klicken Sie auf *Suchen*.

3 Klicken Sie auf den Namen des Treibersatzes.

4 Wählen Sie die Registerkarte *Versch.* für das Treibersatzobjekt.

5 Legen Sie die Parameter für das Tracing fest und klicken Sie auf *OK*. Weitere Informationen zu diesen Parametern finden Sie in Tabelle 2-1 auf Seite 38.

Treiber

1 Wählen Sie in iManager *Identity Manager* > *Identity Manager-Überblick*.

2 Wechseln Sie zu dem Treibersatzobjekt, in dem sich das Treiberobjekt befindet, und klicken Sie auf *Suchen*.

3 Klicken Sie auf die obere rechte Ecke des Treiberobjekts und anschließend auf *Eigenschaften bearbeiten*.

4 Wählen Sie die Registerkarte *Versch.* für das Treiberobjekt.

5 Legen Sie die Parameter für das Tracing fest und klicken Sie auf *OK*. Weitere Informationen finden Sie in Tabelle 2-2 auf Seite 40.

Hinweis: Die Option *Use setting from Driver Set* (Einstellung aus Treibersatz übernehmen) ist in iManager nicht vorhanden.

2.12.3 Erfassen von Identity Manager-Prozessen in einer Datei

Um Identity Manager-Prozesse in einer Datei zu speichern, wird diese über den Parameter im Treiberobjekt oder über DSTRACE gespeichert. Der Parameter im Treiberobjekt ist der Trace-Datei-Parameter.

Mithilfe der folgenden Methoden können Sie Identity Manager-Prozesse über DSTRACE auf verschiedenen Betriebssystemplattformen erfassen und speichern.

NetWare

Verwenden Sie `DSTRACE.NLM` zum Anzeigen von Trace-Meldungen auf der Systemkonsole oder zum Speichern der Meldungen in einer Datei (`SYS:\SYSTEM\DSTRACE.LOG`). `DSTRACE.NLM` zeigt die Trace-Meldungen auf dem Bildschirm „DSTRACE Console“ an.

1 Geben Sie an der Serverkonsole `DSTRACE.NLM` ein.

Dadurch wird `DSTRACE.NLM` in den Arbeitsspeicher geladen.

2 Geben Sie an der Serverkonsole `DSTRACE SCREEN ON` ein.

Ermöglicht, dass Trace-Meldungen auf dem Bildschirm „DSTRACE Console“ angezeigt werden.

3. Geben Sie an der Serverkonsole `DSTRACE FILE ON` ein.

   Erfasst die an „DSTRACE Console“ gesendeten Trace-Meldungen in `DSTRACE.LOG`.

4. Geben Sie an der Serverkonsole `DSTRACE -ALL` ein.

   Dadurch werden alle Trace-Flaggen deaktiviert.

5. Geben Sie an der Serverkonsole `DSTRACE +DXML DSTRACE +DVRS` ein.

   Zeigt die Identity Manager-Ereignisse an.

6. Geben Sie an der Serverkonsole `DSTRACE +TAGS DSTRACE +TIME` ein.

   Zeigt die Tags und Zeitstempel der Meldung an.

7. Wechseln Sie zu „DSTRACE Console“ und achten Sie auf das zu übergebende Ereignis.

8. Wechseln Sie wieder zur Serverkonsole.

9. Geben Sie an der Serverkonsole `DSTRACE FILE OFF` ein.

   Stoppt das Erfassen von Trace-Meldungen in der Protokolldatei. Das Protokollieren von Informationen in der Datei wird dadurch ebenfalls gestoppt.

10. Öffnen Sie die Datei `DSTRACE.LOG` in einem Texteditor und suchen Sie nach dem geänderten Ereignis oder Objekt.

Windows

1. Wählen Sie „Systemsteuerung > NDS Services > dstrace.dlm“ und klicken Sie auf *Starten*.

   Das Fenster „NDS Server Trace Utility“ wird geöffnet.

2. Wählen Sie *Bearbeiten* > *Optionen* und klicken Sie anschließend auf *Alle löschen*.

   Dadurch werden alle Standard-Flaggen gelöscht.

3. Wählen Sie *DirXML* und *DirXML-Treiber*.

4. Klicken Sie auf "OK".

5. Wählen Sie *Datei* > *Neu*.

6. Geben Sie den Dateinamen und den Speicherort an, an dem die DSTRACE-Informationen gespeichert werden sollen, und klicken Sie auf „Öffnen“.

7. Warten Sie, bis das Ereignis auftritt.

8. Wählen Sie *Datei* > *Schließen*.

   Dadurch wird das Schreiben der Informationen in die Protokolldatei gestoppt.

9. Öffnen Sie die Datei in einem Texteditor und suchen Sie nach dem geänderten Ereignis oder Objekt.

UNIX

1. Geben Sie `ndstrace` ein, um das ndstrace-Dienstprogramm zu starten.

2. Geben Sie `set ndstrace=nodebug` ein.

   Dadurch werden alle aktuell gesetzten Trace-Flaggen deaktiviert.

3. Geben Sie `set ndstrace on` ein.

Dadurch werden die Trace-Meldungen an der Konsole angezeigt.

4 Geben Sie `set ndstrace file on` ein.

Dadurch werden alle Trace-Meldungen in der Datei `ndstrace.log` erfasst, die sich in dem Verzeichnis befindet, in dem eDirectory installiert ist. Dies ist standardmäßig `/var/nds`.

5 Geben Sie `set ndstrace=+dxml` ein.

Zeigt die Identity Manager-Ereignisse an.

6 Geben Sie `set ndstrace=+dvrs` ein.

Dadurch werden die Identity Manager-Treiberereignisse angezeigt.

7 Warten Sie, bis das Ereignis auftritt.

8 Geben Sie `set ndstrace file off` ein.

Dadurch wird das Protokollieren der Informationen in der Datei gestoppt.

9 Geben Sie `exit` ein, um das ndstrace-Dienstprogramm zu beenden.

10 Öffnen Sie die Datei in einem Texteditor. Suchen Sie nach dem geänderten Ereignis oder Objekt.

iMonitor

Mit iMonitor können Sie DSTRACE-Informationen über einen Webbrowser abrufen. Dabei spielt es keine Rolle, wo Identity Manager ausgeführt wird. iMonitor wird über die folgenden Dateien ausgeführt:

- `NDSIMON.NLM` - läuft unter NetWare.
- `NDSIMON.DLM` - läuft unter Windows.
- `ndsimonitor` - läuft unter UNIX.

1 Greifen Sie auf iMonitor über „http://*server_ip*:8008/nds“ zu.

Der Standardport ist Port 8008.

2 Geben Sie einen Benutzernamen und ein Passwort mit Administratorrechten ein und klicken Sie auf *Login* (Anmeldung).

3 Wählen Sie auf der linken Seite *Trace Configuration* (Trace-Konfiguration).

4 Klicken Sie auf *Clear all* (Alle löschen).

5 Wählen Sie *DirXML* und *DirXML Drivers* (DirXML-Treiber).

6 Klicken Sie auf *Trace On* (Trace ein).

7 Wählen Sie auf der linken Seite *Trace History* (Trace-Verlauf).

8 Klicken Sie auf das Dokument mit der Änderungszeit „Aktuell“, um einen Live-Trace zu sehen.

9 Ändern Sie das *Aktualisierungsintervall*, wenn die Informationen häufiger angezeigt werden sollen.

10 Wählen Sie *Trace Configuration* (Trace-Konfiguration) auf der linken Seite und klicken Sie auf *Trace Off* (Trace aus), um das Tracing zu deaktivieren.

11 Sie können den Trace-Verlauf anzeigen, indem Sie die Option „Trace History“ (Trace-Verlauf) wählen. Die Dateien werden anhand ihres Zeitstempels unterschieden.

Wenn Sie eine Kopie der HTML-Datei benötigen, finden Sie diese an ihrem Standardspeicherort:

- NetWare: `SYS:\SYSTEM\ndsimon\DSTRACE*.htm`
- Windows: *`Laufwerksbuchstabe_`*`:\Novell\NDS\ndsimon\dstrace\*.htm`
- UNIX: `/var/nds/dstrace/*.htm`

Einrichten eines verbundenen Systems

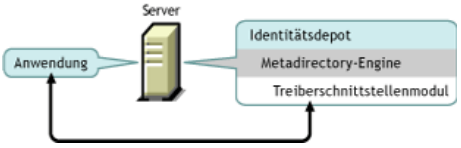
3

Dieser Abschnitt enthält folgende Informationen:

3.1 Überblick

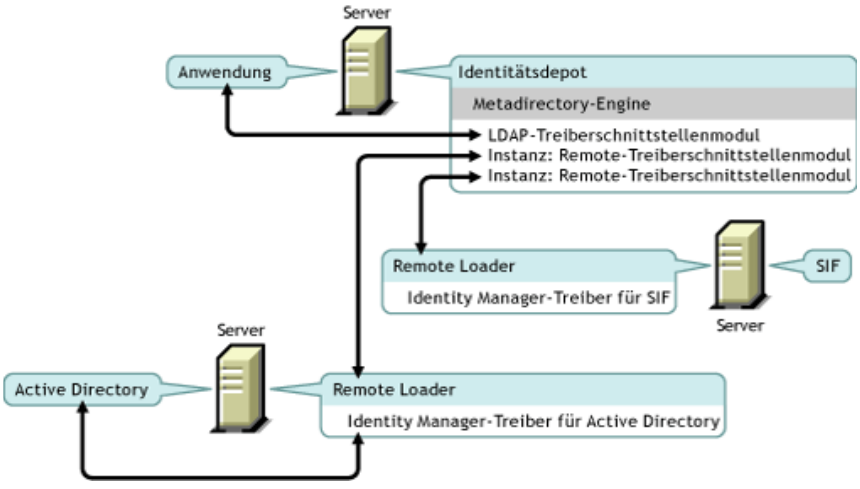
Wie in der folgenden Abbildung dargestellt, wird die Metaverzeichnis-Engine auf einem Server als Teil von eDirectory ausgeführt. Ein Identity Manager-Treiberschnittstellenmodul und seine konfigurierten Treiber kommunizieren mit einer Anwendung und mit der Metaverzeichnis-Engine.

Abbildung 3-1 *Die unter eDirectory ausgeführte Metaverzeichnis-Engine*



Wie in der folgenden Abbildung dargestellt, wird die Identity Manager-Funktionalität über ein verbundenes System anwendungsübergreifend erweitert:

Abbildung 3-2 *Verbundenes System mit dem Remote Loader*



Ein verbundenes System erfordert einen Remote Loader. Dieser Dienst ermöglicht es der Metaverzeichnis-Engine, Daten mit Identity Manager-Treibern auszutauschen, die als unterschiedliche Prozesse und an unterschiedlichen Stellen ausgeführt werden:

- Als separate Prozesse auf dem Server, auf dem die Metaverzeichnis-Engine ausgeführt wird

  Die Metaverzeichnis-Engine wird als Teil des eDirectory-Prozesses ausgeführt. Die Identity Manager-Treiber können auf dem Server ausgeführt werden, auf dem die Metaverzeichnis-Engine läuft. Sie können sogar Teil desselben Prozesses sein, in dem die Metaverzeichnis-Engine ausgeführt wird.

  Aus strategischen Gründen sollten die Identity Manager-Treiber als separater Prozess auf dem Server ausgeführt werden. Die Identity Manager-Treiber werden in der Regel jedoch auf separaten Servern ausgeführt.

  Wenn der Treiber als separater Prozess ausgeführt wird, stellt der Remote Loader einen Kommunikationskanal zwischen der Metaverzeichnis-Engine und dem Treiber zur Verfügung.

- Auf Servern, bei denen es sich nicht um den Server handelt, auf dem die Metaverzeichnis-Engine ausgeführt wird

  Einige der Identity Manager-Treiber können nicht ausgeführt werden, wenn die Metaverzeichnis-Engine läuft. Mithilfe des Remote Loader können Sie die Metaverzeichnis-Engine in einer Umgebung und einen Identity Manager-Treiber auf einem Server in einer anderen Umgebung ausführen. Es ist beispielsweise nicht möglich, den Active Directory-Treiber auf einem NetWare-Server auszuführen. Die Metaverzeichnis-Engine kann auf dem NetWare-Server und der Remote Loader auf einem Active Directory-Server ausgeführt werden.

  Szenario: Separate Server. Die Metaverzeichnis-Engine wird auf einem NetWare-Server ausgeführt. Der Identity Manager-Treiber für Active Directory muss ebenfalls ausgeführt werden. Dieser Treiber kann jedoch nicht auf einem NetWare-Server, sondern muss in einer Active Directory-Umgebung ausgeführt werden. Sie installieren und führen den Remote Loader auf einem Windows 2003-Server aus. Der Remote Loader bietet einen Kommunikationskanal zwischen dem Active Directory-Treiber und der Metaverzeichnis-Engine.

  Szenario: Nicht-Host. Die Metaverzeichnis-Engine läuft unter Solaris. Es muss eine Kommunikationsverbindung zum NIS-System bestehen, auf dem Sie Benutzerkonten bereitstellen möchten. Die Metaverzeichnis-Engine wird in der Regel nicht vom System gehostet. Der Remote Loader und der Identity Manager-Treiber für NIS werden auf dem NIS-System installiert. Der auf dem NIS-System installierte Remote Loader führt den NIS-Treiber aus und ermöglicht den Datenaustausch zwischen der Metaverzeichnis-Engine und dem NIS-Treiber.

Identity Manager 3 stellt die Remote Loader-Funktionalität über dirxml_remote, rdxml oder dirxml_jremote bereit.

Dirxml_remote

Dirxml_remote ist eine Programmdatei, die die Kommunikation der Metaverzeichnis-Engine mit dem unter Windows ausgeführten Identity Manager-Treiber ermöglicht.

Die Remote Loader-Konsole verwendet `dirxml_remote.exe`. Wenn Sie `dirxml_remote.exe` ohne weitere Parameter von der Befehlszeile aus starten, wird der Anwendungsassistent des Remote Loader gestartet. Wenn Sie `dirxml_remote.exe` mit weiteren Parameter angeben, wird der Remote Loader gestartet.

Rdxml

Rdxml ist eine Programmdatei, die die Kommunikation der Metaverzeichnis-Engine mit den unter Solaris, Linux oder AIX-Umgebungen ausgeführten Identity Manager-Treibern ermöglicht.

Rdxml unterstützt native Treiber und Java-Treiber.

Dirxml_jremote

Dirxml_jremote ist ein reiner Java-Remote-Loader. Er wird zum Datenaustausch zwischen der auf dem Server aktiven Metaverzeichnis-Engine und den Identity Manager-Treibern verwendet, die an einem anderen Standort ausgeführt werden, auf dem rdxml oder Dirxml_jremote nicht aktiviert ist. Er sollte auf jedem System mit einer kompatiblen JRE (1.4.0 Minimum, 1.4.2 oder höher empfohlen) und Java Sockets ausgeführt werden können, wird offiziell jedoch nur von den folgenden Systemen unterstützt:

- HP-UX
- AS/400
- OS/390
- z/OS

Überblick: Wichtigste Aufgaben

Für die Arbeit mit dem Remote Loader müssen Sie die folgenden Aufgaben ausführen:

- Wenn Sie SSL (Secure Socket Layer) verwenden möchten, stellen Sie Zertifikate für eine sichere Datenübertragung bereit.
- Den Remote Loader installieren, konfigurieren und ausführen.
- Den Identity Manager-Treiber importieren, konfigurieren und starten.

Einige Administratoren ziehen es vor, den Identity Manager-Treiber vor dem Einrichten des Remote Loader zu importieren und zu konfigurieren. Dies kann sinnvoll sein, wenn der Treiber bereits läuft, Sie ihn jedoch remote ausführen möchten.

Auf der anderen Seite können Sie bei aktiviertem Remote Loader den Treiber importieren, konfigurieren und starten und anschließend sofort überprüfen, ob die Kommunikation zwischen der Metaverzeichnis-Engine, dem Remote Loader und dem Identity Manager-Treiber ordnungsgemäß ausgeführt wird.

3.2 Sichere Datentransfers

Wenn Sie SSL (Secure Socket Layer) zum Bereistellen eines sicheren Datentransfers verwenden möchten, führen Sie die folgenden Schritte aus:

1. Erstellen Sie ein Serverzertifikat.

   Wenn Sie mit der Verwendung von Zertifikaten nicht vertraut sind, erstellen Sie ein neues Zertifikat.

   Wenn bereits ein SSL-Serverzertifikat vorhanden ist und Sie sich mit SSL-Zertifikaten auskennen, können Sie dieses verwenden und müssen kein neues Zertifikat erstellen.

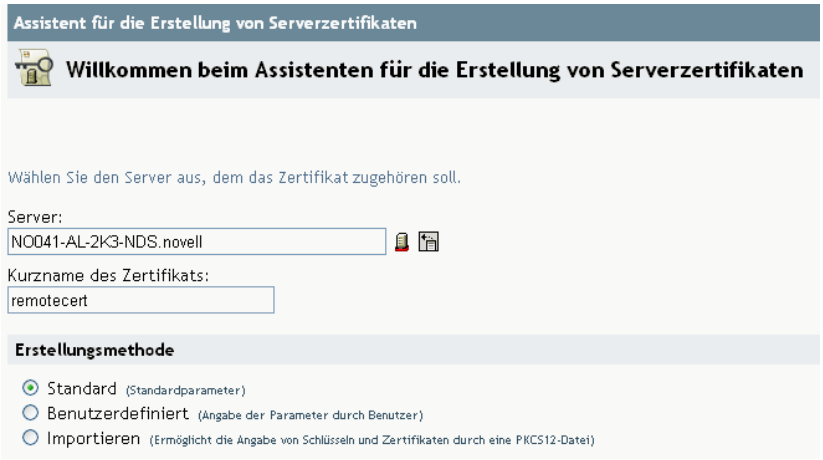
Wenn ein Server mit einer Baumstruktur verknüpft wird, erstellt eDirectory die folgenden Standardzertifikate:

- SSL CertificateIP
- SSL CertificateDNS

2. Exportieren Sie das selbstsignierte Zertifikat.

3.2.1 Serverzertifikat erstellen

1 Klicken Sie in Novell iManager auf *Novell Certificate Server* > *Create Server Certificate* (Serverzertifikat erstellen).



2 Wählen Sie den Server aus, der Eigentümer des Zertifikats sein soll, und geben Sie dem Zertifikat einen Kurznamen (z. B. remotecert).

Wichtig: Vermeiden Sie die Verwendung von Leerzeichen in den Kurznamen der Zertifikate. Beispiel: Verwenden Sie „remotecert“ anstatt „remote cert“.

Notieren Sie sich außerdem den Kurznamen des Zertifikats. Sie benötigen diesen Kurznamen für den KMO-Namen in den Remote-Verbindungsparametern des Treibers.

---

3 Behalten Sie die Erstellungsmethode *Standard* bei und klicken Sie anschließend auf *Weiter*.

4 Überprüfen Sie die Zusammenfassung, klicken Sie auf *Fertig stellen* und anschließend auf *Schließen*.

Das Serverzertifikat wurde erstellt. Fahren Sie fort mit Abschnitt 3.2.2, „Selbstsigniertes Zertifikat exportieren“, auf Seite 48.

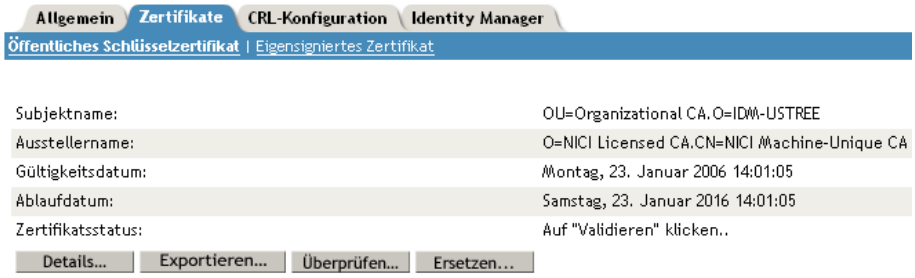
3.2.2 Selbstsigniertes Zertifikat exportieren

1 Klicken Sie in iManager auf *eDirectory-Administration* > *Objekt bearbeiten*.

2 Wechseln Sie zur Zertifizierungsstelle im Sicherheitscontainer, wählen Sie sie aus und klicken Sie anschließend auf *OK*.

Die Zertifizierungsstelle (CA) ist nach dem Baumnamen (Treename-CA.Security) benannt.

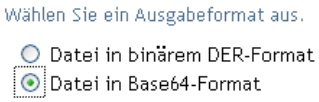
3 Klicken Sie auf die Registerkarte *Zertifikate*, wählen Sie *Eigensigniertes Zertifikat* und klicken Sie anschließend auf *Exportieren*.



4 Wählen Sie im Assistenten zum Exportieren von Zertifikaten *Nein* und klicken Sie anschließend auf *Weiter*.

Der private Schlüssel soll nicht mit dem Zertifikat exportiert werden.

5 Wählen Sie *Datei in Base64-Format*, z. B. akranes-tree CA.b64, und klicken Sie anschließend auf *Weiter*.



6 Klicken Sie auf die Verknüpfung *Save the exported certificate to a file* (Exportiertes Zertifikat als Datei speichern), geben Sie einen Dateinamen und einen Speicherort an und klicken Sie anschließend auf *Speichern*.

Namen von Root-Dateien müssen die Erweiterung .pem erhalten.

7 Kopieren Sie diese Datei im Dialogfeld „Speichern unter“ in ein lokales Verzeichnis.

8 Klicken Sie auf *Schließen*.

3.3 Einrichten von Remote Loadern

Dieser Abschnitt enthält folgende Informationen:

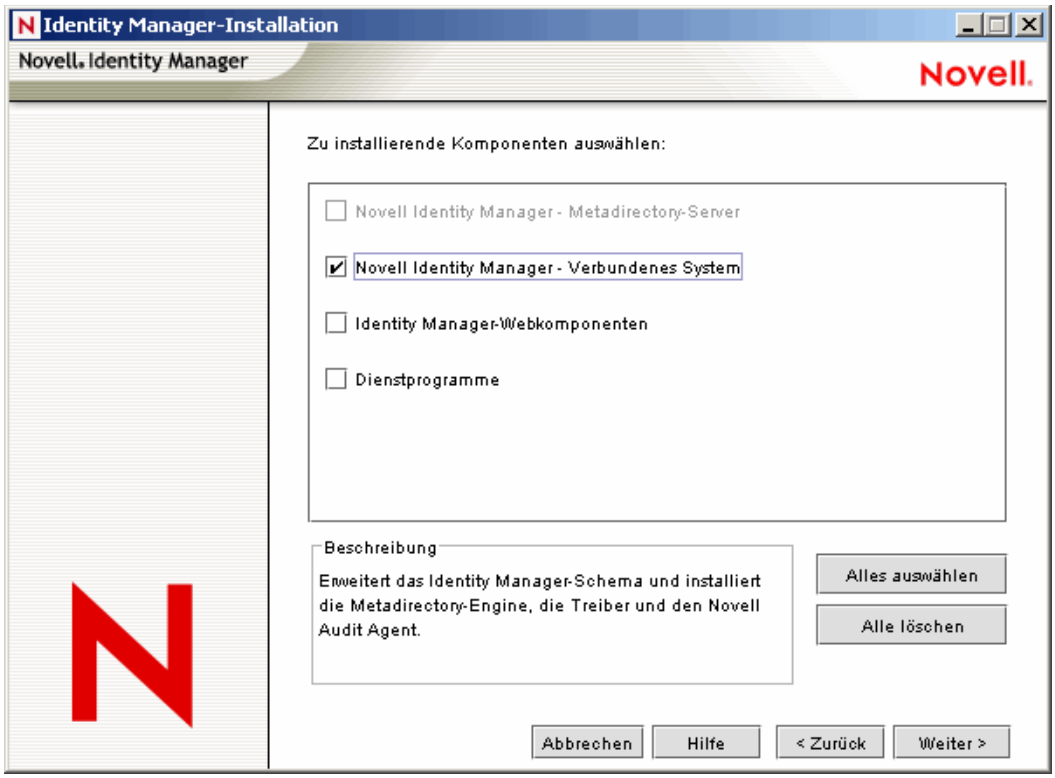
3.3.1 Installieren von Remote Loadern

Dieser Abschnitt enthält folgende Informationen:

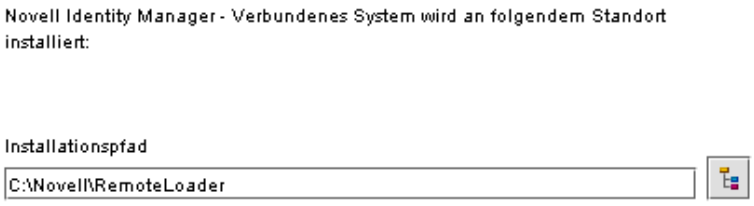
- „Remote Loader auf einem Windows-Server installieren“ auf Seite 50
- „Remote Loader unter Solaris, Linux oder AIX installieren“ auf Seite 51
- „Remote Loader unter HP-UX, AS/400, OS/390 oder z/OS installieren“ auf Seite 52

Remote Loader auf einem Windows-Server installieren

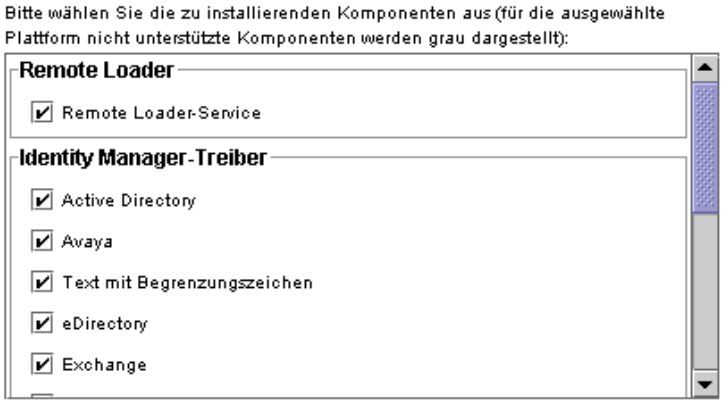
1. Starten Sie das Installationsprogramm von Identity Manager 3 (z. B. \nt\install.exe).
2. Öffnen Sie die Seite „Willkommen“, nehmen Sie die Bedingungen der Lizenzvereinbarung an und zeigen Sie die beiden Überblickseiten an.
3. Deaktivieren Sie im Dialogfeld „Identity Manager-Installation“ alle Komponenten mit Ausnahme von *Verbundenes System* und klicken Sie anschließend auf *Weiter*.



4. Wählen Sie einen Speicherort für das verbundene System aus (Remote Loader- und Remote-Treiberschnittstellenmodule) und klicken Sie auf *Weiter*.



5 Wählen Sie den *Remote Loader-Service* und die Remote-Treiberschnittstellenmodule (Treiber) aus und klicken Sie anschließend auf *Weiter*.



6 Bestätigen Sie die Aktivierungsanforderung, zeigen Sie die zu installierenden Produkte an und klicken Sie anschließend auf *Fertig stellen*.

7 Legen Sie fest, ob Sie das Symbol „Remote Loader-Konsole“ auf Ihrem Desktop platzieren möchten.

Remote Loader unter Solaris, Linux oder AIX installieren

In diesem Abschnitt wird davon ausgegangen, dass Sie Identity Manager 3 bereits heruntergeladen und dekomprimiert haben. Wenn Sie Identity Manager noch herunterladen müssen, wechseln Sie zur Download-Website von Novell (http://download.novell.com).

Führen Sie nach dem Dekomprimieren der von der Novell-Website heruntergeladenen Identity Manager 3-Datei die folgenden Schritte aus:

1 Führen Sie die Ihrer Plattform entsprechende Installationsdatei aus:

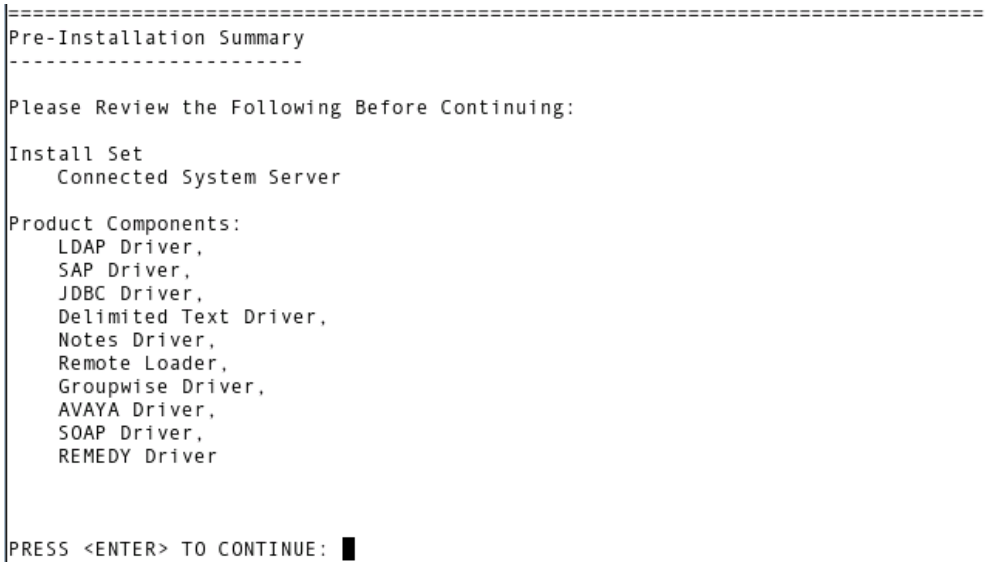
- dirxml_solaris.bin
- dirxml_linux.bin
- dirxml_aix.bin

2 Drücken Sie nach dem Akzeptieren der Lizenzvereinbarung die Eingabetaste. Die Seite „Installationssatz wählen“ wird angezeigt:

```
===============================================================================
Choose Install Set
------------------

Please choose the Install Set to be installed by this installer.

  ->1- Metadirectory Server
    2- Connected System Server
    3- Web-based Administrative Server

    4- Customize...

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
   :
```

3 Geben Sie zum Auswählen des verbundenen System-Servers „2“ ein und drücken Sie die Eingabetaste.

4 Überprüfen Sie im Bildschirm „Übersicht vor der Installation“ die Komponenten, die Sie für die Installation ausgewählt haben, und drücken Sie anschließend die Eingabetaste.



Remote Loader unter HP-UX, AS/400, OS/390 oder z/OS installieren

Für die Plattformen HP-UX, AS/400, OS/390 und z/OS ist ein Java Remote Loader erforderlich.

1 Erstellen Sie ein Verzeichnis auf dem Zielsystem, auf dem der Java Remote Loader ausgeführt werden soll.

2 Kopieren Sie die entsprechende Datei aus dem Verzeichnis `/java_remoteloader` auf der Identity Manager 3-CD oder im heruntergeladenen Image in das in Schritt 1 erstellte Verzeichnis:

Plattform	Datei
HP-UX AS/400 z/OS OS/390	dirxml_jremote.tar.gz dirxml_jremote.tar.gz dirxml_jremote_mvs.tar dirxml_jremote_mvs.tar

3 Wenn Sie HP-UX, AS/400 oder z/OS verwenden, dekomprimieren Sie die Datei dirxml_jremote.

4 Dekomprimieren Sie die gerade kopierte Datei.

Der Java Remote Loader kann nun konfiguriert werden. Da die tar-Datei keine Treiber enthält, müssen Sie die Treiber manuell in das lib-Verzeichnis kopieren. Das lib-Verzeichnis befindet sich in dem von Ihnen zuvor dekomprimierten Verzeichnis.

Informationen zu MVS finden Sie, indem Sie die Datei dirxml_jremote_mvs.tar dekomprimieren. Lesen Sie anschließend das Dokument „usage.html“.

3.3.2 Konfigurieren des Remote Loader

Der Remote Loader kann die in den .DLL-, .SO- oder .JAR-Dateien enthaltenen Identity Manager-Anwendungsschnittstellenmodule hosten. Der Java Remote Loader hostet nur Java-Treiberschnittstellenmodule. Das Laden oder Hosten nativer (C++) Treiberschnittstellenmodule ist nicht möglich.

- „Konfigurieren des Remote Loader unter Windows“ auf Seite 53
- „Konfigurieren des Remote Loader mithilfe von Befehlszeilenoptionen“ auf Seite 58
- „Starten des Remote Loader“ auf Seite 64
- „Stoppen des Remote Loader“ auf Seite 67

Konfigurieren des Remote Loader unter Windows

- „Verwenden des Remote Loader-Konsolendienstprogramms“ auf Seite 53
- „Hinzufügen einer Remote Loader-Instanz“ auf Seite 54
- „Remote Loader-Instanz bearbeiten“ auf Seite 58

Verwenden des Remote Loader-Konsolendienstprogramms

Die Remote Loader-Konsole kann nur unter Windows ausgeführt werden. Über die Konsole können Sie alle Identity Manager-Treiber verwalten, die unter dem Remote Loader auf dem Computer ausgeführt werden:

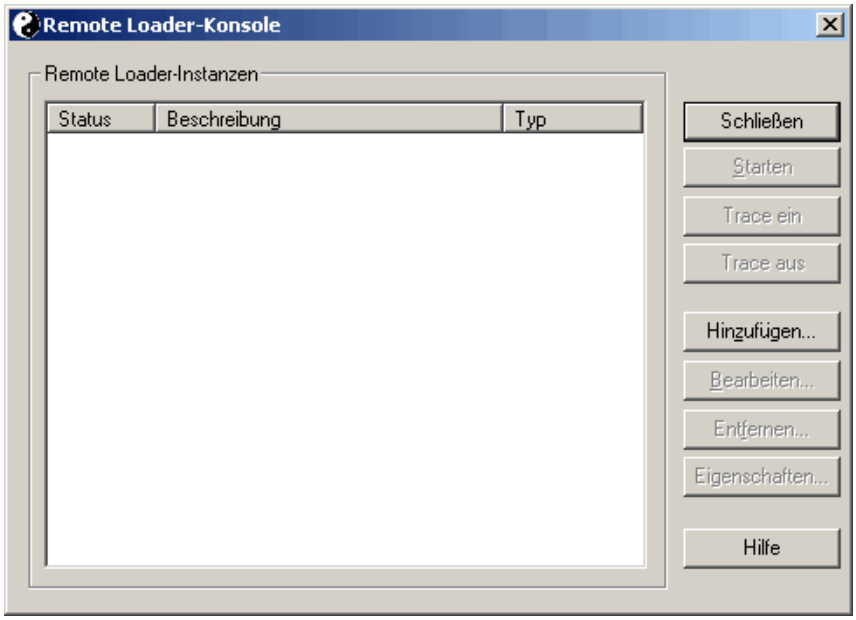
Wenn Sie ein Upgrade auf Identity Manager 3 vornehmen, erkennt und importiert die Konsole vorhandene Instanzen des Remote Loader. (Damit die Treiberkonfiguration automatisch importiert werden kann, müssen Sie sie im Remote Loader-Verzeichnis speichern, üblicherweise ist dies `c:\novell\remoteloader`.) Anschließend können Sie die Remote-Treiber über die Konsole verwalten.

Klicken Sie zum Starten der Remote Loader-Konsole auf das Symbol „Remote Loader-Konsole“ auf Ihrem Desktop.

Abbildung 3-3 *Symbol „Remote Loader-Konsole“*

Über die Remote Loader-Konsole können Sie die Instanzen eines Remote Loader-Service starten, stoppen, hinzufügen, entfernen und bearbeiten.

Abbildung 3-4 *Die Remote Loader-Konsole*



Wenn Sie `dirxml_remote.exe` an der Befehlszeile ohne weitere Parameter eingeben, wird der Anwendungsassistent des Remote Loader gestartet.

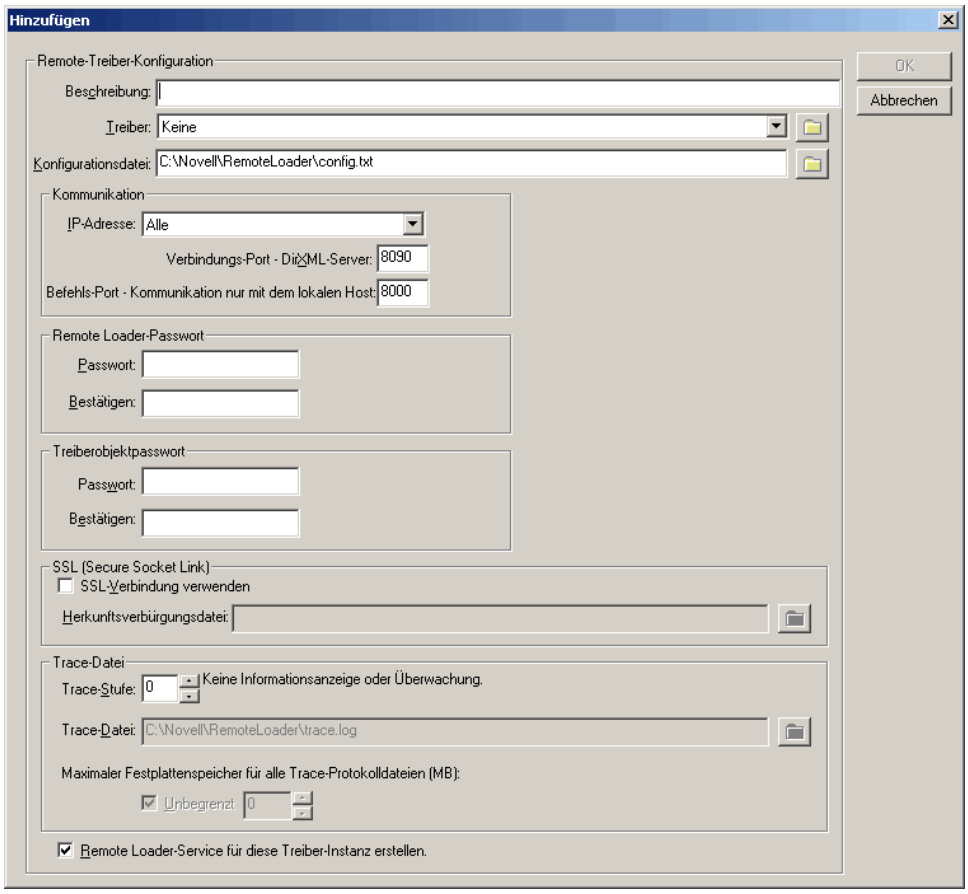
Hinweis: Wenn Sie den Assistenten und die Konsole zusammen verwenden, kann dies zu Fehlern führen. Es wird daher empfohlen, dass Sie in Zukunft die Remote Loader-Konsole verwenden und Ihre vorhandenen Konfigurationen in die Konsole integrieren.

Hinzufügen einer Remote Loader-Instanz

Klicken Sie zum Hinzufügen einer Remote Loader-Instanz auf „Hinzufügen“ und geben Sie anschließend die folgenden Informationen ein:

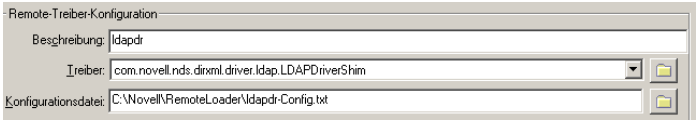
- „Remote-Treiber-Konfiguration“ auf Seite 55
- „Kommunikationsparameter“ auf Seite 56
- „Remote Loader-Passwort“ auf Seite 56
- „Treiberobjektpasswort“ auf Seite 57
- „SSL-Link (Secure Socket Layer)“ auf Seite 57
- „Trace-Datei“ auf Seite 57
- „Erstellen eines Remote Loader-Services für diese Treiber-Instanz“ auf Seite 58

Abbildung 3-5 *Konfigurationsparameter für Remote Loader*



Remote-Treiber-Konfiguration

Abbildung 3-6 *Remote-Treiber-Konfiguration*

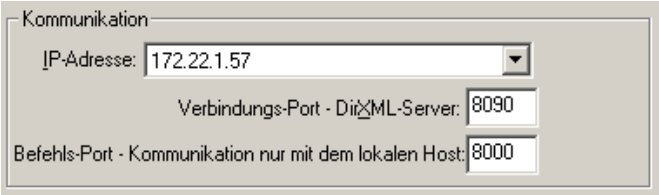


- Beschreibung: Geben Sie eine Beschreibung für die Remote Loader-Instanz ein.
- Treiber: Wählen Sie das entsprechende Schnittstellenmodul für den Treiber aus.
- Konfigurationsdatei: Geben Sie einen Namen für die Konfigurationsdatei ein.

  Die Remote Loader-Konsole fügt die Konfigurationsparameter in diese Textdatei ein und verwendet sie bei der Ausführung.

Kommunikationsparameter

Abbildung 3-7 *Kommunikationsparameter*



- IP-Adresse: Geben Sie die IP-Adresse an, die der Remote Loader auf Verbindungen vom Metaverzeichnis-Server überwacht.
- Verbindungs-Port - Metaverzeichnis-Server. Geben Sie den TCP-Port an, den der Remote Loader auf Verbindungen vom Metaverzeichnis-Server überwacht.

  Der TCP/IP-Standardport für diese Verbindung ist 8090. Die Portnummer erhöht sich bei jeder neu erstellten Instanz automatisch um 1.
- Befehls-Port - Kommunikation nur mit dem lokalen Host: Geben Sie die Nummer des TCP-Ports an, den ein Remote Loader-Service auf Befehle wie „Stop“ und „Change Trace Level“ überwacht.

  Jede Instanz des Remote Loader, die auf einem bestimmten Computer ausgeführt wird, muss eine andere Befehls-Portnummer haben. Der Standard-Befehls-Port für diese Verbindung ist 8000. Die Standard-Portnummer erhöht sich bei jeder neu erstellten Instanz automatisch um 1.

Hinweis: Sie können mehrere Instanzen des Remote Loader auf demselben Server ausführen, der unterschiedliche Treiberinstanzen hostet, indem Sie unterschiedliche Verbindungs- und Befehls-Ports angeben.

Remote Loader-Passwort

Abbildung 3-8 *Remote Loader-Passwort*

- Passwort: Dieses Passwort wird zum Steuern des Zugriffs auf eine Remote Loader-Instanz für einen Treiber verwendet.

  Hierbei muss es sich um dasselbe Passwort (Groß-/Kleinschreibung wird berücksichtigt) handeln, das Sie bei der Konfiguration des Treibers im Feld „Remote Loader-Passwort eingeben“ im Authentifizierungabschnitt auf der Seite für die Identity Manager-Konfiguration angegeben haben.
- Bestätigen: Geben Sie das Passwort erneut ein.

Treiberobjektpasswort

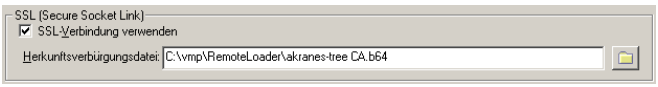
Abbildung 3-9 *Treiberobjektpasswort*

- Passwort: Der Remote Loader verwendet dieses Passwort für die Authentifizierung beim Metaverzeichnis-Server.

  Hierbei muss es sich um dasselbe Passwort handeln, das Sie bei der Konfiguration des Treibers im Feld „Treiberobjektpasswort“ auf der Treiberkonfigurationsseite angegeben haben.
- Bestätigen: Geben Sie das Passwort erneut ein.

SSL-Link (Secure Socket Layer)

Abbildung 3-10 *SSL-Link (Secure Socket Layer)*

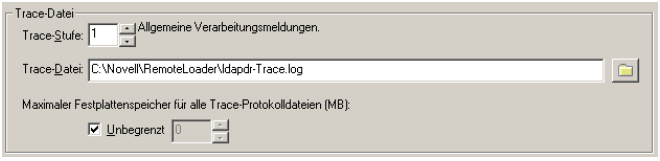


- SSL-Verbindung verwenden: Wählen Sie diese Option zum Angeben einer SSL-Verbindung.
- Herkunftsverbürgungsdatei: Wählen Sie eine Herkunftsverbürgungsdatei aus.

  Dies ist das exportierte selbssignierte Zertifikat aus der Organisationszertifizierungsstelle des eDirectory-Baums. Weitere Informationen hierzu finden Sie unter Abschnitt 3.2.2, „Selbstsigniertes Zertifikat exportieren“, auf Seite 48.

Trace-Datei

Abbildung 3-11 *Trace-Datei*



- Trace-Stufe: Damit die Remote Loader-Instanz ein Trace-Fenster einblendet, das Info-Meldungen sowohl vom Remote Loader als auch vom Treiber enthält, legen Sie die Trace-Stufe größer Null fest. Die gebräuchlichste Einstellung ist Trace-Stufe 3.

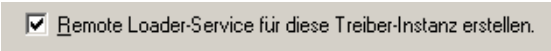
  Wenn Trace-Stufe 0 festgelegt ist, werden im Trace-Fenster keine Meldungen angezeigt.
- Trace-Datei: Geben Sie den Namen einer Trace-Datei an, in die die Trace-Meldungen geschrieben werden sollen.

  Jede Instanz des Remote Loader, die auf einem bestimmten Computer ausgeführt wird, muss eine andere Trace-Datei verwenden. Trace-Meldungen werden nur dann in die Trace-Datei geschrieben, wenn die Trace-Stufe größer Null ist.

- Maximaler Festplattenspeicher für alle Trace-Protokolldateien (MB): Geben Sie die ungefähre Größe der Trace-Datei an, die die Daten für diese Instanz auf der Festplatte belegen dürfen.

Erstellen eines Remote Loader-Services für diese Treiber-Instanz

Abbildung 3-12 *Remote Loader-Service für diese Treiber-Instanz erstellen*



- Wählen Sie diese Option, um die Remote Loader-Instanz als Service zu konfigurieren. Wenn die Option aktiviert ist, wird der Remote Loader beim Computerstart automatisch vom Betriebssystem gestartet.

Remote Loader-Instanz bearbeiten

1. Wählen Sie die Remote Loader-Instanz in der Spalte „Beschreibung“ aus.
2. Klicken Sie auf *Stoppen*, geben Sie das Remote Loader-Passwort ein und klicken Sie anschließend auf *OK*.
3. Klicken Sie auf *Bearbeiten* und bearbeiten Sie die Konfigurationsinformationen. Dieselben Felder werden auch zum Hinzufügen einer Remote Loader-Instanz verwendet.

Konfigurieren des Remote Loader mithilfe von Befehlszeilenoptionen

Zum Ausführen des Remote Loader wird auf allen Plattformen eine Konfigurationsdatei (z. B. LDAPShim.txt) verwendet. Konfigurationsdateien können mithilfe von Befehlszeilenoptionen erstellt und bearbeitet werden. In den folgenden Schritten finden Sie Informationen zu den grundlegenden Parametern der Konfigurationsdateien. Informationen zu zusätzlichen Parametern finden Sie unter Anhang B, „Konfigurationsoptionen für einen Remote Loader“, auf Seite 279.

1. Öffnen Sie einen Texteditor.
2. (Optional) Geben Sie mithilfe der Option -description eine Beschreibung an.

Option	Kurzform	Parameter	Beschreibung
-description	-desc	Kurzbeschrei-bung	Gibt eine kurze Beschreibungszeichenkette (z. B. SAP) an, die für den Titel des Trace-Fensters und für die Nsure Audit-Protokollierung verwendet wird. Beispiel: -description SAP -desc SAP Die Remote Loader-Konsole schreibt lange Formen in die Konfigurationsdateien. Sie können entweder eine lange Form (z. B. -description) oder eine kurze Form (z. B. -desc) verwenden.

3. Geben Sie mithilfe der Option -commandport den von der Remote Loader-Instanz verwendeten TCP/IP-Port an.

Option	Kurzform	Parameter	Beschreibung
-command-port	-cp	Portnummer	Gibt den TCP/IP-Port an, der von der Remote Loader-Instanz zu Steuerungszwecken verwendet wird. Wenn die Remote Loader-Instanz ein Anwendungsschnittstellenmodul hostet, ist der Befehls-Port der Port, über den eine andere Remote Loader-Instanz mit der Instanz kommuniziert, die das Schnittstellenmodul hostet. Wenn die Remote Loader-Instanz einen Befehl an eine Instanz sendet, die ein Anwendungsschnittstellenmodul hostet, ist der Befehls-Port der Port, der von der Host-Instanz überwacht wird. Wenn kein Port angegeben ist, wird standardmäßig Befehls-Port 8000 verwendet. Durch die Angabe unterschiedlicher Verbindungs- und Befehls-Ports können auf dem Server, auf dem unterschiedliche Treiberinstanzen gehostet werden, mehrere Instanzen des Remote Loader ausgeführt werden. Beispiel: -commandport 8001 -cp 8001

4 Geben Sie mithilfe der Option -connection die Parameter für die Verbindung zum Metaverzeichnis-Server an, auf dem das Identity Manager-Remote-Schnittstellenmodul ausgeführt wird.

Geben Sie -connection "*parameter* [parameter] [parameter]" ein.

Geben Sie beispielsweise Folgendes ein:

```
-connection "port=8091 rootfile=server1.pem"
-conn "port=8091 rootfile=server1.pem"
```

Alle Parameter müssen in Anführungszeichen gesetzt werden. Die folgenden Parameter sind verfügbar:

Option	Kurzform	Parameter	Beschreibung
-connection	-conn	Zeichenkette für die Verbindungskonfiguration	Gibt die Verbindungsparameter für die Verbindung zum Metaverzeichnis-Server an, auf dem das Identity Manager-Remote-Schnittstellenmodul ausgeführt wird. Die Standardverbindungsmethode für den Remote Loader ist TCP/IP mit SSL. Der TCP/IP-Standardport für diese Verbindung ist 8090. Es können mehrere Instanzen des Remote Loader auf demselben Server ausgeführt werden. Jede Instanz des Remote Loader hostet eine separate Anwendungsschnittstellenmodulinstanz des Identity Manager. Sie unterscheiden mehrere Instanzen des Remote Loader voneinander, indem Sie für jede Remote Loader-Instanz unterschiedliche Verbindungs- und Befehls-Ports angeben. Beispiel: -connection "port=8091 rootfile=server1.pem" -conn "port=8091 rootfile=server1.pem"
port		Dezimale Portnummer	Ein obligatorischer Parameter. Er gibt den TCP/IP-Port an, den der Remote Loader auf Verbindungen vom Remote-Schnittstellenmodul überwacht. Beispiel: port=8090
address		IP-Adresse	Dieser Parameter ist optional. Er gibt an, dass der Remote Loader eine bestimmte lokale IP-Adresse überwacht. Dies ist hilfreich, wenn der Server, der den Remote Loader hostet, mehrere IP-Adressen hat und der Remote Loader nur eine dieser Adressen überwachen soll. Die folgenden drei Optionen sind verfügbar: address=*Adressnummer* address='localhost' Verwenden Sie diesen Parameter nicht. Wenn Sie den Parameter -address nicht verwenden, überwacht der Remote Loader alle lokalen IP-Adressen. Beispiel: address=137.65.134.83
rootfile			Ein bedingter Parameter. Wenn Sie SSL ausführen und den Remote Loader für die Kommunikation mit einem nativen Treiber benötigen, geben Sie Folgendes ein: `rootfile='trusted certname'`

Option	Kurzform	Parameter	Beschreibung
Keystore			Bedingte Parameter. Wird nur für Identity Manager-Anwendungsschnittstellenmodule in .JAR-Dateien verwendet. Gibt den Dateinamen des Java-Keystores an, der das Herkunftsverbürgungszertifikat des Herausgebers des Zertifikats enthält, das vom Remote-Schnittstellenmodul verwendet wird. Dies ist in der Regel die Zertifizierungsstelle des eDirectory-Baums, der das Remote-Schnittstellenmodul hostet. Wenn Sie SSL ausführen und den Remote Loader für die Kommunikation mit einem Java-Treiber benötigen, geben Sie ein Schlüssel/Wert-Paar ein: `keystore='keystorename' storepass='password'`
-storepass		Keystore-Passwort	Wird nur für Identity Manager-Anwendungsschnittstellenmodule in .JAR-Dateien verwendet. Gibt das Passwort für den Java-Keystore an, der im Parameter „keystore“ festgelegt ist. Beispiel: storepass=MeinPasswort Diese Option gilt nur für den Java Remote Loader.

5 (Optional) Geben Sie einen Trace-Parameter mithilfe der Option -trace an.

Option	Kurzform	Parameter	Beschreibung
-trace	-t	Ganzzahl	Gibt die Trace-Stufe an. Diese Option wird nur beim Hosten eines Anwendungsschnittstellenmoduls verwendet. Die Trace-Stufen entsprechen den auf dem Metaverzeichnis-Server verwendeten Trace-Stufen. Beispiel: -trace 3 -t 3

6 (Optional) Geben Sie eine Trace-Datei mithilfe der Option -tracefile an.

Option	Kurzform	Parameter	Beschreibung
-tracefile	-tf	Dateiname	Gibt eine Datei an, in die die Trace-Meldungen geschrieben werden sollen. Trace-Meldungen werden in die Datei geschrieben, wenn die Trace-Stufe größer als Null ist. Trace-Meldungen werden auch bei geschlossenem Trace-Fenster in die Datei geschrieben. Beispiel: -tracefile c:\temp\trace.txt -tf c:\temp\trace.txt

7 (Optional) Beschränken Sie die Größe der Trace-Datei mithilfe der Option -tracefilemax. Geben Sie beispielsweise Folgendes ein:

```
-tracefilemax 1000M
-tfm 1000M
```

In diesem Beispiel darf die Trace-Datei nicht größer als 1 GB sein.

Option	Kurzform	Parameter	Beschreibung
-tracefilemax	-tfm	Größe	Gibt die Maximalgröße an, die die Trace-Datei auf der Festplatte belegen darf. Bei Angabe dieser Option wird die Trace-Datei mit dem Namen verwendet, der mit der Option „tracefile“ angegeben wurde, sowie bis zu neun zusätzliche „roll-over“-Dateien. Die Rollover-Dateien werden benannt, indem an den Namen der Haupt-Trace-Datei „_*n*“ angehängt wird, wobei 1 bis 9 gültige Werte für n sind. Der Parameter für die Größe gibt die Anzahl der Byte an. Geben Sie die Größe mithilfe der Erweiterungen K, M oder G für Kilobyte, Megabyte oder Gigabyte an. Wenn die Trace-Datei beim Starten des Remote Loader größer als das angegebene Maximum ist, dann behält die Trace-Datei diese Größe bei, bis das Rollover über alle 10 Dateien ausgeführt wurde. Beispiel: -tracefilemax 1000M -tfm 1000M In diesem Beispiel darf die Trace-Datei nicht größer als 1 GB sein.

8 Geben Sie die Klasse mit der Option -class oder das Modul mit der Option -module an.

Option	Kurzform	Parameter	Beschreibung
-class	-cl	Java-Klassen-name	Gibt den Java-Klassennamen des zu hostenden Identity Manager-Anwendungsschnittstellenmoduls an. Einen Java-Treiber können Sie beispielsweise mit einer der folgenden Optionen angeben: -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim Java verwendet zum Lesen von Zertifikaten einen Keystore. Die Optionen „-class“ und „-module“ schließen sich gegenseitig aus. Eine Liste der Java-Klassennamen finden Sie in Tabelle B-2 auf Seite 286 in Anhang B, „Konfigurationsoptionen für einen Remote Loader“, auf Seite 279.
-module	-m	Modulname	Gibt das Modul an, in dem das zu hostende Identity Manager-Anwendungsschnittstellenmodul enthalten ist. Bei einem nativen Treiber können Sie beispielsweise eine der folgenden Optionen angeben: -module "c:\Novell\Remote-Loader\Exchange5Shim.dll" -m "c:\Novell\Remote-Loader\Exchange5Shim.dll" oder: -module "usr/lib/dirxml/NISDriverShim.so" -m "usr/lib/dirxml/NISDriverShim.so" Die Option „-module“ verwendet ein rootfile-Zertifikat. Die Optionen „-module“ und „-class“ schließen sich gegenseitig aus.

9 Geben Sie der Datei einen Namen und speichern Sie sie.

Sie können einige Einstellungen ändern, während der Remote Loader läuft. Informationen zu diesen Einstellungen finden Sie unter Anhang B, „Konfigurationsoptionen für einen Remote Loader“, auf Seite 279.

Parameter	Beschreibung
-commandport	Gibt eine Instanz des Remote Loader an.
-config	Gibt eine Konfigurationsdatei an.
-javadebugport	Gibt an, dass die Remote Loader-Instanz das Java-Debugging auf dem angegebenen Port aktivieren soll.
-password	Ermöglicht die Übergabe von Befehlen.

Parameter	Beschreibung
-service	Installiert eine Instanz als Service. Nur Windows.
-tracechange	Ändert die Trace-Stufe.
-tracefilechange	Ändert den Namen der Trace-Datei, in die geschrieben wird.
-unload	Entlädt die Remote Loader-Instanz.
-window	Öffnet oder schließt das Trace-Fenster in einer Remote Loader-Instanz. Nur Windows.

Einstellen von Umgebungsvariablen unter Solaris, Linux oder AIX

Nach der Installation des Remote Loader können Sie die Umgebungsvariable `RDXML_PATH` einrichten, die das aktuelle rdxml-Verzeichnis ändert. Dieses Verzeichnis wird dann als Basispfad für die nachfolgend erstellten Dateien verwendet. Geben Sie zum Einrichten des Werts der Variable `RDXML_PATH` die folgenden Befehle ein:

- set RDXML_PATH=*path*
- export RDXML_PATH

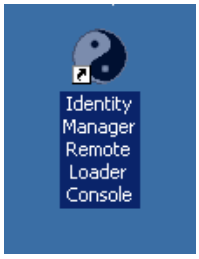
Starten des Remote Loader

- „Starten des Remote Loader unter Windows“ auf Seite 64
- „Starten des Remote Loader von der Befehlszeile aus“ auf Seite 65

Starten des Remote Loader unter Windows

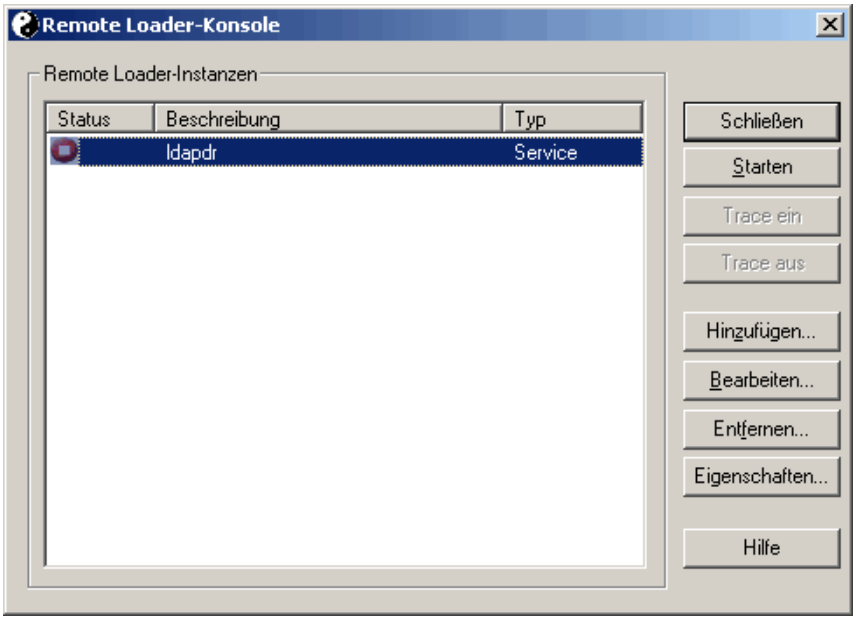
So führen Sie den Remote Loader unter Windows aus:

Abbildung 3-13 *Symbol „Remote Loader-Konsole“*



1 Klicken Sie auf das Symbol „Remote Loader-Konsole“ auf dem Desktop.

Abbildung 3-14 *Die Remote Loader-Konsole*



2 Wählen Sie eine Treiber-Instanz aus und klicken Sie anschließend auf *Starten*.

Starten des Remote Loader von der Befehlszeile aus

Unter Solaris, Linux oder AIX wird die Remote Loader-Funktionalität über die Binärkomponente „rdxml“ bereitgestellt. Diese Komponente befindet sich im Verzeichnis `/usr/bin/`. Unter Windows ist das Standardverzeichnis c:\novell\RemoteLoader.

So starten Sie Remote Loader:

1 Legen Sie das Passwort fest.

Plattform	Befehl
Windows	`dirxml_remote` -config *Pfad_zur_Konfigurationsdatei* -sp *Passwort Passwort*
Solaris, Linux, AIX	`rdxml` -config *Pfad_zur_Konfigurationsdatei* -sp *Passwort Passwort*
HP-UX, AS/400, OS/390, z/OS	`dirxml_jremote` -config *Pfad_zur_Konfigurationsdatei* -sp *Passwort Passwort*

Option	Kurzform	Parameter	Beschreibung
-password	-p	Passwort	Gibt das Passwort für die Befehlsauthentifizierung an. Dieses Passwort muss dasselbe Passwort sein, das mit **setpasswords** für die Loader-Instanz angegeben wurde, die Ziel der Befehle ist. Wenn eine Befehlsoption (z. B. „unload“ oder „tracechange“) angegeben, die Option **password** jedoch nicht angegeben wird, wird der Benutzer aufgefordert, das Passwort für den Loader einzugeben, der Ziel des Befehls ist. Beispiel: -password novell4 -p novell4
-setpass-words	-sp	Passwort Passwort	Gibt das Passwort der Remote Loader-Instanz und das Passwort des Identity Manager-Treiberobjekts des Remote-Schnittstellenmoduls an, mit dem der Remote Loader kommuniziert. Das erste Passwort im Argument ist das Passwort für den Remote Loader. Das zweite Passwort in den optionalen Argumenten ist das Passwort für das Identity Manager-Treiberobjekt, das mit dem Remote-Schnittstellenmodul auf dem Metaverzeichnis-Server verknüpft ist. Es müssen entweder beide oder keine Passwörter angegeben werden. Wenn kein Passwort angegeben wird, fordert der Remote Loader zur Eingabe der Passwörter auf. Dies ist eine Konfigurationsoption. Mithilfe dieser Option wird die Remote Loader-Instanz mit den angegebenen Passwörtern konfiguriert. Es wird jedoch weder ein Identity Manager-Anwendungsschnittstellenmodul geladen noch mit anderen Loader-Instanzen kommuniziert. Beispiel: -setpasswords novell4 staccato3 -sp novell4 staccato3

2 Starten Sie den Remote Loader.

Plattform	Befehl
Windows	`dirxml_remote` -config *Pfad_zur_Konfigurationsdatei*
Solaris, Linux, AIX	`rdxml` -config *Pfad_zur_Konfigurationsdatei*
HP-UX, AS/400, OS/390, z/OS	`dirxml_jremote` -config *Pfad_zur_Konfigurationsdatei*

3 Starten Sie den Treiber mithilfe von iManager.

4 Stellen Sie sicher, dass der Remote Loader ordnungsgemäß funktioniert.

Der Remote Loader lädt das Identity Manager-Anwendungsschnittstellenmodul nur, wenn der Remote Loader mit dem Remote-Schnittstellenmodul auf dem Metaverzeichnis-Server

kommuniziert. Dies bedeutet beispielsweise, dass das Anwendungsschnittstellenmodul heruntergefahren wird, wenn der Remote Loader die Kommunikation mit dem Metaverzeichnis-Server verliert.

Unter Linux, Solaris oder AIX können Sie mit dem Befehl „ps“ oder mit einer Trace-Datei prüfen, ob die Befehls- und Verbindungs-Ports überwacht werden.

Unter HP-UX und ähnlichen Plattformen können Sie den Java Remote Loader überwachen, indem Sie den Befehl „tail“ auf die Trace-Datei anwenden:

```
tail -f trace filename
```

Wenn in der letzten Zeile des Protokolls der nachfolgende Eintrag angezeigt wird, läuft der Loader ordnungsgemäß und wartet auf die vom Identity Manager Remote-Schnittstellenmodul kommenden Verbindungen:

```
TRACE: Remote Loader: Entering listener accept()
```

Informationen zum Konfigurieren von Remote Loader (rdxml), dass er unter UNIX automatisch gestartet wird, finden Sie in TID 10097249 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10097249.htm).

Stoppen des Remote Loader

Plattform	Befehl
Windows	Stoppen Sie eine Treiber-Instanz in der Remote Loader-Konsole.
Solaris Linux AIX	`rdxml` -config *Pfad_zur_Konfigurationsdatei* -u
HP-UX AS/400 OS/390 z/OS	`dirxml_jremote` -config *Pfad_zur_Konfigurationsdatei* -u

Wenn mehrere Remote Loader-Instanzen auf dem Computer ausgeführt werden, übergeben Sie den Befehl -cp *Befehls-Port*, sodass die entsprechende Instanz vom Remote Loader gestoppt werden kann.

Wenn Sie den Remote Loader stoppen, müssen Sie entweder über ausreichende Rechte verfügen oder das Remote-Loader-Passwort eingeben.

Szenario: Ausreichende Rechte. Der Remote Loader läuft als Windows-Dienst. Sie besitzen genügend Rechte, den Dienst zu stoppen. Sie geben ein ungültiges Passwort ein. Der Remote Loader wird trotzdem gestoppt.

Das Passwort wird vom Remote Loader zwar abgelehnt, da es jedoch in diesem Fall nicht erforderlich ist, wird es vom Remote Loader ignoriert. Wenn Sie den Remote Loader als Anwendung und nicht als Dienst ausführen, wird das Passwort verwendet.

3.4 Konfigurieren der Identity Manager-Treiber zur Verwendung mit Remote Loadern

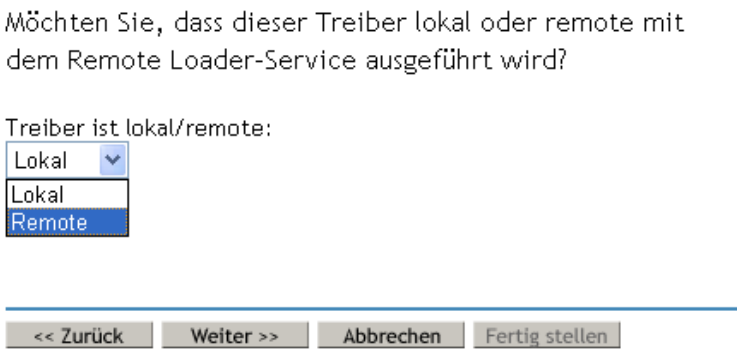
Sie können einen neuen Treiber konfigurieren oder einen vorhandenen Treiber für die Kommunikation mit dem Remote Loader aktivieren. In diesem Abschnitt erhalten Sie allgemeine Informationen darüber, wie Sie Treiber für die Kommunikation mit dem Remote Loader

konfigurieren. Ausführliche und treiberspezifische Informationen finden Sie im Implementierungshandbuch des jeweiligen Treibers.

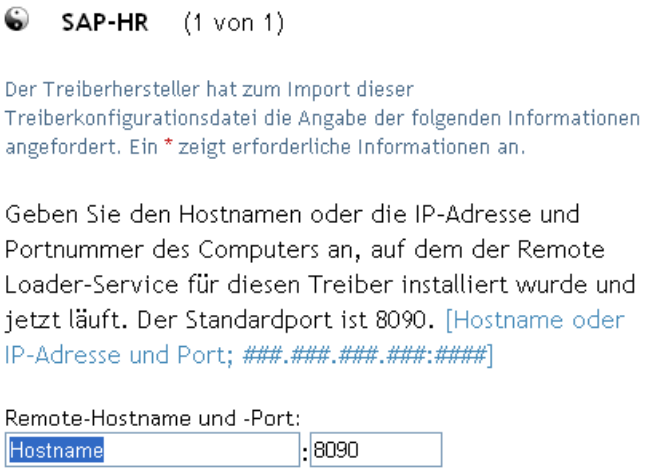
- Abschnitt 3.4.1, „Einen neuen Treiber importieren und konfigurieren“, auf Seite 68
- Abschnitt 3.4.2, „Einen vorhandenen Treiber konfigurieren“, auf Seite 69
- Abschnitt 3.4.3, „Erstellen eines Keystore“, auf Seite 71

3.4.1 Einen neuen Treiber importieren und konfigurieren

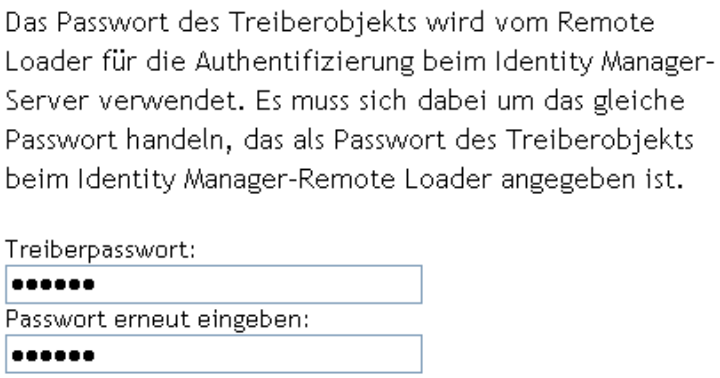
1. Importieren bzw. erstellen und konfigurieren Sie einen neuen Treiber in Novell iManager.
2. Blättern Sie an das Ende der Konfigurationsoptionen und wählen Sie „Remote“ in der Dropdown-Liste aus. Klicken Sie anschließend auf *Weiter*.



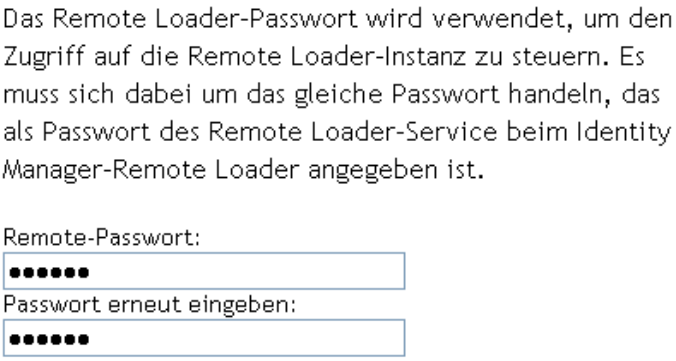
3. Geben Sie einen Remote-Hostnamen und -Port ein.



4 Geben Sie ein Passwort für das Treiberobjekt ein und bestätigen Sie es.



5 Geben Sie das Remote Loader-Passwort ein, bestätigen Sie es und klicken Sie anschließend auf *Weiter*.



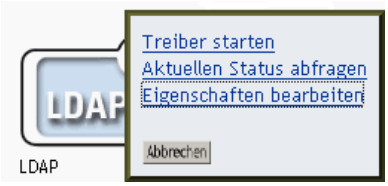
6 Erstellen Sie einen sicherheitsäquivalenten Benutzer, klicken Sie auf *Weiter* und danach auf *Fertig stellen*.

3.4.2 Einen vorhandenen Treiber konfigurieren

Geben Sie die für die Verbindung zum Remote Loader erforderlichen Parameter für das Treiberobjekt an.

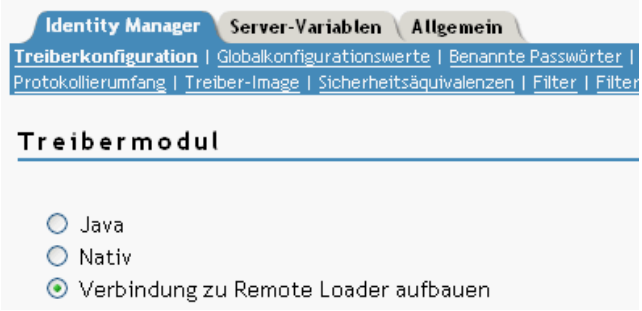
1 Klicken Sie in Novell iManager auf *Identity Manager* > *Identity Manager-Überblick*.

2 Wählen Sie den Treiber aus, den Sie bearbeiten möchten.



3 Klicken Sie auf das Symbol für den Treiberstatus und anschließend auf *Eigenschaften bearbeiten*.

4 Aktivieren Sie unter „Treibermodul“ die Option „Verbindung zu Remote Loader aufbauen“.



5 Geben Sie im Abschnitt „Authentifizierung“ Parameter für den Remote Loader ein.

- Verbindungsparameter für Remote Loader

  Sie haben das selbstsignierte Zertifikat bereits zu einem früheren Zeitpunkt exportiert. Weitere Informationen finden Sie in Abschnitt 3.2.2, „Selbstsigniertes Zertifikat exportieren“, auf Seite 48. Für SSL wird der Kurzname des selbstsignierten Zertifikats benötigt.

  Geben Sie im Textfeld „Verbindungsparameter für Remote Loader“ die Parameter als Schlüssel/Wert-Paare ein. Beispiel:

```
hostname=192.168.0.1 port=8090 kmo=remotecert
hostname=192.168.0.1 port=8090 kmo='remote cert'
```

  - hostname

    Der Hostname oder die IP-Adresse (z. B. 190.162.0.1). Gibt die Adresse oder den Namen des Computers an, auf dem der Remote Loader ausgeführt wird. Wenn Sie die IP-Adresse oder den Servernamen nicht angeben, wird der Standardwert „localhost“ verwendet.

  - port

    Port, über den der Remote Loader die vom Remote-Schnittstellenmodul kommenden Verbindungen akzeptiert. Wenn Sie diesen Kommunikationsparameter nicht eingeben, wird der Standardwert 8090 verwendet.

  - kmo

Gibt den Schlüsselnamen des Schlüsselmaterialobjekts (KMO) an (z. B. kmo=remotecert), das die für SSL verwendeten Schlüssel und Zertifikate enthält.

Wenn im Zertifikatsnamen Leerzeichen enthalten sind, müssen Sie den Kurznamen des KMO-Objekts in einfache Anführungszeichen setzen.

Tipp: Der KMO-Objektname ist der Kurzname, den Sie in Schritt 2 in Abschnitt 3.2.1, „Serverzertifikat erstellen“, auf Seite 48 vergeben haben.

- Anwendungspasswort

  Geben Sie das Passwort für die ID des Anwendungsbenutzers ein. Üblicherweise benötigt das Treiberschnittstellenmodul das Passwort, damit der Treiber eine Verbindung zur Anwendung herstellen kann.

- Remote Loader-Passwort

  Geben Sie das Passwort für den Remote Loader ein. Dieses Passwort wird vom Remote-Schnittstellenmodul für die Authentifizierung beim Remote Loader verwendet.

Hinweis: Das Anwendungspasswort und das Remote Loader-Passwort müssen zugleich festgelegt bzw. zurückgesetzt werden.

---

6 Klicken Sie auf *OK*.

3.4.3 Erstellen eines Keystore

Ein Keystore ist eine Java-Datei, die Verschlüsselungsschlüssel und Zertifikate (optional) enthält. Wenn Sie SSL (Secure Socket Layer) für die Kommunikation des Remote Loader mit der Metaverzeichnis-Engine verwenden möchten und mit einem Java-Schnittstellenmodul arbeiten, müssen Sie eine Keystore-Datei erstellen.

- „Keystore unter Windows“ auf Seite 71
- „Keystore unter Solaris, Linux oder AIX“ auf Seite 71
- „Keystore auf allen Plattformen“ auf Seite 72

Keystore unter Windows

Führen Sie unter Windows das Dienstprogramm „Keytool“ aus. Es befindet sich in der Regel im Verzeichnis `c:\novell\remoteloader\jre\bin`.

Keystore unter Solaris, Linux oder AIX

Verwenden Sie unter Solaris, Linux oder AIX die Datei „create_keystore“. Die Datei „Create_keystore“ wird mit „rdxml“ installiert und ist auch in der Datei „dirxml_jremote.tar.gz“ enthalten, die sich im Verzeichnis `\dirxml\java_remoteloader` befindet. „create_keystore“ ist ein Shell-Skript, das das Keytool-Dienstprogramm aufruft.

Wenn Sie unter UNIX den Keystore mithilfe des selbstsignierten Zertifikats erstellen, können Sie das Zertifikat in das Base64- oder Binärformat (.der) exportieren.

Geben Sie in der Befehlszeile Folgendes ein:

`create_keystore` *Name_des_selbstsignierten_Zertifikats Keystore-Name*

Geben Sie beispielsweise Folgendes ein:

```
create_keystore tree-root.b64 mystore
create_keystore tree-root.der mystore
```

Das create_keystore-Skript legt “dirxml” als hartkodiertes Keystore-Passwort fest. Dies ist kein Sicherheitsrisiko, da im Keystore nur ein öffentliches Zertifikat und ein öffentlicher Schlüssel gespeichert werden.

Keystore auf allen Plattformen

Wenn Sie einen Keystore auf einer belieben Plattform erstellen möchten, geben Sie in der Befehlszeile Folgendes ein:

`keytool` -import -alias trustedroot -file *Name_des_selbstsignierten_Zertifikats* -keystore *Dateiname* -storepass

Als Dateinamen können Sie einen beliebigen Namen eingeben (z. B. rdev_keystore).

Erstellen von Richtlinien

4

Mit Richtlinien können Sie den Informationsfluss in das und aus dem Identitätsdepot an eine bestimmte Umgebung anpassen.

Beispielsweise verwendet ein Unternehmen „inetOrgPerson“ als Hauptbenutzerklasse, während in einem anderen Unternehmen „User“ als Hauptbenutzerklasse verwendet wird. In diesem Fall wird eine Richtlinie erstellt, die der Metaverzeichnis-Engine mitteilt, welche Benutzerklasse auf dem jeweiligen System aufgerufen wird. Identity Manager wendet diese Richtlinie immer dann an, wenn Operationen, die sich auf Benutzer beziehen, zwischen verbundenen Systemen übertragen werden.

Außerdem können Sie mithilfe von Richtlinien neue Objekte erstellen, Attributwerte aktualisieren, Schema-Transformationen ausführen, Übereinstimmungskriterien definieren und Identity Manager-Verknüpfungen verwalten.

Ausführliche Informationen zu Richtlinien finden Sie im *Policy Builder and Driver Customization Guide* (Handbuch zum Richtlinien-Builder und zur Treiberanpassung). Dieses Handbuch enthält:

- Eine detaillierte Beschreibung der zur Verfügung stehenden Richtlinien
- Ein ausführliches Benutzer- und Referenzhandbuch zum Richtlinien-Builder mit Beispielen und Syntaxbeschreibungen der einzelnen Bedingungen, Aktionen, Nomen und Verben.
- Informationen darüber, wie Sie Richtlinien mithilfe von XSLT-Formatvorlagen erstellen können.

Weitere Informationen zu Richtlinien finden Sie im *Policy Builder and Driver Customization Guide* (Handbuch zum Richtlinien-Builder und zur Treiberanpassung).

Passwortsynchronisierung mit verbundenen Systemen

5

5.1 Überblick

Identity Manager ermöglicht eine Passwortsynchronisierung in beide Richtungen. Es verwendet dazu universelle Passwörter und verbundene Systeme zum Veröffentlichen und Abonnieren von Passwörtern.

Wie bei anderen Attributen eines Benutzerkontos können Sie auch hier die maßgeblichen Datenquellen auswählen.

5.1.1 Allgemeines zu Passwörtern

NDS®-Passwörter, einfache Passwörter, Verteilungspasswörter und universelle Passwörter werden für verschiedene Zwecke eingesetzt. In früheren Versionen von eDirectory™ und Identity Manager

konnten verbundene Systeme nur das NDS-Passwort mit einer Synchronisierung in eine Richtung aktualisieren.

Identity Manager verwendet das „universelle Passwort“, ein reversibles Passwort, das mit den anderen Identitätsdepot-Passwörtern synchronisiert werden kann. Das universelle Passwort wurde mit eDirectory 8.7.1 eingeführt und ist durch drei Verschlüsselungsstufen geschützt.

NMAS™ steuert die Relation zwischen dem universellen Passwort und den anderen Identitätsdepot-Passwörtern. Beispielsweise prüft NMAS, ob eine Passwortsynchronisierung zwischen dem universellen Passwort und dem NDS-Passwort, dem einfachen Passwort oder dem Verteilungspasswort besteht. NMAS fängt eingehende Anforderungen zum Ändern von Passwörtern ab und verarbeitet sie gemäß den Einstellungen in den NMAS-Passwortrichtlinien.

Identity Manager steuert die Relation zwischen Identity Vault-Passwörtern und den Passwörtern verbundener Systeme. Hierzu verwendet es das Verteilungspasswort, d. h. das Passwort des Identitätsdepots, das an die verbundenen Systeme verteilt werden kann. Wie das universelle Passwort ist auch das Verteilungspasswort durch drei Verschlüsselungsstufen geschützt und reversibel.

In der NMAS-Passwortrichtlinie können Sie festlegen, ob das Verteilungspasswort mit dem universellen Passwort übereinstimmen muss. (Die entsprechende Einstellung ist *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren*). Wenn das Verteilungspasswort mit dem universellen Passwort übereinstimmt und Sie für verbundene Systeme die bidirektionale Passwortsynchronisierung ausgewählt haben, denken Sie daran, mit Identity Manager das universelle Passwort aus eDirectory zu extrahieren und an andere verbundene Systeme zu senden. Sie müssen sowohl die Übertragung des Passworts als auch die verbundenen Systeme, auf denen es gespeichert wird, absichern. Weitere Informationen finden Sie unter Kapitel 7, „Sicherheit: Best Practices“, auf Seite 213.

Wenn das Verteilungspasswort nicht mit dem universellen Passwort übereinstimmt (da die entsprechende Einstellung in der NMAS-Passwortrichtlinie deaktiviert ist), können Sie Passwörter im „Tunnel-Modus“ an verbundene Systeme übertragen, die das Verteilungspasswort verwenden, ohne dass dies Auswirkungen auf das universelle Passwort oder das NDS-Passwort hat. Beachten Sie, dass beim „Tunneling“ nur Passwörter zwischen verbundenen Systemen synchronisiert werden. Wenn das „Tunneling“ aktiviert ist, wird das Identitätsdepot-/universelle Passwort nicht festgelegt.

Weitere Informationen zu den verschiedenen eDirectory-Passwörtern finden Sie im *Novell Modular Authentication Services (NMAS) 2.3 Administration Guide* (http://www.novell.com/documentation/nmas23/index.html) (Novell Modular Authentication Services (NMAS) 2.3 Administrationshandbuch). Beispiele zu den verschiedenen Methoden der Passwortsynchronisierung in Identity Manager finden Sie in Abschnitt 5.8, „Implementierung der Passwortsynchronisierung“, auf Seite 115.

5.1.2 Was versteht man unter einer bidirektionalen Passwortsynchronisierung?

Bei einer bidirektionalen Passwortsynchronisierung akzeptiert Identity Manager einerseits Passwörter von verbundenen Systemen, die Sie angegeben haben, und verteilt andererseits Passwörter an diese verbundenen Systeme.

Ob die Passwortsynchronisierung in beide Richtungen auf einem bestimmten verbundenen System möglich ist, hängt von den Einstellungen auf dem verbundenen System ab.

Einige verbundene Systeme akzeptieren neue und geänderte Passwörter von Identity Manager und können auch das aktuelle Passwort des Benutzers an Identity Manager übergeben. Die nachfolgend aufgeführten verbundenen Systeme unterstützen die bidirektionale Passwortsynchronisierung von Identity Manager:

- Active Directory
- Novell® eDirectory
- Network Information Services (NIS)
- NT Domain

Bei diesen verbundenen Systemen können Benutzer das Passwort auf einem der Systeme ändern und es anschließend über Identity Manager auf den anderen Systemen synchronisieren. Wenn Sie mit den erweiterten Passwortregeln in Ihren NMAS-Passwortrichtlinien arbeiten, ist es jedoch sinnvoller, dass die Benutzer die Passwörter in der iManager-Selbstbedienungskonsole ändern. Dies ist der beste Ort für Passwortänderungen, da hier alle Regeln, die das Benutzerpasswort erfüllen muss, aufgelistet werden.

Da andere verbundene Systeme das aktuelle Benutzerpasswort nicht weiterleiten können, wird auf diesen Systemen die bidirektionale Passwortsynchronisierung nicht vollständig unterstützt. Mit der Definition von Richtlinien innerhalb der Treiberkonfiguration können sie jedoch Daten bereitstellen, die zum Erstellen von Passwörtern verwendet werden können, und diese an Identity Manager senden.

Verschiedene andere Systeme können Passwörter von Identity Manager akzeptieren und ein Ausgangspasswort für einen neuen Benutzer einrichten oder ein vorhandenes Passwort ändern oder beides. Weitere Informationen hierzu finden Sie in Abschnitt 5.2, „Unterstützung von verbundenen Systemen bei der Passwortsynchronisierung“, auf Seite 86.

5.1.3 Vergleich zwischen Version 1.0 der Passwortsynchronisierung und der Identity Manager-Passwortsynchronisierung

Tabelle 5-1 *Vergleich: Passwortsynchronisierung 1.0 und Identity Manager-Passwortsynchronisierung*

	Passwortsynchronisierung 1.0	**Passwortsynchronisierung mit Identity Manager 2 und 3**
Produktzustellung	Separates Produkt; nicht im Lieferumfang von Identity Manager enthalten.	Teil von Identity Manager; nicht separat erhältlich.

	Passwortsynchronisierung 1.0	Passwortsynchronisierung mit Identity Manager 2 und 3
Plattformen	• Active Directory • NT Domain • eDirectory	Auf den folgenden Plattformen wird die bidirektionale Passwortsynchronisierung vollständig unterstützt: • Active Directory • eDirectory • NIS • NT Domain Auf diesen verbundenen Systemen wird das Veröffentlichen von Benutzerpasswörtern über Identity Manager unterstützt. Da das universelle Passwort und das Verteilungspasswort reversibel sind, kann Identity Manager Passwörter an verbundene Systeme verteilen. Jedes verbundene System, das das Abonnenten-Passwortelement unterstützt, kann Passwörter von Identity Manager abonnieren. Weitere Informationen hierzu finden Sie in Abschnitt 5.2, „Unterstützung von verbundenen Systemen bei der Passwortsynchronisierung“, auf Seite 86.
In einem Identitätsdepot verwendetes Passwort	NDS-Passwort (nicht reversibel)	Universelles Passwort (reversibel) oder Verteilungspasswort (reversibel). Das NDS-Passwort kann auch synchronisiert werden. Beispiele finden Sie in Abschnitt 5.8, „Implementierung der Passwortsynchronisierung“, auf Seite 115.
Hauptfunktionalität für unter Windows verbundene Systeme	Das Senden von Passwörtern an Identity Manager, um das Identitätsdepot-Passwort mit dem Windows-Passwort zu synchronisieren. Da das NDS-Passwort nicht reversibel ist, wurden Passwörter nicht an NT- oder AD-Systeme zurückgesendet.	Bereitstellung der bidirektionalen Passwortsynchronisierung Da das universelle Passwort und das Verteilungspasswort reversibel sind, können Passwörter in beide Richtungen synchronisiert werden.
LDAP-Änderungen	Nicht unterstützt	Unterstützt
Novell® Client™	Erforderlich	Nicht erforderlich
nadLoginName-Attribut	Wird dazu verwendet, Passwörter aktuell zu halten.	Nicht verwendet

	Passwortsynchronisierung 1.0	Passwortsynchronisierung mit Identity Manager 2 und 3
Komponente, die die Funktion zur Passwort-synchro-nisierung enthält	Die Funktionalität zum Aktuali-sieren von nadLoginName ist im Identity Manager-Treiber enthalten.	Die Passwortsynchronisierung basiert auf Iden-tity Manager-Richtlinien in der Treiberkonfigura-tion. Der Treiber führt die Aufgaben aus, die er von der Metaverzeichnis-Engine erhält und die sich aus der Logik der Richtlinien ergeben. Das Treibermanifest, die Globalkonfigurationswerte und die Treiberfiltereinstellungen müssen auch die Passwortsynchronisierung unterstützen. Sie sind in der Beispiel-Treiberkonfiguration enthalten, können aber auch zu einem vorhan-denen Treiber hinzugefügt werden. Weitere Informationen hierzu finden Sie in Abschnitt 5.7, „Upgrade bestehender Treiberkonfigurationen zur Unterstützung der Passwortsynchro-nisierung“, auf Seite 106.
Agenten	Ein separates Software-Modul.	Es werden keine Agenten installiert. Die Funk-tionalität ist jetzt im Treiber enthalten.

5.1.4 Funktionen der Identity Manager-Passwortsynchronisierung

Die Identity Manager-Passwortsynchronisierung ist bidirektional. Identity Manager akzeptiert einerseits Passwörter, die von verbundenen Systemen an ihn gesendet werden, und übergibt andererseits Passwörter an verbundene Systeme, die wiederum von diesen akzeptiert werden.

- „Akzeptieren von Passwörtern von verbundenen Systemen“ auf Seite 79
- „Verteilen von Passwörtern an verbundene Systeme“ auf Seite 80
- „Durchsetzen von Passwortrichtlinien im Datenspeicher und auf verbundenen Systemen“ auf Seite 80
- „Beispielsituationen für die Synchronisierung von Passwörtern“ auf Seite 81
- „Benachrichtigen von Benutzern, wenn bei der Passwortsynchronisierung Fehler aufgetreten sind“ auf Seite 82
- „Überprüfen des Passwortsynchronisierungsstatus eines Benutzers“ auf Seite 82

Akzeptieren von Passwörtern von verbundenen Systemen

Wie bei früheren Versionen von DirXML® und Identity Manager kann jedes verbundene System ein Passwort über das Identitätsdepot veröffentlichen.

Sie legen fest, von welchen verbundenen Systemen Identity Manager Passwörter akzeptiert. Sie können außerdem auswählen, ob Identity Manager das Passwort für Benutzer aktualisieren soll, die sich in demselben Identitätsdepot befinden, in dem Identity Manager läuft, oder ob es nur als Kanal oder “Tunnel” für die Synchronisierung der Passwörter zwischen verbundenen Systemen fungieren soll. Dadurch ist es möglich, das Identitätsdepot-Passwort und das Passwort, das von Identity Manager an die verbundenen Systeme verteilt wird, voneinander zu trennen.

Einige verbundene Systeme (AD, andere Identitätsdepots, NT und NIS) können das aktuelle Passwort des Benutzers bereitstellen, d. h. wenn ein Benutzer das Passwort auf einem verbundenen

System ändert, kann es von Identity Manager synchronisiert und an andere verbundene Systeme weitergeleitet werden.

Bei anderen verbundenen Systemen ist die Bereitstellung des aktuellen Benutzerpassworts nicht möglich. Sie können die Systeme jedoch so konfigurieren, dass Identity Manager ein Passwort über eine Formatvorlage bereitgestellt wird, z. B. ein Ausgangspasswort unter Verwendung des Nachnamens oder der Mitarbeiter-ID.

Verteilen von Passwörtern an verbundene Systeme

Mithilfe der Identity Manager-Passwortsynchronisierung können Sie ein allgemeines Passwort an verbundene Systeme verteilen.

In früheren Versionen von Identity Manager sendete ein Treiber die Passwörter von Benutzerkonten auf verbundene Systeme. Anhand der Passwörter wurden die entsprechenden Benutzer in eDirectory aktualisiert. Da das NDS-Passwort in eDirectory nicht reversibel ist, konnten Passwörter nicht aus dem zentralen Identity Manager-Identitätsdepot an die verbundenen Systeme verteilt werden. Das eDirectory-Passwort konnte nur vor dem Speichern in eDirectory, z. B. über den Novell Client, ermittelt werden.

Das von eDirectory 8.7.3 bereitgestellte universelle Passwort ist reversibel und kann verteilt werden.

Identity Manager kann Passwörter von verbundenen Systemen akzeptieren. Da das universelle Passwort reversibel ist, kann es Identity Manager aus dem Identitätsdepot an verbundene Systeme verteilen, auf denen das Einrichten eines Ausgangspassworts und das Ändern von Passwörtern unterstützt wird.

Unabhängig davon, woher das Passwort kommt, verwendet Identity Manager das Verteilungspasswort als Depot, von dem aus Passwörter an verbundene Systeme verteilt werden. Wie beim universellen Passwort können Passwortrichtlinien auch für das Verteilungspasswort erzwungen werden.

Weitere Informationen zur Verwendung des universellen Passworts und des Verteilungspassworts bei der Synchronisierung von Passwörtern finden Sie unter „Implementierung der Passwortsynchronisierung“ auf Seite 115.

Wie bei anderen Benutzerattributen auch entscheiden Sie, welche Systeme maßgebliche Quellen für Passwörter sind. Identity Manager verteilt die Passwörter von dieser Quelle an die anderen verbundenen Systeme.

Sie können die bidirektionale Passwortsynchronisierung auf den verbundenen Systemen einrichten, die diese Funktion unterstützen.

Durchsetzen von Passwortrichtlinien im Datenspeicher und auf verbundenen Systemen

Identity Manager kann Passwortrichtlinien für eingehende Passwörter erzwingen, indem es NMAS aufruft. Wenn das von einem verbundenen System über Identity Manager veröffentlichte Passwort nicht den Richtlinien entspricht, können Sie festlegen, dass es im Identitätsdepot abgelehnt wird. Dies bedeutet zudem, dass Passwörter, die nicht regelkonform sind, nicht an andere verbundene Systeme verteilt werden.

Identity Manager kann zudem Passwortrichtlinien auf verbundenen Systemen durchsetzen. Sie können festlegen, dass Identity Manager nicht nur die Verteilung des Passworts ablehnt, sondern auch auf dem verbundenen System das nicht regelkonforme Passwort auf das aktuelle

Verteilungspasswort aus dem Identitätsdepot zurücksetzt, wenn das über Identity Manager veröffentlichte Passwort nicht der Richtlinie entspricht.

Angenommen, Sie möchten erzwingen, dass Passwörter mindestens ein numerisches Zeichen enthalten. Das verbundene System kann jedoch eine solche Richtlinie nicht erzwingen. Aus diesem Grund legen Sie fest, dass Identity Manager Passwörter von diesem verbundenen System zurücksetzen soll, wenn sie nicht den in der Richtlinie definierten Regeln entsprechen.

Bei Verwendung von erweiterten Passwortregeln und der Passwortsynchronisierung von Identity Manager empfehlen wir darüber hinaus, dass Sie die Passwortrichtlinien für alle verbundenen Systeme untersuchen, um sicherzustellen, dass die erweiterten Passwortregeln in der eDirectory-Passwortrichtlinie regelkonform sind. Auf diese Weise wird gewährleistet, dass Passwörter erfolgreich synchronisiert werden können.

Sie müssen auch sicherstellen, dass Benutzer, für die NMAS-Passwortrichtlinien gelten, mit den Benutzern übereinstimmen, für die die Passwortsynchronisierung mit verbundenen Systemen ausgeführt werden soll.

NMAS-Passwortrichtlinien werden baumspezifisch zugewiesen. Die Passwortsynchronisierung hingegen wird pro Treiber konfiguriert. Treiber werden außerdem serverspezifisch installiert und können nur solche Benutzer verwalten, die sich in einer Master- oder Lese-/Schreibreproduktion befinden. Damit eine Passwortsynchronisierung die gewünschten Ergebnisse liefert, müssen Sie sicherstellen, dass die Container in der Master- oder Lese-/Schreibreproduktion auf dem Server, auf dem die Treiber für die Passwortsynchronisierung aktiv sind, den Containern entsprechen, für die Sie Passwortrichtlinien mit aktiviertem universellem Passwort zugewiesen haben. Durch Zuweisung einer Passwortrichtlinie an den Partitionsstammcontainer kann sichergestellt werden, dass die Passwortrichtlinie allen in diesem Container und seinen Untercontainern enthaltenen Benutzern zugewiesen wird.

Weitere Informationen darüber, wie Benutzern NMAS-Passwortrichtlinien zugewiesen werden, finden Sie unter „Assigning Password Policies to Users“ im *Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung).

Beispielsituationen für die Synchronisierung von Passwörtern

Mit Identity Manager können Sie angeben, welche Systeme die maßgeblichen Quellen für Passwörter sein sollen. Außerdem entscheiden Sie, wie Passwörter weitergeleitet werden.

Die meisten Funktionen der Passwortsynchronisierung von Identity Manager basieren auf dem universellen Passwort, der vom Identitätsdepot bereitgestellten reversiblen Passwortfunktionalität. In einigen Fällen ist es jedoch nicht erforderlich, das universelle Passwort zu verteilen.

Für die Identity Manager-Passwortsynchronisierung wird auch das Verteilungspasswort verwendet. Wie beim universellen Passwort kann auch beim Verteilungspasswort eine Richtlinie erzwungen werden.

Weitere Informationen zur Verwendung der Passwortsynchronisierung finden Sie unter „Implementierung der Passwortsynchronisierung“ auf Seite 115. Sie können eine oder mehrere dieser Beispielsituationen verwenden, um den Erfordernissen in Ihrer Umgebung gerecht zu werden.

Synchronisieren von Passwörtern unter Windows ohne den Novell Client

Für die Passwortsynchronisierung mit Active Directory und NT Domain wird kein Novell Client mehr benötigt.

Benachrichtigen von Benutzern, wenn bei der Passwortsynchronisierung Fehler aufgetreten sind

Im Abschnitt Durchsetzen von Passwortrichtlinien im Datenspeicher und auf verbundenen Systemen wird beschrieben, dass Identity Manager Passwortrichtlinien erzwingen kann, indem (von verbundenen Systemen stammende) nicht regelkonforme Passwörter abgelehnt werden.

Mit der Funktion der Email-Benachrichtigung können Sie festlegen, dass der Benutzer per Email benachrichtigt wird, wenn seine Passwortänderung nicht erfolgreich war.

Szenario. Sie haben Identity Manager so konfiguriert, dass von NT Domain eingehende Passwörter abgelehnt werden, wenn sie nicht Ihrer Passwortrichtlinie entsprechen. Sie haben die Funktion der Email-Benachrichtigung aktiviert. Eine Regel in Ihrer NMAS-Passwortrichtlinie legt fest, dass der Firmenname nicht als Passwort verwendet werden darf. Ein Benutzer eines verbundenen Systems der NT Domain ändert das Passwort in den Firmennamen. NMAS lehnt das Passwort ab und Identity Manager teilt dem Benutzer in einer Email mit, dass das Passwort nicht synchronisiert wurde.

Bevor Sie diese Funktion verwenden können, müssen Sie den Email-Server und Schablonen einrichten. Sie können Folgendes anpassen:

- Den Text der Meldungen, die von Identity Manager versendet werden
- Die Benachrichtigung, eine Kopie an den Administrator zu senden

Weitere Informationen finden Sie unter „Konfigurieren der Email-Benachrichtigung“ auf Seite 156.

Überprüfen des Passwortsynchronisierungsstatus eines Benutzers

Identity Manager bietet Ihnen die Möglichkeit, den Passwortsynchronisierungsstatus eines Benutzers von einem verbundenen System prüfen zu lassen. Wenn das verbundene System die Funktion zum Prüfen des Passworts unterstützt, können Sie feststellen, ob Passwörter ordnungsgemäß synchronisiert werden.

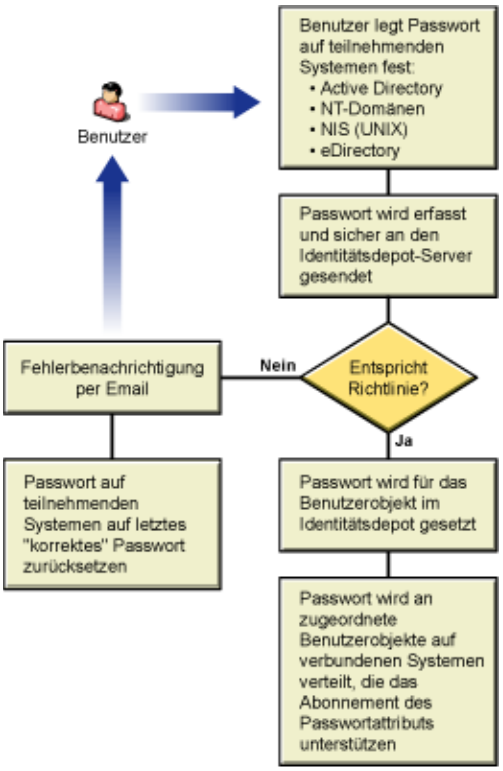
Weitere Informationen zum Überprüfen von Passwörtern finden Sie unter „Überprüfen des Passwortsynchronisierungsstatus eines Benutzers“ auf Seite 155.

Eine Liste der Systeme, von denen die Überprüfung von Passwörtern unterstützt wird, erhalten Sie unter „Unterstützung von verbundenen Systemen bei der Passwortsynchronisierung“ auf Seite 86.

5.1.5 Überblick über den Datenfluss bei der Passwortsynchronisierung

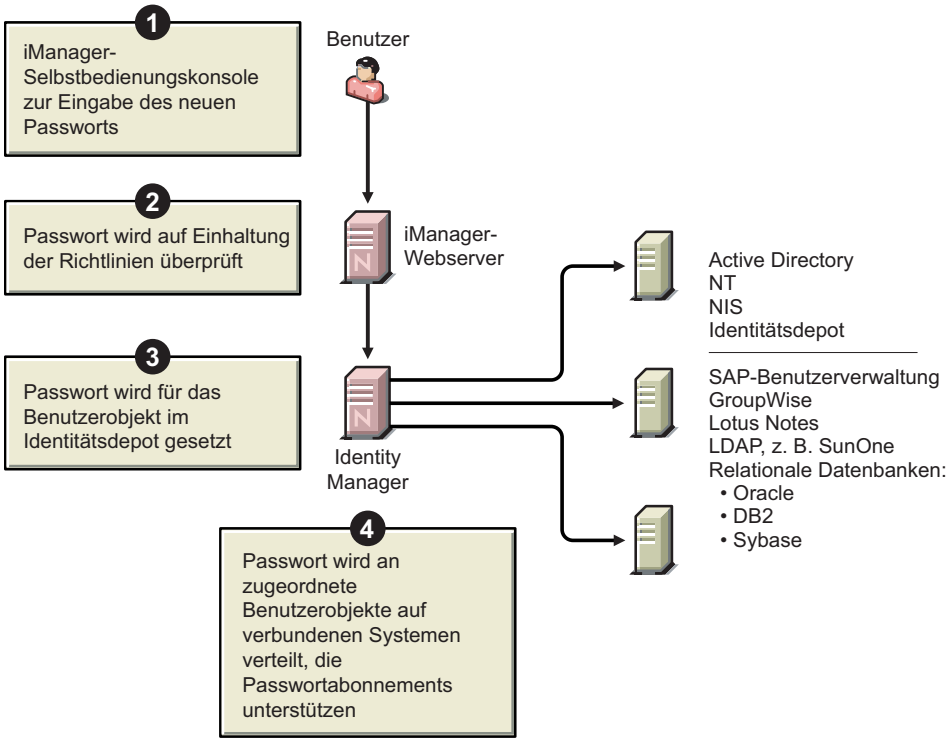
In der folgenden Abbildung sehen Sie, wie verbundene Systeme Passwörter über Identity Manager veröffentlichen.

Abbildung 5-1 *Veröffentlichen von Passwörtern verbundener Systeme über Identity Manager*



In der folgenden Abbildung sehen Sie, wie Identity Manager Passwörter an verbundene Systeme verteilt.

Abbildung 5-2 *Verteilen von Passwörtern von Identity Manager an verbundene Systeme*

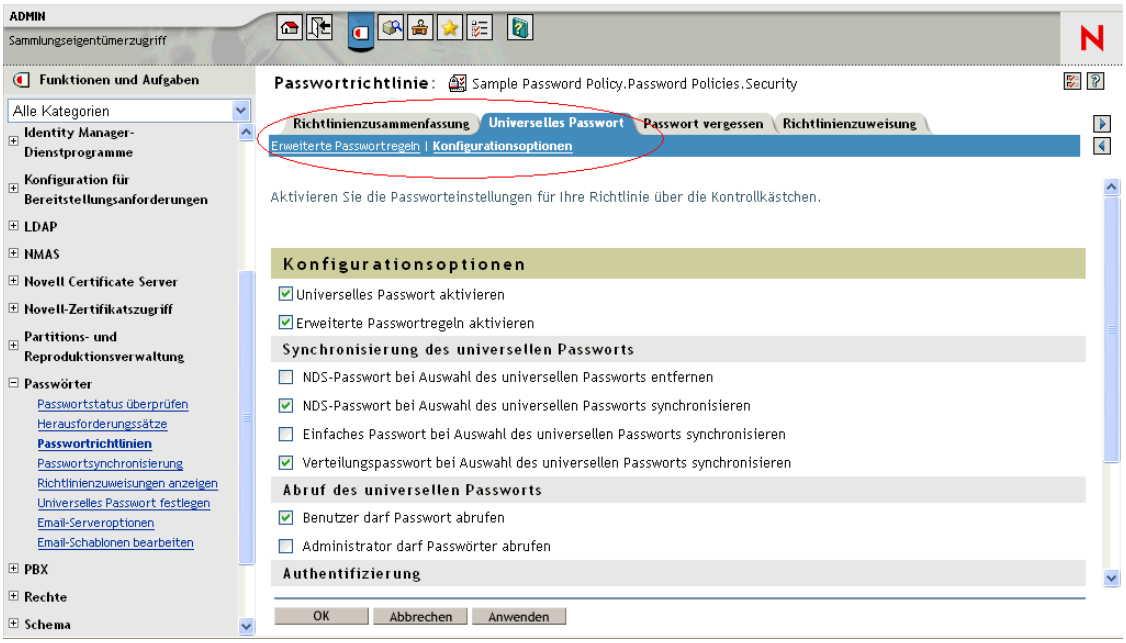


5.1.6 Anzeige von Abbildungen

In dieser Dokumentation werden häufig Abbildungen verwendet, um die Optionen in iManager zu veranschaulichen. Wie die Optionen tatsächlich auf Ihrem Desktop angezeigt werden, hängt davon ab, mit welchem Browser Sie arbeiten.

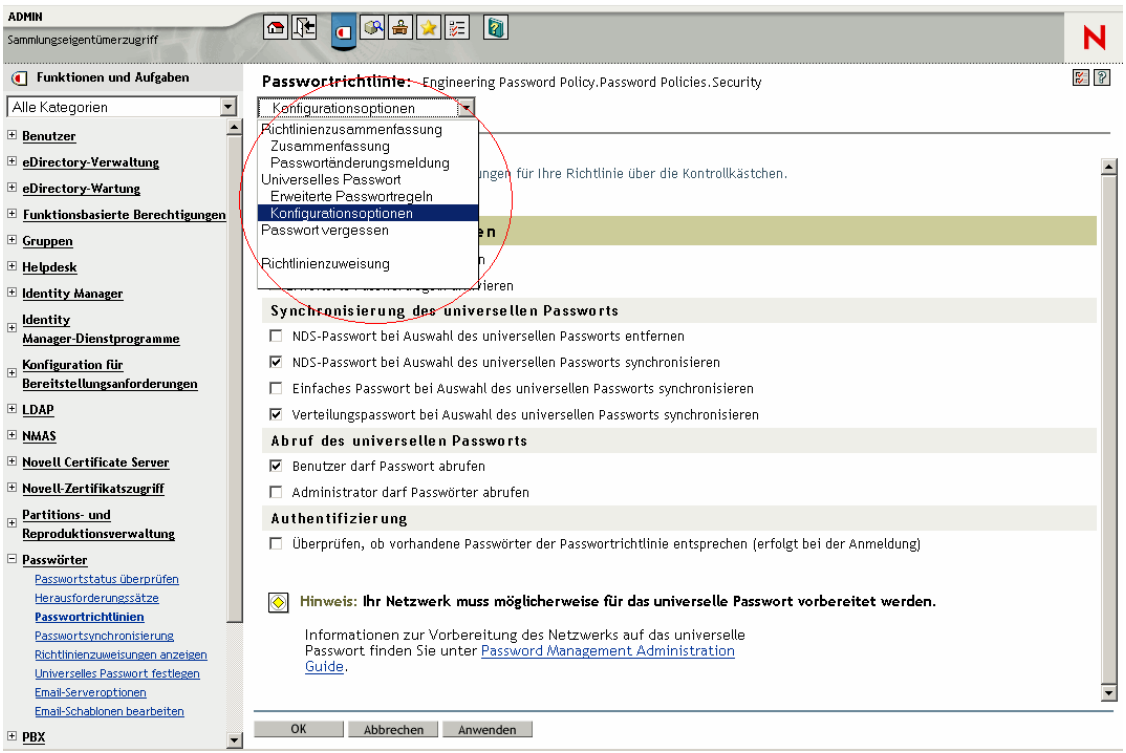
In Internet Explorer werden iManager-Optionen beispielsweise in Registerkarten angezeigt.

Abbildung 5-3 *Registerkarten in iManager*



In Firefox werden die iManager-Optionen dagegen in einer Dropdown-Liste angezeigt.

Abbildung 5-4 *Dropdown-Liste in iManager*



In dieser Dokumentation werden die Abbildungen so angezeigt, wie sie in Firefox erscheinen.

5.2 Unterstützung von verbundenen Systemen bei der Passwortsynchronisierung

Wenn Sie ein Benutzerobjekt erstellt haben, kann Identity Manager immer ein Passwort von einem verbundenen System akzeptieren, auch dann, wenn die Funktion zum Weiterleiten des aktuellen Benutzerpasswords auf dem verbundenen System nicht unterstützt wird.

AD, NT, eDirectory und NIS können sowohl Passwörter von Identity Manager akzeptieren als auch das aktuelle Benutzerpasswort an Identity Manager weiterleiten. Die Passwortsynchronisierung in beide Richtungen wird also vollständig unterstützt.

Wenn Sie eine Richtlinie innerhalb der Treiberkonfiguration auf dem Herausgeberkanal erstellen, können andere Systeme Daten bereitstellen, die für die Erstellung von Passwörtern verwendet werden. Die Beispielkonfigurationen der meisten Treiber enthalten eine Beispielrichtlinie für ein Standardpasswort, das auf dem Nachnamen basiert.

Auf verbundenen Systemen stehen verschiedene Funktionen zum Akzeptieren von Passwörtern von Identity Manager zur Verfügung. Einige verbundene Systeme unterstützen zwar das Erstellen von Ausgangspasswörtern für neue Konten, Passwortänderungen werden jedoch nicht zugelassen.

Die Funktionen der Beispiel-Treiberkonfigurationen sind im Treibermanifest dokumentiert. Die nachfolgenden Tabellen enthalten zusätzliche Informationen, die nicht im Treibermanifest dokumentiert sind. In den Tabellen wird beschrieben, welche Anwendungen Ausgangspasswörter für neue Konten unterstützen und ob Passwortänderungen zugelassen werden. Im Manifest ist lediglich dokumentiert, dass das verbundene System die Möglichkeit bietet, Passwörter zu akzeptieren. Auf Passwortänderungen wird nicht eingegangen.

Da Treiber in Gruppen zusammengefasst sind, gibt es mehrere Beispiel-Treiberkonfigurationen mit ähnlichen Funktionen.

5.2.1 Systeme, die die bidirektionale Passwortsynchronisierung unterstützen

Die folgenden verbundenen Systeme unterstützen die Passwortsynchronisierung in beide Richtungen. Sie können sowohl das aktuelle Passwort des Benutzers auf dem verbundenen System bereitstellen als auch Passwörter von Identity Manager akzeptieren.

Tabelle 5-2 *Systeme, die die bidirektionale Passwortsynchronisierung unterstützen*

Treiber des verbundenen Systems	Abonnentenkanal	Abonnentenkanal	Abonnentenkanal	Herausgeberkanal
	Anwendung akzeptiert Festlegen eines Ausgangspassworts	Anwendung akzeptiert Bearbeitung eines Passworts	Anwendung unterstützt Passwortprüfung	Anwendung stellt Passwort bereit (Synchronisierung)
Active Directory	Ja	Ja	Ja	Ja
eDirectory[1]	Ja	Ja	Ja	Ja
NT Domain	Ja	Ja	Nein	Ja
NIS	Ja	Ja	Ja	Ja

Treiber des verbundenen Systems	Abonnentenkanal	Abonnentenkanal	Abonnentenkanal	Herausgeberkanal
	Anwendung akzeptiert Festlegen eines Ausgangspassworts	Anwendung akzeptiert Bearbeitung eines Passworts	Anwendung unterstützt Passwortprüfung	Anwendung stellt Passwort bereit (Synchronisierung)
SIF	Ja	Ja	Nein	Ja

[1]Die bidirektionale Passwortsynchronisierung zwischen Identitätsdepot-Bäumen wird für Benutzer auch dann unterstützt, wenn das universelle Passwort für diese Benutzer deaktiviert ist. Weitere Informationen hierzu finden Sie unter Abschnitt 5.8.2, „Szenario 1: Synchronisierung zwischen zwei Identitätsdepots über das NDS-Passwort“, auf Seite 117.

5.2.2 Systeme, die Passwörter von Identity Manager akzeptieren

Die folgenden Systeme können Passwörter von Identity Manager begrenzt akzeptieren. Sie können das eigentliche Passwort des Benutzers auf dem verbundenen System nicht an Identity Manager übergeben.

Obwohl diese Systeme nicht imstande sind, das Passwort des Benutzers an Identity Manager zu übergeben, können sie so konfiguriert werden, dass sie mittels einer Richtlinie auf dem Herausgeberkanal ein Passwort erstellen können, das auf anderen Benutzerdaten des verbundenen Systems basiert. (Die Beispiel-Treiberkonfigurationen veranschaulichen das Erstellen eines auf dem Nachnamen des Benutzers basierenden Standardpassworts.)

Tabelle 5-3 *Systeme, die Passwörter von Identity Manager akzeptieren*

Treiber des verbundenen Systems	Abonnentenkanal	Abonnentenkanal	Abonnentenkanal	Herausgeberkanal
	Anwendung akzeptiert Festlegen eines Ausgangspassworts	Anwendung akzeptiert Bearbeitung eines Passworts	Anwendung unterstützt Passwortprüfung	Anwendung stellt Passwort bereit (Synchronisierung)
Groupwise®	Ja	Ja	Nein	Nein[2]
JDBC	Ja[3]	Nein4	Nein	Nein[5]
LDAP	Ja[6]	Ja[6]	Ja	Nein
Notes	Ja	Ja[7]	Ja[7]	Nein
SAP-Benutzerverwaltung	Ja	Ja	Nein	Nein

[2]GroupWise unterstützt zwei Authentifizierungsmethoden:

- GroupWise verwendet seine eigene Authentifizierungsmethode und verwaltet die Benutzerpasswörter.
- GroupWise führt die Authentifizierung über LDAP bei eDirectory durch und verwaltet keine Passwörter.

Bei Verwendung dieser Option ignoriert GroupWise vom Treiber synchronisierte Passwörter.

[3]Die Möglichkeit zum Festlegen eines Ausgangspassworts besteht bei allen Datenbanken, bei denen das Benutzerkonto der Datenbank nicht mit dem Benutzerkonto des Betriebssystems identisch ist (z. B. bei Oracle*, MS SQL, MySQL* oder Sybase*).

[4]Der Identity Manager-Treiber für JDBC kann zum Bearbeiten eines Passworts auf dem verbundenen System verwendet werden. Diese Funktion wird jedoch durch die Beispiel-Treiberkonfiguration nicht veranschaulicht.

[5]Passwörter können wie Daten synchronisiert werden, wenn sie in einer Tabelle gespeichert sind.

[6]Wenn der LDAP-Zielserver das Einstellen des Attributs „userpassword“ zulässt.

[7]Der Notes-Treiber kann nur für das Feld „HTTPPassword“ in Lotus Notes eine Passwortänderung akzeptieren und Passwörter überprüfen.

5.2.3 Systeme, die keine Passwörter akzeptieren oder bereitstellen

Die folgenden verbundenen Systeme können unter Verwendung der Beispiel-Treiberkonfiguration Passwörter weder entgegennehmen noch auf dem verbundenen System bereitstellen.

Obwohl diese Systeme nicht imstande sind, das Passwort des Benutzers an Identity Manager zu übergeben, können sie so konfiguriert werden, dass sie mittels einer Richtlinie auf dem Herausgeberkanal ein Passwort erstellen können, das auf anderen Benutzerdaten im verbundenen System basiert. (Die Beispiel-Treiberkonfigurationen veranschaulichen das Erstellen eines auf dem Nachnamen des Benutzers basierenden Standardpassworts.)

Tabelle 5-4 *Systeme, die keine Passwörter akzeptieren oder bereitstellen*

Treiber des verbundenen Systems	Abonnentenkanal	Abonnentenkanal	Abonnentenkanal	Herausgeberkanal
	Anwendung akzeptiert Festlegen eines Ausgangspassworts	Anwendung akzeptiert Bearbeitung eines Passworts	Anwendung unterstützt Passwortprüfung	Anwendung stellt Passwort bereit (Synchronisierung)
Text mit Begrenzungszeichen	Nein[8]	Nein[8]	Nein[8]	Nein[8]
Exchange 5.5	Nein	Nein	Nein	Nein
PeopleSoft 3.6	Nein	Nein	Nein	Nein
PeopleSoft 4.0	Nein	Nein	Nein	Nein
SAP HR	Nein	Nein	Nein	Nein

[8]Der Identity Manager-Treiber für Text mit Begrenzungszeichen verfügt im Treiberschnittstellenmodul über keine Funktionen, die eine Passwortsynchronisierung direkt unterstützen. Der Treiber kann jedoch in Abhängigkeit von dem verbundenen System, mit dem die Synchronisierung erfolgt, für die Verarbeitung von Passwörtern konfiguriert werden.

5.2.4 Systeme, die keine Passwortsynchronisierung unterstützen

Die folgenden verbundenen Systeme sind nicht zur Verwendung mit der Passwortsynchronisierung vorgesehen.

Tabelle 5-5 *Systeme, die keine Passwortsynchronisierung unterstützen*

Treiber des verbundenen Systems	Abonnentenkanal	Abonnentenkanal	Abonnentenkanal	Herausgeberkanal
	Anwendung akzeptiert Festlegen eines Ausgangspassworts	Anwendung akzeptiert Bearbeitung eines Passworts	Anwendung unterstützt Passwortprüfung	Anwendung stellt Passwort bereit (Synchronisierung)
Avaya* PBX	Nein	Nein	Nein	Nein
Berechtigungs-Service-Treiber	Nein	Nein	Nein	Nein
LoopBack-Service-Treiber	Nein	Nein	Nein	Nein
Service-Treiber für manuelle Aufgaben	Nein	Nein	Nein	Nein

5.3 Voraussetzungen für die Passwortsynchronisierung

Damit die Passwortsynchronisierung funktioniert, müssen folgende Voraussetzungen erfüllt sein:

- „Unterstützung eines universellen Passworts“ auf Seite 89
- „Im Treibermanifest beschriebene Möglichkeiten zur Passwortsynchronisierung“ auf Seite 90
- „Steuerung der Passwortsynchronisierung über Globalkonfigurationswerte“ auf Seite 90
- „In der Treiberkonfiguration benötigte Richtlinien“ auf Seite 94
- „Filter, die auf dem verbundenen System installiert sein müssen, zum Erfassen von Passwörtern“ auf Seite 99
- „Für Benutzer erstellte NMAS-Passwortrichtlinien“ auf Seite 99
- „NMAS-Anmeldemethoden“ auf Seite 99

5.3.1 Unterstützung eines universellen Passworts

Für die Passwortsynchronisierung mit verbundenen Systemen benötigt Identity Manager ein universelles Passwort. Informationen hierzu finden Sie in den folgenden Abschnitten:

- “Deploying Universal Password” (Bereitstellung eines universellen Passworts) im *Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung)

- Abschnitt 5.4.3, „Vorbereitungen für die Verwendung des universellen Passworts“, auf Seite 101

5.3.2 Im Treibermanifest beschriebene Möglichkeiten zur Passwortsynchronisierung

Im Treibermanifest ist dokumentiert, ob ein verbundenes System die folgenden Funktionen der Passwortsynchronisierung unterstützt:

- Übergabe des tatsächlichen Benutzerpassworts an Identity Manager
- Akzeptieren eines Passworts von Identity Manager

  Das Manifest unterscheidet nicht, ob die Erstellung eines Ausgangspassworts oder Änderungen an einem bestehenden Passwort akzeptiert werden.
- Zulässigkeit der Passwortüberprüfung auf dem verbundenen System durch Identity Manager, um den Status der Passwortsynchronisierung eines Benutzers ermitteln zu können.

Hinweis: Das Treibermanifest wird vom Entwickler des Treibers oder vom Identity Manager-Experten geschrieben, der die Treiberkonfiguration erstellt. Eine Bearbeitung des Manifests durch einen Netzwerkverwalter ist nicht vorgesehen. Im Treibermanifest sind die tatsächlichen Möglichkeiten des Treiberschnittstellenmoduls und der Konfiguration dokumentiert. Das bloße Abändern des Manifests ändert nichts an der Funktionalität des Treibers. Zur Erweiterung der Funktionalität muss das Treiberschnittstellenmodul, das verbundene System oder die Treiberkonfiguration erweitert werden.

Die mit Identity Manager gelieferten Beispiel-Treiberkonfigurationen enthalten Einträge im Treibermanifest. Informationen dazu, wie Sie diese Einträge in vorhandene Treiber einbinden können, finden Sie in Abschnitt 5.7, „Upgrade bestehender Treiberkonfigurationen zur Unterstützung der Passwortsynchronisierung“, auf Seite 106.

5.3.3 Steuerung der Passwortsynchronisierung über Globalkonfigurationswerte

Anhand von Globalkonfigurationswerten können Sie einen konstanten Wert festlegen, auf den in einer Richtlinie verwiesen werden kann. Globalkonfigurationswerte werden auch als Server-Variablen bezeichnet, weil sie in einem Attribut festgehalten sind, d. h. sie sind pro Reproduktion verfügbar.

Im Kontext der Passwortsynchronisierung können mit Globalkonfigurationswerten Einstellungen für den Transfer von Passwörtern zwischen dem verbundenen System und Identity Manager erstellt werden. Da das Synchronisierungsverhalten der Passwortsynchronisierungsrichtlinien von Identity Manager in der Treiberkonfiguration von den jeweiligen Einstellungen im Globalkonfigurationswert abhängig ist, kann der Passwort-Transfer problemlos geändert werden, ohne die Richtlinien selbst bearbeiten zu müssen.

Über Globalkonfigurationswerte können Sie die nachfolgend aufgeführten Einstellungen für jedes verbundene System separat steuern.

Tabelle 5-6 *Einstellungen für verbundene Systeme*

Einstellung	Beschreibung
Entgegennahme von Passwörtern aus dem verbundenen System durch Identity Manager	Diese Einstellung gilt für Passwörter, die vom verbundenen System bereitgestellt werden, sowie für Passwörter, die über Identity Manager-Richtlinien in der Treiberkonfiguration auf dem Herausgeberkanal erstellt werden können. Wenn Sie diese Einstellung deaktivieren, werden beide Arten von Passwörtern ausgeschlossen und erreichen somit Identity Manager nicht.
Von Identity Manager verwendete Synchronisierungsmethode: direkte Aktualisierung des universellen Passworts oder direkte Aktualisierung des Verteilungspassworts	Identity Manager kontrolliert den Einstiegspunkt (d. h. das von Identity Manager aktualisierte Passwort). NMAS kontrolliert in Abhängigkeit von den Einstellungen in der NMAS-Passwortrichtlinie den Passwort-Transfer zwischen den einzelnen Passwortarten. So zeigen Sie eine NMAS-Passwortrichtlinie an: 1. Klicken Sie in iManager auf *Passwörter* > *Passwortrichtlinien*. 2. Wählen Sie eine Richtlinie in der *Passwortrichtlinienliste* aus. 3. Klicken Sie auf *Bearbeiten*. 4. Wählen Sie im Dropdown-Listenfeld oder in der Registerkarte (je nach Versionsstand von iManager) eine Option aus. Beispielszenarios für diese Methoden finden Sie in Abschnitt 5.8, “Implementierung der Passwortsynchronisierung”.
Erzwingung der NMAS-Passwortrichtlinien bei Passwörtern, die Identity Manager von einem verbundenen System entgegennimmt	Wenn diese Richtlinien erzwungen werden, werden eingehende,unzulässige Passwörter nicht in den Datenspeicher von Identity Manager geschrieben.
Verwendung des Identity Manager-Passworts durch Identity Manager für das Erzwingen von NMAS-Passwortrichtlinien auf einem verbundenen System durch Zurücksetzen von Passwörtern, die den Richtlinienregeln nicht entsprechen	Diese Option wird auf der NMAS-Benutzeroberfläche grau angezeigt, wenn sie vom verbundenen System nicht unterstützt wird (gemäß Treibermanifest). Das Passwort wird nur zurückgesetzt, wenn auf dem Herausgeberkanal bei einem Passwortvorgang ein Fehler auftritt.
Entgegennahme von Passwörtern durch das verbundene System	Diese Einstellung gilt sowohl für Passwörter, die von Identity Manager bereitgestellt werden, als auch für Passwörter, die über Identity Manager-Richtlinien in der Treiberkonfiguration auf dem Abonnentenkanal erstellt werden. Wenn Sie diese Einstellung deaktivieren, werden beide Arten von Passwörtern ausgeschlossen und erreichen somit das verbundene System nicht. Diese Option wird auf der Benutzeroberfläche grau angezeigt, wenn sie vom verbundenen System nicht unterstützt wird (gemäß Treibermanifest).
Benachrichtigung des Benutzers per Email, wenn das Passwort nicht synchronisiert werden konnte	Mit dieser Einstellung wird festgelegt, ob betroffene Benutzer automatisch per Email benachrichtigt werden.

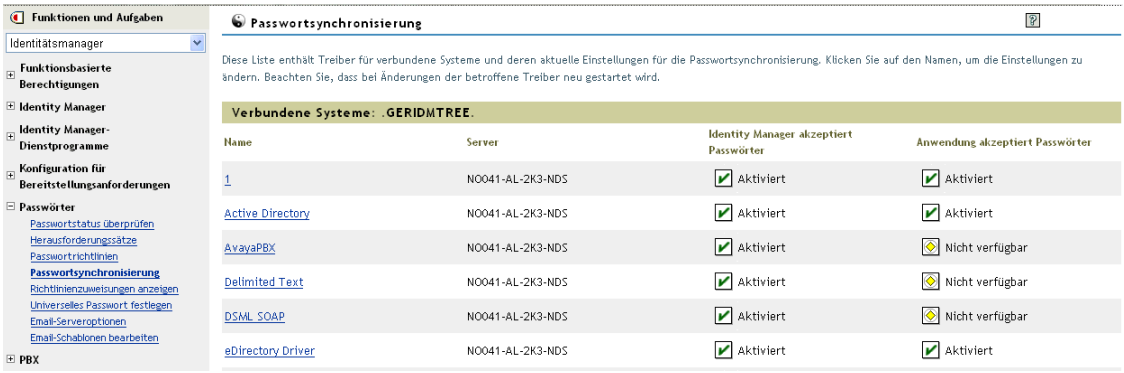
Die mit Identity Manager gelieferten Treiberkonfigurationen enthalten Einträge im Treibermanifest. Informationen dazu, wie Sie diese Einträge in vorhandene Treiber einbinden können, finden Sie in

Abschnitt 5.7, „Upgrade bestehender Treiberkonfigurationen zur Unterstützung der Passwortsynchronisierung“, auf Seite 106.

So bearbeiten Sie Globalkonfigurationswerte:

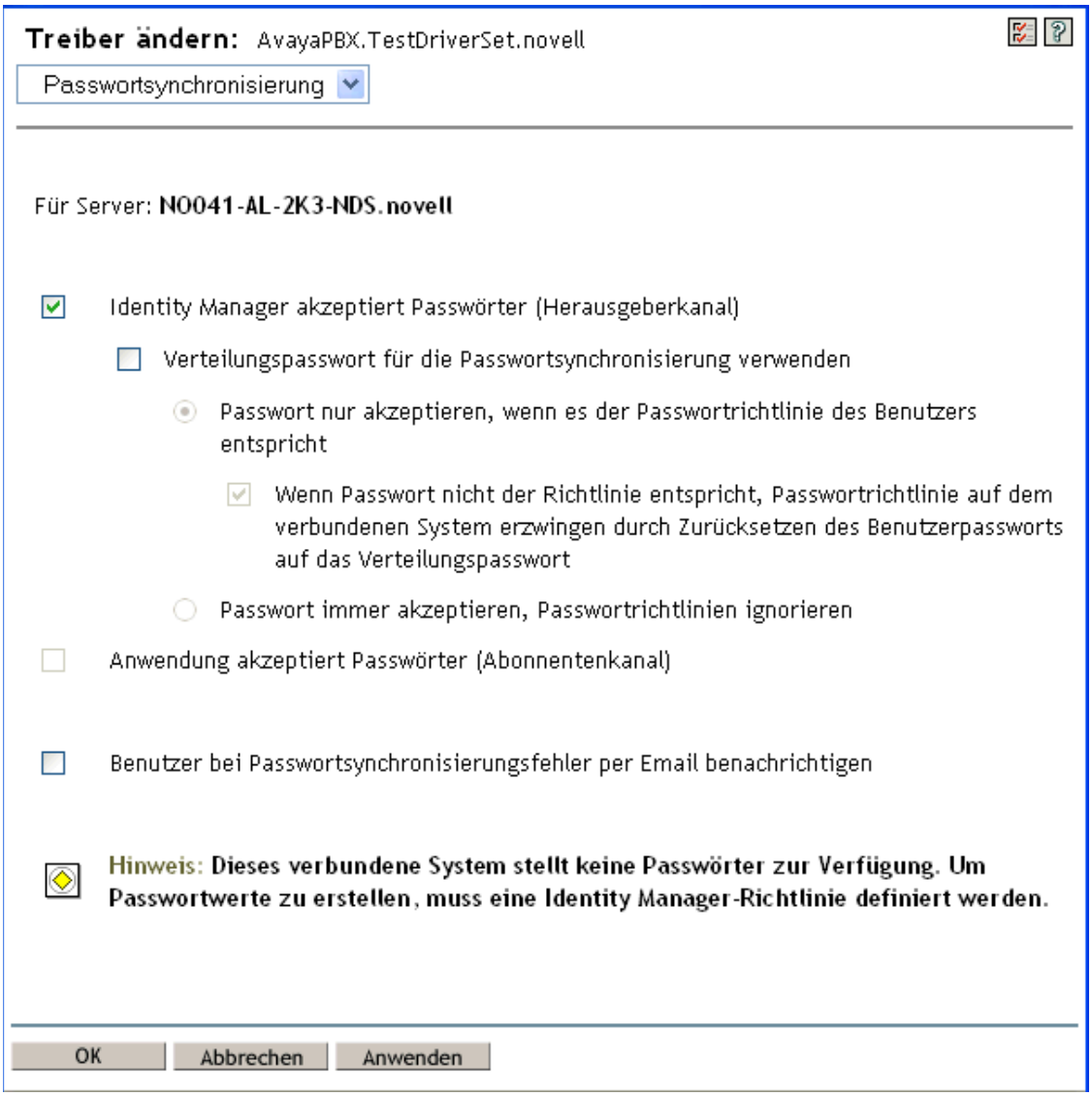
1. Klicken Sie in iManager auf *Passwörter* > *Passwortsynchronisierung*.
2. Suchen Sie nach einem Treiber.

   Nachdem Sie angegeben haben, wo Sie nach Treibern des verbundenen Systems suchen möchten, wird in iManager eine Übersicht über die verfügbaren Einstellungen für den Passwort-Transfer zwischen allen gefundenen Systemtreibern und iManager angezeigt.



3. Klicken Sie zum Anzeigen der Einstellungen auf einen Treibernamen.

Auf der Seite „Treiber ändern“ werden die Globalkonfigurationswerte für die Passwortsynchronisierung angezeigt.



Wenn eine Option auf dieser Seite grau angezeigt wird, wird die entsprechende Option nicht vom verbundenen System unterstützt.

4 Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf *OK*.

Hinweis: Sie können Globalkonfigurationswerte separat für jeden Treiber festlegen. Globalkonfigurationswerte für einen bestimmten Treiber haben Vorrang vor den Werten des Treibersatzes. Durch die treiberspezifische Festlegung der Werte kann der Datenaustausch differenzierter gesteuert werden. Auf dieser Seite werden nur die für den jeweiligen Treiber vorhandenen Globalkonfigurationswerte angezeigt.

Wenn Sie Globalkonfigurationswerte für das Treibersatzobjekt festlegen, werden diese Werte von einem Treiber im betreffenden Treibersatz geerbt, wenn der Treiber über keine eigenen Werte verfügt. Wenn der Treiber keine eigenen Werte besitzt und die Globalkonfigurationswerte aus dem Treibersatz erbt, werden diese nicht in iManager angezeigt. Obwohl iManager geerbte

Globalkonfigurationswerte nicht anzeigt, werden diese dennoch von den Passwortsynchronisierungsrichtlinien berücksichtigt.

5.3.4 In der Treiberkonfiguration benötigte Richtlinien

Die Identity Manager-Richtlinien der Herausgeber- und Abonnentenkanäle der einzelnen Treiber steuern den Passwort-Transfer auf Grundlage der zuvor erläuterten Einstellungen in den Globalkonfigurationsvariablen. Diese Richtlinien sind Bestandteil der Treiberkonfigurationen in Identity Manager.

Wenn Sie eine vorhandene Treiberkonfiguration nicht ersetzen, sondern aktualisieren, müssen Sie die Konfiguration um bestimmte Richtlinien ergänzen. Weitere Informationen finden Sie in Abschnitt 5.7, „Upgrade bestehender Treiberkonfigurationen zur Unterstützung der Passwortsynchronisierung“, auf Seite 106. Damit die Passwortsynchronisierung funktioniert, müssen sich diese Richtlinien in der Treiberkonfiguration an der richtigen Stelle befinden.

- „Im Herausgeber-Befehlsumwandlungssatz benötigte Richtlinien“ auf Seite 94
- „Im Herausgeber-Eingabetransformationsrichtliniensatz benötigte Richtlinien“ auf Seite 97
- „Im Richtliniensatz für Abonnenten-Befehlsumwandlung benötigte Richtlinien“ auf Seite 97
- „Im Abonnenten-Ausgabetransformationsrichtliniensatz benötigte Richtlinien“ auf Seite 98

Im Herausgeber-Befehlsumwandlungssatz benötigte Richtlinien

Die in der Spalte „Name der Passwortsynchronisierungsrichtlinie“ aufgeführten Richtlinien müssen in der angegebenen Reihenfolge vorhanden sein. Zudem müssen diese als letzte Richtlinien im Richtliniensatz für Herausgeber-Befehlsumwandlungen enthalten sein.

Tabelle 5-7 *Im Herausgeber-Befehlsumwandlungssatz benötigte Richtlinien*

Position in der Treiberkonfiguration	Name der Passwortsynchronisierungsrichtlinie	Auswirkung der Richtlinie
Herausgeber-Befehlsumwandlung	Password(Pub)-Default Password Policy	Ergänzt ein Add-Objekt um ein Standardpasswort, wenn das Add-Objekt kein Passwort enthält. Diese Richtlinie und die Richtlinie „Password(Sub)-Default Password“ sind die einzigen Richtlinien, die geändert oder entfernt werden können. Damit die Passwortsynchronisierung ordnungsgemäß funktioniert, sollten die anderen Richtlinien unverändert verwendet werden.
	Password(Pub)-Check Password GCV	Stellt durch eine GCV-Prüfung (GVC = „Global Configuration Value“, globaler Konfigurationswert) fest, ob Sie Identity Manager so konfiguriert haben, dass Passwörter von diesem verbundenen System akzeptiert werden. Wenn nicht, werden sämtliche Passwortelemente ausgeschlossen. Der Name des GCV lautet „enable-password-publish“ und der Anzeigename lautet *Identity Manager akzeptiert Passwörter von der Anwendung*.
	Password(Pub)-Publish Distribution Password	Wandelt das <password>-Element so um, dass es die Aktualisierung des universellen Passworts zulässt. Diese Richtlinie verwendet folgende GCVs: • publish-password-to-dp • enforce-password-policy
	Password(Pub)-Publish NDS Password	Lässt das <password>-Element durch, wenn Sie festgelegt haben, dass das NDS-Passwort aktualisiert werden soll. Wenn nicht, wird das <password>-Element ausgeschlossen. Diese Richtlinie verwendet den GCV „publish-password-to-nds“.
	Password(Pub)-Add Password Payload	Fügt Nutzlastdaten ein, die in der Engine zum Zwecke der Email-Benachrichtigung durchgereicht werden.

Position in der Treiberkonfiguration	Name der Passwortsynchronisierungsrichtlinie	Auswirkung der Richtlinie
	Password(Sub)-Add Password Payload	Fügt Nutzlastdaten ein, die in der Engine zum Zwecke der Email-Benachrichtigung durchgereicht werden.

Im Herausgeber-Eingabetransformationsrichtliniensatz benötigte Richtlinien

Wir empfehlen, die Email-Benachrichtigungsrichtlinie „Password(Pub)-Sub“ an die letzte Stelle zu setzen, wenn die Eingabetransformation mehrere Richtlinien enthält.

Tabelle 5-8 *Im Herausgeber-Eingabetransformationsrichtliniensatz benötigte Richtlinien*

Position in der Treiberkonfiguration	Name der Passwortsynchronisierungsrichtlinie	Auswirkung der Richtlinie
Herausgeber-Eingabetransformation	Password(Pub)-Sub Email Notifications	Wenn die Passwort-Nutzlastdaten durchgereicht werden und der Status ein Problem erkennen lässt, wird eine Email an den Benutzer gesendet. Die Email wird an die im Attribut für die Internet-Email-Adresse in eDirectory enthaltene Email-Adresse des Benutzers gesendet. Diese Richtlinie verwendet den GCV „notify-user-on-password-dist-failure“, um festzustellen, ob Email-Benachrichtigungen gesendet werden müssen.

Im Richtliniensatz für Abonnenten-Befehlsumwandlung benötigte Richtlinien

Die in der Spalte „Name der Passwortsynchronisierungsrichtlinie“ aufgeführten Richtlinien müssen in der angegebenen Reihenfolge vorhanden sein. Zudem müssen diese als letzte Richtlinien im Richtliniensatz für Abonnenten-Befehlsumwandlungen enthalten sein.

Tabelle 5-9 *Im Richtliniensatz für Abonnenten-Befehlsumwandlung benötigte Richtlinien*

Position in der Treiberkonfiguration	Name der Passwortsynchronisierungsrichtlinie	Auswirkung der Richtlinie
Abonnenten-Befehlsumwandlung	Password(Sub)-Transform Distribution Password	Wandelt das universelle Passwort in ein <password>-Element um.
	Password(Sub)-Default Password Policy	Ergänzt ein Add-Objekt um ein Standardpasswort, wenn das Add-Objekt kein Passwort enthält. Diese Richtlinie und die Password(Pub)-Standardpasswort-Richtlinie sind die einzigen Richtlinien, die geändert oder entfernt werden können. Damit die Passwortsynchronisierung einwandfrei funktioniert, sollten die anderen Richtlinien unverändert verwendet werden.
	Password(Sub)-Check Password GCV	Stellt durch eine GCV-Prüfung fest, ob Sie festgelegt haben, dass das verbundene System Passwörter akzeptieren soll. Wenn nicht, werden sämtliche Passwortelemente ausgeschlossen. Der Name des GCV lautet „enable-password-subscribe“ und der Anzeigename lautet *Anwendung akzeptiert Passwörter von Identity Manager*.
	Password(Sub)-Add Password Payload	Fügt Passwortnutzlastdaten ein, die in der Engine zum Zwecke der Email-Benachrichtigung durchgereicht werden.

Im Abonnenten-Ausgabetransformationsrichtliniensatz benötigte Richtlinien

Wir empfehlen, die Email-Benachrichtigungsrichtlinie „Password(Sub)-Pub“ an die letzte Stelle zu setzen, wenn die Ausgabetransformation mehrere Richtlinien enthält.

Tabelle 5-10 Im Abonnenten-Ausgabetransformationsrichtliniensatz benötigte Richtlinien

Position in der Treiberkonfiguration	Name der Passwortsynchronisierungsrichtlinie	Auswirkung der Richtlinie
Abonnenten-Ausgabetransformation	Password(Sub)-Pub Email Notifications	Wenn die Passwort-Nutzlastdaten durchgereicht werden und der Status ein Problem erkennen lässt, wird eine Email an den Benutzer gesendet. Diese Richtlinie verwendet den GCV „notify-user-on-password-dist-failure“, um festzustellen, ob Email-Benachrichtigungen gesendet werden müssen.

5.3.5 Filter, die auf dem verbundenen System installiert sein müssen, zum Erfassen von Passwörtern

Für AD, NT Domain und NIS müssen Filter installiert werden, um das Passwort des Benutzers erfassen zu können.

Weitere Informationen hierzu finden Sie in Abschnitt 5.9, „Einrichten von Passwortfiltern“, auf Seite 151.

5.3.6 Für Benutzer erstellte NMAS-Passwortrichtlinien

Einige Funktionen der Passwortsynchronisierung können auch ohne universelles Passwort verwendet werden. Dennoch muss das universelle Passwort durch Passwortrichtlinien für die Benutzer aktiviert werden. In einer Passwortrichtlinie können Sie auch erweiterte Passwortregeln erstellen und festlegen, ob bestehende Passwörter von Benutzern auf Regelkonformität überprüft werden sollen.

Damit Sie die Passwortsynchronisierung in Identity Manager nutzen können, benötigen Sie Kenntnisse über Passwortrichtlinien. Eine Erklärung der Passwortrichtlinien finden Sie im Kapitel „Managing Passwords by Using Password Policies“ im *Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung).

5.3.7 NMAS-Anmeldemethoden

Für bestimmte Situationen muss die NMAS-Methode der Anmeldung mit einfachem Passwort eingerichtet sein, um Passwortfunktionen nutzen zu können. Diese Methode wird beispielsweise von LDAP benötigt.

Informationen zu Anmeldemethoden finden Sie im Administrationshandbuch *Novell Modular Authentication Services (NMAS) 3.0* (http://www.novell.com/documentation/nmas30/index.html).

5.4 Vorbereitungen zur Nutzung der Identity Manager-Passwortsynchronisierung und des universellen Passworts

5.4.1 Umstellen der Benutzer vom NDS-Passwort auf das universelle Passwort

Wenn Sie das universelle Passwort mit einer Passwortrichtlinie für eine Benutzergruppe aktivieren, muss das universelle Passwort für jeden Benutzer hinterlegt werden.

Wenn Sie das NDS-Passwort bisher über die Passwortsynchronisierung aktualisiert haben, müssen Sie für die Umstellung der Benutzerpasswörter einige Vorbereitungen treffen. Durch eine der folgenden Maßnahmen können Sie bewirken, dass die Benutzer ein universelles Passwort erstellen und somit den Übergang zur Verwendung des universellen Passworts ermöglichen:

- Wenn Sie den Novell Client verwenden, stellen Sie den Novell Client bereit, der das universelle Passwort unterstützt.

  Der Novell Client wird zur Identity Manager-Passwortsynchronisierung nicht benötigt.

  Nachdem Sie den Novell Client bereitgestellt haben, wird das NDS-Passwort bei der nächsten Anmeldung eines Benutzers am Novell Client noch vor der Hash-Kodierung abgefangen und als universelles Passwort hinterlegt. (Siehe “Planning Login and Change Password Methods for your Users” („Planung von Methoden zur Anmeldung und Passwortänderung für Benutzer“) im „Password Management Administration Guide“ [Administrationshandbuch zur Passwortverwaltung]).
- Wenn Sie den Novell Client nicht verwenden, fordern Sie die Benutzer auf, sich über die iManager-Selbstbedienungskonsole anzumelden. Durch diese Anmeldemethode wird das universelle Passwort hinterlegt. Wechseln Sie zum Zugriff auf die iManager-Selbstbedienungskonsole in das Verzeichnis /nps auf dem iManager-Server. Beispiel: https://www.myiManager.com/nps.
- Fordern Sie die Benutzer auf, sich über einen beliebigen Service anzumelden, der die Authentifizierung über einen LDAP-Server durchführt, der das universelle Passwort unterstützt. Die Anmeldung kann beispielsweise über ein Firmenportal erfolgen.

5.4.2 Hilfe für Benutzer beim Ändern von Passwörtern

Wenn ein Benutzer ein Passwort in iManager, in der iManager-Selbstbedienungskonsole oder im Novell Client ändert, werden die erweiterten Passwortregeln aus der NMAS-Passwortrichtlinie angezeigt. Dadurch kann der Benutzer problemlos ein regelkonformes Passwort erstellen.

Je nach Konfiguration des Passwort-Transfers kann ein Benutzer ein Passwort auf einem verbundenen System ändern, woraufhin das Passwort mit Identity Manager und anderen

verbundenen Systemen synchronisiert wird. Die erweiterten Passwortregeln werden auf den verbundenen Systemen jedoch nicht angezeigt, wenn der Benutzer ein Passwort ändert.

Wenn Sie die erweiterten Passwortregeln erzwingen und unzulässige Passwörter verhindern möchten, sollten Sie die Benutzer anweisen, das Passwort ausschließlich über die iManager-Selbstbedienungskonsole oder im Novell Client zu ändern. Stellen Sie zumindest sicher, dass die erweiterten Passwortregeln von den Benutzern problemlos eingesehen werden können.

Auf einem verbundenen System kann der Benutzer das Passwort ändern, ohne dass die Regeln der Passwortrichtlinie angezeigt werden. Daher ist es möglich, dass der Benutzer die Regeln nicht genau kennt. Bei der Änderung des Passworts sind nur die Richtlinien des verbundenen Systems obligatorisch. Je nach den geltenden Identity Manager-Einstellungen können die folgenden Probleme auftreten, wenn ein Benutzer auf einem verbundenen System ein nicht regelkonformes Passwort erstellt:

- Wenn Sie die Einstellung aktiviert haben, mit der die Richtlinie von verbundenen Systemen an Identity Manager übertragene Passwörter erzwingt, erfolgt keine Synchronisierung des neuen Passwort des Benutzers mit dem Identitätsdepot. Wenn Sie Identity Manager so konfiguriert haben, dass der Benutzer bei Fehlern informiert wird, wird dem Benutzer per Email mitgeteilt, dass das Passwort nicht synchronisiert werden konnte.
- Wenn Sie Identity Manager darüber hinaus so konfiguriert haben, dass nicht regelkonforme Passwörter auf verbundenen Systemen ersetzt werden, kann sich der Benutzer mit dem von ihm gewählten neuen Passwort nicht auf dem verbundenen System anmelden.

  Identity Manager setzt das Passwort auf dem verbundenen System auf das Verteilungspasswort zurück; bei dem es sich in der Regel um das letzte vom Benutzer erstellte, regelkonforme Passwort handelt.

5.4.3 Vorbereitungen für die Verwendung des universellen Passworts

Eine Beschreibung der Vorbereitungen für die Verwendung des universellen Passworts finden Sie im Kapitel “Deploying Universal Password” im *Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung). Einen Großteil der benötigten Informationen finden Sie in diesem Kapitel.

Wichtig in diesem Zusammenhang ist auch Folgendes:

- Für die Verwendung des universellen Passworts wird eDirectory 8.7.1 oder höher benötigt. NetWare® 6.5 wird nicht benötigt.
- Für die Identity Manager-Passwortsynchronisierung wird sowohl das universelle Passwort als auch das Verteilungspasswort benötigt. Das Verteilungspasswort ist das Depot, von dem aus Identity Manager Passwörter an verbundene Systeme verteilt. Wie beim universellen Passwort können auch für das Verteilungspasswort NMAS-Richtlinien erzwungen werden.
- Die mit Identity Manager gelieferten iManager-Plugins beinhalten auch Plugins für die Passwortverwaltung. Mit diesen Plugins können Sie Passwortrichtlinien erstellen und festlegen, wie das universelle Passwort mit dem NDS-Passwort, dem einfachen Passwort und dem Verteilungspasswort synchronisiert werden soll.

  Diese Plugins treten an die Stelle der mit NetWare 6.5 gelieferten Plugins für das universelle Passwort. Eine Beschreibung hierzu finden Sie im Kapitel “Managing Passwords by Using Password Policies” im *Password Management Administration Guide* (http://www.novell.com/

documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung).

- eDirectory 8.6.2 kann nicht für den Baum verwendet werden, den Identity Manager verwendet. eDirectory 8.6.2 wird jedoch von einer Teilmenge der Funktionen für die Passwortsynchronisierung unterstützt. Sie können eDirectory 8.6.2 also für andere Bäume verwenden, wenn Sie sich mit der Aktualisierung des gesamten Systems noch etwas Zeit lassen möchten.
- Eine Möglichkeit, die Belastung zu reduzieren, die durch das Upgraden der Software zur Unterstützung des universellen Passworts entsteht, besteht darin, für Identity Manager einen separaten Baum als Identitätsdepot anzulegen. Viele Umgebungen verwenden bereits ein Identitätsdepot für Identity Manager und die Treiber.
- Das universelle Passwort bietet die Möglichkeit, Passwortrichtlinien durchzusetzen und Sonderzeichen zu verwenden, die von früheren Werkzeugen für die Passwortverwaltung nicht unterstützt wurden.
- Es ist sehr wichtig, dass der Novell Client und andere Dienstprogramme aktualisiert werden, damit das NDS-Passwort und das universelle Passwort stets synchron bleiben und sich keine „Passwortdivergenz“ einstellt. Siehe „Planning Login and Change Password Methods for your Users (Planung von Methoden zur Anmeldung und Passwortänderung für Benutzer)“ im *Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung).
- Die neueste Version des Novell Client unterstützt das universelle Passwort, kann für alle Benutzer bei der erstmaligen Aktivierung dieser Option ein universelles Passwort hinterlegen und NMAS-Passwortrichtlinien anzeigen und erzwingen, wenn Benutzer ihre Passwörter ändern.
- Auf einem verbundenen System werden die von Ihnen in einer Passwortrichtlinie erstellten erweiterten Passwortregeln nicht angezeigt. Dies ist auch beim Novell Client noch nicht der Fall, die Passwortregeln werden von ihm jedoch erzwungen.

  Es empfiehlt sich, die Benutzer anzuweisen, das Passwort ausschließlich über die iManager-Selbstbedienungskonsole zu ändern.

  Wenn Sie es den Benutzern erlauben, Passwörter auf einem verbundenen System oder unter Verwendung der neuesten Version des Novell Client zu ändern, können Sie die Benutzer beim Erstellen regelkonformer Passwörter unterstützen, indem Sie sicherstellen, dass die Regeln der Passwortrichtlinie von den Benutzern problemlos eingesehen werden können.
- Stellen Sie sicher, dass die Administratoren und Helpdesk-Mitarbeiter darüber Bescheid wissen, dass ConsoleOne® das universelle Passwort nur unterstützt, wenn es auf einem NetWare® 6.5-Server oder höher eingesetzt wird, oder wenn es auf einem Computer verwendet wird, auf dem der neueste Novell Client installiert ist.
- Stellen Sie sicher, dass den Administratoren und Helpdesk-Mitarbeitern die Besonderheiten bei der Verwendung von Dienstprogrammen bekannt sind, die nur NDS-Passwörter unterstützen. Solche Dienstprogramme können zur Anmeldung verwendet werden, nicht jedoch zum Ändern von Passwörtern. Dadurch kann eine Passwortdivergenz vermieden werden.

  Der *Novell Modular Authentication Services (NMAS) 3.0 Administration Guide* (http://www.novell.com/documentation/nmas30/index.html) (Novell Modular Authentication Services 3.0 Administrationshandbuch) enthält einen Verweis auf eine TID, die Informationen zur Unterstützung des universellen Passworts durch bestimmte Dienstprogramme enthält.

5.4.4 Abgleichen der Container

NMAS-Passwortrichtlinien werden baumspezifisch zugewiesen. Die Passwortsynchronisierung hingegen wird pro Treiber konfiguriert. Treiber werden serverspezifisch installiert und können nur Benutzer verwalten, die sich in einer Master- oder Lese-/Schreibreproduktion befinden.

Damit eine Passwortsynchronisierung die gewünschten Ergebnisse liefert, müssen Sie sicherstellen, dass die Container in der Master- oder Lese-/Schreibreproduktion auf dem Server, auf dem die Treiber für die Passwortsynchronisierung aktiv sind, den Containern entsprechen, für die Sie Passwortrichtlinien mit aktiviertem universellem Passwort zugewiesen haben. Durch Zuweisung einer Passwortrichtlinie an den Partitionsstammcontainer kann sichergestellt werden, dass die Passwortrichtlinie allen in diesem Container und seinen Untercontainern enthaltenen Benutzern zugewiesen wird.

5.4.5 Einrichten der Email-Benachrichtigung

Führen Sie die folgenden Schritte aus, wenn Sie die Email-Benachrichtigungsfunktion nutzen möchten:

- Richten Sie den Email-Server mit der Aufgabe „Benachrichtigungskonfiguration“ in iManager ein.
- Ändern Sie gegebenenfalls die Email-Schablonen mit der Aufgabe „Benachrichtigungskonfiguration“ in iManager.
- Stellen Sie sicher, dass das Attribut „Internet-Email-Adresse“ für die im Identitätsdepot enthaltenen Benutzer hinterlegt wurde.

Befolgen Sie die Anweisungen in Abschnitt 5.12, „Konfigurieren der Email-Benachrichtigung“, auf Seite 156.

5.5 Konfigurieren und Synchronisieren eines neuen Treibers

Wenn Sie Version 1.0 des Passwortsynchronisierungsmoduls in Ihrer Umgebung noch nicht eingesetzt haben und einen Treiber erstellen oder eine vorhandene Konfiguration durch eine neue Identity Manager-Konfiguration ersetzen möchten, müssen Sie zunächst die Identity Manager-Passwortsynchronisierung einrichten.

1. Überzeugen Sie sich davon, dass die Verwendung des universellen Passworts in Ihrer Umgebung möglich ist.

   Weitere Informationen hierzu finden Sie in Abschnitt 5.4, „Vorbereitungen zur Nutzung der Identity Manager-Passwortsynchronisierung und des universellen Passworts“, auf Seite 100.

2. Erstellen Sie einen Treiber oder ersetzen Sie die Konfiguration eines bereits vorhandenen Treibers durch die Konfiguration von Identity Manager 3.

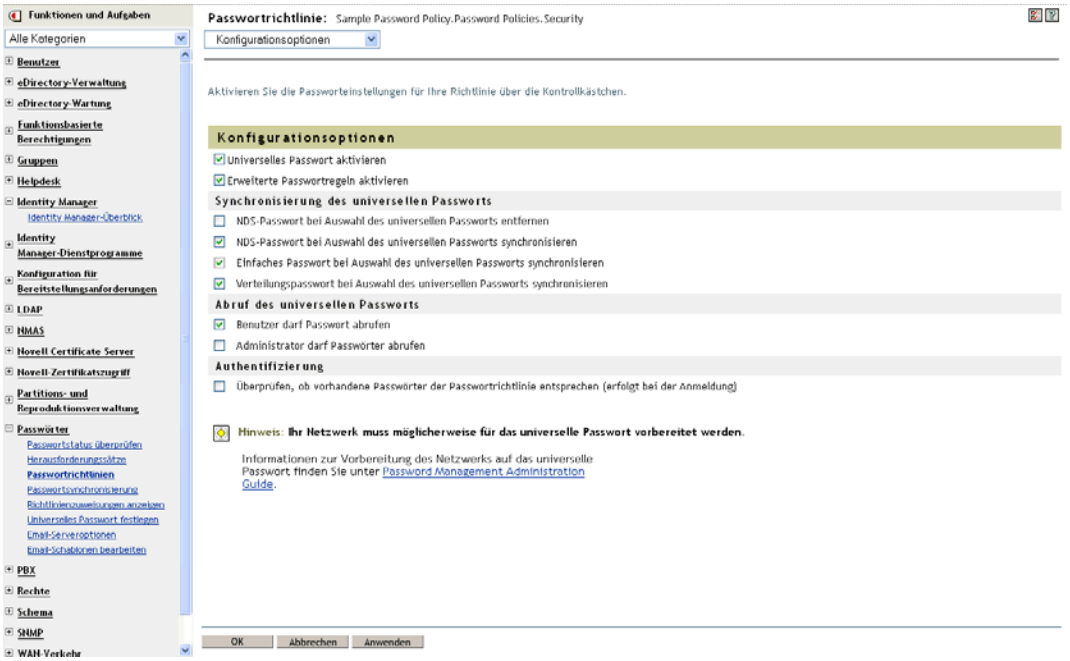
   Die Identity Manager-Konfigurationen enthalten die Identity Manager-Richtlinien und weitere Elemente, die für die Identity Manager-Passwortsynchronisierung erforderlich sind. Informationen zum Importieren der neuen Beispiel-Treiberkonfigurationen finden Sie in den entsprechenden Treiberhandbüchern von Identity Manager (http://www.novell.com/documentation/beta/dirxmldrivers).

3 Aktivieren Sie das universelle Passwort für Benutzer, indem Sie NMAS-Passwortrichtlinien mit aktiviertem universellem Passwort erstellen.

Informationen hierzu finden Sie im Kapitel “Creating Password Policies” im *Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung). Beachten Sie bitte die zusätzlichen Arbeitsschritte im Kapitel “(NetWare 6.5 Only) Re-Creating Universal Password Assignments” des *Password Management Administration Guide* (Administrationshandbuch zur Passwortverwaltung), wenn Sie das universelle Passwort bisher mit NetWare 6.5 verwendet haben.

Zur Vereinfachung der Administration empfiehlt es sich, Passwortrichtlinien einer möglichst hohen Ebene im Baum zuzuweisen.

Auf der Seite „Konfigurationsoptionen“ können Sie festlegen, wie NMAS die verschiedenen Passwortarten synchronisieren soll.



Szenarios für die Verwendung der Passwortsynchronisierung und das Einbinden von Identity Manager-Passwortrichtlinien finden Sie in Abschnitt 5.8, „Implementierung der Passwortsynchronisierung“, auf Seite 115 sowie in der Online-Hilfe.

4 (Nur für Active Directory, NIS oder NT Domain) Wenn die verbundenen Systeme die Benutzerpasswörter an Identity Manager übergeben sollen, müssen Sie neue Passwort-Synchronisierungsfilter installieren und konfigurieren.

Weitere Informationen hierzu finden Sie in den Implementierungshandbüchern der einzelnen Treiber unter Identity Manager Drivers (http://www.novell.com/documentation/lg/dirxmldrivers/index.html).

5 Überzeugen Sie sich davon, dass der Passwort-Transfer auf allen verbundenen Systemen wie gewünscht konfiguriert ist.

5a Klicken Sie in iManager auf *Passwörter* > *Passwortsynchronisierung* und suchen Sie die Treiber für die verbundenen Systeme, die Sie verwalten möchten.

5b Überprüfen Sie die aktuellen Einstellungen für den Passwort-Transfer.

Hierbei handelt es sich um eine grafische Benutzeroberfläche für die Globalkonfigurationswerte (GCV). Klicken Sie zum Bearbeiten eines GCV auf den Namen eines Treibers. Sie können die folgenden Einstellungen bearbeiten:

- Entgegennahme von Passwörtern aus diesem System durch Identity Manager.
- Das Passwort, das von Identity Manager aktualisiert werden soll: direkte Aktualisierung des universellen Passworts oder direkte Aktualisierung des Verteilungspassworts.

  Identity Manager kontrolliert den Einstiegspunkt (d. h. das von Identity Manager aktualisierte Passwort). NMAS kontrolliert in Abhängigkeit von den Einstellungen in den Konfigurationsoptionen den Passwort-Transfer zwischen den einzelnen Passwortarten. Beachten Sie hierzu die Abbildung zu Schritt 3 auf Seite 104.
- Das Erzwingen der Passwortrichtlinie für den Benutzer bei Passwortänderungen, die an Identity Manager übergeben werden.
- Das Erzwingen der Passwortrichtlinie für den Benutzer auf dem verbundenen System durch Zurücksetzen von Passwörtern, die nicht regelkonform sind.
- Die Annahme von Passwörtern durch dieses verbundene System.
- Das Senden von Email-Benachrichtigungen bei nicht erfolgter Passwortsynchronisierung.

6 Testen Sie die Passwortsynchronisierung.

- Überzeugen Sie sich davon, dass das Identity Manager-Passwort an die von Ihnen angegebenen Systeme verteilt wird.
- Überzeugen Sie sich davon, dass die von Ihnen angegebenen verbundenen Systeme Passwörter gegenüber Identity Manager veröffentlichen.

Tipps zur Problemlösung finden Sie in Abschnitt 5.8, „Implementierung der Passwortsynchronisierung“, auf Seite 115.

5.6 Upgrade von Version 1.0 der Passwortsynchronisierung

Dieses Verfahren ist nur für vorhandene Identity Manager-Treiber für Active Directory und NT Domain erforderlich, die zusammen mit Version 1.0 der Passwortsynchronisierung verwendet werden.

Die genaue Einhaltung dieses Verfahrens beim Upgraden von Version 1.0 der Passwortsynchronisierung ist von größter Wichtigkeit.

Eine entsprechende Anleitung finden Sie in den Treiber-Implementierungshandbüchern zu den Identity Manager-Treibern für Active Directory und NT Domain unter Identity Manager Drivers (http://www.novell.com/documentation/dirxmldrivers/index.html).

5.7 Upgrade bestehender Treiberkonfigurationen zur Unterstützung der Passwortsynchronisierung

In diesem Abschnitt wird erklärt, wie bestehende Treiberkonfigurationen um Unterstützung für die Identity Manager-Passwortsynchronisierung erweitert werden können, anstatt diese Treiberkonfigurationen durch die Identity Manager-Beispielkonfigurationen zu ersetzen.

Die Unterstützung dieser Funktion muss für jeden Treiber hinzugefügt werden, der an der Passwortsynchronisierung teilnehmen soll. Dazu importieren Sie eine “Overlay”-Konfigurationsdatei, um die Richtlinien, das Treibermanifest und die GCVs gleichzeitig hinzuzufügen.

Nach dem Hinzufügen der Richtlinien, des Treibermanifests und der GCVs müssen Sie das Attribut „nspmDistributionPassword“ zum Treiberfilter hinzufügen.

Wichtig: Befolgen Sie beim Upgrade eines mit Version 1.0 der Passwortsynchronisierung verwendeten Identity Manager-Treibers für AD oder NT Domain die Upgrade-Anleitung in den Implementierungshandbüchern zu den Identity Manager-Treibern für Active Directory und NT Domain unter Identity Manager Drivers (http://www.novell.com/documentation/dirxmldrivers/index.html).

Die in diesem Verfahren hinzugefügten Richtlinien ermöglichen die Passwortsynchronisierung über das universelle Passwort und das Verteilungspasswort. Wenn Sie den Identity Manager-Treiber lediglich zum Synchronisieren des NDS-Passworts verwenden, sollten Sie die Richtlinien in der Identity Manager-Treiberkonfiguration nicht verwenden. Das NDS-Passwort wird nicht über diese Richtlinien, sondern über Attribute für den privaten und öffentlichen Schlüssel synchronisiert (siehe Abschnitt 5.8.2, „Szenario 1: Synchronisierung zwischen zwei Identitätsdepots über das NDS-Passwort“, auf Seite 117).

Voraussetzungen

- ❑ Erstellen Sie mithilfe des Assistenten zum Exportieren von Treibern eine Sicherung Ihrer vorhandenen Treiber.
- ❑ Stellen Sie sicher, dass Sie das neue Treiberschnittstellenmodul installiert haben.

  Bestimmte Funktionen der Passwortsynchronisierung (z. B. „Passwortstatus überprüfen“) funktionieren ohne das neue Identity Manager-Treiberschnittstellenmodul nicht.

  Wichtig: Wenn Sie einen Identity Manager-Treiber für AD oder NT Domain upgraden möchten und dieser Treiber in Verbindung mit Version 1.0 der Passwortsynchronisierung verwendet wird, sollten Sie das Treiberschnittstellenmodul erst installieren, nachdem Sie sich die Upgrade-Anleitung durchgelesen haben. Befolgen Sie die Upgrade-Anleitung in den Treiber-Implementierungshandbüchern zu den Identity Manager-Treibern für Active Directory

und NT Domain unter Identity Manager Drivers (http://www.novell.com/documentation/dirxmldrivers/index.html).

5.7.1 1. Schritt: Treiber in das Format von Identity Manager 3 konvertieren

1 Überzeugen Sie sich davon, dass die Verwendung des universellen Passworts in Ihrer Umgebung problemlos möglich ist.

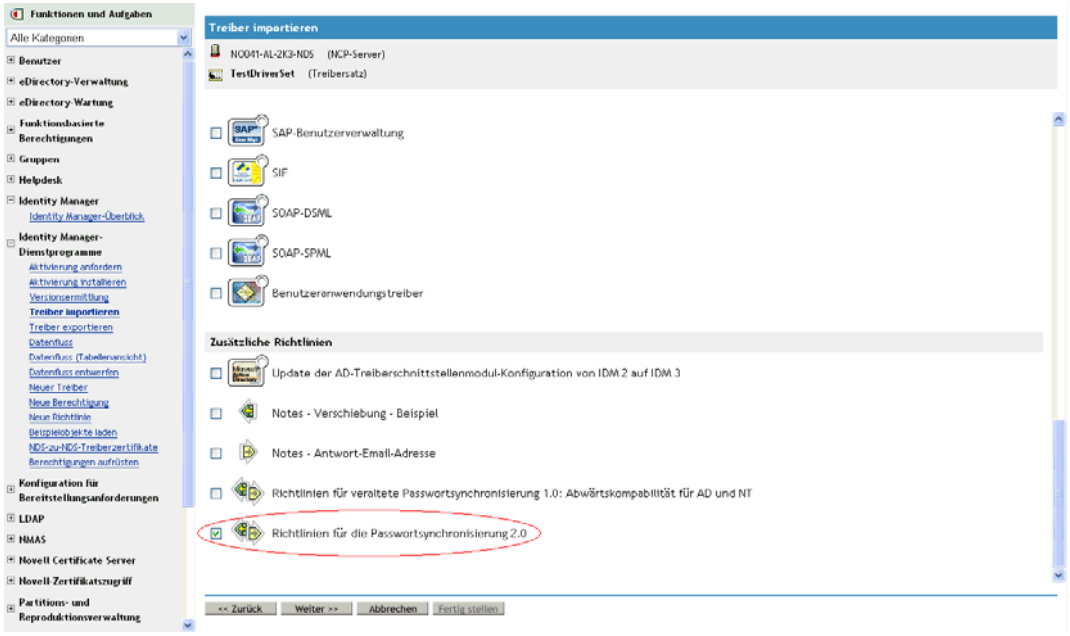
Weitere Informationen hierzu finden Sie in Abschnitt 5.4, „Vorbereitungen zur Nutzung der Identity Manager-Passwortsynchronisierung und des universellen Passworts“, auf Seite 100.

Beachten Sie bei Verwendung von DirXML® 1.1a Abschnitt 2.3, „Upgrade einer Treiberkonfiguration von DirXML 1.1 auf ein Identity Manager-Format“, auf Seite 21.

2 Klicken Sie in iManager auf *Identity Manager-Dienstprogramme* > *Treiber importieren*.

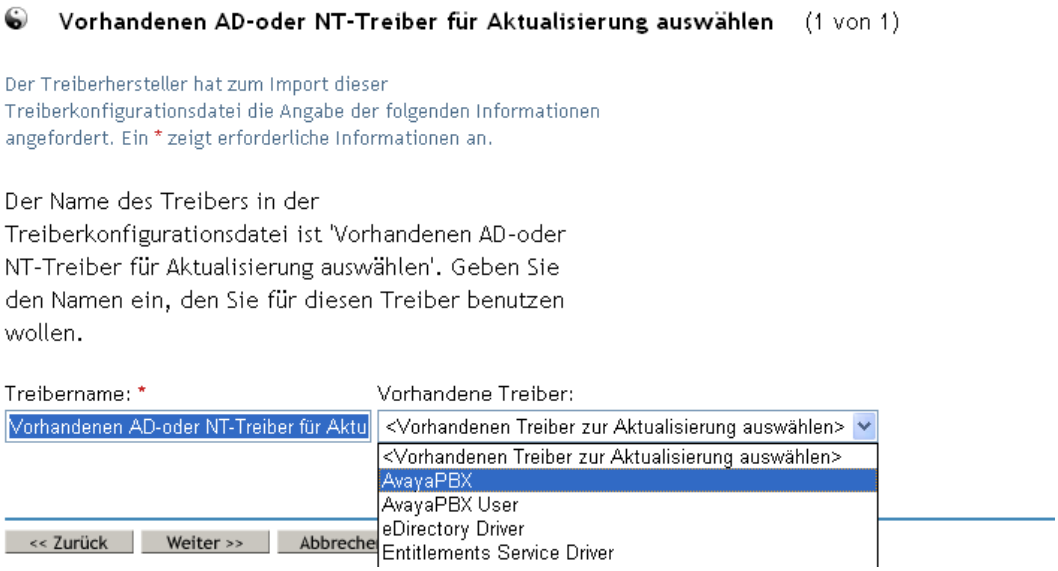
3 Wählen Sie den Treibersatz aus, in dem sich der vorhandene Treiber befindet, und klicken Sie auf *Weiter*.

4 Blättern Sie in der Liste der Treiberkonfigurationen zum Eintrag *Zusätzliche Richtlinien* und wählen Sie nur *Richtlinien für die Passwortsynchronisierung 2.0* aus.



5 Klicken Sie auf *Weiter*.

6 Wählen Sie im Dropdown-Listenfeld *Vorhandene Treiber* den Treiber aus, den Sie aktualisieren möchten.



7 Wählen Sie im Dropdown-Listenfeld *Verbundenes System* den Typ des verbundenen Systems aus.

Falls der Treibername im Dropdown-Listenfeld nicht angezeigt wird, klicken Sie auf *Andere Systeme*.

In Abhängigkeit vom Treibertyp fügt der Assistent zum Importieren von Treibern Einträge in das Treibermanifest ein, die über die Funktionen der Treiberkonfiguration und des verbundenen Systems Auskunft geben:

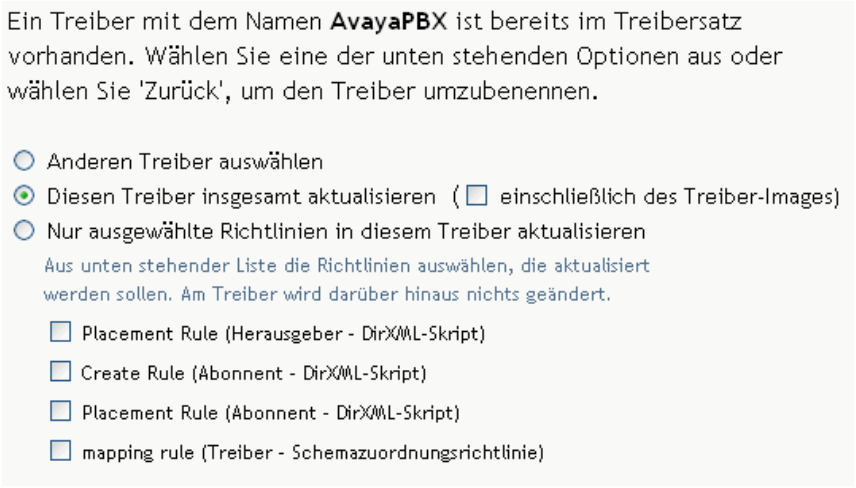
- Übergabe von Passwörtern vom verbundenen System an Identity Manager.

  Dies bezieht sich nur auf das tatsächliche Passwort auf dem verbundenen System, nicht aber auf ein Passwort, das mittels einer Formatvorlage erstellt werden kann. Dies ist nur bei AD, eDirectory und NIS möglich.

- Entgegennahme von Passwörtern aus Identity Manager durch das verbundene System.
- Die Überprüfung eines Passworts durch das verbundene System, um festzustellen, ob es mit dem Passwort in Identity Manager übereinstimmt.

Damit die Passwortsynchronisierungsrichtlinien funktionieren können, muss das Treibermanifest die richtigen Einträge enthalten. Das Treibermanifest gibt Auskunft über die kombinierten Funktionen des verbundenen Systems, des Identity Manager-Treiberschnittstellenmoduls und der Treiberkonfigurationsrichtlinien und sollte im Normalfall nicht vom Netzwerkverwalter bearbeitet werden.

8 Klicken Sie auf *Weiter*.



9 Falls Sie keine Treibermanifest- oder GCV-Werte speichern möchten, wählen Sie *Diesen Treiber insgesamt aktualisieren*.

Diese Option liefert das Treibermanifest, die Globalkonfigurationswerte (GCVs) und die Identity Manager-Richtlinien, die zur Passwortsynchronisierung benötigt werden.

Bereits vorhandene Werte werden vom Treibermanifest und den GCVs überschrieben. Da diese Treiberparameter in Identity Manager 2 neu waren, sollte ein DirXML 1.*x*-Treiber keine Werte enthalten, die überschrieben werden.

Durch die Passwortsynchronisierungsrichtlinien werden keine vorhandenen Richtlinienobjekte überschrieben. Diese werden lediglich zum Treiberobjekt hinzugefügt.

Hinweis: Falls Sie Treibermanifest- oder GCV-Werte speichern möchten, wählen Sie *Nur ausgewählte Richtlinien in diesem Treiber aktualisieren* und aktivieren Sie die Kontrollkästchen aller Richtlinien. Mit dieser Option werden die Passwortrichtlinien importiert, das Treibermanifest und die GCVs jedoch nicht geändert. Etwaige zusätzliche Werte müssen Sie manuell einfügen.

---

10 Klicken Sie auf *Weiter* und anschließend auf *Fertig stellen*, um den Assistenten abzuschließen.

Sie haben nun die neuen Richtlinien als Richtlinienobjekte unter dem Treiberobjekt erstellt, müssen diese aber noch in die Treiberkonfiguration einbinden. Dazu müssen Sie die einzelnen Richtlinien manuell an der richtigen Stelle in der Treiberkonfiguration auf dem Abonnenten- und Herausgeberkanal einfügen.

5.7.2 2. Schritt: Zur Treiberkonfiguration hinzufügen

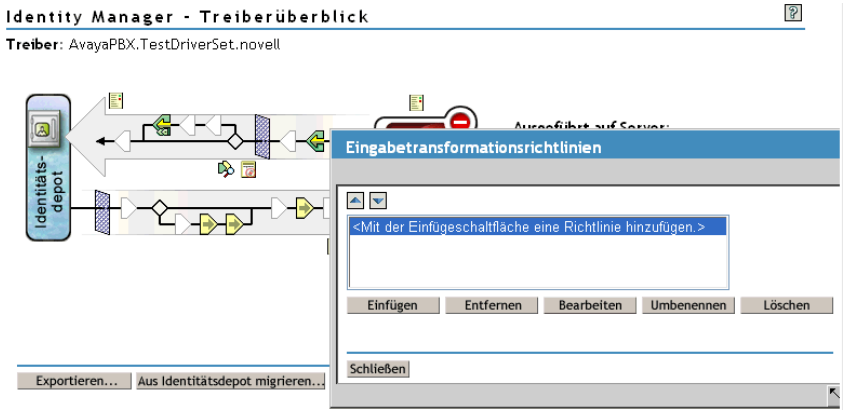
Eine Liste der hinzuzufügenden Richtlinien mit den entsprechenden Einfügepositionen finden Sie in Abschnitt 5.3.4, „In der Treiberkonfiguration benötigte Richtlinien“, auf Seite 94.

Fügen Sie die neuen Richtlinien nacheinander an den richtigen Stellen in der vorhandenen Treiberkonfiguration ein.

Sollte der Richtliniensatz mehrere Richtlinien enthalten, müssen diese Identity Manager-Passwortsynchronisierungsrichtlinien an letzter Stelle stehen.

Wiederholen Sie die folgenden Schritte für jede Richtlinie.

1. Wählen Sie *Identity Manager > Identity Manager-Überblick* und suchen Sie den Treibersatz, der den zu aktualisierenden Treiber enthält.
2. Klicken Sie auf den Treiber, den Sie soeben aktualisiert haben (z. B. AvayaPBX).
3. Klicken Sie auf das Symbol (z. B. „Befehlstransformationsrichtlinien“ auf dem Herausgeberkanal) für die Stelle, an der Sie eine der neuen Richtlinien einfügen möchten.



4. Klicken Sie auf „Einfügen“, um die neue Richtlinie hinzuzufügen.

5. Klicken Sie auf *Vorhandene Richtlinie verwenden*, suchen Sie das neue Richtlinienobjekt und klicken Sie auf *OK*.
6. Falls die Liste zu einer der neuen Richtlinien mehr als eine Richtlinie enthält, verwenden Sie die Pfeilschaltflächen , um die neuen Richtlinien an die richtige Stelle in der Liste zu verschieben.

   Achten Sie darauf, dass die Richtlinien in der in Abschnitt 5.3.4, „In der Treiberkonfiguration benötigte Richtlinien“, auf Seite 94 beschriebenen Reihenfolge aufgeführt werden.

5.7.3 3. Schritt: Filtereinstellungen ändern

1 Stellen Sie sicher, dass das Attribut „nspmDistributionPassword“ für die Objektklassen, für die Sie Passwörter synchronisieren möchten (z. B. „User“), mit den folgenden Einstellungen im Filter enthalten ist:

- Setzen Sie den Filter auf dem Herausgeberkanal für das Attribut *nspmDistributionPassword* auf *Ignorieren*.
- Setzen Sie den Filter auf dem Abonnentenkanal für das Attribut *nspmDistributionPassword* auf *Benachrichtigen*.

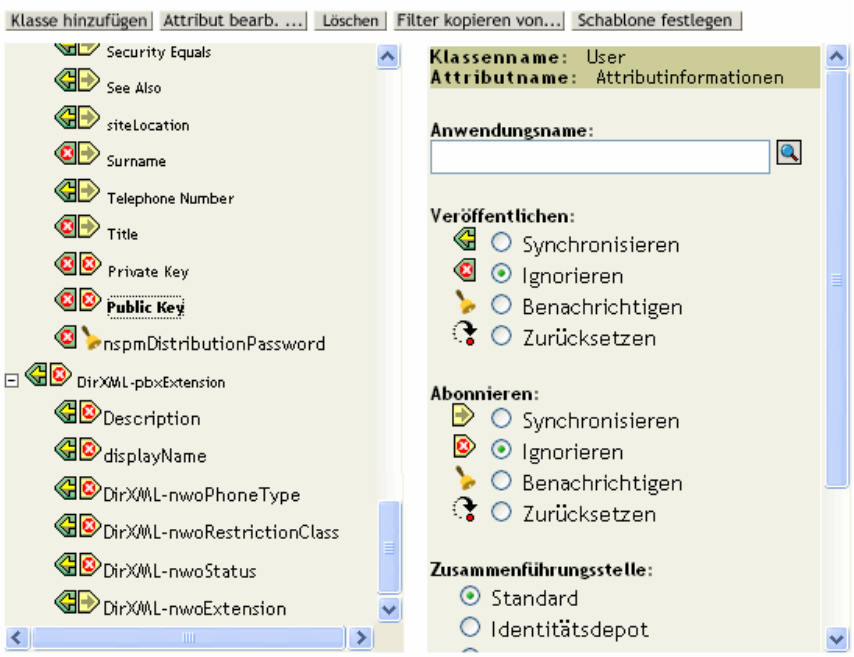
Um das Attribut sehen zu können, müssen Sie eventuell zur betreffenden Klasse (z. B. „User“) blättern und diese auswählen, bevor Sie durch die Attribute blättern.

Wenn das Attribut „nspmDistributionPassword“ nicht aufgeführt ist:

1a Vergewissern Sie sich, dass die Klasse ausgewählt ist, und klicken Sie auf *Attribut hinzufügen*.

1b Wählen Sie das Attribut „nspmDistributionPassword“ aus und klicken Sie auf „OK“.

2 Setzen Sie für alle Objekte, bei denen der Wert *Benachrichtigen* für das Attribut *nspmDistributionPassword* eingestellt ist, die Attribute „Öffentlicher Schlüssel“ und „Privater Schlüssel“ auf „Ignorieren“.



3 Wiederholen Sie für jeden Treiber, den Sie zur Unterstützung der Passwortsynchronisierung aktualisieren möchten, Schritt 2 auf Seite 107 (unter “Treiber in das Format von Identity Manager 3 konvertieren”) bis Schritt 2 in diesem Abschnitt (“Filtereinstellungen ändern”).

Der Treiber verfügt jetzt über das neue Treiberschnittstellenmodul, das erforderliche Identity Manager-Format und die anderen Elemente, die in der Treiberkonfiguration erforderlich sind, damit die Passwortsynchronisierung unterstützt wird: Treibermanifest, GCVs, Passwortsynchronisierungsrichtlinien und Filtereinstellungen.

4 Sehen Sie in den Implementierungshandbüchern zu den einzelnen Treibern nach, ob zusätzliche Schritte oder Informationen zum Einrichten der Identity Manager-Passwortsynchronisierung erforderlich sind. Siehe Identity Manager Drivers (http://www.novell.com/documentation/lg/dirxmldrivers/index.html).

5 Aktivieren Sie das universelle Passwort für Benutzer, indem Sie Passwortrichtlinien mit aktiviertem universellem Passwort erstellen.

Informationen hierzu finden Sie im Kapitel “Creating Password Policies” im *Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung). Beachten Sie bitte die zusätzlichen Arbeitsschritte im Kapitel “(NetWare 6.5 Only) Re-Creating Universal Password Assignments” des *Password Management Administration Guide* (Administrationshandbuch zur Passwortverwaltung), wenn Sie das universelle Passwort bisher mit NetWare 6.5 verwendet haben.

Zur Vereinfachung der Administration empfiehlt es sich, Passwortrichtlinien einer möglichst hohen Ebene im Baum zuzuweisen.

Auf der Seite „Konfigurationsoptionen“ können Sie mithilfe bestimmter Optionen festlegen, wie NMAS die verschiedenen Passwortarten synchronisieren soll. Bei den meisten Implementierungen funktionieren die Standardeinstellungen. Weitere Informationen finden Sie in der Online-Hilfe zu dieser Seite.

Szenarios für die Verwendung der Passwortsynchronisierung und das Einbinden von Passwortrichtlinien finden Sie in Abschnitt 5.8, „Implementierung der Passwortsynchronisierung“, auf Seite 115.

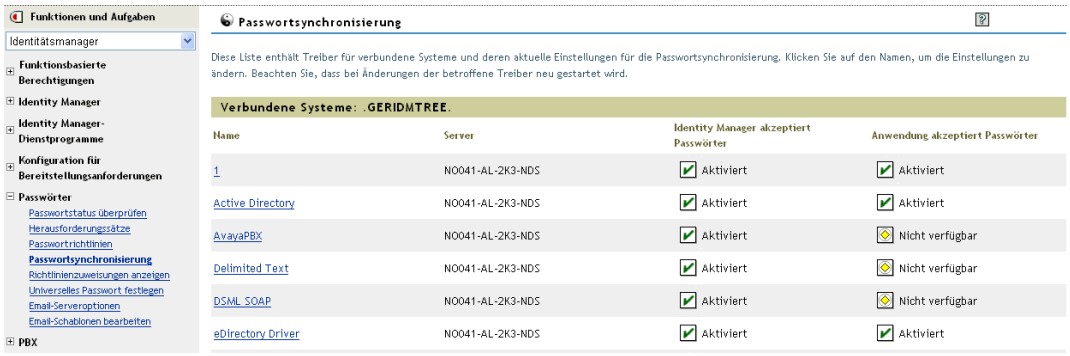
NMAS-Passwortrichtlinien werden baumspezifisch zugewiesen. Die Passwortsynchronisierung hingegen wird pro Treiber konfiguriert. Treiber werden serverspezifisch installiert und können nur Benutzer verwalten, die sich in einer Master- oder Lese-/Schreibreproduktion befinden.

Damit eine Passwortsynchronisierung die gewünschten Ergebnisse liefert, müssen Sie sicherstellen, dass die Container in der Master- oder Lese-/Schreibreproduktion auf dem Server, auf dem die Treiber für die Passwortsynchronisierung aktiv sind, den Containern entsprechen, für die Sie Passwortrichtlinien mit aktiviertem universellem Passwort zugewiesen haben. Durch Zuweisung einer Passwortrichtlinie an den Partitionsstammcontainer kann sichergestellt werden, dass die Passwortrichtlinie allen in diesem Container und seinen Untercontainern enthaltenen Benutzern zugewiesen wird.

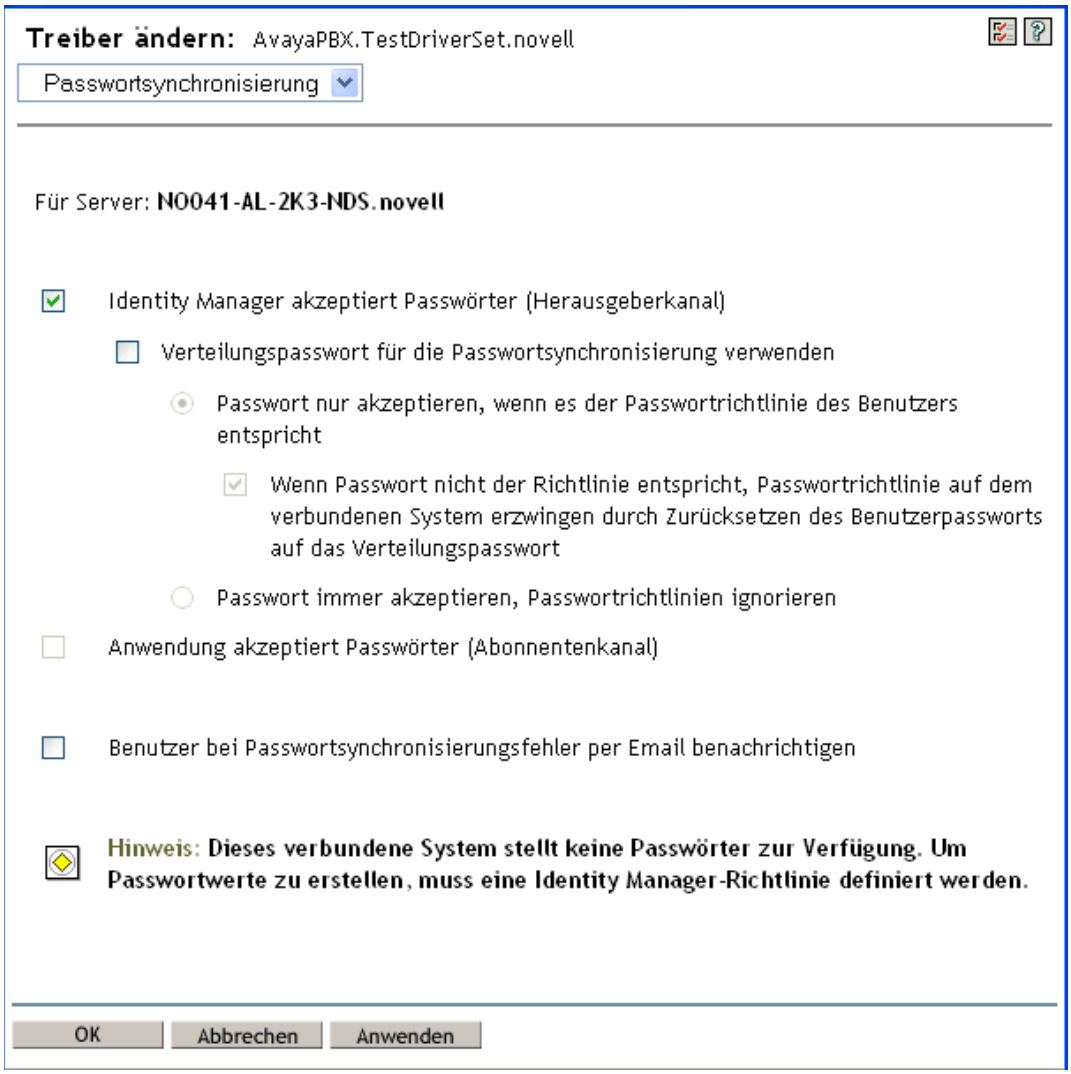
5.7.4 4. Schritt: Einrichten des Transfers für die Passwortsynchronisierung

Überzeugen Sie sich davon, dass der Passwort-Transfer auf allen verbundenen Systemen wie gewünscht konfiguriert ist.

1. Klicken Sie in iManager auf *Passwörter* > *Passwortsynchronisierung*.
2. Durchsuchen Sie einen Baum oder Container nach Treibern für verbundene Systeme, die Sie verwalten möchten.



3 Klicken Sie auf einen Treiber, um die aktuellen Einstellungen für den Passwort-Transfer anzuzeigen.



Diese Seite enthält eine Aufstellung der Globalkonfigurationswerte (GCVs). Ändern Sie diese durch Auswählen der entsprechenden Optionen.

Identity Manager kontrolliert den Einstiegspunkt (d. h. das von Identity Manager aktualisierte Passwort). NMAS kontrolliert in Abhängigkeit von den Einstellungen in den Konfigurationsoptionen den Passwort-Transfer zwischen den einzelnen Passwortarten. (Schritt 3 auf Seite 92 zeigt die Seite „Konfigurationsoptionen“ an.) Wenn Sie die Option *Verteilungspasswort für die Passwortsynchronisierung verwenden* aktivieren, verwendet Identity Manager das Verteilungspasswort direkt. Wenn Sie diese Option deaktivieren, verwendet Identity Manager das universelle Passwort direkt.

Informationen und Abbildungen zu diesen Optionen finden Sie in Abschnitt 5.8, „Implementierung der Passwortsynchronisierung“, auf Seite 115 sowie in der Online-Hilfe.

4 Testen Sie die Passwortsynchronisierung.

Überzeugen Sie sich davon, dass das Identity Manager-Passwort an die von Ihnen angegebenen Systeme verteilt wird.

Überzeugen Sie sich davon, dass die von Ihnen angegebenen verbundenen Systeme Passwörter gegenüber Identity Manager veröffentlichen.

Tipps zur Problemlösung finden Sie in Abschnitt 5.8, „Implementierung der Passwortsynchronisierung“, auf Seite 115.

5.8 Implementierung der Passwortsynchronisierung

Mit der Funktion für die Passwortsynchronisierung in Identity Manager können Sie verschiedene Szenarios implementieren. In diesem Abschnitt werden einfache Szenarios beschrieben, um zu verdeutlichen, wie sich die Einstellungen der Identity Manager-Passwortsynchronisierung und die NMAS-Passwortrichtlinien auf die Synchronisierung von Passwörtern auswirken. Sie können ein oder mehrere dieser Szenarios verwenden, um den Erfordernissen Ihrer Umgebung gerecht zu werden.

5.8.1 Überblick über die Relation zwischen Identity Manager und NMAS

Dienstprogramme und NMAS

Dienstprogramme wie iManager und der Novell Client kommunizieren mit NMAS, anstatt ein bestimmtes Passwort direkt zu aktualisieren. NMAS ist die Instanz, die entscheidet, welche Passwörter aktualisiert werden.

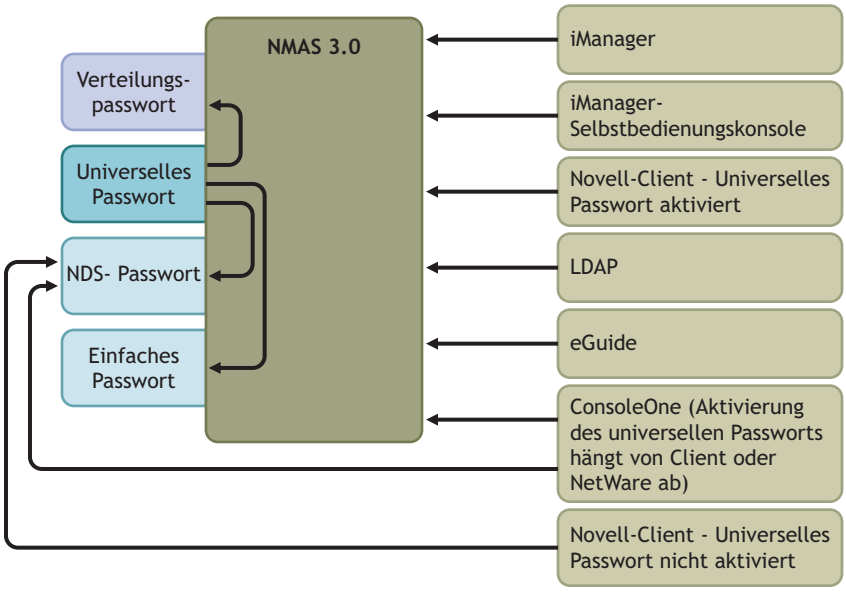
NMAS synchronisiert Passwörter innerhalb eines Identitätsdepots und verwendet dazu die Einstellungen aus den NMAS-Passwortrichtlinien.

Ältere Dienstprogramme, die das universelle Passwort noch nicht unterstützen, aktualisieren das NDS-Passwort direkt, anstatt mit NMAS zu kommunizieren und NMAS die Entscheidung zu

überlassen, welche Passwörter aktualisiert werden müssen. Beachten Sie, wie Benutzer und Helpdesk-Administratoren in Ihrer Umgebung ältere Dienstprogrammen nutzen. Da ältere Dienstprogramme das NDS-Passwort nicht über NMAS, sondern direkt aktualisieren, kann es zu einer Passwortdivergenz (d. h. zu fehlender Synchronisierung zwischen dem universellen Passwort und dem NDS-Passwort) kommen, wenn Sie das universelle Passwort und NMAS 2.3 verwenden.

Damit das universelle Passwort unterstützt wird, müssen Sie sicherstellen, dass die Benutzer auf den Novell Client aufrüsten und die Helpdesk-Benutzer ConsoleOne nur in Verbindung mit der neuesten Version des Novell Client oder von NetWare einsetzen.

Abbildung 5-5 *Passwortsynchronisierung über NMAS*



Identity Manager und NMAS

Identity Manager steuert den “Einstiegspunkt” (für die direkte Aktualisierung des universellen Passworts oder des Verteilungspassworts). NMAS steuert den Transfer bei der Passwortsynchronisierung innerhalb des Identitätsdepots.

In Szenario 1 kann der Identity Manager-Treiber für eDirectory verwendet werden, um das NDS-Passwort direkt zu aktualisieren. Dieses Szenario entspricht im Wesentlichen dem in DirXML 1.*x* angegebenen Szenario.

In Szenario 2, Szenario 3 und Szenario 4 wird Identity Manager zur Aktualisierung des universellen Passworts oder des Verteilungspassworts verwendet. Identity Manager nimmt über NMAS Passwortänderungen vor. Auf diese Weise kann NMAS andere Passwörter im Identitätsdepot gemäß den Einstellungen der NMAS-Passwortrichtlinie aktualisieren und erweiterte Passwortregeln aus NMAS-Passwortrichtlinien bei Passwörtern durchsetzen, die mit verbundenen Systemen synchronisiert werden. In diesen Szenarios verteilt Identity Manager stets das Verteilungspasswort an die verbundenen Systeme.

Szenario 2, Szenario 3 und Szenario 4 unterscheiden sich durch die unterschiedlichen Kombinationen der Einstellungen für die NMAS-Passwortrichtlinien und die Identity Manager-Passwortsynchronisierung für jeden verbundenen Systemtreiber.

5.8.2 Szenario 1: Synchronisierung zwischen zwei Identitätsdepots über das NDS-Passwort

Wie bereits in Version 1.0 der Passwortsynchronisierung können Sie das NDS-Passwort unter Verwendung des eDirectory-Treibers zwischen zwei Identitätsdepots synchronisieren. Für dieses Szenario muss das universelle Passwort nicht implementiert sein; das Verfahren kann mit eDirectory 8.6.2 oder höher durchgeführt werden. Diese Art der Passwortsynchronisierung wird als Synchronisierung des öffentlichen/privaten Schlüsselpaars bezeichnet.

Diese Methode sollte nur zum Synchronisieren von Passwörtern zwischen zwei Identitätsdepots angewandt werden. Da NMAS hierbei nicht zur Verwendung kommt, können mit dieser Methode keine Passwörter für verbundene Anwendungen synchronisiert werden.

- „Vor- und Nachteile von Szenario 1“ auf Seite 117
- „Einrichten von Szenario 1“ auf Seite 118
- „Fehlersuche bei Szenario 1“ auf Seite 119

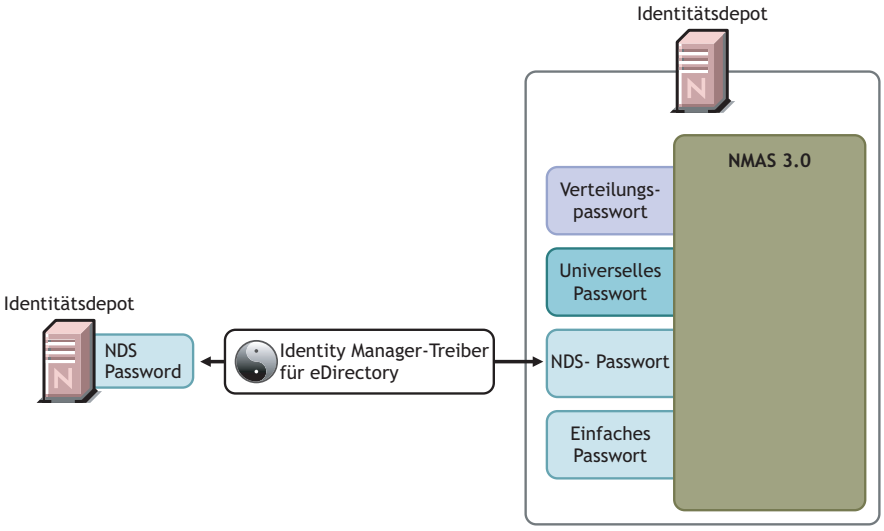
Vor- und Nachteile von Szenario 1

Tabelle 5-11 *Vorteile: Passwortsynchronisierung zwischen eDirectory und eDirectory mittels NDS-Passwort*

Vorteile	Nachteile
Einfache Konfiguration. Es müssen lediglich die richtigen Attribute in den Treiberfilter aufgenommen werden. Wenn Sie Identity Manager 3 und eDirectory 8.7.3 stufenweise implementieren, kann diese Methode die allmähliche Implementierung erleichtern. • Es ist nicht erforderlich, die Treiberkonfigurationen um die neuen Passwort-Synchronisierungsrichtlinien zu erweitern. • Das universelle Passwort muss nicht im Identitätsdepot implementiert sein. • Kann mit verbundenen Depots verwendet werden, auf denen eDirectory 8.6.2 oder höher läuft. • NMAS 2.3 ist nicht erforderlich. Setzt die grundlegenden Passworteinschränkungen durch, die für das NDS-Passwort festgelegt werden können.	Mit dieser Methode können Passwörter zwischen Identitätsdepots synchronisiert werden. Eine Synchronisierung von Passwörtern gegenüber anderen verbundenen Systemen ist nicht möglich. Führt keine Aktualisierung des universellen Passworts oder des Verteilungspassworts durch. Da diese Methode NMAS nicht verwendet, können Passwörter nicht mit erweiterten Passwortregeln in Richtlinien für Passwörter validiert werden, die aus einem anderen Identitätsdepot stammen. Da diese Methode NMAS nicht verwendet, können keine Passwörter im verbundenen Identitätsdepot zurückgesetzt werden, die der NMAS-Passwortrichtlinie nicht entsprechen. Bei fehlgeschlagener Passwortsynchronisierung erfolgt keine Email-Benachrichtigung. Der Aufruf der Funktion „Passwortstatus überprüfen“ aus iManager heraus wird nicht unterstützt. (Für diese Funktion wird das Verteilungspassword benötigt.)

Das folgende Diagramm zeigt, dass der Identity Manager-Treiber für eDirectory wie in DirXML 1.*x* verwendet werden kann, um das NDS-Passwort zwischen zwei Identitätsdepots zu synchronisieren. In diesem Szenario wird NMAS nicht verwendet.

Abbildung 5-6 *Synchronisierung zwischen zwei Identitätsdepots über das NDS-Passwort*



Einrichten von Szenario 1

Damit Sie diese Art der Passwortsynchronisierung einrichten können, müssen Sie zunächst den Treiber konfigurieren.

Implementierung des universellen Passworts

Nicht erforderlich.

Konfiguration der Passwortrichtlinie

Keine.

Einstellungen für die Passwortsynchronisierung

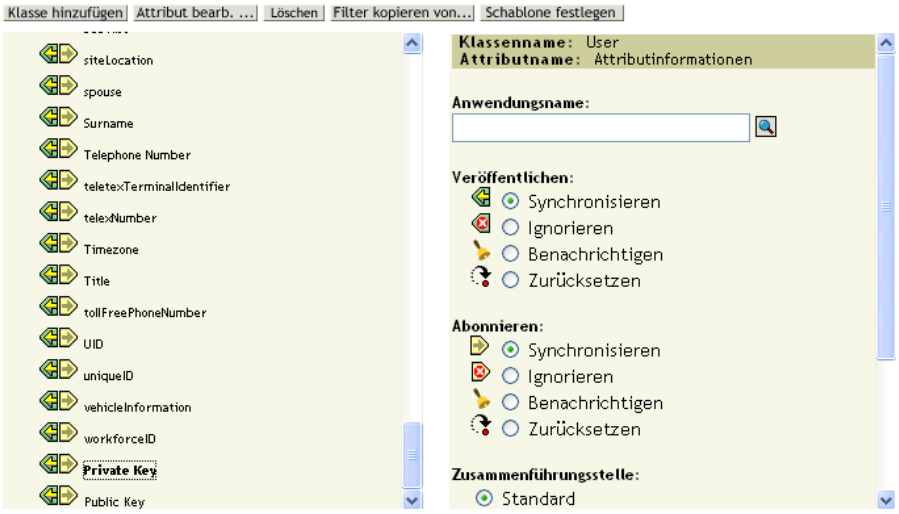
Keine. Die Einstellungen auf der Seite „Passwortsynchronisierung“ für einen Treiber haben bei dieser Methode der Synchronisierung eines NDS-Passworts keine Auswirkungen.

Treiberkonfiguration

Entfernen Sie die in Abschnitt 5.3.4, „In der Treiberkonfiguration benötigte Richtlinien“, auf Seite 94 aufgeführten Passwortsynchronisierungsrichtlinien. Diese Richtlinien zielen auf die Unterstützung des universellen Passworts und des Verteilungspassworts ab. Das NDS-Passwort wird nicht über diese Richtlinien, sondern über die Attribute für den privaten und öffentlichen Schlüssel synchronisiert.

Stellen Sie sicher, dass der Treiberfilter für die Treiber beider Identitätsdepots die Attribute des öffentlichen und des privaten Schlüssels für alle Objektklassen synchronisiert, für die Passwörter synchronisiert werden sollten. Die folgende Abbildung zeigt hierfür ein Beispiel.

Abbildung 5-7 *Synchronisieren der Attribute für den privaten und den öffentlichen Schlüssel*



Fehlersuche bei Szenario 1

- Aktivieren Sie die Option „DSTrace“.
- Kontrollieren Sie den Treiberfilter, um sicherzustellen, dass die Attribute „Öffentlicher Schlüssel“ und „Privater Schlüssel“ nicht ignoriert, sondern synchronisiert werden.
- Beachten Sie auch die Tipps in Abschnitt 5.13, „Fehlersuche bei der Passwortsynchronisierung“, auf Seite 169.

5.8.3 Szenario 2: Synchronisieren unter Verwendung des universellen Passworts

Mit Identity Manager können Sie ein Passwort aus einem verbundenen System mit dem universellen Passwort im Identitätsdepot synchronisieren.

Wenn das universelle Passwort aktualisiert wird, kann auch das NDS-Passwort, das Verteilungspasswort oder das einfache Passwort aktualisiert werden (in Abhängigkeit von den Einstellungen in der NMAS-Passwortrichtlinie).

Jedes verbundene System kann Passwörter an Identity Manager veröffentlichen, wenn auch nicht alle Systeme das tatsächliche Passwort des Benutzers bereitstellen können. So kann beispielsweise Active Directory das tatsächliche Passwort eines Benutzers an Identity Manager veröffentlichen. Obwohl PeopleSoft kein Passwort aus dem System bereitstellt, kann es ein Ausgangspasswort bereitstellen, das in einer Richtlinie in der Treiberkonfiguration erstellt wurde (z. B. unter Verwendung der Mitarbeiter-ID oder des Nachnamens). Nicht alle Treiber können Passwortänderungen von Identity Manager abonnieren. Weitere Informationen hierzu finden Sie in Abschnitt 5.2, „Unterstützung von verbundenen Systemen bei der Passwortsynchronisierung“, auf Seite 86.

- „Vor- und Nachteile von Szenario 2“ auf Seite 120

- „Einrichten von Szenario 2“ auf Seite 121
- „Fehlersuche bei Szenario 2“ auf Seite 126

Vor- und Nachteile von Szenario 2

Tabelle 5-12 *Vorteile: Synchronisieren unter Verwendung des universellen Passworts*

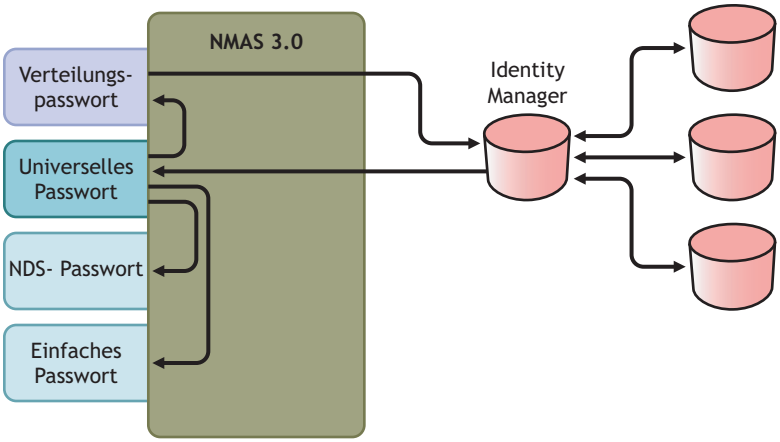
Vorteile	Nachteile
Ermöglicht die Synchronisierung von Passwörtern zwischen dem Identitätsdepot und dem verbundenen System (in beiden Richtungen). Ermöglicht die Bestätigung von Passwörtern auf Basis der NMAS-Passwortrichtlinie. Ermöglicht Email-Benachrichtigungen bei fehlerhaften Passwortoperationen, z. B. wenn ein aus dem verbundenen System eingehendes Passwort nicht der Passwortrichtlinie entspricht. Unterstützt die Aufgabe „Passwortstatus überprüfen“ in iManager, wenn das universelle Passwort mit dem Verteilungspasswort synchronisiert wird und das verbundene System Passwortprüfungen unterstützt. NMAS erzwingt die erweiterten Passwortregeln in den Passwortrichtlinien, wenn die Regeln aktiviert sind. Wenn ein aus dem verbundenen System eingehendes Passwort nicht regelkonform ist, wird eine Fehlermeldung erzeugt. Wenn die entsprechende Option aktiviert ist, erhalten Sie eine Email-Benachrichtigung. Wenn Sie nicht möchten, dass die Regeln der Passwortrichtlinie erzwungen werden, können Sie die Option „Erweiterte Passwortregeln aktivieren“ in der NMAS-Passwortrichtlinie deaktivieren.	Das Zurücksetzen von Passwörtern im verbundenen System ist bei dieser Methode nicht möglich, da das Verteilungspasswort und das universelle Passwort unter Umständen nicht identisch sind (in Abhängigkeit von den Einstellungen in den Passwortrichtlinien).

Das Diagramm zu diesem Szenario zeigt folgenden Verlauf:

1. Passwörter treffen über Identity Manager ein.
2. Identity Manager verwendet NMAS für die direkte Aktualisierung des universellen Passworts.
3. NMAS synchronisiert das universelle Passwort unter Berücksichtigung der Einstellungen der NMAS-Passwortrichtlinien mit dem Verteilungspasswort und anderen Passwörtern.
4. Identity Manager ruft das Verteilungspasswort ab, um es an verbundene Systeme zu verteilen, die Passwörter akzeptieren.

Obwohl in diesem Diagramm gleich mehrere Systeme mit Identity Manager verbunden sind, gilt es zu beachten, dass die Einstellungen für die Treiber jedes verbundenen Systems einzeln festgelegt werden müssen.

Abbildung 5-8 *Passwortsynchronisierung über das universelle Passwort*



Einrichten von Szenario 2

So richten Sie diese Art der Passwortsynchronisierung ein:

- „Implementierung des universellen Passworts“ auf Seite 121
- „Konfiguration der Passwortrichtlinie“ auf Seite 121
- „Einstellungen für die Passwortsynchronisierung“ auf Seite 123
- „Treiberkonfiguration“ auf Seite 125

Implementierung des universellen Passworts

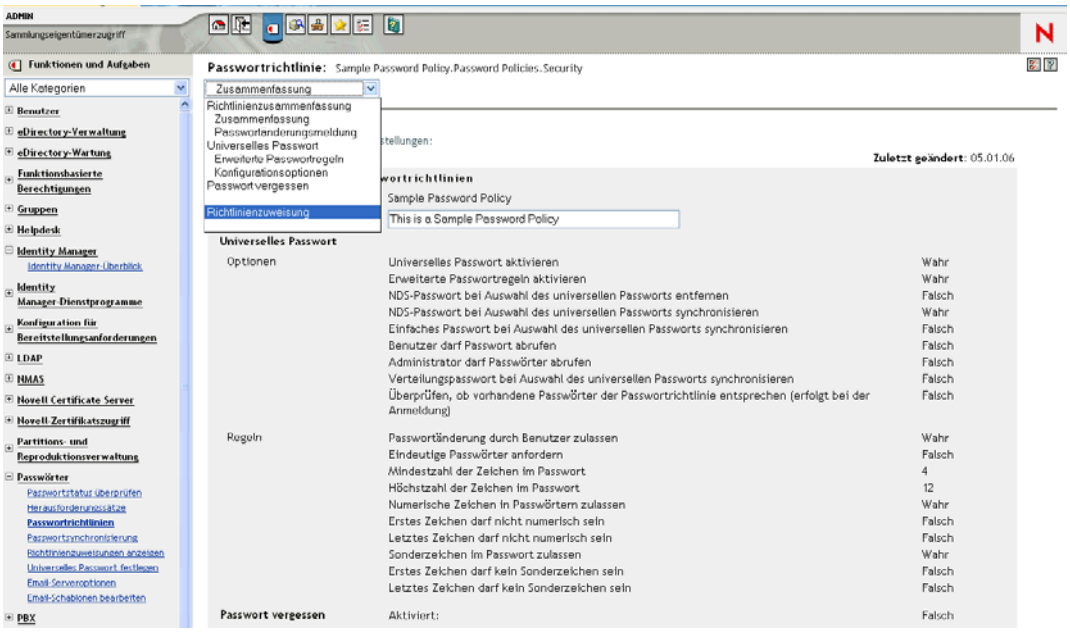
Überzeugen Sie sich davon, dass die Verwendung des universellen Passworts in Ihrer Umgebung möglich ist. Weitere Informationen hierzu finden Sie in Abschnitt 5.4, „Vorbereitungen zur Nutzung der Identity Manager-Passwortsynchronisierung und des universellen Passworts“, auf Seite 100.

Konfiguration der Passwortrichtlinie

Stellen Sie sicher, dass den Teilen des Identitätsdepots, für die Sie diese Art der Passwortsynchronisierung einrichten möchten, eine NMAS-Passwortrichtlinie zugewiesen ist.

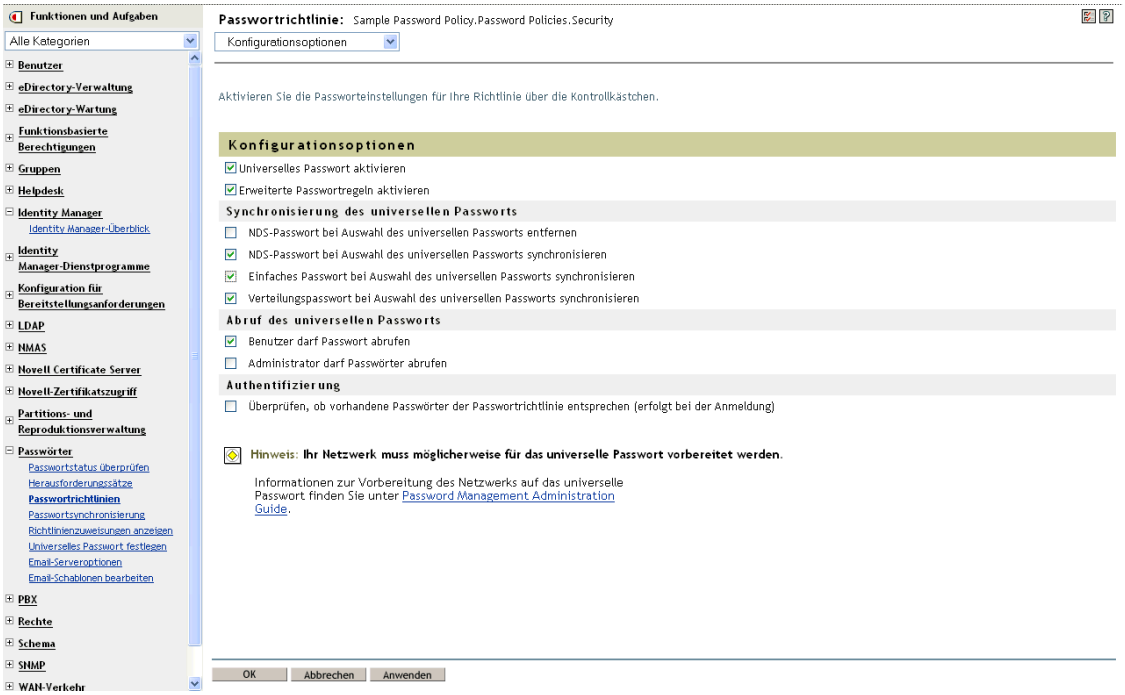
1. Klicken Sie in iManager auf *Passwörter* > *Passwortrichtlinien*.
2. Wählen Sie eine Richtlinie aus und klicken Sie anschließend auf *Bearbeiten*.

3 Suchen Sie das Objekt, in dem die Passwortsynchronisierung stattfinden soll, und wählen Sie es aus.



Sie können die Richtlinie der gesamten Baumstruktur (durch Auswahl des Objekts „Login Policy“ [Anmelderichtlinie] im Sicherheitscontainer), einem Partitionsstammcontainer, einem Container oder einem bestimmten Benutzer zuweisen. Es empfiehlt sich, Passwortrichtlinien einer möglichst hohen Ebene im Baum zuzuweisen, um die Verwaltung zu vereinfachen.

4 In der Passwortrichtlinie müssen folgende Optionen ausgewählt sein:



- *Universelles Passwort aktivieren*
- *NDS-Passwort bei Auswahl des universellen Passworts synchronisieren*
- *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren*

  Da Identity Manager das Verteilungspasswort abruft, um Passwörter an verbundene Systeme zu verteilen, ist eine Passwortsynchronisierung in beide Richtungen nur möglich, wenn diese Option aktiviert ist.

5 Vervollständigen Sie die Passwortrichtlinie nach Bedarf.

NMAS erzwingt die erweiterten Passwortregeln in den Passwortrichtlinien, wenn die Regeln aktiviert sind. Wenn Sie nicht möchten, dass die Regeln der Passwortrichtlinie erzwungen werden, können Sie die Option *Erweiterte Passwortregeln aktivieren* deaktivieren.

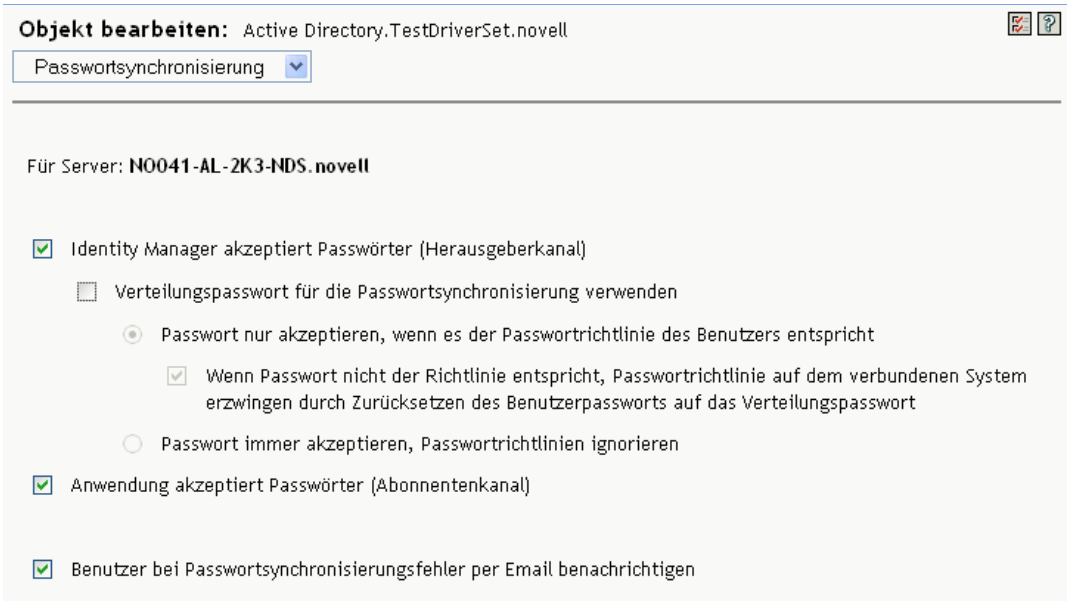
Bei der Verwendung von erweiterten Passwortregeln müssen Sie sicherstellen, dass diese nicht im Widerspruch zu den Passwortrichtlinien auf den verbundenen Systemen stehen, die Passwörter abonnieren.

Einstellungen für die Passwortsynchronisierung

1 Klicken Sie in iManager auf *Passwörter* > *Passwortsynchronisierung*.

2 Suchen Sie nach Treibern für die verbundenen Systeme und wählen Sie dann einen Treiber aus.

3 Nehmen Sie Einstellungen für den Treiber für das verbundene System vor.



Stellen Sie sicher, dass die folgenden Optionen ausgewählt sind:

- *Identity Manager akzeptiert Passwörter (Herausgeberkanal)*

  Wenn das Treibermanifest die Funktion „password-publish“ nicht enthält, wird auf der Seite eine entsprechende Meldung angezeigt. Auf diese Weise wird dem Benutzer mitgeteilt, dass keine Passwörter aus der Anwendung abgerufen werden können und diese nur durch Erstellen eines Passworts mittels einer Richtlinie in der Treiberkonfiguration veröffentlicht werden können.

- *Anwendung akzeptiert Passwörter (Abonnentenkanal)*

  Wenn das verbundene System Passwörter nicht akzeptiert, wird die Option grau angezeigt.

Diese Einstellungen ermöglichen die Passwortsynchronisierung in beide Richtungen, wenn diese vom verbundenen System unterstützt wird.

Sie können die Einstellungen an Ihre Geschäftsrichtlinien für die autorisierte Quelle für Passwörter anpassen. Wenn ein verbundenes System Passwörter z. B. nur abonnieren, jedoch nicht veröffentlichen soll, wählen Sie nur die Option *Anwendung akzeptiert Passwörter (Abonnentenkanal)*.

4 Stellen Sie sicher, dass die Option *Verteilungspasswort für die Passwortsynchronisierung verwenden* nicht aktiviert ist:

In diesem Szenario aktualisiert Identity Manager das universelle Passwort direkt. Das Verteilungspasswort wird weiterhin für die Verteilung von Passwörtern an verbundene Systeme verwendet, es wird jedoch anstelle von Identity Manager von NMAS über das universelle Passwort aktualisiert.

5 (Optional) Wählen Sie gegebenenfalls Folgendes aus:

- *Benutzer bei Passwortsynchronisierungsfehler per Email benachrichtigen*

  Denken Sie daran, dass das Attribut „Internet-Email-Adresse“ des eDirectory-Benutzerobjekts in mit einem Wert belegt sein muss, damit Email-Benachrichtigungen gesendet werden können.

Email-Benachrichtigungen sind nicht-invasiv, d. h., sie haben keinerlei Auswirkungen auf die Verarbeitung des XML-Dokuments, das das Versenden der Email ausgelöst hat. Tritt beim Versand der Email-Benachrichtigung ein Fehler auf, wird der Vorgang nur dann wiederholt, wenn die Operation selbst wiederholt wird. Debug-Meldungen zu Email-Benachrichtigungen werden trotzdem in die Trace-Datei geschrieben.

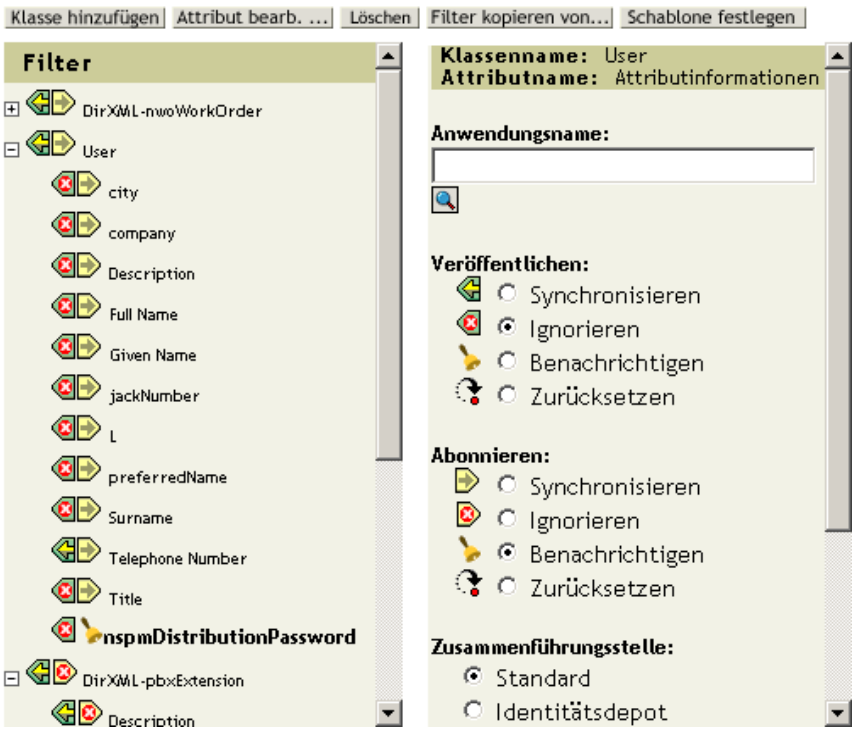
Treiberkonfiguration

1. Stellen Sie sicher, dass die erforderlichen Passwortsynchronisierungsrichtlinien für das Identity Manager-Skript in den Treiberkonfigurationen aller Treiber enthalten sind, die an der Passwortsynchronisierung teilnehmen sollen.

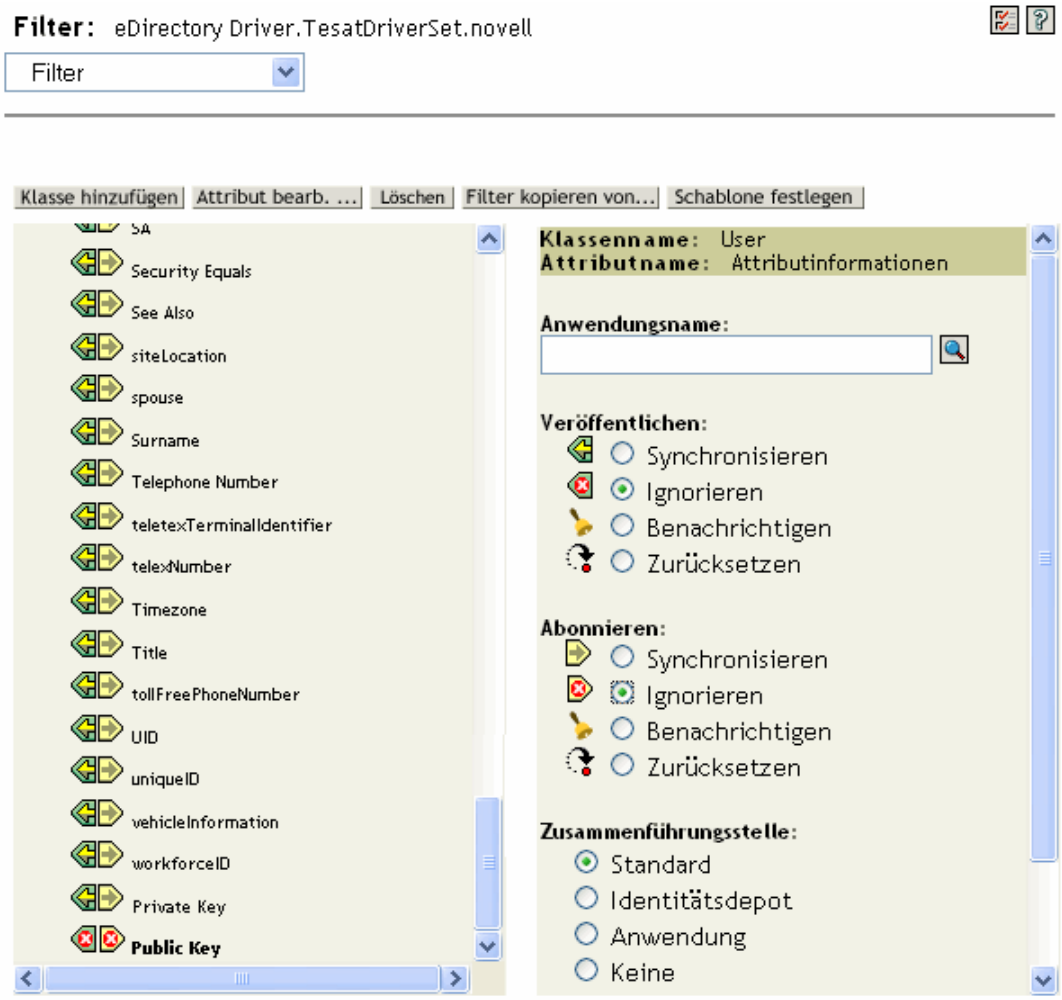
   Die Richtlinien müssen sich in der Treiberkonfiguration an der richtigen Stelle und in der richtigen Reihenfolge befinden. Eine Aufstellung der Richtlinien finden Sie in Abschnitt 5.3.4, „In der Treiberkonfiguration benötigte Richtlinien“, auf Seite 94.

   Die Identity Manager-Beispielkonfigurationen enthalten die Richtlinien bereits. Wenn Sie einen vorhandenen Treiber upgraden, können Sie die Richtlinien wie in Abschnitt 5.7, „Upgrade bestehender Treiberkonfigurationen zur Unterstützung der Passwortsynchronisierung“, auf Seite 106 beschrieben hinzufügen.

2. Stellen Sie den Filter für das Attribut „nspmDistributionPassword“ richtig ein:
   - Setzen Sie den Filter auf dem Herausgeberkanal bei allen Objektklassen für das Attribut *nspmDistributionPassword* auf „Ignorieren“.
   - Setzen Sie den Treiberfilter auf dem Abonnentenkanal bei allen Objektklassen, die Passwortänderungen abonnieren sollen, für das Attribut *nspmDistributionPassword* auf „Benachrichtigen“.



3 Setzen Sie für alle Objekte, bei denen der Wert *Benachrichtigen* für das Attribut „nspmDistributionPassword“ eingestellt ist, die Attribute „Public Key“ und „Private Key“ auf *Ignorieren*.



4 Damit die Passwortsicherheit gewährleistet ist, müssen Sie die Kontrolle darüber behalten, wer Zugriffsrechte auf Identity Manager-Objekte haben soll.

Fehlersuche bei Szenario 2

- „Flussdiagramm für Szenario 2“ auf Seite 127
- „Probleme bei der Anmeldung im Identitätsdepot“ auf Seite 128
- „Probleme bei der Anmeldung an einem anderen verbundenen System, das Passwörter abonniert“ auf Seite 128
- „Keine Email-Generierung bei Passwortfehlern“ auf Seite 129
- „Fehler beim Ausführen der Task „Objektpasswort überprüfen““ auf Seite 129
- „Hilfreiche DSTrace-Befehle“ auf Seite 130

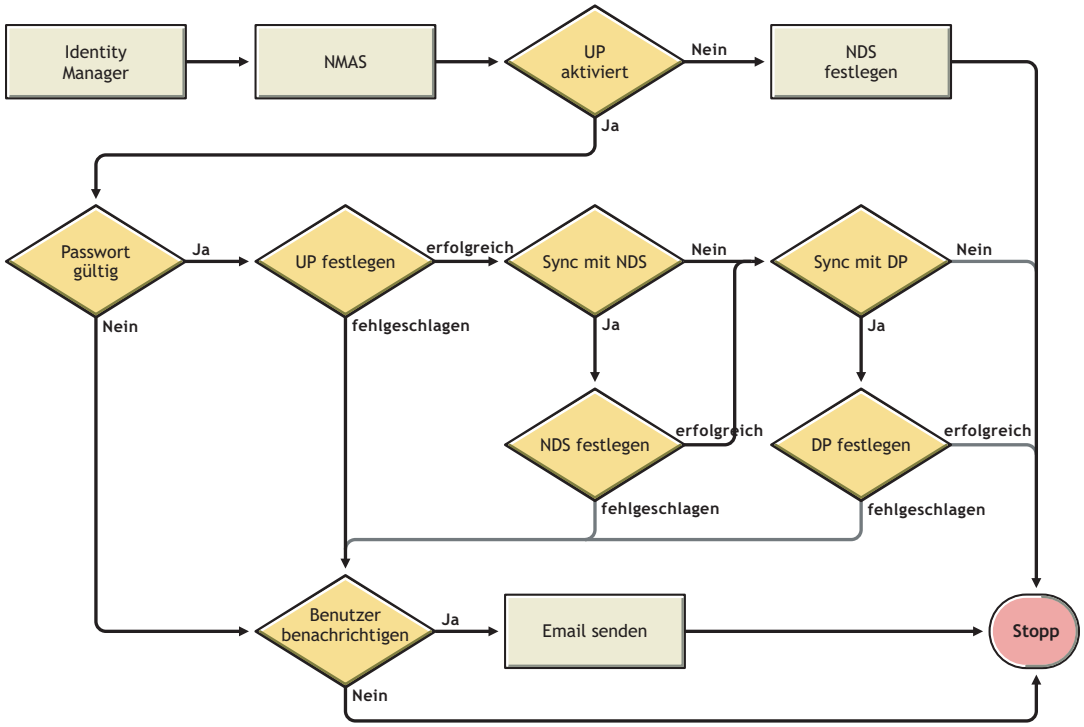
Beachten Sie auch die Tipps in Abschnitt 5.13, „Fehlersuche bei der Passwortsynchronisierung“, auf Seite 169.

Flussdiagramm für Szenario 2

Das folgende Flussdiagramm zeigt, wie NMAS mit dem von Identity Manager empfangenen Passwort verfährt. In diesem Szenario wird das Passwort mit dem universellen Passwort synchronisiert. NMAS entscheidet nach den folgenden Kriterien, wie das Passwort zu behandeln ist:

- Ist das universelle Passwort in der NMAS-Passwortrichtlinie aktiviert?
- Sind erweiterte Passwortregeln aktiviert, die eingehende Passwörter einhalten müssen?
- Welche anderen Einstellungen sind in der Passwortrichtlinie für das Synchronisieren des universellen Passworts mit den anderen Passwörtern festgelegt?

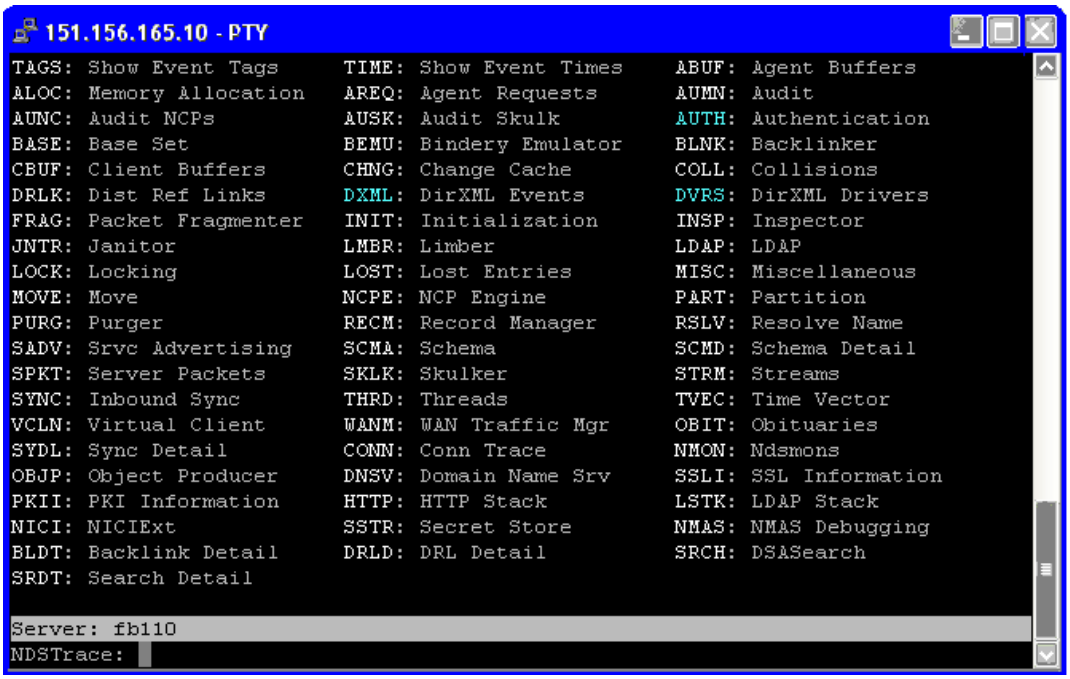
Abbildung 5-9 *Wie NMAS mit dem von Identity Manager empfangenen Passwort verfährt*



Probleme bei der Anmeldung im Identitätsdepot

- Aktivieren Sie in DSTrace die Einstellungen *+AUTH*, *+DXML* und *+DVRS*.

  Abbildung 5-10 *DSTrace-Befehle*



- Überzeugen Sie sich davon, dass das Element <password> oder <modify-password> an Identity Manager übergeben wird. Während diese Optionen aktiviert sind, beobachten Sie den Trace-Bildschirm, um sicherzustellen, dass sie übergeben werden.
- Überzeugen Sie sich davon, dass das Passwort gemäß den Regeln der Passwortrichtlinie gültig ist.
- Überprüfen Sie die Konfiguration und Zuweisung der NMAS-Passwortrichtlinie. Weisen Sie die Richtlinie versuchsweise einem Benutzer direkt zu, um sicherzustellen, dass die korrekte Richtlinie verwendet wird.
- Stellen Sie sicher, dass auf der Seite „Passwortsynchronisierung“ für den Treiber die Option *DirXML akzeptiert Passwörter* ausgewählt ist.
- Stellen Sie sicher, dass in der Passwortrichtlinie die Option *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren* ausgewählt ist.

Probleme bei der Anmeldung an einem anderen verbundenen System, das Passwörter abonniert

Dieser Abschnitt befasst sich mit der Fehlersuche in Fällen, in denen ein verbundenes System Passwörter gegenüber Identity Manager veröffentlicht, aber ein anderes verbundenes System, das Passwörter veröffentlicht, keine Änderungen von dem anderen System mitgeteilt bekommt. Bei dieser Konstellation spricht man auch von einem „sekundären verbundenen System“, weil das

zweite verbundene System die Passwörter über Identity Manager vom ersten verbundenen System erhält.

- Aktivieren Sie in DSTrace die Einstellungen *+DXML* und *+DVRS*, um sich die Regelverarbeitung durch Identity Manager ansehen zu können.
- Stellen Sie die Identity Manager LDAP Trace-Stufe für den Treiber auf *3* ein.
- Stellen Sie auf der Seite „Passwortsynchronisierung“ sicher, dass die Option *Identity Manager akzeptiert Passwörter* ausgewählt ist.
- Überprüfen Sie den Treiberfilter, um sicherzustellen, dass das Attribut „nspmDistributionPassword“ korrekt eingestellt ist (siehe Schritt 2 auf Seite 125).
- Überzeugen Sie sich davon, dass das <*password*> für ein „Add“- oder <`modify-password`>-Element an das verbundene System gesendet wird. Beobachten Sie zur Kontrolle den DSTrace-Bildschirm oder die DSTrace-Datei bei aktivierten Trace-Optionen, wie in den ersten Arbeitsschritten erläutert.
- Überzeugen Sie sich davon, dass die Treiberkonfiguration die Passwortrichtlinien für das Identity Manager-Skript an der richtigen Stelle und in der richtigen Reihenfolge enthält, wie in Abschnitt 5.3.4, „In der Treiberkonfiguration benötigte Richtlinien“, auf Seite 94 beschrieben.
- Vergleichen Sie die NMAS-Passwortrichtlinie im Identitätsdepot mit etwaigen Passwortrichtlinien, die von dem verbundenen System erzwungen werden, und stellen Sie sicher, dass diese kompatibel sind.

Keine Email-Generierung bei Passwortfehlern

- Aktivieren Sie in DSTrace die Einstellung *+DXML*, um sich die Regelverarbeitung durch Identity Manager ansehen zu können.
- Stellen Sie die Identity Manager LDAP Trace-Stufe für den Treiber auf *3* ein.
- Überzeugen Sie sich davon, dass die Regel für das Erzeugen einer Email-Benachrichtigung ausgewählt ist.
- Überzeugen Sie sich davon, dass das Identitätsdepot-Objekt im Attribut „Internet EMail Address“ die richtige Email-Adresse des Benutzers enthält.
- Stellen Sie sicher, dass der SMTP-Server und die Email-Schablone in der Aufgabe „Benachrichtigungskonfiguration“ richtig konfiguriert sind. Weitere Informationen hierzu finden Sie in Abschnitt 5.12, „Konfigurieren der Email-Benachrichtigung“, auf Seite 156.

Fehler beim Ausführen der Task „Objektpasswort überprüfen“

Die Task „Passwortstatus überprüfen“ in iManager bewirkt, dass der Treiber die Aktion „Objektpasswort überprüfen“ ausführt. Wenn dabei Probleme auftreten, sollten Sie Folgendes überprüfen:

- Wenn die Task „Objektpasswort überprüfen“ den Code „-603“ zurückgibt, fehlt im Identitätsdepot-Objekt das Attribut „nspmDistributionPassword“. Überprüfen Sie, ob der Treiberfilter die richtigen Einstellungen für die Attribute „nspmDistributionPassword“ enthält. Stellen Sie außerdem sicher, dass in der Passwortrichtlinie die Option *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren* ausgewählt ist.
- Wenn die Task „Objektpasswort überprüfen“ die Meldung `Nicht synchronisiert` zurückgibt, vergewissern Sie sich, dass die Treiberkonfiguration die entsprechenden Passwortsynchronisierungsrichtlinien enthält.

- Vergleichen Sie die NMAS-Passwortrichtlinie im Identitätsdepot mit etwaigen Passwortrichtlinien, die von dem verbundenen System erzwungen werden, und stellen Sie sicher, dass diese kompatibel sind.
- Ausgangspunkt für die Task „Objektpasswort überprüfen“ ist das Verteilungspasswort. Wenn das Verteilungspasswort nicht aktualisiert wird, meldet die Aktion „Objektpasswort überprüfen“ eventuell nicht, dass die Passwörter synchronisiert wurden.
- Denken Sie daran, dass die Task „Passwortstatus überprüfen“ nur beim Identity Manager-Treiber das NDS-Passwort anstelle des Verteilungspassworts überprüft.

Hilfreiche DSTrace-Befehle

+DXML: Zum Anzeigen der Regelverarbeitung durch Identity Manager und möglicher Fehlermeldungen

+DVRS: Zum Anzeigen der Meldungen des Identity Manager-Treibers

+AUTH: Zum Anzeigen der Änderungen am NDS-Passwort

5.8.4 Szenario 3: Synchronisieren des Identitätsdepots und der verbundenen Systeme mit Aktualisierung des Verteilungspassworts durch Identity Manager

In diesem Szenario aktualisiert Identity Manager das Verteilungspasswort direkt und lässt NMAS entscheiden, wie die anderen Passwörter des Identitätsdepots synchronisiert werden sollen.

Jedes verbundene System kann Passwörter an Identity Manager veröffentlichen, wenn auch nicht alle Systeme das tatsächliche Passwort des Benutzers bereitstellen können. So kann beispielsweise Active Directory das tatsächliche Passwort eines Benutzers an Identity Manager veröffentlichen. Obwohl PeopleSoft kein Passwort aus dem System bereitstellt, kann es ein Ausgangspasswort bereitstellen, das in einer Richtlinie in der Treiberkonfiguration erstellt wurde (z. B. unter Verwendung der Mitarbeiter-ID oder des Nachnamens). Nicht alle Treiber können Passwortänderungen von Identity Manager abonnieren. Weitere Informationen hierzu finden Sie in Abschnitt 5.2, „Unterstützung von verbundenen Systemen bei der Passwortsynchronisierung“, auf Seite 86.

- „Vor- und Nachteile von Szenario 3“ auf Seite 131
- „Einrichten von Szenario 3“ auf Seite 132
- „Fehlersuche bei Szenario 3“ auf Seite 137

Vor- und Nachteile von Szenario 3

Tabelle 5-13 *Vorteile: Synchronisieren des Identitätsdepots und der verbundenen Systeme durch Aktualisierung des Verteilungspassworts*

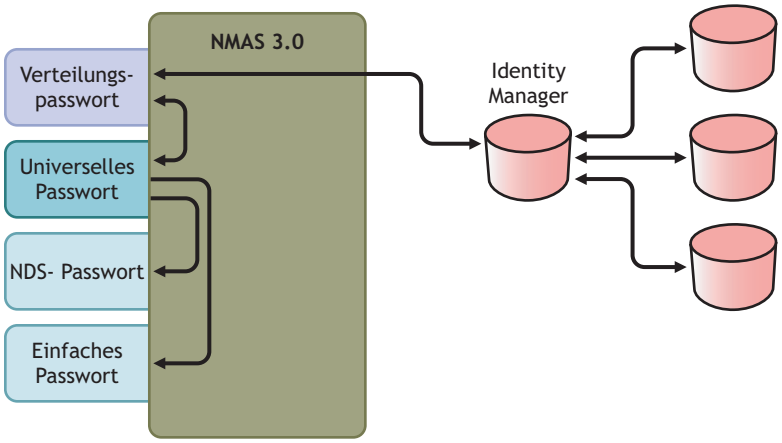
Vorteile	Nachteile
Ermöglicht die Synchronisierung von Passwörtern zwischen dem Identitätsdepot und verbundenen Systemen. Sie können auswählen, ob Richtlinien für die von verbundenen Systemen übergebenen Passwörter erzwungen werden sollen oder nicht. Sie können festlegen, dass eine Benachrichtigung gesendet wird, falls bei der Passwortsynchronisierung ein Fehler auftritt. Wenn Sie sich für das Erzwingen von Passwortrichtlinien entscheiden, haben Sie die Möglichkeit, ein nicht regelkonformes Passwort auf dem verbundenen System auf das Verteilungspasswort zurückzusetzen.	

Das Diagramm zu diesem Szenario zeigt folgenden Verlauf:

1. Passwörter treffen über Identity Manager ein.
2. Identity Manager geht über NMAS, um das Verteilungspasswort direkt zu aktualisieren.
3. Identity Manager verwendet das Verteilungspasswort auch, um Passwörter an verbundene Systeme zu übergeben, die Sie für das Akzeptieren von Passwörtern konfiguriert haben.
4. NMAS synchronisiert das universelle Passwort unter Berücksichtigung der Einstellungen der NMAS-Passwortrichtlinien mit dem Verteilungspasswort und anderen Passwörtern.

Obwohl in diesem Diagramm gleich mehrere Systeme mit Identity Manager verbunden sind, gilt es zu beachten, dass die Einstellungen für die Treiber jedes verbundenen Systems einzeln festgelegt werden müssen.

Abbildung 5-11 *Synchronisieren des Identitätsdepots und der verbundenen Systeme durch Aktualisierung des Verteilungspassworts*



Einrichten von Szenario 3

So richten Sie diese Art der Passwortsynchronisierung ein:

- „Implementierung des universellen Passworts“ auf Seite 132
- „Konfiguration der Passwortrichtlinie“ auf Seite 132
- „Einstellungen für die Passwortsynchronisierung“ auf Seite 133
- „Treiberkonfiguration“ auf Seite 135

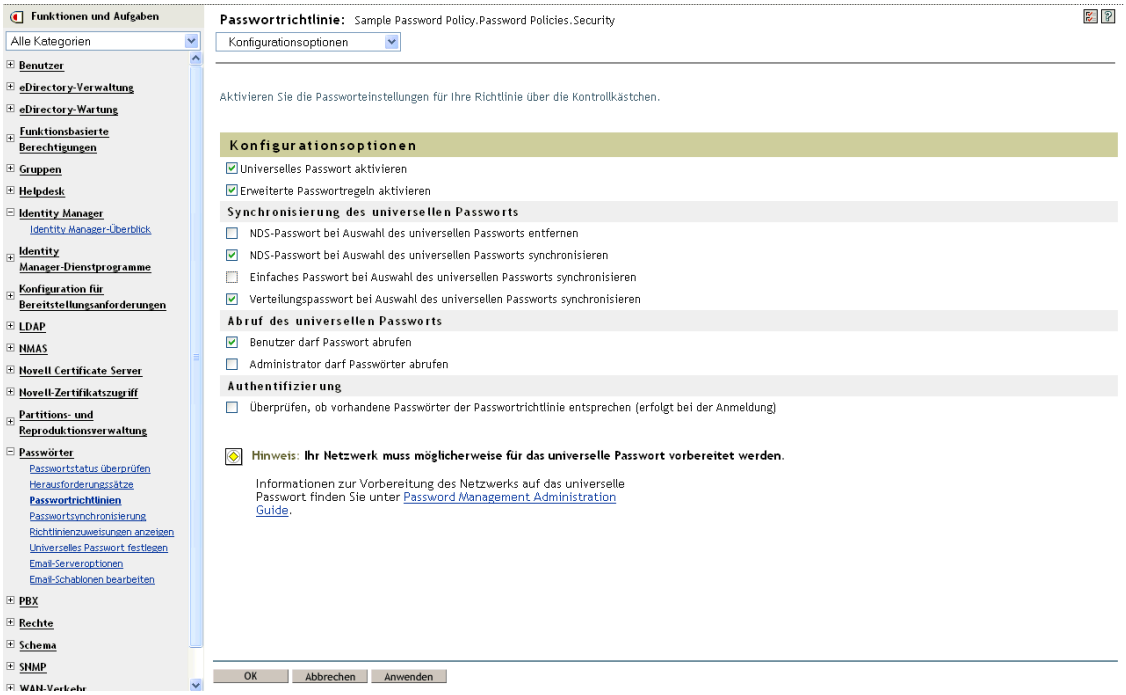
Implementierung des universellen Passworts

Überzeugen Sie sich davon, dass die Verwendung des universellen Passworts in Ihrer Umgebung problemlos möglich ist. Weitere Informationen hierzu finden Sie in Abschnitt 5.4, „Vorbereitungen zur Nutzung der Identity Manager-Passwortsynchronisierung und des universellen Passworts“, auf Seite 100.

Konfiguration der Passwortrichtlinie

1. Klicken Sie in iManager auf *Passwörter* > *Passwortrichtlinien*.
2. Stellen Sie sicher, dass den Teilen des Identitätsdepot-Baums, für die Sie diese Art der Passwortsynchronisierung einrichten möchten, eine Passwortrichtlinie zugewiesen ist. Sie können diese Richtlinie der gesamten Baumstruktur, einem Partitionsstammcontainer, einem Container oder einem bestimmten Benutzer zuweisen. Es empfiehlt sich, Passwortrichtlinien einer möglichst hohen Ebene im Baum zuzuweisen, um die Verwaltung zu vereinfachen.

3 In der Passwortrichtlinie müssen folgende Optionen ausgewählt sein:



- *Universelles Passwort aktivieren*
- *NDS-Passwort bei Auswahl des universellen Passworts synchronisieren*
- *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren*

  Da Identity Manager das Verteilungspasswort abruft, um Passwörter an verbundene Systeme zu verteilen, ist eine Passwortsynchronisierung in beide Richtungen nur möglich, wenn diese Option ausgewählt ist.

4 Bei der Verwendung von erweiterten Passwortregeln müssen Sie sicherstellen, dass diese nicht im Widerspruch zu den Passwortrichtlinien auf den verbundenen Systemen stehen, die Passwörter abonnieren.

Einstellungen für die Passwortsynchronisierung

1 Klicken Sie in iManager auf *Passwörter* > *Passwortsynchronisierung*.

2 Suchen Sie nach Treibern für die verbundenen Systeme und wählen Sie dann einen Treiber aus.

3 Nehmen Sie Einstellungen für den Treiber für das verbundene System vor.

Stellen Sie sicher, dass die folgenden Optionen ausgewählt sind:

- *Identity Manager akzeptiert Passwörter (Herausgeberkanal)*
- *Verteilungspasswort für die Passwortsynchronisierung verwenden*

  Wenn das Treibermanifest die Funktion “password-publish” nicht enthält, wird auf der Seite eine entsprechende Meldung angezeigt. Auf diese Weise wird dem Benutzer mitgeteilt, dass keine Passwörter aus der Anwendung abgerufen werden können und diese nur durch Erstellen eines Passworts mittels einer Richtlinie in der Treiberkonfiguration veröffentlicht werden können.
- *Anwendung akzeptiert Passwörter (Abonnentenkanal)*

Diese Einstellungen ermöglichen die Passwortsynchronisierung in beide Richtungen, wenn diese vom verbundenen System unterstützt wird.

Sie können die Einstellungen an Ihre Geschäftsrichtlinien für die autorisierte Quelle für Passwörter anpassen. Wenn ein verbundenes System Passwörter z. B. nur abonnieren, jedoch nicht veröffentlichen soll, wählen Sie nur die Option *Anwendung akzeptiert Passwörter (Abonnentenkanal)*.

4 Legen Sie mit den Optionen unter *Verteilungspasswort für die Passwortsynchronisierung verwenden* fest, ob NMAS-Passwortrichtlinien erzwungen oder ignoriert werden sollen.

5 (Sofern zutreffend) Wenn Sie festgelegt haben, dass Passwortrichtlinien erzwungen werden sollen, müssen Sie auch angeben, ob Identity Manager das Passwort des verbundenen Systems zurücksetzen soll, wenn es nicht regelkonform ist.

6 (Optional) Wählen Sie gegebenenfalls Folgendes aus:

- *Benutzer bei Passwortsynchronisierungsfehler per Email benachrichtigen*

  Denken Sie daran, dass das Attribut „Internet-Email-Adresse“ im Benutzerobjekt in eDirectory mit einem Wert belegt sein muss, damit Email-Benachrichtigungen gesendet werden können.

Email-Benachrichtigungen sind nicht-invasiv, d. h., sie haben keinerlei Auswirkungen auf die Verarbeitung des XML-Dokuments, das die Email ausgelöst hat. Tritt beim Versand der Email-Benachrichtigung ein Fehler auf, wird der Vorgang nur dann wiederholt, wenn die Operation selbst wiederholt wird. Debug-Meldungen zu Email-Benachrichtigungen werden trotzdem in die Trace-Datei geschrieben.

Treiberkonfiguration

1. Stellen Sie sicher, dass die erforderlichen Passwortsynchronisierungsrichtlinien für das Identity Manager-Skript in den Treiberkonfigurationen aller Treiber enthalten sind, die an der Passwortsynchronisierung teilnehmen sollen.

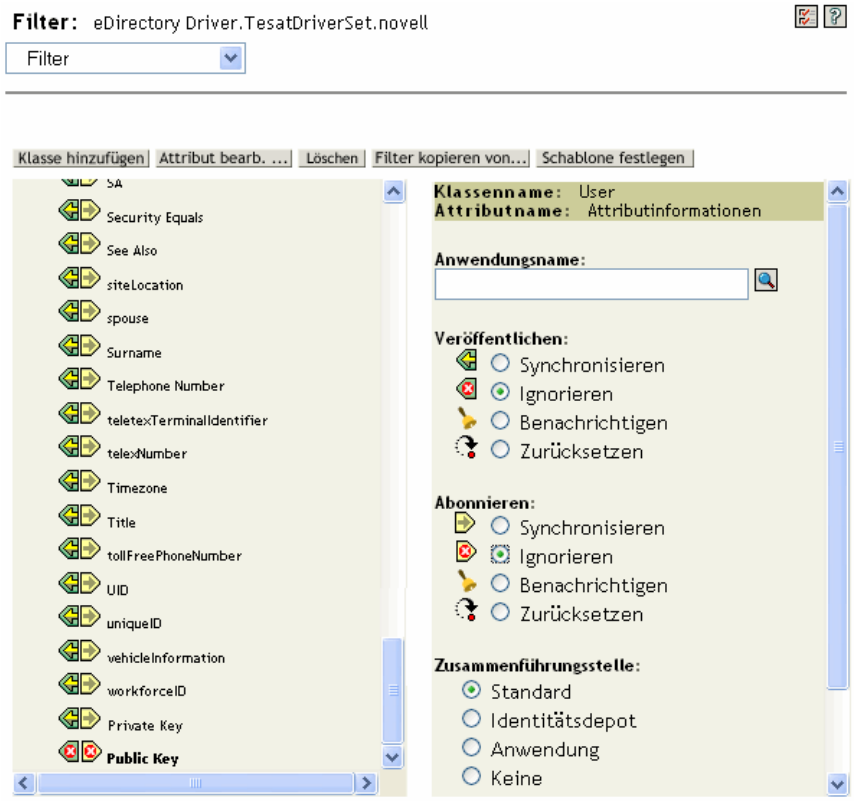
   Die Richtlinien müssen sich in der Treiberkonfiguration an der richtigen Stelle und in der richtigen Reihenfolge befinden. Eine Aufstellung der Richtlinien finden Sie in Abschnitt 5.3.4, „In der Treiberkonfiguration benötigte Richtlinien“, auf Seite 94.

   Die Identity Manager-Beispielkonfigurationen enthalten die Richtlinien bereits. Wenn Sie einen vorhandenen Treiber upgraden möchten, können Sie die Richtlinien wie in Abschnitt 5.7, „Upgrade bestehender Treiberkonfigurationen zur Unterstützung der Passwortsynchronisierung“, auf Seite 106 beschrieben hinzufügen.

2. Stellen Sie den Filter für das Attribut „nspmDistributionPassword“ richtig ein:
   - Auf dem Herausgeberkanal setzen Sie den Treiberfilter auf *Ignorieren* für das Attribut „nspmDistributionPassword“ für alle Objektklassen.
   - Auf dem Abonnentenkanal setzen Sie den Treiberfilter auf *Benachrichtigen* für das Attribut „nspmDistributionPassword“ für alle Objektklassen, die Passwortänderungen abonnieren sollen.


Klasse hinzufügen
Attribut bearb. ...
Löschen
Filter kopieren von...
Schablone festlegen
Filter
DirXML-nwoWorkOrder
User
city
company
Description
Full Name
Given Name
jackNumber
L
preferredName
Surname
Telephone Number
Title
nspmDistributionPassword
DirXML-pbxExtension
Description
Klassenname: User
Attributname: Attributinformationen
Anwendungsname:
Veröffentlichen:
Synchronisieren
Ignorieren
Benachrichtigen
Zurücksetzen
Abonnieren:
Synchronisieren
Ignorieren
Benachrichtigen
Zurücksetzen
Zusammenführungsstelle:
Standard
Identitätsdepot

3 Setzen Sie für alle Objekte, bei denen der Wert *Benachrichtigen* für das Attribut „nspmDistributionPassword“ eingestellt wurde, die Attribute „Öffentlicher Schlüssel“ und „Privater Schlüssel“ im Treiberfilter auf *Ignorieren*.



4 Damit die Passwortsicherheit gewährleistet ist, müssen Sie die Kontrolle darüber behalten, wer Zugriffsrechte auf Identity Manager-Objekte haben soll.

Fehlersuche bei Szenario 3

- „Flussdiagramm für Szenario 3“ auf Seite 138
- „Probleme bei der Anmeldung bei eDirectory“ auf Seite 139
- „Probleme bei der Anmeldung an einem anderen verbundenen System, das Passwörter abonniert“ auf Seite 140
- „Keine Email-Generierung bei Passwortfehlern“ auf Seite 140
- „Fehler beim Ausführen der Task „Passwortstatus überprüfen““ auf Seite 141
- „Hilfreiche DSTrace-Befehle“ auf Seite 141

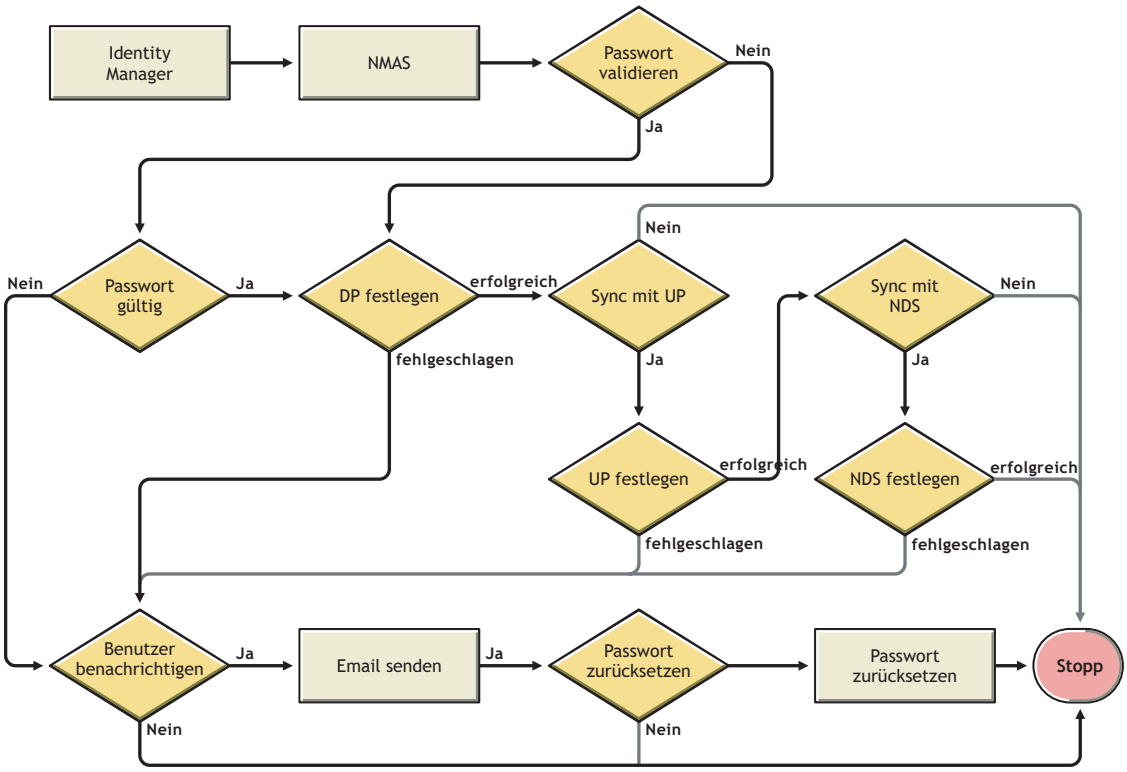
Beachten Sie auch die Tipps in Abschnitt 5.13, „Fehlersuche bei der Passwortsynchronisierung“, auf Seite 169.

Flussdiagramm für Szenario 3

Das folgende Flussdiagramm zeigt, wie NMAS mit dem von Identity Manager empfangenen Passwort verfährt. In diesem Szenario wird das Passwort mit dem Verteilungspasswort synchronisiert; dabei trifft NMAS folgende Entscheidungen:

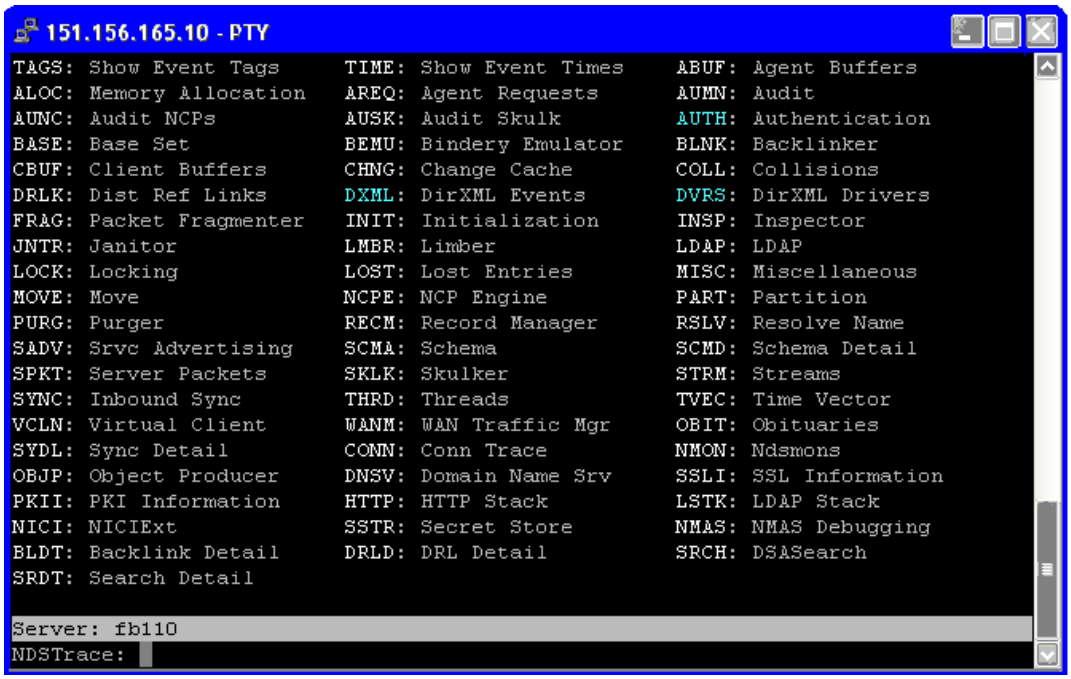
- Wie das Passwort zu verarbeiten ist, und zwar abhängig davon, ob eingehende Passwörter auf ihre Regelkonformität mit der Passwortrichtlinie überprüft werden (wenn das universelle Passwort und erweiterte Passwortregeln aktiviert sind).
- Welche anderen Einstellungen in der Passwortrichtlinie für das Synchronisieren des universellen Passworts mit den anderen Passwörtern festgelegt sind.

Abbildung 5-12 *Das Passwort aus Identity Manager wird mit dem Verteilungspasswort synchronisiert*



- Aktivieren Sie in DSTrace die Einstellungen *+AUTH*, *+DXML* und *+DVRS* .

Abbildung 5-13 *DSTrace-Befehle*



- Überzeugen Sie sich davon, dass das Element <password> oder <modify-password> an Identity Manager übergeben wird. Beobachten Sie zur Kontrolle den DSTrace-Bildschirm oder die Trace-Datei bei aktivierten Trace-Optionen, wie im ersten Arbeitsschritt erläutert.
- Überzeugen Sie sich davon, dass das Passwort gemäß den Regeln der NMAS-Passwortrichtlinie gültig ist.
- Überprüfen Sie die Konfiguration und Zuweisung der NMAS-Passwortrichtlinie. Weisen Sie die Richtlinie versuchsweise dem Benutzer direkt zu, um sicherzustellen, dass die korrekte Richtlinie verwendet wird.
- Stellen Sie sicher, dass auf der Seite „Passwortsynchronisierung“ für den Treiber die Option *Identity Manager akzeptiert Passwörter (Herausgeberkanal)* ausgewählt ist.
- Stellen Sie sicher, dass in der NMAS-Passwortrichtlinie die Option *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren* ausgewählt ist.
- Stellen Sie sicher, dass in der NMAS-Passwortrichtlinie die Option *NDS-Passwort bei Auswahl des universellen Passworts synchronisieren* ausgewählt ist, falls dieses Verhalten gewünscht wird.
- Wenn sich Benutzer über den Novell Client oder ConsoleOne anmelden, überprüfen Sie die Versionsnummer. Ältere Novell Clients und ConsoleOne können sich unter Umständen nicht beim Identitätsdepot anmelden, wenn das universelle Passwort nicht mit dem NDS-Passwort synchronisiert ist.

  Es sind Versionen des Novell Client und von ConsoleOne verfügbar, die das universelle Passwort erkennen. Weitere Informationen hierzu finden Sie im *NMAS 3.0 Administration*

Guide (http://www.novell.com/documentation/nmas30/index.html) (MAS 3.0 Administrationshandbuch).

- Einige ältere Dienstprogramme authentifizieren unter Verwendung des NDS-Passworts und können sich ebenfalls nicht beim Identitätsdepot anmelden, wenn das universelle Passwort nicht mit dem NDS-Passwort synchronisiert ist. Wenn Sie das NDS-Passwort für die meisten Benutzer nicht verwenden möchten, einige Administratoren oder Helpdesk-Benutzer jedoch die Authentifizierung über ältere Dienstprogramme nutzen müssen, können Sie den Helpdesk-Benutzern versuchsweise eine andere Passwortrichtlinie zuweisen. Auf diese Weise können andere Optionen für die Synchronisierung des universellen Passworts festgelegt werden.

Probleme bei der Anmeldung an einem anderen verbundenen System, das Passwörter abonniert

Dieser Abschnitt befasst sich mit der Fehlersuche in Situationen, in denen ein verbundenes System Passwörter gegenüber Identity Manager veröffentlicht, ein anderes verbundenes System, das ebenfalls Passwörter veröffentlicht, jedoch anscheinend keine Änderungen von dem anderen System mitgeteilt bekommt. Bei dieser Konstellation spricht man auch von einem „sekundären verbundenen System“, weil das zweite verbundene System die Passwörter über Identity Manager vom ersten verbundenen System erhält.

- Aktivieren Sie in DSTrace die Einstellungen +DXML und *+DVRS*, um sich die Regelverarbeitung durch Identity Manager und mögliche Fehlermeldungen ansehen zu können.
- Stellen Sie die Identity Manager LDAP Trace-Stufe für den Treiber auf *3* ein.
- Stellen Sie sicher, dass auf der Seite „Passwortsynchronisierung“die Option *Identity Manager akzeptiert Passwörter (Herausgeberkanal)* ausgewählt ist.
- Stellen Sie sicher, dass in der Passwortrichtlinie die Option *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren* nicht ausgewählt ist.

  Identity Manager verwendet das Verteilungspasswort, um Passwörter mit verbundenen Systemen zu synchronisieren. Das universelle Passwort muss mit dem Verteilungspasswort synchronisiert sein, damit diese Synchronisierungsmethode funktioniert.
- Kontrollieren Sie im Treiberfilter das Attribut „nspmDistributionPassword“.
- Überzeugen Sie sich davon, dass das <password>-Element für ein Add- oder <modify-password>-Element für das Attribut „nspmDistributionPassword“ in die Attributoperationen „Add“ bzw. „Modify“ umgeändert wurde. Beobachten Sie zur Kontrolle den DSTrace-Bildschirm oder die DSTrace-Datei bei aktivierten Trace-Optionen, wie im ersten Arbeitsschritt erläutert.
- Überzeugen Sie sich davon, dass die Treiberkonfiguration die Passwortrichtlinien für das Identity Manager-Skript an der richtigen Stelle und in der richtigen Reihenfolge enthält, wie in Abschnitt 5.3.4, „In der Treiberkonfiguration benötigte Richtlinien“, auf Seite 94 beschrieben.
- Vergleichen Sie die Passwortrichtlinie im Identitätsdepot mit etwaigen Passwortrichtlinien, die von dem verbundenen System durchgesetzt werden, um sicherzustellen, dass die Richtlinien kompatibel sind.

Keine Email-Generierung bei Passwortfehlern

- Aktivieren Sie in DSTrace die Einstellung *+DXML*, um sich die Regelverarbeitung durch Identity Manager ansehen zu können.
- Stellen Sie die Identity Manager LDAP Trace-Stufe für den Treiber auf *3* ein.

- Überzeugen Sie sich davon, dass die Regel für das Erzeugen einer Email-Benachrichtigung ausgewählt ist.
- Überzeugen Sie sich davon, dass das Identitätsdepot-Objekt im Attribut „Internet EMail Address“ den richtigen Wert für den Benutzer enthält.
- Stellen Sie sicher, dass der SMTP-Server und die Email-Schablone in der Aufgabe „Benachrichtigungskonfiguration“ richtig konfiguriert sind. Weitere Informationen hierzu finden Sie in Abschnitt 5.12, „Konfigurieren der Email-Benachrichtigung“, auf Seite 156.

Email-Benachrichtigungen sind nicht-invasiv, d. h., sie haben keinerlei Auswirkungen auf die Verarbeitung des XML-Dokuments, das das Versenden der Email ausgelöst hat. Tritt beim Versand der Email-Benachrichtigung ein Fehler auf, wird der Vorgang nur dann wiederholt, wenn die Operation selbst wiederholt wird. Debug-Meldungen zu Email-Benachrichtigungen werden in die Trace-Datei geschrieben.

Fehler beim Ausführen der Task „Passwortstatus überprüfen“

Die Task „Passwortstatus überprüfen“ in iManager bewirkt, dass der Treiber die Aktion „Objektpasswort überprüfen“ ausführt.

- Stellen Sie sicher, dass das verbundene System das Überprüfen von Passwörtern unterstützt. Weitere Informationen hierzu finden Sie in Abschnitt 5.2, „Unterstützung von verbundenen Systemen bei der Passwortsynchronisierung“, auf Seite 86.

  Wenn das Treibermanifest nicht anzeigt, dass das verbundene System das Überprüfen von Passwörtern unterstützt, kann diese Operation über iManager nicht ausgeführt werden.
- Wenn die Task „Objektpasswort überprüfen“ den Code „-603“ zurückgibt, fehlt im Identitätsdepot-Objekt das Attribut „nspmDistributionPassword“. Überprüfen Sie den Treiberfilter und die Option *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren* innerhalb der Passwortrichtlinie.
- Wenn die Task „Objektpasswort überprüfen“ die Meldung `Nicht synchronisiert` zurückgibt, vergewissern Sie sich, dass die Treiberkonfiguration die entsprechenden Identity Manager-Passwortsynchronisierungsrichtlinien enthält.
- Vergleichen Sie die Passwortrichtlinie im Identitätsdepot mit etwaigen Passwortrichtlinien, die von dem verbundenen System durchgesetzt werden, um sicherzustellen, dass die Richtlinien kompatibel sind.
- Die Task *Objektpasswort überprüfen* überprüft das Verteilungspasswort. Wenn das Verteilungspasswort nicht aktualisiert wird, meldet die Aktion *Objektpasswort überprüfen* eventuell nicht, dass die Passwörter synchronisiert wurden.
- Denken Sie daran, dass die Task *Passwortstatus überprüfen* für das Identitätsdepot das NDS-Passwort anstelle des universellen Passworts überprüft. Wenn also in der Passwortrichtlinie des Benutzers keine Synchronisierung des NDS-Passworts mit dem universellen Passwort festgelegt ist, wird immer gemeldet, dass die Passwörter nicht synchronisiert wurden. Das Verteilungspasswort und das Passwort auf dem verbundenen System können durchaus synchronisiert sein, die Task „Passwortstatus überprüfen“ liefert jedoch erst dann ein korrektes Ergebnis, wenn das NDS-Passwort und das Verteilungspasswort mit dem universellen Passwort synchronisiert wurden.

Hilfreiche DSTrace-Befehle

+DXML: Zum Anzeigen der Regelverarbeitung durch Identity Manager und möglicher Fehlermeldungen.

+DVRS: Zum Anzeigen der Meldungen des Identity Manager-Treibers

*+AUTH:*Zum Anzeigen der Änderungen am NDS-Passwort

5.8.5 Szenario 4: Tunneling – Synchronisieren verbundener Systeme (aber nicht eines Identitätsdepots) mit Aktualisierung des Verteilungspassworts durch Identity Manager

Identity Manager bietet die Möglichkeit, Passwörter zwischen verbundenen Systemen zu synchronisieren und das Identitätsdepot-Passwort separat zu behandeln. Diese Verfahrensweise wird als „Tunneling“ bezeichnet.

In diesem Szenario aktualisiert Identity Manager das Verteilungspasswort direkt. Dieses Szenario entspricht weitgehend Abschnitt 5.8.4, „Szenario 3: Synchronisieren des Identitätsdepots und der verbundenen Systeme mit Aktualisierung des Verteilungspassworts durch Identity Manager“, auf Seite 130. Der einzige Unterschied besteht darin, dass Sie dafür sorgen, dass das universelle Passwort und das Verteilungspasswort nicht synchronisiert werden. Dazu verzichten Sie entweder auf die Verwendung von NMAS-Passwortrichtlinien oder Sie verwenden Passwortrichtlinien, bei denen die Option *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren* deaktiviert ist.

Vor- und Nachteile von Szenario 4

Tabelle 5-14 *Vorteile durch Tunneling*

Vorteile	Nachteile
Ermöglicht die Synchronisierung von Passwörtern zwischen verbundenen Systemen bei separater Behandlung des Identitätsdepot-Passworts. Passwortrichtlinien sind nicht erforderlich. Wenn Sie eine Passwortrichtlinie verwenden, muss darin das universelle Passwort nicht aktiviert sein. Die Umgebung muss jedoch das universelle Passwort unterstützen. Unterstützt die Aufgabe „Passwortstatus überprüfen“ in iManager, wenn diese vom verbundenen System unterstützt wird. Sie können festlegen, dass eine Benachrichtigung gesendet wird, falls bei der Passwortsynchronisierung ein Fehler auftritt. Sie können das Passwort eines verbundenen Systems zurücksetzen, wenn dieses nicht der Passwortrichtlinie entspricht. Wenn das universelle Passwort und erweiterte Passwortregeln aktiviert sind, werden Passwortrichtlinien erzwungen, wenn Sie dies festlegen, und Passwörter auf verbundenen Systemen können zurückgesetzt werden.	Wenn das universelle Passwort oder die erweiterten Passwortregeln nicht aktiviert sind, werden keine Passwortrichtlinien erzwungen und Passwörter auf verbundenen Systemen können nicht zurückgesetzt werden.

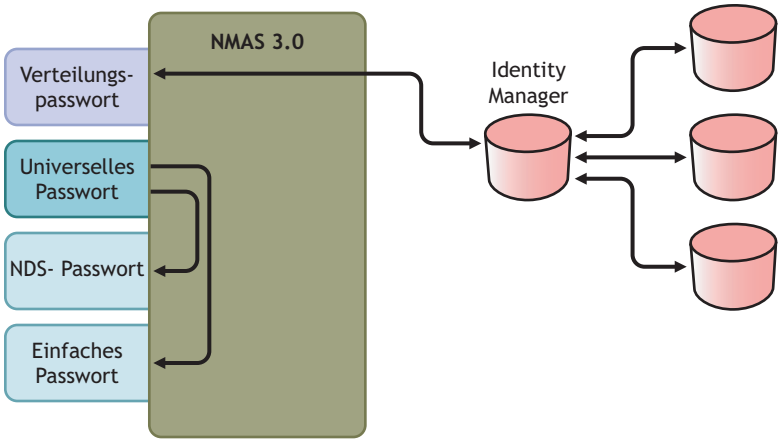
Das Diagramm zu diesem Szenario zeigt folgenden Verlauf:

1. Passwörter treffen über Identity Manager ein.
2. Identity Manager geht über NMAS, um das Verteilungspasswort direkt zu aktualisieren.
3. Identity Manager verwendet das Verteilungspasswort auch, um Passwörter an verbundene Systeme zu übergeben, die Sie für das Akzeptieren von Passwörtern konfiguriert haben.

Entscheidend bei diesem Szenario ist, dass in der NMAS-Passwortrichtlinie die Option *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren* deaktiviert ist. Da das Verteilungspasswort nicht mit dem universellen Passwort synchronisiert wird, synchronisiert Identity Manager Passwörter zwischen verbundenen Systemen, ohne dass dies Auswirkungen auf Passwörter im Identitätsdepot hat.

Obwohl in diesem Diagramm gleich mehrere Systeme mit Identity Manager verbunden sind, gilt es zu beachten, dass die Einstellungen für die Treiber jedes verbundenen Systems einzeln festgelegt werden müssen.

Abbildung 5-14 *Tunneling mit Aktualisierung des Verteilungspassworts durch Identity Manager*



Einrichten von Szenario 4

Damit Sie diese Art der Passwortsynchronisierung einrichten können, müssen Sie Folgendes konfigurieren:

- „Implementierung des universellen Passworts“ auf Seite 144
- „Konfiguration der Passwortrichtlinie“ auf Seite 144
- „Einstellungen für die Passwortsynchronisierung“ auf Seite 145
- „Treiberkonfiguration“ auf Seite 145

Implementierung des universellen Passworts

Obwohl in den Passwortrichtlinien das universelle Passwort nicht aktiviert sein muss, muss Ihre Umgebung dennoch eDirectory 8.7.3 (mit Unterstützung für das universelle Passwort) verwenden. Weitere Informationen hierzu finden Sie in Abschnitt 5.4, „Vorbereitungen zur Nutzung der Identity Manager-Passwortsynchronisierung und des universellen Passworts“, auf Seite 100.

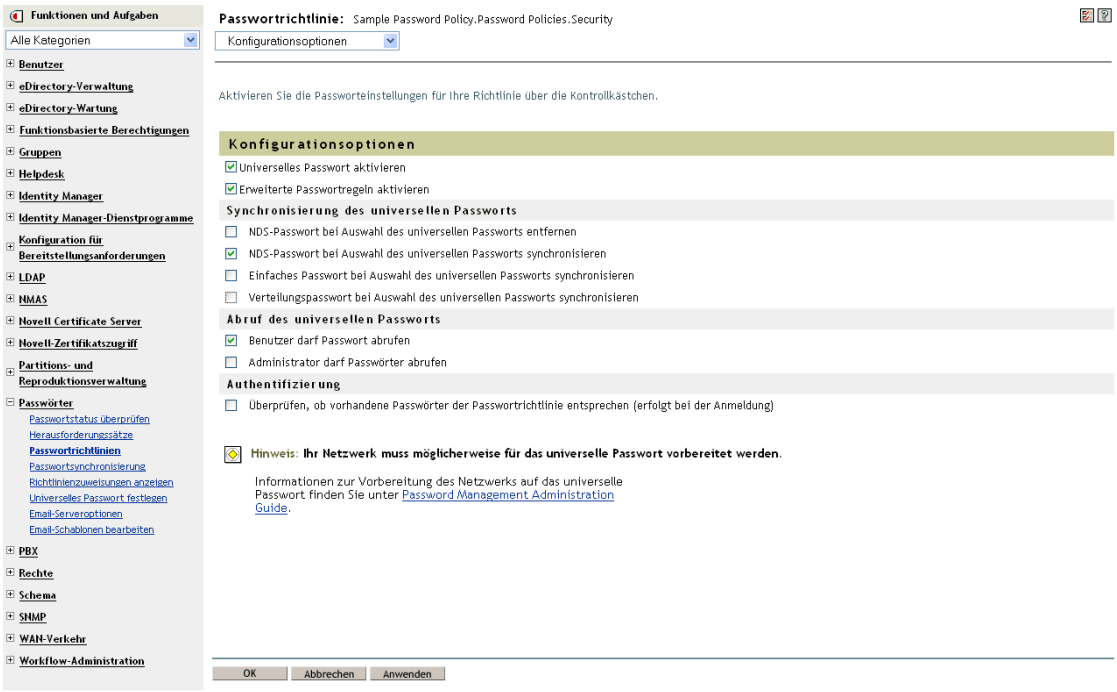
Konfiguration der Passwortrichtlinie

Bei dieser Methode wird für Identitätsdepot-Benutzer keine Passwortrichtlinie benötigt.

Wenn Sie dennoch eine Passwortrichtlinie verwenden möchten, müssen Sie Folgendes tun:

1. Stellen Sie sicher, dass die folgenden Optionen nicht ausgewählt sind:
   - *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren*

     Dieser Punkt ist entscheidend für das Tunneling von Passwörtern unter Ausschluss des Identitätsdepot-Passworts. Da das Verteilungspasswort nicht mit dem universellen Passwort synchronisiert wird, wird das Verteilungspasswort separat behandelt und nur von Identity Manager nur für verbundene Systeme verwendet. Identity Manager tritt dabei als „Tunnel“ auf, der Passwörter unter Ausschluss des Identitätsdepot-Passworts mit anderen verbundenen Systemen austauscht.



2 Vervollständigen Sie die anderen Einstellungen der Passwortrichtlinie nach Bedarf.

Die anderen Passworteinstellungen in der Passwortrichtlinie sind optional.

Einstellungen für die Passwortsynchronisierung

Verwenden Sie die gleichen Einstellungen wie unter Einstellungen für die Passwortsynchronisierung in Abschnitt 5.8.4, „Szenario 3: Synchronisieren des Identitätsdepots und der verbundenen Systeme mit Aktualisierung des Verteilungspassworts durch Identity Manager“, auf Seite 130.

Treiberkonfiguration

Verwenden Sie die gleichen Einstellungen wie unter Treiberkonfiguration in Abschnitt 5.8.4, „Szenario 3: Synchronisieren des Identitätsdepots und der verbundenen Systeme mit Aktualisierung des Verteilungspassworts durch Identity Manager“, auf Seite 130.

Fehlersuche bei Szenario 4

Wenn beim Tunneling eine Passwortsynchronisierung eingerichtet ist, unterscheidet sich das Verteilungspasswort vom universellen Passwort und vom NDS-Passwort.

- „Probleme bei der Anmeldung an einem anderen verbundenen System, das Passwörter abonniert“ auf Seite 146
- „Ausbleiben der Email bei Passwortfehlern“ auf Seite 146
- „Fehler beim Ausführen der Task „Passwortstatus überprüfen““ auf Seite 147
- „Hilfreiche DSTrace-Befehle“ auf Seite 147

Beachten Sie auch die Tipps in Abschnitt 5.13, „Fehlersuche bei der Passwortsynchronisierung“, auf Seite 169.

Probleme bei der Anmeldung an einem anderen verbundenen System, das Passwörter abonniert

Dieser Abschnitt befasst sich mit der Fehlersuche in Situationen, in denen ein verbundenes System Passwörter gegenüber Identity Manager veröffentlicht, ein anderes verbundenes System, das ebenfalls Passwörter veröffentlicht, jedoch anscheinend keine Änderungen von dem anderen System mitgeteilt bekommt. Bei dieser Konstellation spricht man auch von einem „sekundären verbundenen System“, weil das zweite verbundene System die Passwörter über Identity Manager vom ersten verbundenen System erhält.

- Aktivieren Sie in DSTrace die Einstellungen +DXML und *+DVRS*, um sich die Regelverarbeitung durch Identity Manager und mögliche Fehlermeldungen ansehen zu können.
- Stellen Sie die Identity Manager LDAP Trace-Stufe für den Treiber auf *3* ein.
- Stellen Sie sicher, dass auf der Seite „Passwortsynchronisierung“ die Option *Identity Manager akzeptiert Passwörter (Herausgeberkanal)* ausgewählt ist.
- Stellen Sie sicher, dass in der Passwortrichtlinie die Option *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren* nicht ausgewählt ist.

  Identity Manager verwendet das Verteilungspasswort, um Passwörter mit verbundenen Systemen zu synchronisieren. Das universelle Passwort muss mit dem Verteilungspasswort synchronisiert sein, damit diese Synchronisierungsmethode funktioniert.
- Stellen Sie sicher, dass der Treiberfilter die richtigen Einstellungen für das Attribut „nspmDistributionPassword“ enthält.
- Überzeugen Sie sich davon, dass das `<password>`-Element für ein Add- und ein `<modify-password>`-Element für das Attribut „nspmDistributionPassword“ in die Attributoperationen „Add“ bzw. „Modify“ umgeändert wurden. Beobachten Sie zur Kontrolle den DSTrace-Bildschirm oder die Trace-Datei bei aktivierten Trace-Optionen, wie im ersten Arbeitsschritt erläutert.
- Überzeugen Sie sich davon, dass die Treiberkonfiguration die Passwortrichtlinien für das Identity Manager-Skript an der richtigen Stelle und in der richtigen Reihenfolge enthält, wie in Abschnitt 5.3.4, „In der Treiberkonfiguration benötigte Richtlinien“, auf Seite 94 beschrieben.
- Vergleichen Sie die Passwortrichtlinie im Identitätsdepot mit etwaigen Passwortrichtlinien, die von dem verbundenen System durchgesetzt werden, um sicherzustellen, dass die Richtlinien kompatibel sind.

Ausbleiben der Email bei Passwortfehlern

- Aktivieren Sie in DSTrace die Einstellung *+DXML*, um sich die Regelverarbeitung durch Identity Manager ansehen zu können.
- Stellen Sie die Identity Manager LDAP Trace-Stufe für den Treiber auf *3* ein.
- Überzeugen Sie sich davon, dass die Regel für das Erzeugen einer Email-Benachrichtigung ausgewählt ist.
- Überzeugen Sie sich davon, dass das Identitätsdepot-Objekt im Attribut „Internet EMail Address“ den richtigen Wert für den Benutzer enthält.
- Kontrollieren Sie den SMTP-Server und die Email-Schablone in der Aufgabe „Benachrichtigungskonfiguration“. Weitere Informationen hierzu finden Sie in Abschnitt 5.12, „Konfigurieren der Email-Benachrichtigung“, auf Seite 156.

Email-Benachrichtigungen sind nicht-invasiv, d. h., sie haben keinerlei Auswirkungen auf die Verarbeitung des XML-Dokuments, das das Versenden der Email ausgelöst hat. Tritt beim Versand

der Email-Benachrichtigung ein Fehler auf, wird der Vorgang nur dann wiederholt, wenn die Operation selbst wiederholt wird. Debug-Meldungen zu Email-Benachrichtigungen werden in die Trace-Datei geschrieben.

Fehler beim Ausführen der Task „Passwortstatus überprüfen“

Die Task „Passwortstatus überprüfen“ in iManager bewirkt, dass der Treiber die Aktion „Objektpasswort überprüfen“ ausführt.

- Stellen Sie sicher, dass das verbundene System das Überprüfen von Passwörtern unterstützt. Weitere Informationen hierzu finden Sie in Abschnitt 5.2, „Unterstützung von verbundenen Systemen bei der Passwortsynchronisierung“, auf Seite 86.

  Wenn das Treibermanifest nicht anzeigt, dass das verbundene System das Überprüfen von Passwörtern unterstützt, kann diese Operation über iManager nicht ausgeführt werden.
- Wenn die Task „Objektpasswort überprüfen“ den Code „-603“ zurückgibt, fehlt im Identitätsdepot-Objekt das Attribut „nspmDistributionPassword“. Überprüfen Sie den Filter für das Identity Manager-Attribut und die Option *Verteilungspasswort bei Auswahl des universellen Passworts synchronisieren* innerhalb der Passwortrichtlinie.
- Wenn die Aktion „Objektpasswort überprüfen“ die Meldung `Nicht synchronisiert` zurückgibt, vergewissern Sie sich, dass die Treiberkonfiguration die entsprechenden Identity Manager-Passwortsynchronisierungsrichtlinien enthält.
- Vergleichen Sie die Passwortrichtlinie im Identitätsdepot mit etwaigen Passwortrichtlinien, die von dem verbundenen System durchgesetzt werden, um sicherzustellen, dass die Richtlinien kompatibel sind.
- Die Aktion „Objektpasswort überprüfen“ überprüft das Verteilungspasswort. Wenn das Verteilungspasswort nicht aktualisiert wird, meldet die Aktion „Objektpasswort überprüfen“ eventuell nicht, dass die Passwörter synchronisiert wurden.

Hilfreiche DSTrace-Befehle

+DXML: Zum Anzeigen der Regelverarbeitung durch Identity Manager und möglicher Fehlermeldungen.

+DVRS: Zum Anzeigen der Meldungen des Identity Manager-Treibers

+AUTH: Zum Anzeigen der Änderungen am NDS-Passwort

+DCLN: Zum Anzeigen von Meldungen des NDS DClient

5.8.6 Szenario 5: Synchronisieren von Anwendungspasswörtern mit dem einfachen Passwort

Dieses Szenario stellt eine Spezialverwendung der Funktionen für die Passwortsynchronisierung dar. Mit Identity Manager und NMAS können Sie ein Passwort aus einem verbundenen System direkt mit dem einfachen Passwort des Identitätsdepots synchronisieren. Wenn das verbundene System nur Hash-kodierte Passwörter liefert, können Sie diese mit dem einfachen Passwort synchronisieren, ohne die Hash-Kodierung umkehren zu müssen. Danach können sich andere Anwendungen gegenüber dem Identitätsdepot unter Verwendung dieses Passworts (im Klartext oder Hash-kodiert) über LDAP oder den Novell Client authentifizieren, wobei die NMAS-Komponenten so konfiguriert sind, dass sie das einfache Passwort als Anmeldemethode verwenden.

Wenn das Passwort auf dem verbundenen System im Klartext vorliegt, kann es in dieser Form vom verbundenen System aus im Speicherbereich des Identitätsdepots für einfache Passwörter veröffentlicht werden.

Wenn das verbundene System nur Hash-kodierte Passwörter bereitstellt (unterstützt werden die Algorithmen MD5, SHA, SHA1 und UNIX Crypt), müssen Sie diese unter Angabe der verwendeten Hash-Kodierung (z. B. {MD5}) gegenüber dem einfachen Passwort veröffentlichen.

Soll eine andere Anwendung mit dem gleichen Passwort eine Authentifizierung durchführen, müssen Sie die andere Anwendung so anpassen, dass diese sich unter Verwendung des Benutzerpassworts über LDAP gegenüber dem einfachen Passwort authentifiziert.

NMAS vergleicht den Passwortwert, den es von der Anwendung erhält, mit dem Wert im einfachen Passwort. Wenn es sich bei dem im einfachen Passwort gespeicherten Passwort um einen Hash-Wert handelt, erstellt NMAS zunächst aus dem Wert des von der Anwendung übergebenen Passworts den korrekten Hash-Wert und führt dann den Vergleich durch. Wenn das Passwort aus der Anwendung und das einfache Passwort identisch sind, authentifiziert NMAS den Benutzer.

In diesem Szenario kann das universelle Passwort nicht verwendet werden.

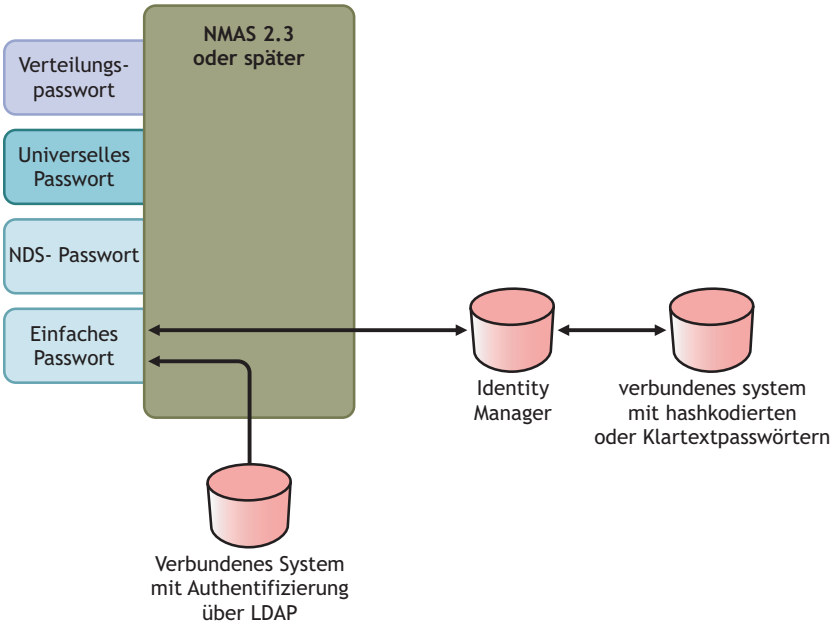
- „Vorteile beim Synchronisieren mit dem NDS-Passwort“ auf Seite 148
- „Szenario 5 einrichten“ auf Seite 149

Vorteile beim Synchronisieren mit dem NDS-Passwort

Tabelle 5-15 *Vorteile beim Synchronisieren mit dem NDS-Passwort*

Vorteile	Nachteile
• Ermöglicht die direkte Aktualisierung des einfachen Passworts. • Ermöglicht das Synchronisieren eines Hash-kodierten Passworts und dessen Verwendung für mehr als eine Anwendung, ohne die Hash-Kodierung umkehren zu müssen.	• In diesem Szenario ist die Verwendung des universellen Passworts nicht möglich. • Die Funktionen „Passwort vergessen“ und „Passwortselbstbedienung“ können weiterhin in dem Maße verwendet werden, wie sie für das NDS-Passwort unterstützt werden, nicht jedoch in Verbindung mit dem einfachen Passwort. • Da die Aufgabe „Universelles Passwort festlegen“ vom universellen Passwort abhängig ist, kann der Administrator mit dieser Aufgabe kein Benutzerpasswort im Identitätsdepot festlegen.

Abbildung 5-15 *Synchronisieren mit dem NDS-Passwort*



Szenario 5 einrichten

- „Konfiguration der Passwortrichtlinie“ auf Seite 149
- „Einstellungen für die Passwortsynchronisierung“ auf Seite 149
- „Treiberkonfiguration“ auf Seite 150

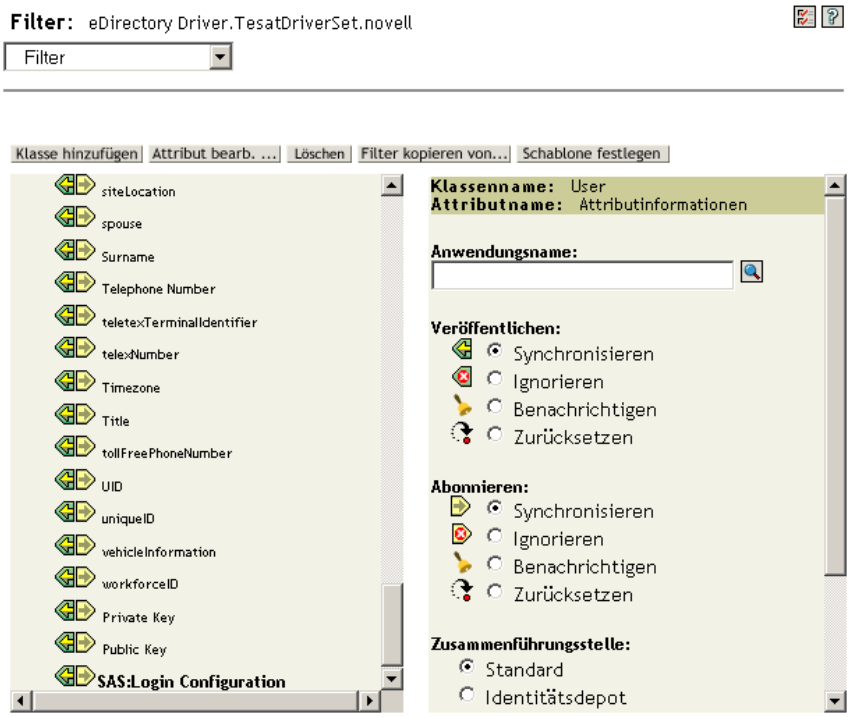
Konfiguration der Passwortrichtlinie

Bei dieser Methode wird für Benutzer keine Passwortrichtlinie benötigt. Das universelle Passwort kann nicht verwendet werden.

Einstellungen für die Passwortsynchronisierung

Bei diesem Szenario verwenden Sie Identity Manager Script, um das Attribut „SAS:Login Configuration“ direkt zu bearbeiten. Das bedeutet, dass die auf der Seite „Passwortsynchronisierung“ in iManager festgelegten Globalkonfigurationswerte (GCVs) für die Passwortsynchronisierung unwirksam sind.

1 Stellen Sie sicher, dass das Attribut „SAS:Login Configuration“ im Filter sowohl für den Herausgeberkanal als auch für den Abonnentenkanal auf *Synchronisieren* eingestellt ist.



2 Konfigurieren Sie die Treiberrichtlinien so, dass das Passwort aus dem verbundenen System veröffentlicht wird.

3 Konfigurieren Sie die Treiberrichtlinien für Hash-kodierte Passwörter so, dass der Hash-Typ dem Passwort vorangestellt wird (falls dieser nicht schon von der Anwendung geliefert wird).

- {MD5}*hashed_password*

  Dieses Passwort ist Base 64-kodiert.

- {SHA}*hashed_password*

  Dieses Passwort ist Base 64-kodiert.

- {CRYPT}*hashed_password*

Klartextpasswörter und mit Unix Crypt Hash-kodierte Passwörter sind nicht Base64-kodiert.

4 Um das Passwort an das einfache Passwort zu übergeben, konfigurieren Sie die Treiberrichtlinien so, dass das Attribut „SAS:Login Configuration“ verändert wird.

Das folgende Beispiel zeigt, wie das Element „modify-attr“ innerhalb einer modify-Operation verwendet wird, um das einfache Passwort in ein mit MD5 Hash-kodiertes Passwort umzuändern:

```
<modify-attr attr-name="SAS:Login Configuration>
    <add-value>
        <value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value>
```

```
    </add-value>
</modify-attr>
```

Richten Sie sich bei Klartextpasswörtern nach folgendem Beispiel:

```
<modify-attr attr-name="SAS:Login Configuration>
    <add-value>
        <value>clearpwd</value>
    </add-value>
</modify-attr>
```

Bei add-Operationen enthält das Element „add-attr“ eine der folgenden Werte:

```
<add-attr attr-name="SAS:Login Configuration>
    <value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value>
</add-attr>
```

oder:

```
<add-attr attr-name="SAS:Login Configuration>
    <value>clearpwd</value>
</add-attr>
```

5.9 Einrichten von Passwortfiltern

Manche verbundenen Systeme können das tatsächliche Passwort des Benutzers an Identity Manager übergeben.

Wenn Sie Passwörter unter Active Directory, NIS und NT Domain erfassen möchten, müssen Sie kleinere Eingriffe an der Konfiguration vornehmen, um Passwortfilter auf verbundenen Systemen installieren zu können.

- Abschnitt 5.9.1, „Einrichten von Passwortsynchronisierungsfiltern für Active Directory und NT Domain“, auf Seite 151
- Abschnitt 5.9.2, „Einrichten von Passwortsynchronisierungsfiltern für NIS“, auf Seite 152

5.9.1 Einrichten von Passwortsynchronisierungsfiltern für Active Directory und NT Domain

Diese Informationen finden Sie in den Abschnitten zur Passwortsynchronisierung in den Treiber-Implementierungshandbüchern zu den Identity Manager-Treibern für Active Directory und NT Domain unter Identity Manager Drivers (http://www.novell.com/documentation/dirxmldrivers/index.html).

Es genügt, wenn der Identity Manager-Treiber für AD oder NT Domain auf einem einzigen Windows-Computer installiert wird. Auf den anderen Domänencontrollern muss der Treiber nicht installiert sein, allerdings muss auf jedem Domänencontroller die Datei `pwfilter.dll` installiert sein, um Passwörter erfassen und an Identity Manager senden zu können.

Zur Vereinfachung der Konfiguration und Administration wird ein Dienstprogramm bereitgestellt, das diese Installation von dem Windows-Computer aus, auf dem der Treiber installiert ist, für alle Domänencontroller durchführt.

5.9.2 Einrichten von Passwortsynchronisierungsfiltern für NIS

Der Identity Manager-Treiber für NIS 3.0 unterstützt drei Datenspeicher für die UNIX-Authentifizierung: Dateien, NIS und NIS+. Ein PAM-Modul übernimmt das Erfassen der Passwörter und ihre Übergabe an den Identity Manager-Treiber für NIS.

Die Implementierung des PAM-Moduls für den NIS-Treiber ist im *Identity Manager Driver for NIS Implementation Guide* (Identity Manager-Treiber für NIS Implementierungshandbuch) unter Identity Manager Drivers (http://www.novell.com/documentation/lg/dirxmldrivers/index.html) beschrieben.

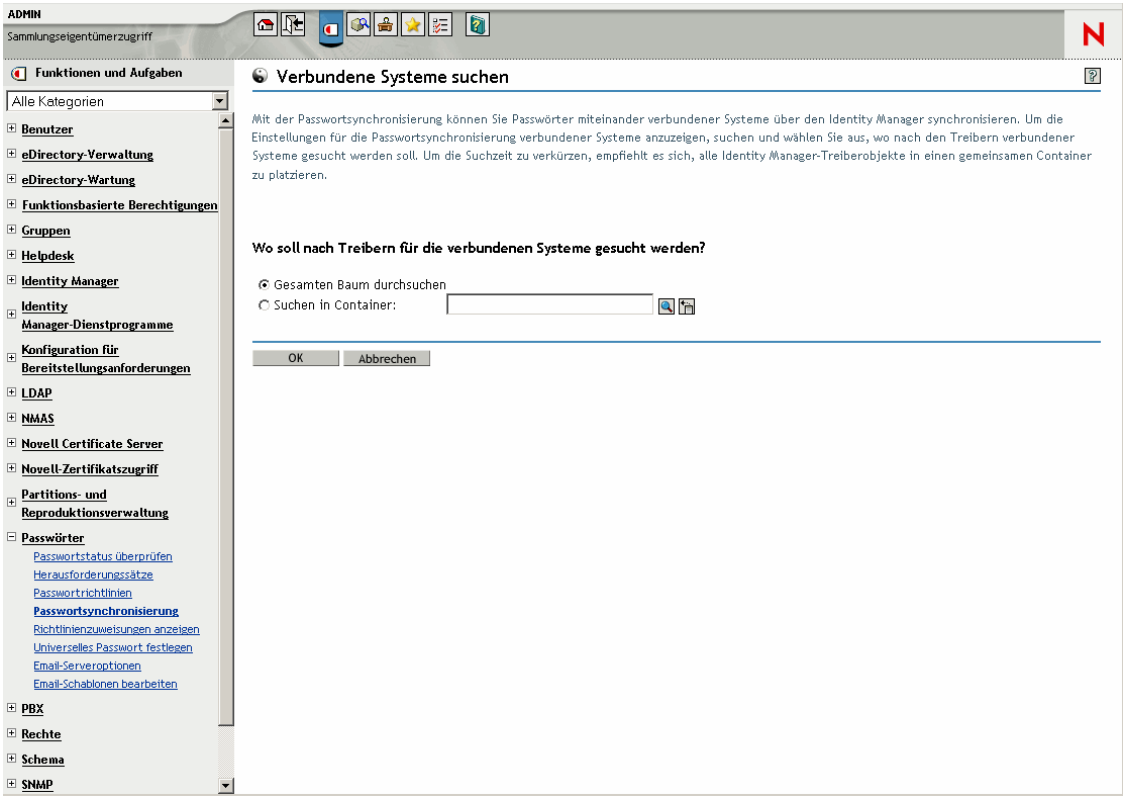
5.10 Verwalten der Passwortsynchronisierung

- „Einrichten des Passwort-Transfers zwischen den Systemen“ auf Seite 152
- „Durchsetzen von Passwortrichtlinien auf verbundenen Systemen“ auf Seite 154
- „eDirectory-Passwort vom synchronisierten Passwort getrennt halten“ auf Seite 154

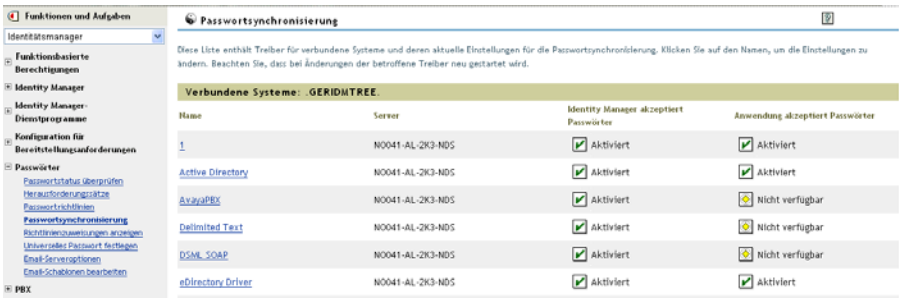
5.10.1 Einrichten des Passwort-Transfers zwischen den Systemen

So zeigen Sie die Einstellungen der Systeme für die Annahme oder das Veröffentlichen von Passwörtern an:

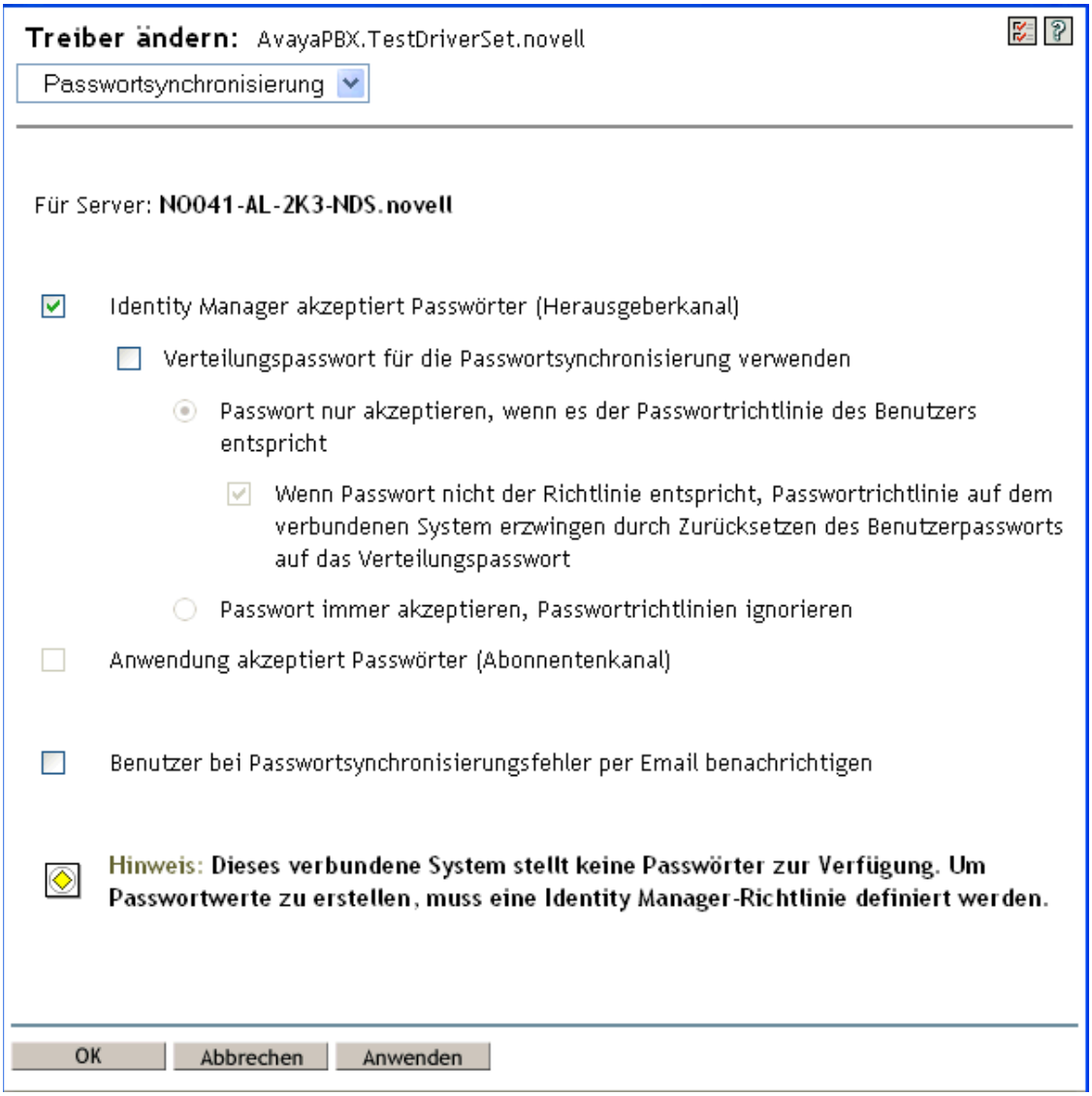
1. Klicken Sie in iManager auf *Passwörter* > *Passwortsynchronisierung*.
2. Suchen Sie nach Treibern für die verbundenen Systeme.



In den Suchergebnissen werden die Einstellungen für den Passwortaustausch zwischen Identity Manager und den verbundenen Systemen angezeigt.



Klicken Sie zum Ändern dieser Einstellungen auf den Treibernamen eines verbundenen Systems.



Auf der Seite „Treiber ändern“ können Sie einstellen, ob eine Passwortrichtlinie für Passwörter durchgesetzt werden soll, die bei Identity Manager eingehen, und ob eine Passwortrichtlinie auf dem

verbundenen System durch Zurücksetzen des Passworts aus dem verbundenen System durchgesetzt werden soll.

Bei den Einstellungen auf dieser Seite handelt es sich um Globalkonfigurationswerte (GCVs), die serverspezifisch gespeichert werden. Weitere Informationen hierzu finden Sie in Abschnitt 5.3.3, „Steuerung der Passwortsynchronisierung über Globalkonfigurationswerte“, auf Seite 90.

5.10.2 Durchsetzen von Passwortrichtlinien auf verbundenen Systemen

Bei Verwendung von erweiterten Passwortregeln und der Identity Manager-Passwortsynchronisierung werden folgende Schritte empfohlen:

1. Untersuchen Sie die Passwortrichtlinien der verbundenen Systeme.
2. Stellen Sie sicher, dass die erweiterten Passwortregeln mit den Passwortrichtlinien auf den verbundenen Systemen kompatibel sind.

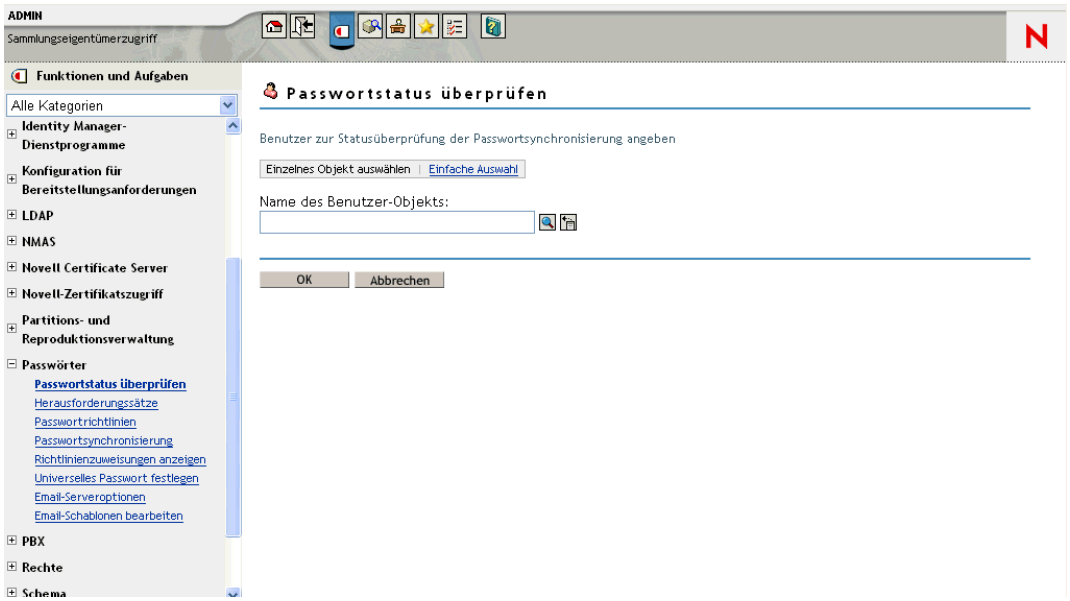
5.10.3 eDirectory-Passwort vom synchronisierten Passwort getrennt halten

Dieses Szenario ist in Abschnitt 5.8.5, „Szenario 4: Tunneling – Synchronisieren verbundener Systeme (aber nicht eines Identitätsdepots) mit Aktualisierung des Verteilungspassworts durch Identity Manager“, auf Seite 142 beschrieben.

5.11 Überprüfen des Passwortsynchronisierungsstatus eines Benutzers

Sie können feststellen, ob das Verteilungspasswort eines bestimmten Benutzers mit dem Passwort im verbundenen System identisch ist.

1 Klicken Sie in iManager auf *Passwörter* > *Passwortstatus überprüfen*.



2 Wählen Sie einen Benutzer aus.

Die Aufgabe *Passwortstatus überprüfen* bewirkt, dass der Treiber die Aktion „Objektpasswort überprüfen“ ausführt.

Nicht alle Treiber unterstützen die Passwortüberprüfung. Bei Treibern, die diese Funktion unterstützen, muss dies im Treibermanifest vorgesehen sein. iManager verhindert die Übergabe von Operationen zum Überprüfen von Passwörtern an Treiber, bei denen diese Funktion im Treibermanifest nicht vorgesehen ist.

Die Aktion „Objektpasswort überprüfen“ überprüft das Verteilungspasswort. Wenn das Verteilungspasswort nicht aktualisiert wird, meldet die Aktion „Objektpasswort überprüfen“ eventuell, dass die Passwörter nicht synchronisiert sind.

Das Verteilungspasswort wird in den folgenden Situationen nicht aktualisiert:

- Sie verwenden die in Abschnitt 5.8.2, „Szenario 1: Synchronisierung zwischen zwei Identitätsdepots über das NDS-Passwort“, auf Seite 117 beschriebene Synchronisierungsmethode.
- Sie synchronisieren das universelle Passwort (wie in Abschnitt 5.8.3, „Szenario 2: Synchronisieren unter Verwendung des universellen Passworts“, auf Seite 119 beschrieben), haben jedoch in der Passwortrichtlinie nicht die Konfigurationsoption für das Synchronisieren des universellen Passworts mit dem Verteilungspasswort aktiviert.

Hinweis: Denken Sie daran, dass die Aktion „Passwortstatus überprüfen“ für das Identitätsdepot das NDS-Passwort anstelle des universellen Passworts überprüft. Wenn also in der Passwortrichtlinie des Benutzers keine Synchronisierung des NDS-Passworts mit dem universellen Passwort vorgesehen ist, wird immer gemeldet, dass die Passwörter nicht synchronisiert wurden. Das Verteilungspasswort und das Passwort auf dem verbundenen System können durchaus synchronisiert sein, die Task „Passwortstatus überprüfen“ liefert jedoch erst dann ein korrektes Ergebnis, wenn das NDS-Passwort und das Verteilungspasswort mit dem universellen Passwort synchronisiert wurden.

5.12 Konfigurieren der Email-Benachrichtigung

Mit iManager-Tasks können Sie den Email-Server festlegen und die Email-Benachrichtigungsschablonen anpassen.

Email-Schablonen werden bereitgestellt, um den Funktionen „Passwortsynchronisierung“ und „Passwortselbstbedienung“ das Senden automatisch erstellter Emails an Benutzer zu ermöglichen.

Diese Schablonen werden nicht von Ihnen erstellt. Sie werden vielmehr von der Anwendung bereitgestellt, die sie verwendet. Bei den Email-Schablonen handelt es sich um Schablonenobjekte im Identitätsdepot, die im Sicherheitscontainer abgelegt werden; der sich in der Regel im Stammordner des Baums befindet. Obwohl es sich um Objekte des Identitätsdepots handelt, sollten Sie diese nur mit iManager bearbeiten.

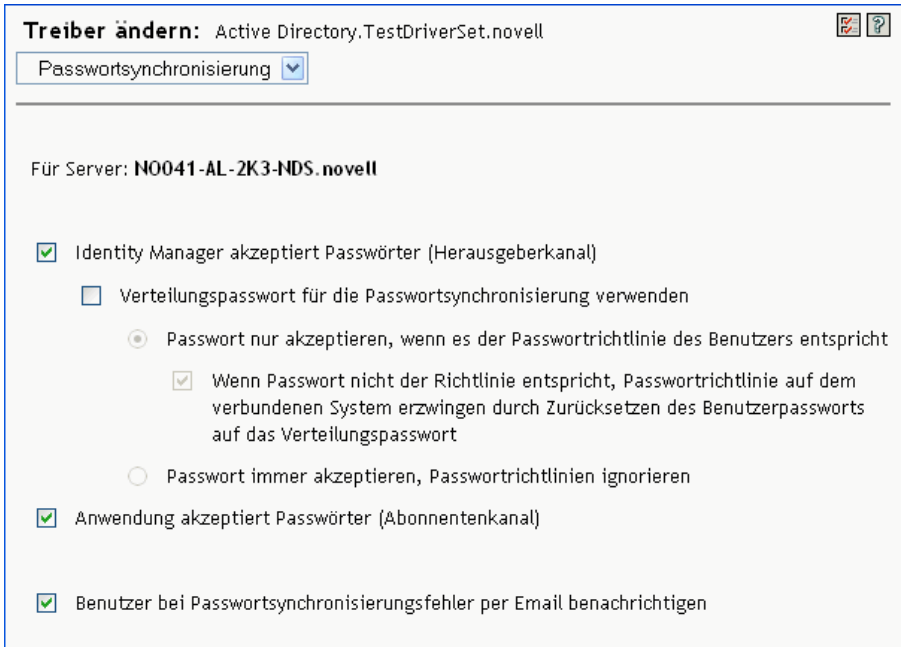
Es handelt sich um ein modulares Framework. Beim Hinzufügen neuer Anwendungen, die diese Email-Schablonen verwenden, können gleichzeitig auch die Schablonen installiert werden.

Über die Optionen in iManager legen Sie fest, ob Emails gesendet werden oder nicht. In Verbindung mit der Funktion „Passwort vergessen“ werden Email-Benachrichtigungen nur gesendet, wenn Sie eine der folgenden Aktionen der Funktion „Passwort vergessen“ auswählen, durch die das Senden einer Email ausgelöst wird: Das Senden eines Passworts oder eines Passworthinweises an den Benutzer per Email. Siehe “Providing Users with Forgotten Password Self-Service” im *Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung).

Wenn Sie die Option *Benutzer bei Passwortsynchronisierungsfehler per Email benachrichtigen* auswählen, wird die Passwortsynchronisierung so konfiguriert, dass Emails nur bei

Passwortsynchronisierungsfehlern und nur bei den von Ihnen festgelegten Treibern gesendet werden.

Abbildung 5-16 *Passwortsynchronisierung konfigurieren*



Darüber hinaus müssen Sie sicherstellen, dass die Informationen für die SMTP-Authentifizierung in den Treiberrichtlinien enthalten sind.

- Abschnitt 5.12.1, „Voraussetzungen“, auf Seite 157
- Abschnitt 5.12.2, „Den SMTP-Server für das Senden von Email-Benachrichtigungen einrichten“, auf Seite 158
- „Einrichten von Email-Schablonen für Benachrichtigungen“ auf Seite 159
- Abschnitt 5.12.4, „Bereitstellen von SMTP-Authentifizierungsdaten in Treiberrichtlinien“, auf Seite 160
- Abschnitt 5.12.5, „Hinzufügen eigener Platzhalter-Tags zu Email-Benachrichtigungsschablonen“, auf Seite 162
- Abschnitt 5.12.6, „Senden von Email-Benachrichtigungen an den Administrator“, auf Seite 168
- Abschnitt 5.12.7, „Übersetzen von Email-Benachrichtigungsschablonen“, auf Seite 169

5.12.1 Voraussetzungen

- ❑ Stellen Sie sicher, dass das Attribut „Internet EMail Address“ für die im Identitätsdepot enthaltenen Benutzer hinterlegt wurde.
- ❑ Bei Verwendung von Email-Benachrichtigungen für die Passwortsynchronisierung müssen Sie sicherstellen, dass die Treiberrichtlinien für die Passwortsynchronisierung das Passwort für den SMTP-Server enthalten. Weitere Informationen hierzu finden Sie in Abschnitt 5.12.4, „Bereitstellen von SMTP-Authentifizierungsdaten in Treiberrichtlinien“, auf Seite 160.

- ❑ Wenn Sie sich nicht sicher sind, ob die Email-Adresse bei allen Benutzern eingetragen ist, oder eine Email-Chronik aller Fehlerbenachrichtigungen möchten, können Sie das Konto eines Passwort-Administrators angeben, an den sämtliche an die Benutzer gerichteten Email-Benachrichtigungen ebenfalls gesendet werden.

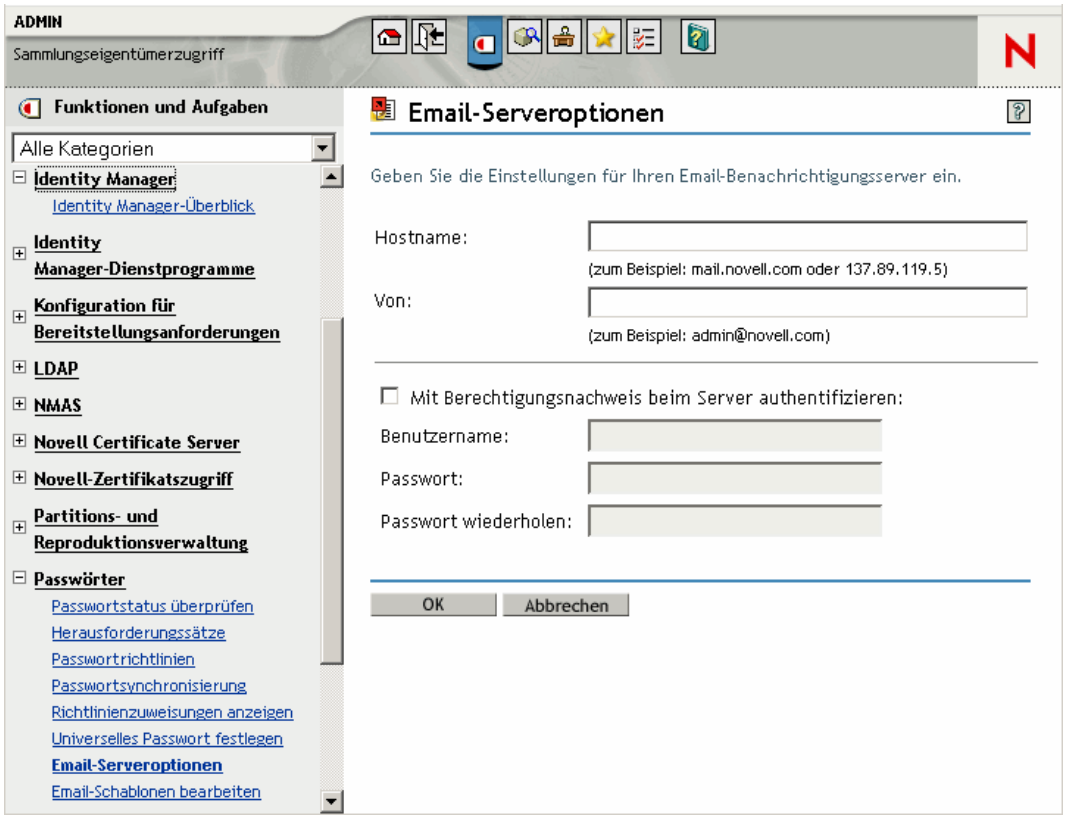
  Diese Email-Adresse sollte im Feld *An* der Identity Manager-Skriptrichtlinie stehen. Weitere Informationen finden Sie unter Abschnitt 5.12.6, „Senden von Email-Benachrichtigungen an den Administrator“, auf Seite 168.

- ❑ Wenn eDirectory und Identity Manager auf einem UNIX-Server laufen, muss der Server eine Reproduktion der Email-Schablonenobjekte bereithalten.

  Diese Objekte sind im Sicherheitscontainer gespeichert (im Stamm). Der Server benötigt somit eine Reproduktion der Stammpartition.

5.12.2 Den SMTP-Server für das Senden von Email-Benachrichtigungen einrichten

1 Klicken Sie in iManager auf *Passwörter* > *Email-Serveroptionen*.



2 Geben Sie Folgendes ein:

- Hostname
- Der Name (z. B. „Administrator“), der im Absenderfeld der Email angezeigt werden soll
- Der Benutzername und das Passwort für die Authentifizierung beim Server, falls erforderlich

3 Klicken Sie auf *OK*.

4 Wenn Sie die Passwortsynchronisierung mit den Identity Manager-Treibern verwenden und die Funktion „Email-Benachrichtigung“ verwenden möchten, müssen Sie auch Folgendes tun:

4a Wenn vor dem Senden einer Email eine Authentifizierung beim SMTP-Server erforderlich ist, müssen Sie sicherstellen, dass das Passwort in den Treiberrichtlinien enthalten ist. Weitere Informationen hierzu finden Sie in Abschnitt 5.12.4, „Bereitstellen von SMTP-Authentifizierungsdaten in Treiberrichtlinien“, auf Seite 160.

Für Benachrichtigungen in Verbindung mit der Funktion „Passwort vergessen“ genügt es, die Authentifizierungsdaten auf der Seite „Email-Serveroptionen“ in Schritt 2 einzugeben, nicht jedoch für Benachrichtigungen in Verbindung mit der Passwortsynchronisierung.

4b Starten Sie die Identity Manager-Treiber neu, die mit den Änderungen aktualisiert werden müssen.

Der Treiber liest die Schablonen und die SMTP-Serverdaten nur beim Starten ein.

5 Passen Sie die Email-Schablonen wie unter „Einrichten von Email-Schablonen für Benachrichtigungen“ auf Seite 159 beschrieben an.

Nachdem Sie den Email-Server eingerichtet haben, können Email-Benachrichtigungen von den Anwendungen gesendet werden, wenn Sie Funktionen verwenden, die das Versenden von Email-Benachrichtigungen auslösen.

5.12.3 Einrichten von Email-Schablonen für Benachrichtigungen

Sie können diese Schablonen mit benutzerdefiniertem Text anpassen. Der Verwendungszweck einer Schablone geht aus ihrem Namen hervor.

1 Klicken Sie in iManager auf *Passwörter* > *Email-Schablonen bearbeiten*.

2 Bearbeiten Sie die Schablonen nach Ihren Vorstellungen.

Beachten Sie, dass zusätzliche Schritte erforderlich sein können, wenn Sie Platzhalter-Tags hinzufügen möchten. Befolgen Sie die Anweisungen in Abschnitt 5.12.5, „Hinzufügen eigener Platzhalter-Tags zu Email-Benachrichtigungsschablonen“, auf Seite 162.

3 Starten Sie die Identity Manager-Treiber neu, die mit den Änderungen aktualisiert werden müssen.

   Der Treiber liest die Schablonen und die SMTP-Serverdaten nur beim Starten ein.

5.12.4 Bereitstellen von SMTP-Authentifizierungsdaten in Treiberrichtlinien

Legen Sie den Benutzernamen und das Passwort für den SMTP-Server wie in Abschnitt 5.12.2, „Den SMTP-Server für das Senden von Email-Benachrichtigungen einrichten“, auf Seite 158 beschrieben fest. Diese Angaben reichen für Email-Benachrichtigungen in Verbindung mit der Funktion „Passwort vergessen“ aus.

Für Email-Benachrichtigungen in Verbindung mit Passwortsynchronisierungen müssen Sie jedoch das Passwort auch in die Treiberrichtlinien aufnehmen. Die Metaverzeichnis-Engine kann auf den Benutzernamen, nicht jedoch auf das Passwort zugreifen. Dieses muss von der Treiberrichtlinie bereitgestellt werden.

Sie müssen diesen Ablauf in den folgenden Situationen einhalten:

- Der SMTP-Server ist gesichert und verlangt vor dem Senden von EMails eine Authentifizierung.
- Sie verwenden die Identity Manager-Passwortsynchronisierung mit einem Identity Manager-Treiber.
- Sie haben in den Einstellungen des Treibers für die Passwortsynchronisierung die Option *Benutzer bei Passwortsynchronisierungsfehler per Email benachrichtigen* ausgewählt.

So nehmen Sie das Passwort für den SMTP-Server in die Treiberrichtlinie auf:

1 Stellen Sie sicher, dass der Treiber die zur Passwortsynchronisierung erforderlichen Richtlinien enthält.

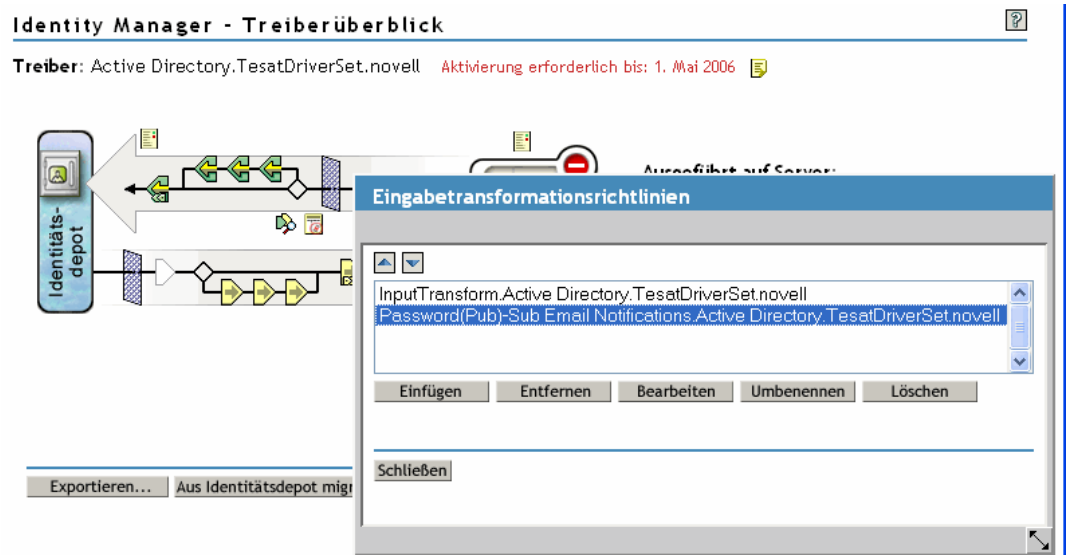
   Diese Richtlinien sind in der Beispiel-Treiberkonfiguration enthalten, können aber auch wie in Abschnitt 5.7, „Upgrade bestehender Treiberkonfigurationen zur Unterstützung der Passwortsynchronisierung“, auf Seite 106 beschrieben hinzugefügt werden.

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

3 Suchen Sie den gewünschten Treibersatz oder wählen Sie einen Container aus, der den Treibersatz enthält.

4 Klicken Sie auf der Seite „Identity Manager - Treiberüberblick“ auf das Symbol für den Treiber.

5 Klicken Sie auf ein Eingabetransformations- oder Ausgabetransformationssymbol.



6 Wählen Sie eine Richtlinie aus und klicken Sie anschließend auf *Bearbeiten*.

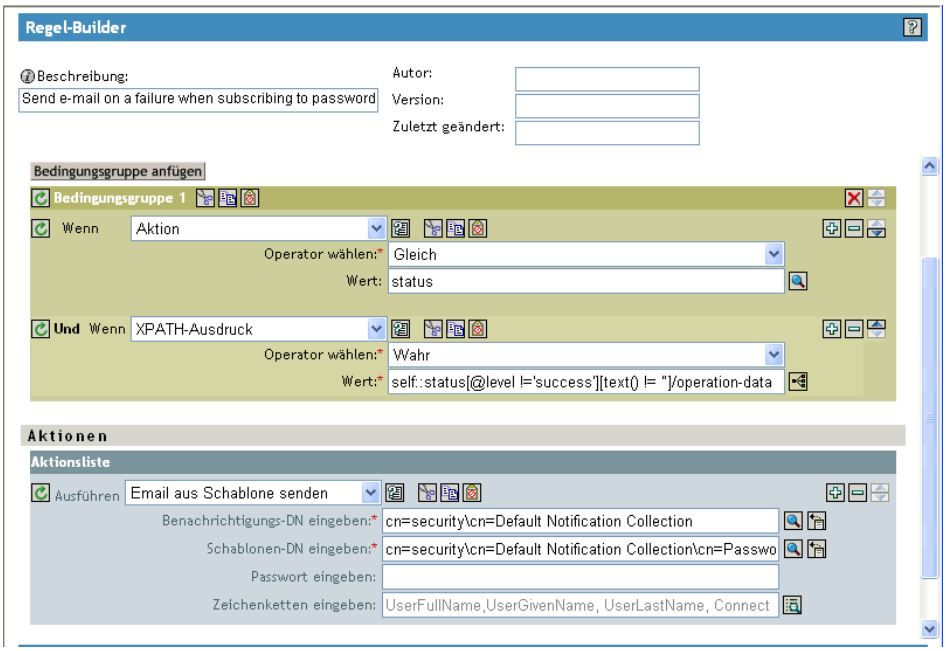
7 Klicken Sie auf eine Regel.

8 Geben Sie das Passwort für den SMTP-Server in den Regeln an, die Aktionen vom Typ „Email aus Schablone senden“ beinhalten.

Wenn Sie beispielsweise die Beispiel-Treiberkonfigurationen verwenden, müssen Sie die folgenden Passwortsynchronisierungsrichtlinien ändern.

Richtliniensatz	Richtlinienname	Regelname
Eingabetransformation	Password(Pub)-Sub Email Notifications	• Email senden, wenn beim Passwortabonnement Fehler auftreten • Email senden, wenn beim Zurücksetzen des Passworts des verbundenen Systems mit dem Passwort der Identity Manager-Datenablage Fehler auftreten
Ausgabetransformation	Password(Sub)-Pub Email Notifications	• Email senden, wenn bei Passwortveröffentlichungen Fehler auftreten

Die folgende Abbildung zeigt ein Beispiel für eine Aktion vom Typ „Email aus Schablone senden“, für die das Passwort erforderlich ist.



Das Passwort wird unkenntlich gemacht, wenn es im Identitätsdepot gespeichert wird.

9 Wählen Sie die Regel aus und klicken Sie auf OK.

5.12.5 Hinzufügen eigener Platzhalter-Tags zu Email-Benachrichtigungsschablonen

Die Email-Benachrichtigungsschablonen enthalten einige vordefinierte Tags, um Ihnen das Personalisieren der Benachrichtigung für den Benutzer zu erleichtern. Sie haben aber auch die Möglichkeit, eigene Tags hinzuzufügen.

Welche Tags Sie hinzufügen können, hängt von der Anwendung ab, von der die Email-Schablone verwendet werden soll.

- „Hinzufügen von Platzhalter-Tags zu Email-Benachrichtigungsschablonen des Typs „Passwortsynchronisierung““ auf Seite 162
- „Hinzufügen von Platzhalter-Tags zu Email-Benachrichtigungsschablonen des Typs „Passwort vergessen““ auf Seite 168

Hinzufügen von Platzhalter-Tags zu Email-Benachrichtigungsschablonen des Typs „Passwortsynchronisierung“

Sie können Platzhalter-Tags in Email-Benachrichtigungsschablonen einfügen. Diese Tags funktionieren allerdings erst, wenn Sie in den Regeln sämtlicher Passwortsynchronisierungsrichtlinien, die auf die betreffenden Email-Benachrichtigungsschablonen verweisen, definiert sind. Bei Verwendung einer Aktion vom Typ „DoSendEmailFromTemplate“ müssen alle in der Schablone enthaltenen Platzhalter-Tags als untergeordnete „arg-strings“-Elemente der Aktion definiert sein.

Identity Manager stellt beispielsweise Standard-Platzhalter-Tags zur Verfügung, die in den Email-Benachrichtigungsschablonen enthalten sind. Außerdem stellt Identity Manager in den Treiberkonfigurationen Standardrichtlinien für die Passwortsynchronisierung bereit. Jeder Standard-Tag in einer Email-Schablone ist auch in jeder Regel der Passwortsynchronisierungsrichtlinie definiert, die die Email-Schablone verwendet.

Der Tag „UserGivenName“ ist beispielsweise einer der Standard-Tags in der Email-Schablone „Password Set Fail“ (Festlegen des Passworts fehlgeschlagen). Eine Richtlinie mit der Bezeichnung *Email bei fehlerhaften Passwortveröffentlichungen senden* verweist in der Aktion „DoSendEmailFromTemplate“ auf diese Email-Schablone. Diese Regel wird in einer Richtlinie verwendet, um einen Benutzer zu benachrichtigen, wenn bei der Passwortsynchronisierung ein Fehler aufgetreten ist. Das gleiche UserGivenName-Tag wird in dieser Regel als Element vom Typ „arg-string“ definiert.

Wie in diesem Beispiel erläutert, muss jedes neue Tag sowohl in der Email-Schablone als auch in den Richtlinienregeln definiert sein, die auf die Email-Schablone verweisen, damit die Metaverzeichnis-Engine weiß, wie sie das Platzhalter-Tag beim Senden der Email an den Benutzer durch die entsprechenden Daten ersetzen soll.

Sie können sich dabei an den Tags in den mitgelieferten Identity Manager-Treiberkonfigurationen orientieren.

Beachten Sie dabei Folgendes:

- Die in den Email-Schablonen enthaltenen Platzhalter-Tags heißen im Kontext des Richtlinien-Builders „Token“.
- Sie sollten den Richtlinien-Builder verwenden, um das Definieren der Argument-Strings für Platzhalter-Tags zu vereinfachen, wie in den Verfahrensschritten oben beschrieben.
- Sie können z. B. folgende Platzhalter-Tags hinzufügen:
  - Ausgangs- oder Zielattribute für den Benutzer

    Anders als beim Einfügen von Tags in Email-Schablonen des Typs „Passwort vergessen“ funktioniert ein solches Tag nicht automatisch, wenn es denselben Namen wie ein Attribut des Benutzerobjekts im Identitätsdepot hat. Wie bei allen Tags in Email-Benachrichtigungsschablonen zur Passwortsynchronisierung müssen Sie das Tag auch in der Richtlinie definieren, die auf die Email-Schablone verweist.
  - Ein Globalkonfigurationswert
  - Ein XPATH-Ausdruck

  In diesen Punkten unterscheiden sich Tags für die Passwortsynchronisierung von Tags in der Schablone „Passwort vergessen“, die ausschließlich als Platzhalter für eDirectory-Benutzerattribute dienen.
- Anders als beim Einfügen von Tags in Email-Schablonen des Typs „Passwort vergessen“ (mit der obligatorischen Verwendung des exakten Namens eines eDirectory-Benutzerattributs), können Sie die Platzhalter-Tags beliebig benennen, solange der Tag-Name mit dem Namen identisch ist, der zum Definieren des Tags in den Richtlinien verwendet wurde, die auf die Email-Schablone verweisen.

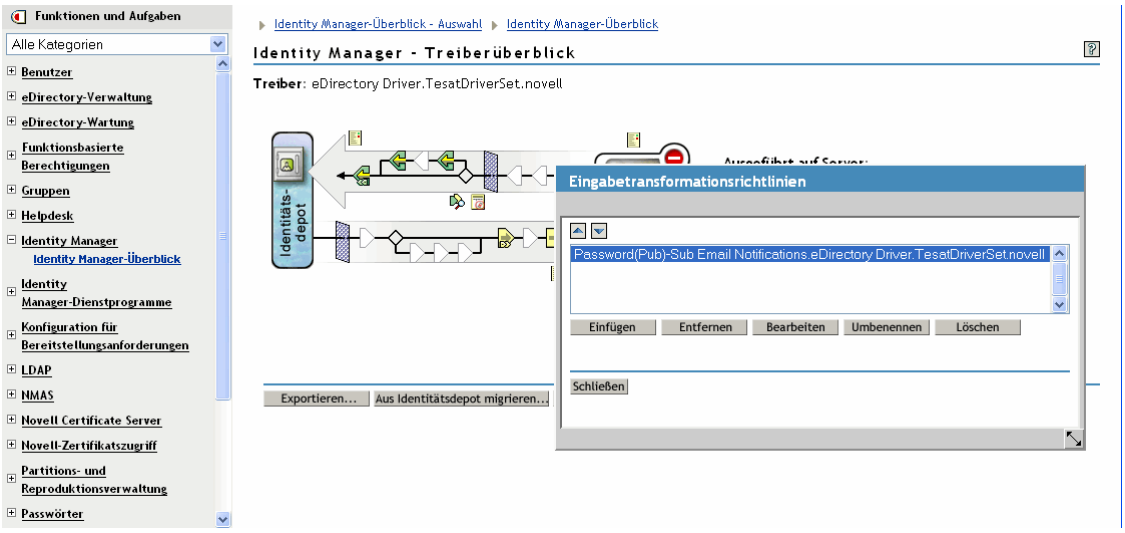
Suchen Sie zum Definieren der Tags in einer Richtlinie alle Richtlinien, die auf die betreffende Email-Benachrichtigungsschablone verweisen, und verwenden Sie dann den Richtlinien-Builder zum Einfügen der Tags. Bearbeiten Sie in jeder Richtlinie sämtliche Regeln, die auf die Schablone verweisen.

Eine Möglichkeit, um zuverlässig alle auf die Email-Benachrichtigungsschablonen verweisenden Richtlinien aufzufinden, besteht darin, die Treiberkonfiguration zu exportieren und anschließend das XML-Dokument nach Aktionen vom Typ „do-send-e-mail“ zu durchsuchen, die eine Schablone des gleichen Namens wie die Schablone für die Email-Benachrichtigungen verwendet.

1. Klicken Sie in iManager auf *Identity Manager > Identity Manager-Überblick*.
2. Wählen Sie den Treibersatz aus, der den Treiber mit der zu bearbeitenden Richtlinie enthält.
3. Klicken Sie auf das Symbol für den Treiber mit der gewünschten Richtlinie.
4. Klicken Sie im Herausgeber- oder Abonnentenkanal auf den Richtliniensatz, der die gewünschte Richtlinie enthält.

   Die Treiberkonfiguration für den mit Identity Manager gelieferten eDirectory-Treiber enthält beispielsweise im Richtliniensatz für Eingabetransformationen eine Richtlinie, die auf beide Email-Benachrichtigungsschablonen zur Passwortsynchronisierung verweist.
5. Klicken Sie auf die Richtlinie und anschließend auf *Bearbeiten*.

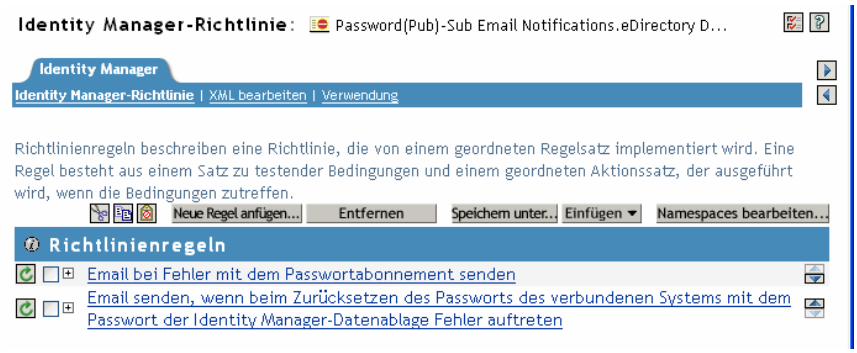
   Die folgende Abbildung zeigt das Bearbeiten der Richtlinie „Password(Pub)-Sub Email Notifications“ für die eDirectory-Treiber:



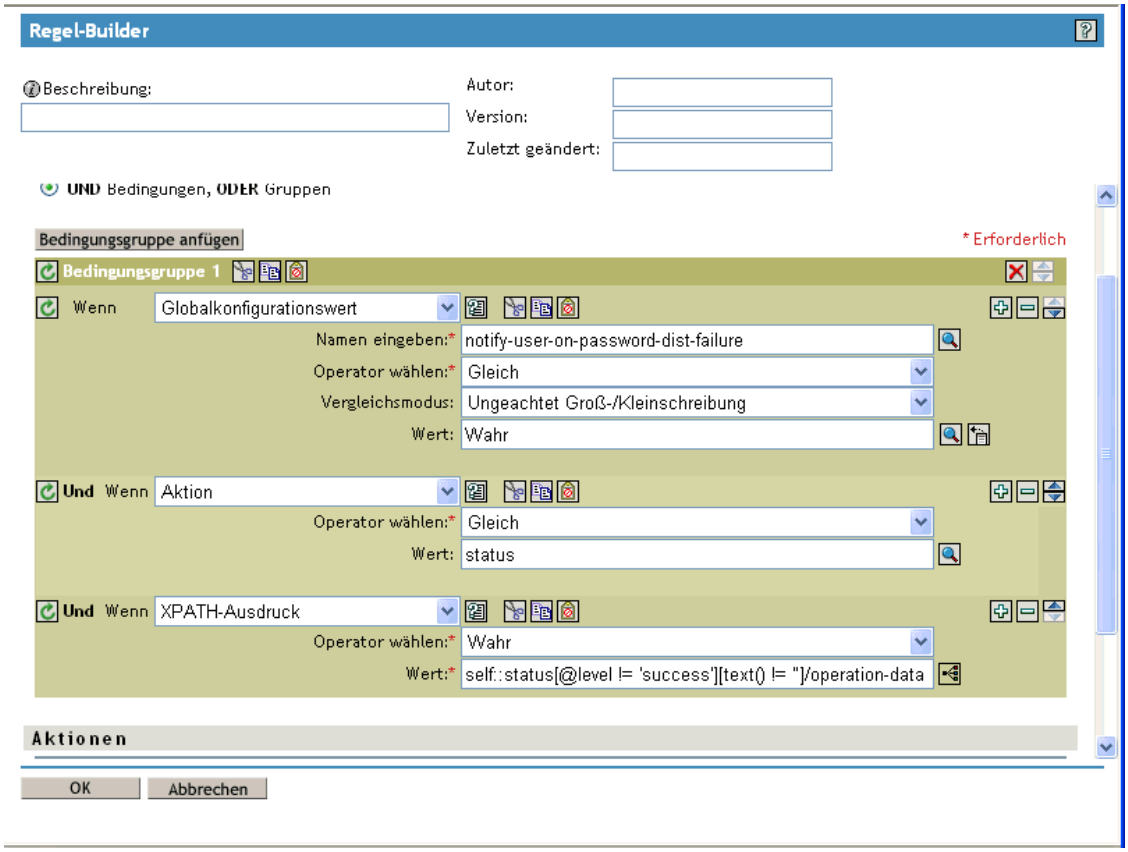
6. Klicken Sie in der Regelliste auf die Regel, die auf die Email-Benachrichtigungsschablone verweist.

   Bei der Richtlinie „Password(Pub)-Sub Email Notifications “ wird beispielsweise die abgebildete Regelliste angezeigt. Beide Regeln verweisen auf eine der Email-Schablonen für

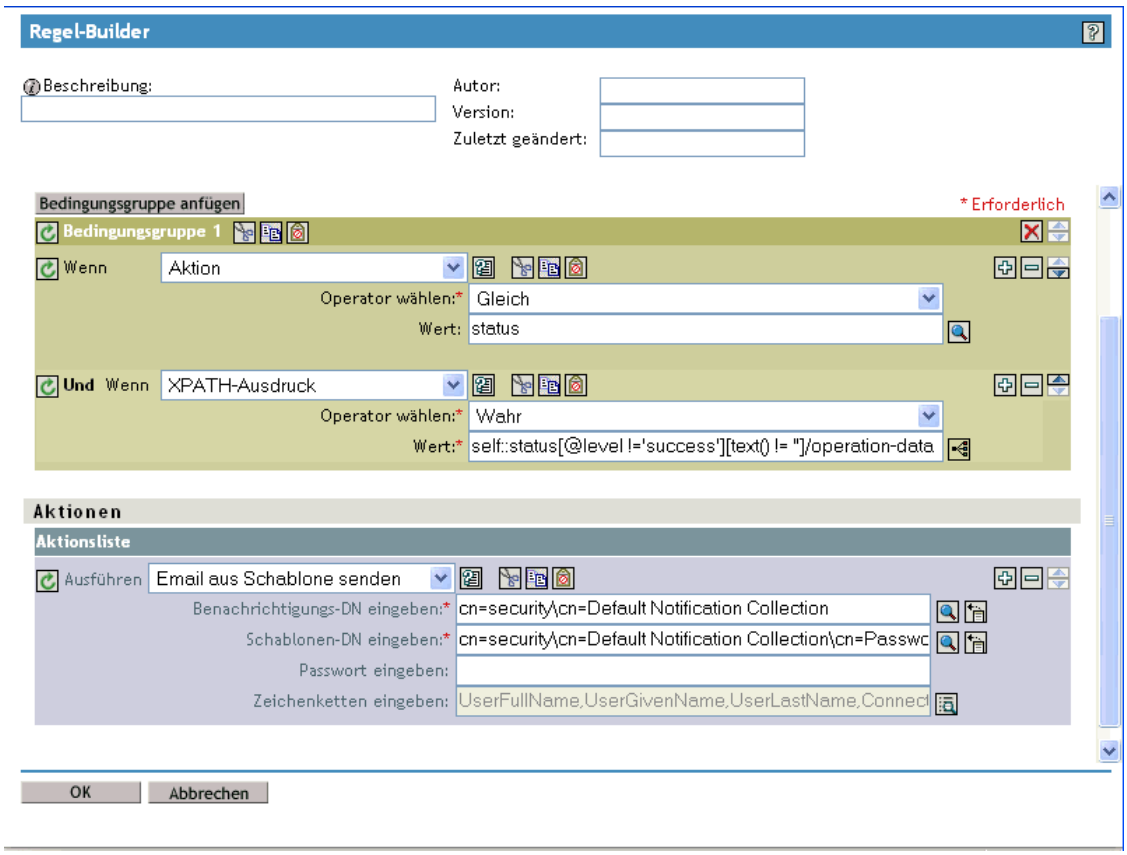
die Passwortsynchronisierung. Sie müssen beide Regeln bearbeiten, wenn Sie Tags in beide Schablonen einfügen möchten.



Wenn Sie auf die erste Regel klicken, wird die folgende Seite angezeigt:

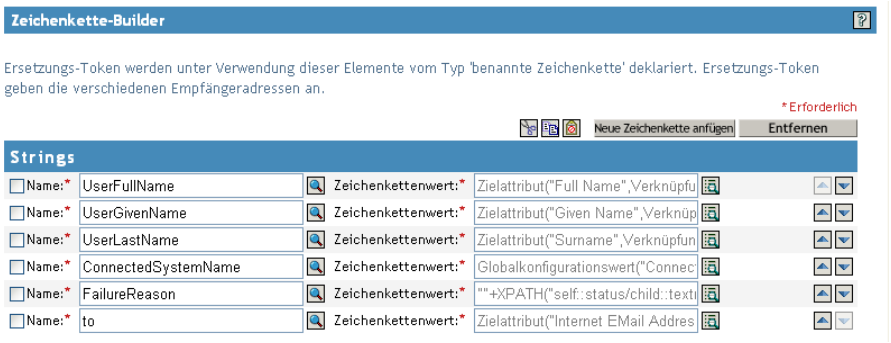


7 Blättern Sie zum Abschnitt *Aktionen*.



8 Klicken Sie für die Regel *Email aus Schablone senden* auf die Schaltfläche „Durchsuchen“ neben dem Feld *Zeichenketten eingeben*.

Der Zeichenkette-Builder wird geöffnet. Die folgende Abbildung zeigt die Liste der Zeichenketten, die bei dieser Beispielregel angezeigt wird. Beachten Sie, dass die in den Email-Benachrichtigungsschablonen verwendeten Standard-Tags bereits in den Passwortsynchronisierungsrichtlinien definiert sind, die - wie in diesem Fall - Bestandteil der Identity Manager-Treiberkonfigurationen sind. Sie können die Standard-Tags als Beispiele verwenden.



9 Klicken Sie zum Definieren eines Tags, das Sie in einer Email-Benachrichtigungsschablone verwenden können, auf *Neue Zeichenkette anfügen* und geben Sie anschließend einen Namen für das Tag ein.

Achten Sie darauf, dass Sie den Namen genau so wie in der Email-Benachrichtigungsschablone eingeben.

10 Klicken Sie neben dem Feld *Zeichenkettenwert* auf die Schaltfläche „Durchsuchen“ , um den Tag leichter definieren zu können.

11 Geben Sie auf der Seite „Argument-Builder“ den Wert an, der eingefügt werden soll, wenn dieses Tag in einer Email-Benachrichtigungsschablone verwendet wird.

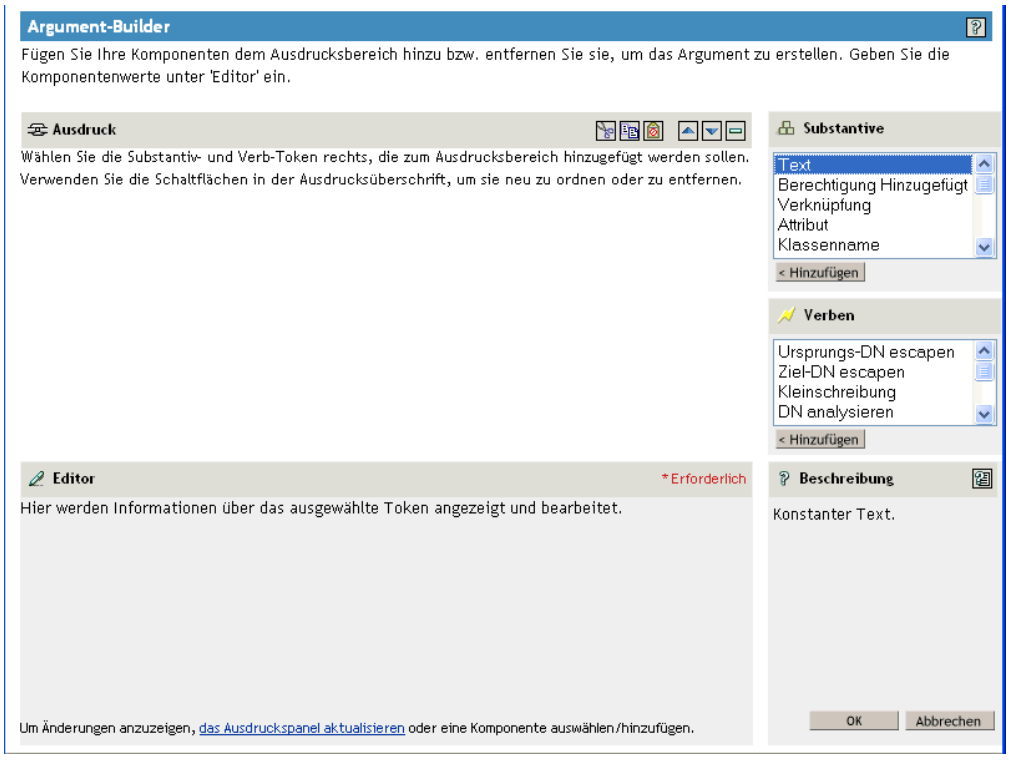
Das Tag kann folgende Werte annehmen:

- Ausgangs- oder Zielattribute für den Benutzer

  Anders als beim Einfügen von Tags in Email-Schablonen des Typs „Passwort vergessen“ funktioniert ein solches Tag nicht automatisch, wenn es denselben Namen wie ein Attribut des Benutzerobjekts im Identitätsdepot hat. Wie bei allen Tags in Email-Benachrichtigungsschablonen zur Passwortsynchronisierung müssen Sie das Tag auch in der Richtlinie definieren, die auf die Email-Schablone verweist.

- Ein Globalkonfigurationswert
- Ein XPATH-Ausdruck

Die folgende Abbildung zeigt, wie Sie das Tag definieren:



Nachdem Sie das Tag definiert und auf *OK* geklickt haben, wird es auf der Seite „Zeichenkette-Builder“ als Zeichenkette aufgeführt.

12 Achten Sie darauf, dass Sie die Bearbeitung auf allen Seiten mit *OK* abschließen, damit die geänderte Richtlinie gespeichert wird.

13 Wiederholen Sie diese Schritte, um die Regeln sämtlicher Richtlinien zu bearbeiten, die auf die Email-Benachrichtigungsschablone verweisen.

14 Fügen Sie das in der Richtlinie definierte Tag zu der Email-Benachrichtigungsschablone hinzu und verwenden Sie dabei denselben Namen, den Sie in der Richtlinie verwendet haben.

   Von jetzt an können Sie das Tag im Text der Email-Benachrichtigungsschablone verwenden.

15 Speichern Sie die Änderungen und starten Sie den Treiber neu.

Hinzufügen von Platzhalter-Tags zu Email-Benachrichtigungsschablonen des Typs „Passwort vergessen“

Mit dem folgenden Verfahren können Sie Tags zu Email-Benachrichtigungsschablonen des Typs „Passwort vergessen“ hinzufügen:

- Sie können nur Tags hinzufügen, die den LDAP-Attributen des Benutzerobjekts entsprechen, an das die Benachrichtigung gesendet werden soll.
- Der Name des hinzuzufügenden Tags muss exakt dem LDAP-Attributnamen des Benutzerobjekts entsprechen.

  Informationen dazu, wie LDAP-Attribute zu eDirectory-Attributnamen in Relation stehen, können Sie der Schemazuordnungsrichtlinie entnehmen, die Bestandteil des Identity Manager-Treibers für LDAP ist.
- Es sind keine weiteren Konfigurationsschritte erforderlich.

5.12.6 Senden von Email-Benachrichtigungen an den Administrator

In der Standardkonfiguration werden Email-Benachrichtigungen nur an den Benutzer gesendet. Die mit Identity Manager gelieferten Richtlinien verwenden die Email-Adresse aus dem Identitätsdepot-Objekt für den betreffenden Benutzer.

Sie können die Passwortsynchronisierungsrichtlinien so konfigurieren, dass die Email-Benachrichtigungen auch an den Administrator gesendet werden. Dazu müssen Sie das Identity Manager-Skript zu einer der Richtlinien bearbeiten.

Senden Sie eine Blindkopie an den Administrator, indem Sie das Token mit der EMail-Adresse des Administrators definieren.

Bearbeiten Sie zum Senden einer Kopie an einen Administrator die Richtlinie zum Erzeugen der Email (z. B. die Richtlinie „PublishPasswordEmails.xml“, aus der die Richtlinie die Email-Adresse entnimmt, an die die Benachrichtigungen gesendet werden) und fügen Sie ein zusätzliches `<arg-string>`-Element mit der Email-Adresse des Administrators hinzu.

Im folgenden Beispiel wird gezeigt, wie das zusätzliche arg-string-Element angegeben wird:

```
<arg-string name="to">

<token-text>Admin@company.com</token-text>
```

```
</arg-string>
```

Denken Sie daran, den Treiber neu zu starten, nachdem Sie diese Änderungen vorgenommen haben.

5.12.7 Übersetzen von Email-Benachrichtigungsschablonen

Beachten Sie hierbei Folgendes:

- Die Standardschablonen liegen in englischer Sprache vor, Sie können den Text jedoch in andere Sprachen übersetzen.
- Die Namen und Definitionen der Platzhalter-Tags müssen jedoch auf Englisch bleiben, damit die Definitionen für das arg-string-Token in den Richtlinien mit den Namen der Platzhalter-Tags übereinstimmen.
- Eine Besonderheit ist bei Email-Benachrichtigungen des Typs „Passwort vergessen“ zu beachten: Hier müssen Sie angeben, in welcher Kodierung die Email erstellt werden soll. Fügen Sie dazu eine entsprechende Einstellung in der Datei `portalservlet.properties` ein. Zum Beispiel:

  ```
  ForgottenPassword.MailEncoding=EUC-JP
  ```

  Wenn diese Einstellung nicht vorhanden ist, erfolgt die Mail-Transformation ohne Kodierung.
- Bei Email-Benachrichtigungen zur Passwortsynchronisierung kann für folgende Elemente das XML-Attribut „charset“ angegeben werden: `<mail>`, `<message>` und `<‘>`.

  Informationen zur Verwendung dieser Elemente finden Sie im *DirXML Driver for Manual Task Service Implementation Guide* (http://www.novell.com/documentation/dirxmldrivers/index.html) (Implementierungshandbuch zum DirXML-Service-Treiber für manuelle Aufgaben). In diesem Handbuch wird ausführlicher auf Email-Schablonen eingegangen.

5.13 Fehlersuche bei der Passwortsynchronisierung

- Beachten Sie die Tipps in Abschnitt 5.8, „Implementierung der Passwortsynchronisierung“, auf Seite 115.
- Achten Sie darauf, dass die Methode der Anmeldung mit einfachem Passwort zusammen mit NMAS installiert wurde.
- Stellen Sie sicher, dass Sie über eine Kopie des Stamms der Baumstruktur auf den Servern verfügen, auf denen NMAS Passwortrichtlinien bei eDirectory-Anmeldemethoden oder bei Passwörtern aus verbundenen Systemen erzwungen soll, die von Identity Manager synchronisiert werden.
- Stellen Sie sicher, dass die Benutzer, bei denen eine Passwortsynchronisierung erforderlich ist, auf demselben Server reproduziert werden, der auch den für das Synchronisieren der Passwörter zuständigen Treiber enthält. Wie auch bei anderen Treiberfunktionen, kann der Treiber nur Benutzer verwalten, die sich in einer Master- oder Lese-/Schreibreproduktion auf demselben Server befinden.
- Stellen Sie sicher, dass SSL zwischen Webserver und Identitätsdepot richtig konfiguriert ist.
- Falls schon beim Erstellen eines Benutzers gemeldet wird, dass das Passwort nicht regelkonform ist, das Passwort im Identitätsdepot jedoch korrekt hinterlegt ist, entspricht das

Standardpasswort in der Treiberrichtlinie möglicherweise nicht der für diesen Benutzer geltenden Passwortrichtlinie.

Im folgenden Szenario wird der Active Directory-Treiber verwendet. Bei einem anderen Treiber wäre diese Situation jedoch auch denkbar.

Bereitstellen eines Ausgangspassworts: Sie möchten, dass der Active Directory-Treiber das Ausgangspasswort für einen Benutzer bereitstellt, wenn der Treiber im Identitätsdepot ein neues Benutzerobjekt als passendes Gegenstück zu einem Benutzer in Active Directory erstellt. Die Beispielkonfiguration für den Active Directory-Treiber sendet das Ausgangspasswort in einem von der Benutzererstellung getrennten Vorgang. Darüber hinaus enthält die Beispielkonfiguration auch eine Richtlinie, die ein Standardpasswort für einen Benutzer bereitstellt, wenn Active Directory kein Passwort liefert.

Da das Hinzufügen des Benutzers und das Festlegen des Passworts separat erfolgen, erhält ein neuer Benutzer in diesem Fall immer das Standardpasswort, wenn auch möglicherweise nur kurzzeitig. Das Standardpasswort wird schon bald aktualisiert, weil der Active Directory-Treiber das Passwort unmittelbar nach dem Hinzufügen des Benutzers sendet. Wenn das Standardpasswort nicht der Passwortrichtlinie des Identitätsdepots für den Benutzer entspricht, wird eine Fehlermeldung angezeigt.

Wenn das Standardpasswort beispielsweise aus dem Nachnamen des Benutzers erstellt wird, diese aber zu kurz ist und der Passwortrichtlinie nicht entspricht, wird durch den Fehlercode „-216“ angezeigt, dass das Passwort zu kurz ist. Diese Situation wird behoben, indem der Active Directory-Treiber ein konformes Ausgangspasswort sendet.

Unabhängig vom verwendeten Treiber müssen Sie eine der nachstehend beschriebenen Maßnahmen in Erwägung ziehen, wenn ein verbundenes System, das Benutzerobjekte erstellt, das Ausgangspasswort bereitstellen soll. Diese Maßnahmen sind besonders wichtig, wenn das Ausgangspasswort nicht mit dem Add-Ereignis, sondern mit einem nachgeordneten Ereignis übergeben wird.

- Ändern Sie die zum Erstellen des Standardpassworts verwendete Richtlinie auf dem Herausgeberkanal so ab, dass das Standardpasswort den Passwortrichtlinien entspricht, die für Ihre Organisation im Identitätsdepot definiert wurden. (Klicken Sie auf *Passwörter* und anschließend auf *Passwortrichtlinien*.)

  Wenn das Ausgangspasswort von der autorisierten Anwendung stammt, ersetzt es das Standardpasswort.

  Diese Möglichkeit ist vorzuziehen, weil zur Wahrung eines möglichst hohen Maßes an Sicherheit innerhalb des Systems das Vorhandensein einer Standardpasswortrichtlinie empfohlen wird.

- Entfernen Sie auf dem Herausgeberkanal die Richtlinie, die das Standardpasswort erstellt. In der Beispielkonfiguration wird diese Richtlinie im Befehlstransformationsrichtliniensatz bereitgestellt. Das Hinzufügen eines Benutzers ohne Passwort ist im Identitätsdepot zulässig. Die Überlegung hierbei ist, dass das Passwort für das neu erstellte Benutzerobjekt früher oder später über den Herausgeberkanal übergeben wird und dem Benutzerobjekt nur für kurze Zeit kein Passwort zugewiesen ist.

- Passwortrichtlinien werden baumspezifisch zugewiesen. Die Passwortsynchronisierung hingegen wird pro Treiber konfiguriert. Treiber werden serverspezifisch installiert und können nur Benutzer verwalten, die sich in einer Master- oder Lese-/Schreibreproduktion befinden.

  Damit eine Passwortsynchronisierung die gewünschten Ergebnisse liefert, müssen Sie sicherstellen, dass die Container in der Master- oder Lese-/Schreibreproduktion auf dem Server, auf dem die Treiber für die Passwortsynchronisierung aktiv sind, den Containern

entsprechen, für die Sie Passwortrichtlinien mit aktiviertem universellem Passwort zugewiesen haben. Durch Zuweisung einer Passwortrichtlinie an den Partitionsstammcontainer kann sichergestellt werden, dass die Passwortrichtlinie allen in diesem Container und seinen Untercontainern enthaltenen Benutzern zugewiesen wird.

- Hilfreiche DSTrace-Befehle:

  +DXML: Zum Anzeigen der Regelverarbeitung durch Identity Manager und möglicher Fehlermeldungen.

  +DVRS: Zum Anzeigen der Meldungen des Identity Manager-Treibers

  +AUTH: Zum Anzeigen der Änderungen am NDS-Passwort

  +DCLN: Zum Anzeigen von Meldungen des NDS DClient

Erstellung und Verwendung von Berechtigungen

6

Mit Identity Manager können Sie Daten zwischen verbundenen Systemen synchronisieren. Anhand von Berechtigungen können Sie Kriterien für eine Person oder Gruppe erstellen. Wenn diese Kriterien erfüllt sind, lösen sie ein Ereignis aus, das den Zugriff auf Geschäftsressourcen innerhalb des verbundenen Systems erteilt oder entzieht. Dadurch erhalten Sie eine weitere Kontroll- und Automatisierungsebene für das Erteilen und Entziehen von Ressourcen.

Das Funktionieren von Berechtigungen ist von zwei Aspekten abhängig: dem Erstellen und dem Verwalten der Berechtigung. Berechtigungen werden über iManager oder über Designer erstellt. Klicken Sie zum Erstellen einer Berechtigung in iManager unter dem Titel „Identity Manager-Dienstprogramme“ auf die Option *Berechtigung erstellen*. Weitere Informationen hierzu finden Sie in Abschnitt 6.4, „Erstellen von Berechtigungen in XML mit iManager“, auf Seite 178.

Sie haben auch die Möglichkeit, Berechtigungen in Designer zu erstellen und in vorhandene Identity Manager-Treiber zu implementieren. In Designer erstellen Sie Berechtigungen mit der grafischen Oberfläche des Assistenten für Berechtigungen, der Sie Schritt für Schritt durch den Vorgang leitet. In iManager erstellen Sie Berechtigungen über eine einfache Schnittstelle, fügen jedoch unter Verwendung eines XML-Editors zusätzliche Eigenschaften hinzu. Wegen seiner grafischen Oberfläche wird Designer zum Erstellen und Bearbeiten von Berechtigungen empfohlen.

Nachdem Sie Berechtigungen erstellt (oder die mit bestimmten Identity Manager-Treibern mitgelieferten, vorkonfigurierten Berechtigungen verwendet) haben, müssen Sie die Berechtigungen verwalten. Berechtigungen werden durch zwei Pakete oder Agenten verwaltet: durch iManager über funktionsbasierte Berechtigungsrichtlinien oder durch die Benutzeranwendung über Workflow-basierte Bereitstellung.

Bei funktionsbasierten Berechtigungsrichtlinien können Sie Geschäftsressourcen erteilen, wenn die Kriterien erfüllt sind. Wenn beispielsweise ein Benutzer die Kriterien 1, 2 und 3 erfüllt, wird der Benutzer bei einer funktionsbasierten Berechtigungsrichtlinie Mitglied der Gruppe H. Erfüllt der Benutzer hingegen die Kriterien 4 und 5, wird er Mitglied der Gruppe I. Damit diese Berechtigung bei einer Workflow-basierten Bereitstellung funktioniert, ist zuerst eine Genehmigung erforderlich.

6.1 Terminologie

Nachfolgend sind einige Begriffe aufgeführt, die Ihnen im Laufe dieses Kapitels häufiger begegnen werden.

Tabelle 6-1 *Terminologie*

Begriff	Erklärung
Berechtigung	Ein Identitätsdepot-Objekt, das eine Geschäftsressource in einem verbundenen System repräsentiert.
Berechtigungsagent	Erteilt und entzieht Berechtigungen. Bei funktionsbasierten Berechtigungen ist der Agent der Berechtigungsservice-Treiber.
Erteilen oder Entziehen	Die Interpretation des Erteilens oder Entziehens einer Berechtigung wird durch Globalkonfigurationsvariablen (GCVs) eines Identity Manager-Treibers gesteuert.
Berechtigungsendkonsument	Jeder Prozess, der berechtigungsrelevante Daten verwendet. Zu Berechtigungsendkonsumenten zählen iManager, die Benutzeranwendung und Identity Manager-Richtlinien.

6.2 Erstellen von Berechtigungen: Überblick

- Abschnitt 6.2.1, „Identity Manager-Treiber mit Vorkonfigurationen, die Berechtigungen unterstützen“, auf Seite 175
- Abschnitt 6.2.2, „Aktivieren von Berechtigungen bei anderen Identity Manager-Treibern“, auf Seite 176

Sie sollten im Voraus wissen, was Sie mit den Berechtigungen erreichen möchten. Berechtigungen sind an die Funktionalitäten gekoppelt, die Sie anhand von Richtlinien in Identity Manager-Treiber integrieren. Diese Treiberrichtlinien implementieren Regeln und verarbeiten die Ereignisse zwischen dem Identitätsdepot und dem verbundenen System. Wenn die Richtlinien im Identity Manager-Treiber nicht das angeben, was Sie bewirken möchten, können die Berechtigungen nicht funktionieren. Wenn Sie beispielsweise den Aktionsabschnitt der Regel „'Benutzer ändern' für Gruppenmitgliedschaften aktivieren, die zugewiesen oder entzogen werden“ in der Richtlinie „Befehl“ nicht angeben, wird jeder Versuch, eine Gruppenmitgliedschaftsberechtigung zu erteilen oder zu entziehen, ignoriert.

Sie müssen genau wissen, was Sie mit Identity Manager erreichen möchten. Nur dann können Sie Zugriffsmöglichkeiten auf Ressourcen verbundener Systeme sinnvoll erteilen oder entziehen. Bei der Planung und Verwendung von Berechtigungen können Ihnen die vier folgenden Schritte helfen:

1. Machen Sie sich klar, was Sie in Ihrer Geschäftssituation erreichen möchten. Sie können alles nur Denkbare mit Identity Manager entwickeln und implementieren. Bevor Sie jedoch etwas implementieren, das noch nicht definiert ist, müssen Sie genau wissen, was Sie vorhaben. Erstellen Sie eine nummerierte Liste der gewünschten Ziele.
2. Definieren Sie eine Berechtigung für einen einzelnen Punkt in Ihrer Liste. Sie können Berechtigungen mit und ohne Wert erstellen. Berechtigungen mit Werten beziehen diese Werte aus einer externen Abfrage. Sie können vom Administrator oder frei definiert sein. Entsprechende Beispiele finden Sie in Abschnitt 6.4.6, „Beispielberechtigungen zum leichteren Erstellen eigener Berechtigungen“, auf Seite 188.

3. Fügen Sie Richtlinien zum Identity Manager-Treiber hinzu, um die von Ihnen entworfene Berechtigung zu implementieren. Damit Sie eine Richtlinie für einen Identity Manager-Treiber erstellen können, müssen Sie mit XSLT- oder DirXML-Skripten, mit der Übernahme und Verarbeitung von Daten durch das verbundene System und mit der Art und Weise der Speicherung dieser Daten durch Novell® eDirectory™ vertraut sein. Wenn Sie kein erfahrener DirXML*-Programmierer sind, sollte diese Aufgabe von Experten durchgeführt werden.
4. Richten Sie einen Verwaltungsagenten zum Erteilen oder Entziehen der Berechtigung ein. Wenn Sie einen automatisierten Prozess wünschen, verwenden Sie funktionsbasierte Berechtigungen; wenn Sie einen manuellen Prozess wünschen, verwenden Sie die Workflow-basierte Bereitstellung.

6.2.1 Identity Manager-Treiber mit Vorkonfigurationen, die Berechtigungen unterstützen

Zu Identity Manager gehören mehrere vorkonfigurierte Treiber, die bereits Berechtigungen und Richtlinien für die Implementierung von Berechtigungen enthalten. Zudem sind diese Treiber so konfiguriert, dass sie den Datenverkehr auf Berechtigungsaktivitäten überwachen. Sie müssen Berechtigungen bei der erstmaligen Installation eines Treibers aktivieren, damit die entsprechend vorkonfigurierten Elemente des Treibers wirksam werden. Die folgenden Treiber verfügen über Vorkonfigurationen, die Berechtigungen unterstützen:

- Active Directory*
- Exchange
- GroupWise®
- LDAP
- NIS
- Lotus* Notes*
- NT Domain
- RACF

Bei diesen vorkonfigurierten Treibern sind die ersten drei der oben beschriebenen vier Schritte bereits umgesetzt. Die verschiedenen Arten von Beispiel-Berechtigungen, die diese Treiber unterstützen, eignen sich für die gängigsten Szenarios: Erteilen und Entziehen von Benutzerkonten, Gruppenmitgliedschaften und Email-Verteilerlisten. Nachfolgend die Möglichkeiten der einzelnen Treiber:

- Active Directory: Erteilen und Entziehen von Konten, Gruppenmitgliedschaften, Exchange-Postfach
- Exchange 5.5: Erteilen und Entziehen von Mailbox- und Gruppenmitgliedschaften
- GroupWise: Erteilen und Entziehen von Konten, Erteilen und Entziehen der Zugehörigkeit zu Verteilerlisten
- LDAP: Erteilen und Entziehen von Benutzerkonten
- Linux* und UNIX*: Erteilen und Entziehen von Konten
- Lotus Notes: Erteilen und Entziehen von Benutzerkonten und Gruppenmitgliedschaften
- NT Domain: Erteilen und Entziehen von Benutzerkonten und Gruppenmitgliedschaften
- RACF: Erteilen und Entziehen von Gruppenkonten und Gruppenmitgliedschaften

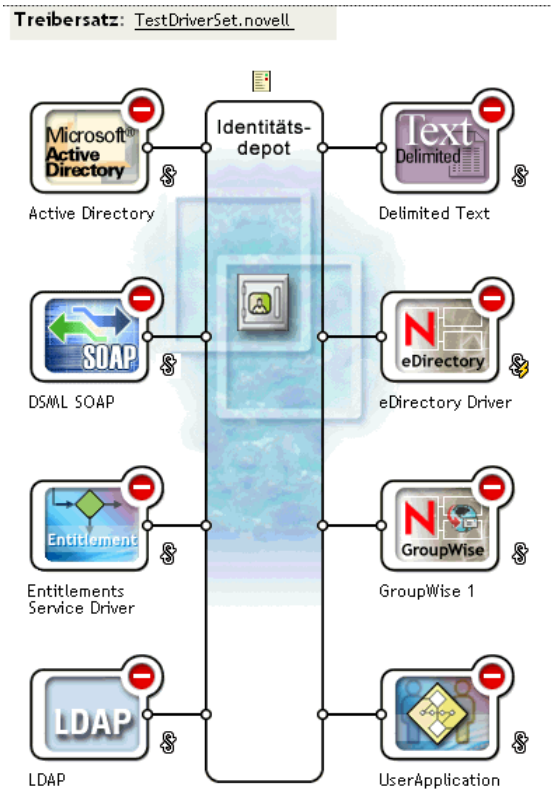
Diese Beispielberechtigungen und -richtlinien können Sie unverändert übernehmen, wenn sie Ihren Vorstellungen entsprechen. Sie haben aber auch die Möglichkeit, die Treiber abzuwandeln oder als Beispielvorlagen zu verwenden, und eigene Treiber mit iManager oder Designer zu erstellen. Wichtig ist, wie bereits erwähnt, dass Sie die vorkonfigurierten Berechtigungen dieser Treiber nur verwenden können, wenn Sie Berechtigungen beim Erstellen des vorkonfigurierten Treibers in Designer oder iManager aktivieren. Vorkonfigurierte Berechtigungen können später nicht mehr hinzugefügt werden, ohne den Treiber neu zu erstellen.

Wenn Sie Berechtigungen bisher mit Identity Manager 2.x verwendet haben und diese Berechtigungen jetzt mit Identity Manager 3 nutzen möchten, müssen Sie die Option *Berechtigungen aufrüsten* unter *Identity Manager-Dienstprogramme* ausführen.

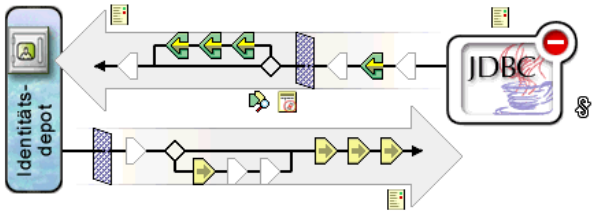
6.2.2 Aktivieren von Berechtigungen bei anderen Identity Manager-Treibern

Sie können auch weiterhin Berechtigungen bei Identity Manager-Treibern verwenden, die nicht entsprechend vorkonfiguriert sind. Um die Unterstützung von Berechtigungen durch den Treiber zu aktivieren, fügen Sie das Attribut „DirXML-EntitlementRef“ zum Treiberfilter hinzu. Dazu gehen Sie wie folgt vor:

1. Wählen Sie *Identity Manager > Identity Manager-Überblick*.
2. Wechseln Sie zu dem Treibersatz, der den Treiber enthält, und klicken Sie anschließend auf *Suchen*.
3. Wählen Sie das Treiberobjekt auf der Seite „Identity Manager-Überblick“ aus dem angezeigten Treibersatz aus.

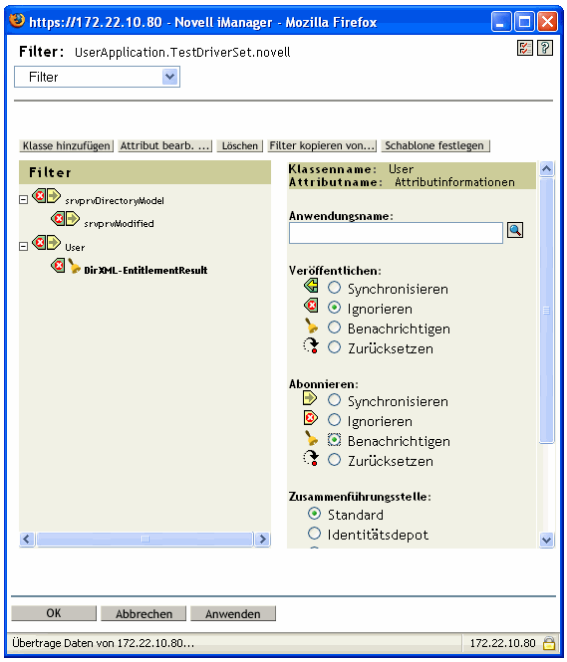


4. Doppelklicken Sie im Treibersatz auf den gewünschten Treiber, um die Treiberseite zu öffnen. Klicken Sie auf das Symbol *Treiberfilter* rechts neben dem Identitätsdepot (rot eingekreist).



5. Wählen Sie auf der Filterseite *Attribut hinzufügen*, blättern Sie nach unten und wählen Sie *Alle Attribute anzeigen*. Wählen Sie das Attribut *DirXML-EntitlementRef* und klicken Sie auf *OK*.

6. Wählen Sie auf der Seite „Filter“ das Attribut *DirXML-EntitlementRef* aus. Wählen Sie unter „Abonnieren“ die Option *Benachrichtigen*. Klicken Sie auf *OK*.



7. Dieser Vorgang wird automatisch durchgeführt, wenn Sie Berechtigungen für einen Treiber mit Designer erstellen.

6.3 Voraussetzungen für Berechtigungen

- ❑ eDirectory 8.7.3 oder höher
- ❑ Identity Manager 2 oder 3
- ❑ Ein Berechtigungs-Service-Treiber

  Jeder Treibersatz, in dem Berechtigungen verwendet werden sollen, muss einen Berechtigungs-Service-Treiber enthalten. Dazu ist eine sehr einfache, einmalige Konfiguration jedes Treibersatzes erforderlich.
- ❑ Eine Treiberkonfiguration, die Berechtigungen unterstützt

  Bevor Sie Berechtigungen mit einem verbundenen System verwenden können, müssen Sie einen der folgenden Schritte ausführen:

  - Importieren Sie die Identity Manager-Treiberkonfiguration für den Treiber und geben Sie an, dass die Unterstützung von Berechtigungen im Treiber aktiviert ist.
  - Aktivieren Sie die Unterstützung von Berechtigungen durch den Treiber. Dazu gehen Sie wie folgt vor:

    a. Erstellen Sie Berechtigungen mit iManager oder Designer (vorzugsweise Designer).

    b. Fügen Sie das Attribut „DirXML-EntitlementRef“ wie in Abschnitt 6.2.2, „Aktivieren von Berechtigungen bei anderen Identity Manager-Treibern“, auf Seite 176 beschrieben zum Treiberfilter hinzu.

    c. Erstellen Sie Richtlinien, um die in Schritt 1 erstellten Berechtigungen zu implementieren.

6.4 Erstellen von Berechtigungen in XML mit iManager

Zum besseren Verständnis der wichtigsten Bestandteile einer Berechtigung lohnt sich ein Blick auf die Berechtigungen und Richtlinien in einem der mit Unterstützung für Berechtigungen vorkonfigurierten Treiber: Active Directory (AD). Dazu sollten Sie sich die von Novell mitgelieferte DTD (Dokumenttypdefinition) für Berechtigungen sowie einige XML-Beispiele für das Erstellen von Berechtigungen ansehen, die auf der DTD basieren.

Dieser Abschnitt umfasst:

6.4.1 Vom Active Directory-Treiber bei der Aktivierung von Berechtigungen beigesteuerte Komponenten

Die Struktur des AD-Treibers wird bei Aktivierung der Unterstützung für Berechtigungen folgendermaßen verändert:

- Hinzufügen des Attributs „DirXML-EntitlementRef“ zum Treiberfilter. Das Attribut „DirXML-EntitlementRef“ gestattet es dem Treiberfilter, den Datenfluss auf Berechtigungsaktivitäten zu überwachen.
- Erstellen einer Benutzerkontoberechtigung. Über die Benutzerkontoberechtigung wird dem Benutzer in Active Directory ein Konto erteilt oder entzogen. Wenn das Konto erteilt wird, erhält der Benutzer ein aktiviertes Anmeldekonto. Wenn das Konto entzogen wird, wird das Anmeldekonto in Abhängigkeit von der Treiberkonfiguration deaktiviert oder gelöscht.
- Erstellen einer Gruppenmitgliedschaftsberechtigung. Über die Gruppenberechtigung wird die Mitgliedschaft in einer Gruppe in Active Directory erteilt oder entzogen. Die betreffende Gruppe muss einer Gruppe im Identitätsdepot zugeordnet sein. Wenn die Mitgliedschaft entzogen wird, wird der Benutzer aus der Gruppe entfernt. Die Gruppenmitgliedschaftsberechtigung wird nicht auf dem Herausgeberkanal erzwungen. Wenn ein Benutzer durch ein externes Werkzeug zu einer kontrollierten Gruppe in Active Directory hinzugefügt wird, wird der Benutzer nicht durch den Treiber entfernt. Zudem gilt, dass der AD-Treiber nichts unternimmt, wenn die Berechtigung nicht entzogen, sondern vom Benutzerobjekt entfernt wird.
- Erstellen einer Exchange-Postfach-Berechtigung. Die Gruppenberechtigung erteilt oder entzieht dem Benutzer in Microsoft Exchange ein Exchange-Postfach.
- Hinzufügen von Berechtigungsinformationen zu vielen Richtlinien.

Die folgenden Richtlinien enthalten zusätzliche Regeln, die für das Funktionieren von Berechtigungen erforderlich sind:

- InputTransform (Treiberebene). Die Regel „Check Target Of Add Association For Group Membership Entitlements“ in dieser Richtlinie überprüft das Ziel der Aktion “add-association” auf vorhandene Gruppenmitgliedschaftsberechtigungen. Gruppenmitgliedschaftsberechtigungen, die für in Active Directory erstellte Benutzer gelten, können erst verarbeitet werden, nachdem der Benutzer erfolgreich erstellt wurde. „add-association“ signalisiert, dass vom Treiber ein Objekt in Active Directory erstellt wurde. Wenn das Objekt darüber hinaus für eine Gruppenberechtigungsverarbeitung vorgemerkt ist, wird diese Verarbeitung jetzt ausgeführt.
- „Event Transform“ (Herausgeberkanal). Die Regel „Disallow User Account Delete“ in dieser Richtlinie bewirkt, dass das Löschen eines Benutzerkontos im Identitätsdepot nicht zulässig ist. Bei Verwendung der Benutzerkontoberechtigung werden die verwalteten Benutzerkonten durch die Berechtigung im Identitätsdepot kontrolliert. Ein Löschvorgang in Active Directory löscht nicht das kontrollierende Objekt im Identitätsdepot. Durch eine spätere Änderung des Objekts im Identitätsdepot oder eine Zusammenführungsoperation könnte das Konto in Active Directory neu erstellt werden.
- Befehl (Abonnentenkanal). Die Befehlsrichtlinie enthält folgende Regeln, die für Berechtigungen relevant sind:
  - Die Regel „User Account Entitlement Change (Delete Option)“. Über die Benutzerkontoberechtigung wird dem Benutzer in Active Directory ein aktiviertes Konto erteilt. Durch Entziehen der Berechtigung wird das Konto in Active Directory deaktiviert oder gelöscht, in Abhängigkeit von dem Wert, den Sie für die globale Variable *Bei Entzug*

der Kontoberechtigung gewählt haben. Diese Regel wird ausgeführt, wenn sich die Berechtigung ändert und Sie die Option „Löschen“ gewählt haben.

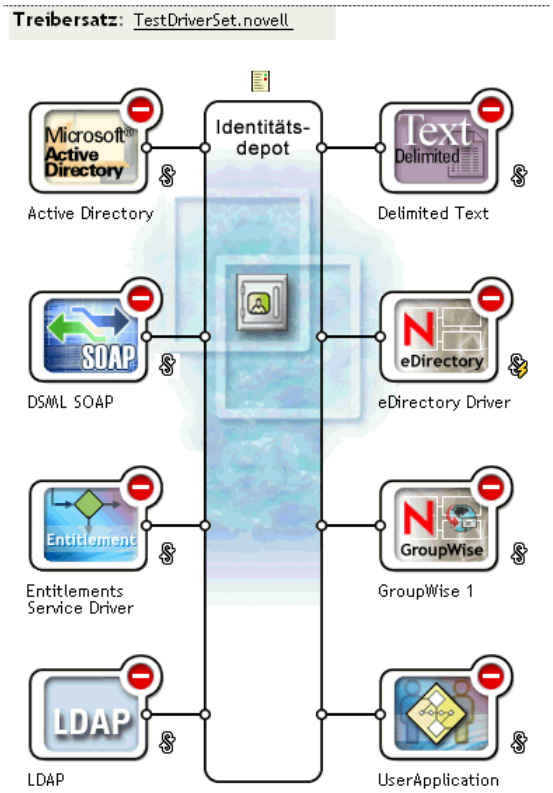
- Die Regel „User Account Entitlement Change (Disable Option)“. Über die Benutzerkontoberechtigung wird dem Benutzer in Active Directory ein aktiviertes Konto erteilt. Durch Entziehen der Berechtigung wird das Konto in Active Directory deaktiviert oder gelöscht, in Abhängigkeit von dem Wert, den Sie für die globale Variable *Bei Entzug der Kontoberechtigung* gewählt haben. Diese Regel wird ausgeführt, wenn sich die Berechtigung ändert und Sie die Option „Deaktivieren“ gewählt haben.
- Die Regel „Check User Modify for Group Membership Being Granted or Revoked“.
- Die Regel „Check User Modify for Exchange Mailbox Being Granted or Revoked“.

- Entsprechung (Abonnentenkanal). Dies ist die Regel „Account Entitlement: Do Not Match Existing Accounts“ für diese Richtlinie. Bei Verwendung der Benutzerkontoberechtigung mit der Identity Manager-Benutzeranwendung oder mit funktionsbasierten Berechtigungen werden Konten durch Erteilen oder Entziehen der Berechtigung erstellt und gelöscht (oder deaktiviert). Die Standardrichtlinie gilt nicht für ein entsprechendes, in Active Directory bereits vorhandenes Konto, wenn dem Benutzer kein Konto in Active Directory zusteht. Bearbeiten oder entfernen Sie diese Regel, wenn die Berechtigungsrichtlinie für entsprechende Konten in Active Directory gelten soll. Dadurch kann das Konto in Active Directory gelöscht oder deaktiviert werden.
- Erstellung (Abonnentenkanal). Die Erstellungsrichtlinie enthält folgende Regeln, die für Berechtigungen relevant sind:
  - „Account Entitlement: Block Account Creation When Entitlement Not Granted“. Bei Verwendung der Benutzerkontoberechtigung mit der Identity Manager-Benutzeranwendung oder mit funktionsbasierten Berechtigungen werden Konten nur für Benutzer erstellt, denen die Kontoberechtigung explizit erteilt wurde. Diese Regel legt ein Veto gegen die Erstellung des Benutzerkontos ein, wenn die Berechtigung nicht erteilt wurde.
  - „Identity Vault Accounts Are Enabled if Login Disabled Does Not Exist“.
  - „Prepare To Check Group Entitlements After Add“. Gruppenberechtigungen werden nach dem Hinzufügen des Objekts verarbeitet, weil das hinzugefügte Objekt vorhanden sein muss, um zu einer Gruppe hinzugefügt werden zu können. Das erfolgte Hinzufügen des Objekts wird durch eine Operationseigenschaft gekennzeichnet, die bei Abschluss des Hinzufügens während der Eingabetransformation überprüft wird.
  - „Signal the Need To Check Exchange Entitlements After the Add“.
  - „Map User Name to Windows Logon Name“. Wenn „userPrincipalName“ so konfiguriert ist, dass der Wert dem Benutzernamen in eDirectory entsprechen soll, setzen Sie „userPrincipalName“ auf den eDirectory-Objektnamen plus den Namen der Active Directory-Domäne.

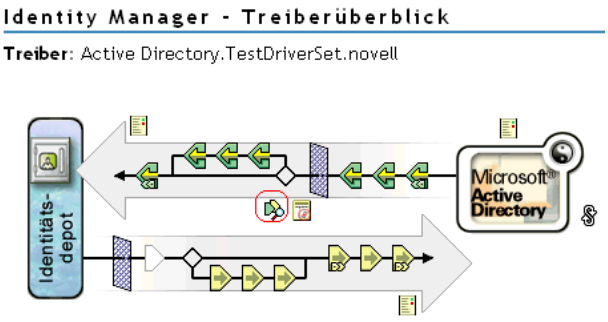
Mit dem folgenden Verfahren können Sie sich in iManager den XML-Code für jede Richtlinie ansehen:

1. Wählen Sie *Identity Manager > Identity Manager-Überblick*.
2. Wechseln Sie zu dem Treibersatz, der den Treiber enthält, und klicken Sie anschließend auf *Suchen*.

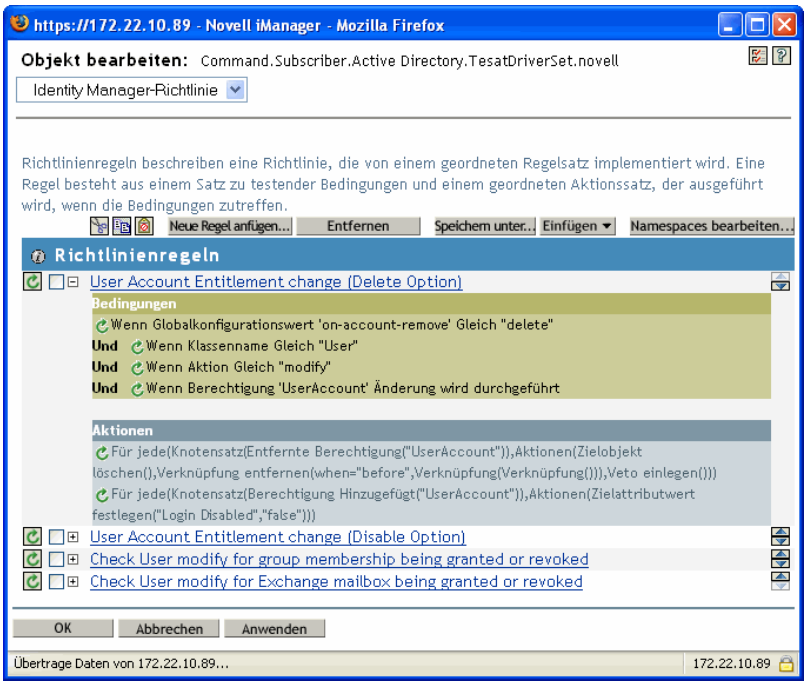
3. Wählen Sie auf der Seite „Identity Manager-Überblick“ das Treiberobjekt im angezeigten Treibersatz aus.



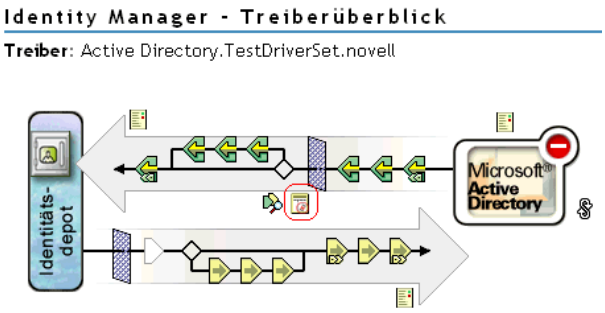
4. Doppelklicken Sie im Treibersatz auf den gewünschten Treiber, um die Treiberseite zu öffnen. Klicken Sie in der Treibermitte auf das Symbol *Alle Richtlinien anzeigen* (rot eingekreist).



5. Wenn Sie auf der Seite „Alle Richtlinien anzeigen“ eine Richtlinie auswählen, können Sie sich die Bedingungen und Aktionen ansehen, aus denen ist die Richtlinie zusammengesetzt.



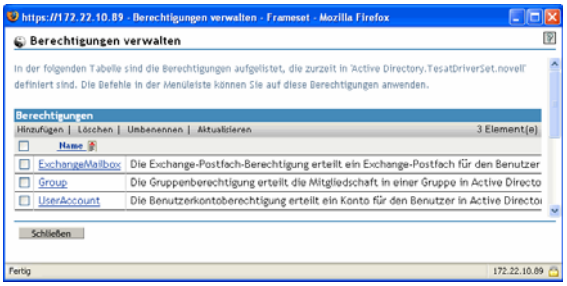
6. Wählen Sie zum Anzeigen des eigentlichen XML-Codes hinter den Richtlinien im Dropdown-Listenfeld die Option *XML bearbeiten* aus. (Standardmäßig ist in diesem Listenfeld die Option „Identity Manager-Richtlinie“ aktiviert.) Informationen zum Erstellen und Bearbeiten von Richtlinien finden Sie im *Policy Builder and Driver Customization Guide* (Handbuch zum Richtlinien-Builder und zur Treiberanpassung). Das Erstellen von Richtlinien für einen bestimmten Treiber ist im dazugehörigen (http://www.novell.com/documentation/dirxmldrivers/index.html) Identity Manager-Treiberhandbuch beschrieben.
7. Führen Sie zum Anzeigen der bei entsprechend vorkonfigurierten Treibern verfügbaren Berechtigungen (in diesem Beispiel: Active Directory) Schritt 1 bis Schritt 4 durch. Wählen Sie dabei in der Treibermitte das Symbol *Alle Berechtigungen anzeigen* (rot eingekreist).



8. Klicken Sie auf der Seite „Berechtigungen verwalten“ auf den Namen der Berechtigung, um die Berechtigung im XML-Viewer zu öffnen. Klicken Sie zum Bearbeiten des Berechtigungscodes auf *XML-Bearbeitung aktivieren*.

Der Active Directory-Treiber mit aktivierten Berechtigungen enthält drei Berechtigungen: „Benutzerkonto“, „Gruppe“ und „Exchange Mail“.

Abbildung 6-1 *Im AD-Treiber vorkonfigurierte Berechtigungen*



Sie können sich Beispiele aus dem XML-Code für diese Berechtigungen in Abschnitt 6.4.6, „Beispielberechtigungen zum leichteren Erstellen eigener Berechtigungen“, auf Seite 188 ansehen.

6.4.2 Die Berechtigungs-Dokumenttypdefinition (DTD) von Novell

Einige Berechtigungen sind bei Treibern mit aktivierter Unterstützung für Berechtigungen bereits vordefiniert. Sie können diese Berechtigungen verwenden oder eigene Berechtigungen in iManager oder Designer erstellen. Die folgende Berechtigungs-DTD von Novell dient als Beispiel, aus dem Sie eigene Berechtigungen ableiten können.

An die nachfolgende Erklärung der DTD schließen sich vier Beispiele für das Erstellen von Berechtigungen in diesem XML-Format mit iManager an. Wenn Ihnen die XML-Formatierung nicht liegt, können Sie in Designer Ihre Berechtigungen mit dem Assistenten für Berechtigungen auf einfachere Weise erstellen.

Berechtigungs-DTD von Novell

```
<!-************************************************************->
<!-- DirXML Entitlements DTD  <!-- Novell Inc. <!-- 1800 South Novell
Place <!-- Provo, UT 84606-6194 <!-- Version=1.0.0 <!-- Copyright 2005
Novell, Inc. All rights reserved --> <!--
********************************************************** --> <!--
Entitlement definition stored in the XmlData attribute of a
DirXML-Entitlement object. --> <!ELEMENT entitlement (values?)>
<!ATTLIST entitlement conflict-resolution (priority | union)
"priority" display-name CDATA #REQUIRED description CDATA #REQUIRED >
<!ELEMENT values (query-app | value+)?> <!ATTLIST values multi-valued
(true | false) "true" > <!ELEMENT value (#PCDATA)> <!ELEMENT query-app
(query-xml, result-set)> <!ELEMENT query-xml ANY> <!ELEMENT result-set
(display-name, description, ent-value)> <!ELEMENT display-name(token-
attr | token-src-dn | token-association)> <!ELEMENT ent-value (token-
association | token-src-dn | token-attr)> <!ELEMENT description
(token-association | token-src-dn | token-attr)> <!ELEMENT token-
association EMPTY> <!ELEMENT token-attr EMPTY> <!ATTLIST token-attr
attr-name CDATA #REQUIRED > <!ELEMENT token-src-dn EMPTY> <!--
Entitlement reference stored in the DirXML-EntitlementRef attribute of
a DirXML-EntitlementRecipient or a DirXML-SharedProfile object. -->
```

```
<!ELEMENT ref (src?, id?, param?)> <!ELEMENT param (#PCDATA)>
<!ELEMENT id (#PCDATA)> <!ELEMENT src (#PCDATA)> <!--     Entitlement
result stored in the DirXML-EntitlementResult attribute of a DirXML-
EntitlementRecipient object. --> <!ELEMENT result(dn, src, id?,
param?, state, status, msg?,timestamp)> <!ELEMENT dn (#PCDATA)>
<!ELEMENT state (#PCDATA)> <!ELEMENT status (#PCDATA)> <!ELEMENT msg
ANY> <!ELEMENT timestamp (#PCDATA)> <!--    Cached query results stored
in the DirXML-SPCachedQuery attribute of a DirXML-Entitlement object.
--> <!ELEMENT items (item*)> <!ELEMENT item (item-display-name?, item-
description?, item-value)> <!ELEMENT item-display-name (#PCDATA)>
<!ELEMENT item-description (#PCDATA)> <!ELEMENT item-value (#PCDATA)>
<!--    Representation of a DirXML-EntitlementRef within the DirXML
Script and within the operation-data of an operation in an XDS
document. --> <!ELEMENT entitlement-impl (#PCDATA)> <!ATTLIST
entitlement-impl name CDATA #REQUIRED src CDATA #REQUIRED id CDATA
#IMPLIED state (0 | 1) #REQUIRED src-dn CDATA #REQUIRED src-entry-id
CDATA #IMPLIED >
```

6.4.3 Erläuterung der Berechtigungs-DTD

Die Berechtigungs-DTD besteht aus fünf Teilen: Definition, Referenz, Ergebnis, gecachte Abfrage und interne Referenzinformationen. Der Header ist optional und enthält lediglich einen Kommentar. Die Kopfzeile der Berechtigungsdefinition in der DTD lautet:

```
<!-- Entitlement definition stored in the XmlData attribute of a
DirXML-Entitlement object. -->
```

Auf Kopfzeilen folgen Elemente (ELEMENT) und Attributlisten (ATTLIST). Nachfolgend finden Sie eine ausführliche Erklärung der Elemente und Attribute unter der Kopfzeile „Entitlement Definition“. Dies ist die wichtigste Kopfzeile, auf die Sie beim Erstellen von Berechtigungen achten müssen.

```
<!ELEMENT entitlement (values?)>
```

Das Element der Stammebene lautet `<entitlement>`. Es kann ein einzelnes, optionales, untergeordnetes Element vom Typ `<values>` enthalten. Daran schließt sich die Attributliste mit den Attributen „conflict-resolution“, „display-name“ und „description“ an. Das Attribut „conflict-resolution“ (Konfliktlösung) verwendet die Attributwerte „priority“ (Priorität) oder „union“ (Zusammenführung).

```
conflict-resolution (priority | union) "priority"
```

Funktionsbasierte Berechtigungen verwenden das Attribut für Konfliktlösung, um festzulegen, wie bei mehrfacher Anwendung einer mit Werten belegten Berechtigung auf dasselbe Objekt vorzugehen ist. Beispiel: Benutzer U ist Mitglied von Berechtigungsrichtlinie A und Berechtigungsrichtlinie B, die beide auf die gleiche, mit Werten (jedoch mit unterschiedlichen Wertesätzen) belegte Berechtigung E verweisen. Berechtigung E der Berechtigungsrichtlinie A besitzt einen Wertesatz (a, b, c). Berechtigung E der Berechtigungsrichtlinie B besitzt ebenfalls einen Wertesatz (c, d, e).

Das Konfliktlösungsattribut entscheidet, welcher Wertesatz für Benutzer U gelten soll. Wenn „union“ eingestellt ist, werden Benutzer U beide Wertesätze (a, b, c, d, e) zugewiesen. Wenn „priority“ eingestellt ist, wird Benutzer U nur ein Wertesatz zugewiesen, abhängig davon, welche Berechtigungsrichtlinie die höhere Priorität hat.

Wenn eine Berechtigung nur einen Wert besitzt, müssen Konflikte über die Priorität gelöst werden, da eine Zusammenführung („union“) von Werten dazu führen würde, dass mehr als ein Wert zugewiesen wird. Derzeit verwenden funktionsbasierte Berechtigungen dieses Attribut. In Zukunft werden möglicherweise auch Workflow-basierte Berechtigungen dieses Attribut verwenden.

```
display-name CDATA #REQUIRED description CDATA #REQUIRED
```

Der tatsächliche Name einer Berechtigung soll nicht immer in der Berechtigung angezeigt werden. Die Attribute „display-name“ (Anzeigename) und „description“ (Beschreibung) geben an, was dem Benutzer angezeigt wird. (In Designer gibt es eine Option, mit der Sie einen Anzeigenamen auswählen können, der vom eigentlichen Namen der Berechtigung abweicht.)

```
<!ELEMENT values (query-app | value+)?> <!ATTLIST values multi-
valued (true | false) "true"
```

Das Element <values> (Werte) ist optional und zeigt an, dass eine Berechtigung Werte besitzt. Wenn Sie dieses Element nicht verwenden, bedeutet dies, dass die Berechtigung nicht mit einem Wert belegt ist. Eine Berechtigung, die die Zugehörigkeit zu einer Verteilerliste erteilt, ist ein Beispiel für eine mit Werten belegte Berechtigung. Eine Berechtigung, die ein Konto in einer Anwendung erteilt (etwa die Benutzerkontoberechtigung des Active-Directory-Treibers), ist ein Beispiel für eine Berechtigung, die nicht mit Werten belegt ist.

Berechtigungen, die mit Werten belegt sind, beziehen ihre Werte aus drei Quellen. Eine dieser Quellen ist die externe Anwendung (vorgegeben durch das Element <query-app>). Die zweite Quelle ist eine vordefinierte, durchnummerierte Werteliste (ein oder mehrere <value>-Elemente). Die dritte Quelle ist der Client der Berechtigung (ein <values>-Element ohne übergeordnete <value> Elemente). Diese Beispiele veranschaulichen die Funktionsweise von Werten.

Mit Werten belegte Berechtigungen können ein- oder mehrwertig sein. Standardmäßig sind solche Berechtigungen mehrwertig. Für das Erzwingen dieser Einschränkung ist der Client der Berechtigung zuständig.

```
<!ELEMENT value (#PCDATA)>
```

Berechtigungswerte sind typenlose Zeichenketten.

```
<!ELEMENT query-app (query-xml, result-set)>
```

Wenn Werte von einer externen Anwendung bezogen werden sollen (z. B. von einer Email-Verteilerliste), müssen Sie mit dem Element <query-xml> eine Anwendungsabfrage festlegen. Verwenden Sie zum Exrahieren der Ergebnisse aus der Abfrage das Element <result-set>. In „Beispiel 2: Anwendungsabfrageberechtigung: Externe Abfrage“ auf Seite 189 finden Sie dazu zwei Beispiele.

```
<!ELEMENT query-xml ANY>
```

XML-Abfragen sind XDS-formatiert. Der Befehl <query-xml> dient zum Auffinden und Auslesen von Objekten aus der verbundenen Anwendung. Die Funktionalität für DirXML-Regeln, Objektmigration usw. hängt von der Implementierung dieses Abfragebefehls im Treiber ab. Weitere Informationen zu XML-Abfragen finden Sie in der Dokumentation der Novell-Entwickler zu Abfragen (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html).

```
<!ELEMENT result-set (display-name, description, ent-value)>
<!ELEMENT display-name(token-attr | token-src-dn | token-
association)> <!ELEMENT ent-value (token-association | token-src-dn
| token-attr)> <!ELEMENT description (token-association | token-
```

```
src-dn | token-attr)> <!ELEMENT token-association EMPTY> <!ELEMENT
token-attr EMPTY> <!ATTLIST token-attr attr-name CDATA #REQUIRED
```

Verwenden Sie das Element „result-set“ (Ergebnis-Set) als Hilfe bei der Interpretation der Ergebnisse aus der Abfrage einer externen Anwendung. Drei Datenelemente sind dabei von Interesse: der Anzeigename des Werts (das untergeordnete Element „display-name“), die Beschreibung des Werts (das untergeordnete Element „description“) und der nicht angezeigte Literale des Berechtigungswerts (das untergeordnete Element „ent-value“).

Die Token-Elemente `<token-src-dn>`, `<token-association>` und `<token-attr>` sind im Grunde genommen Platzhalter für XPATH-Ausdrücke, die die Attributwerte „src-dn“, „association“ oder „attr“ aus einem XDS-formatierten XML-Dokument extrahieren. Die DTD geht davon aus, dass das Abfrageergebnis in XDS vorliegt.

Weitere Kopfzeilen in der DTD

Auch die übrigen Berechtigungskopfzeilen in der Berechtigungs-DTD erfüllen bestimmte Funktionen, spielen jedoch beim Erstellen einer Berechtigung zunächst keine Rolle.

```
<!-- Entitlement reference stored in the DirXML-EntitlementRef
attribute of a DirXML-EntitlementRecipient or a DirXML-
SharedProfile object. -->
```

Die in der DTD unter „Entitlement reference...“ enthaltenen Informationen verweisen auf ein Berechtigungsobjekt. Diese Informationen werden vom zuständigen Verwaltungsagenten an dieser Stelle eingefügt (z. B. vom funktionsbasierten Berechtigungstreiber `Entitlement.xml` oder vom Genehmigungsablauftreiber `UserApplication.xml`). Dies ist das auslösende Ereignis für eine Aktion in einem verbundenen System. Sie müssen in der DTD unter dieser Kopfzeile nichts verändern, können diese Informationen jedoch verwenden, um sicherzustellen, dass auf das Berechtigungsobjekt verwiesen wird.

```
<!-- Entitlement result stored in the DirXML-EntitlementResult
attribute of a DirXML-EntitlementRecipient object. -->
```

Der Abschnitt unter „Entitlement result...“ erhält Angaben dazu, ob eine Berechtigung erteilt oder entzogen wurde. Dazu gehören der Zustand oder Status des Ereignisses und der Zeitpunkt der Erteilung oder Entziehung des Ereignisses (per Zeitstempel). Sie können die Elemente und Attribute unter dieser Kopfzeile unverändert lassen.

```
<!-- Cached query results stored in the DirXML-SPCachedQuery
attribute of a DirXML-Entitlement object. -->
```

Der Abschnitt unter „Entitlement query...“ enthält die von einer externen Anwendung gesammelten Berechtigungswerte. Diese Informationen können später wiederverwertet werden, wenn der Berechtigungsclient diese Informationen anzeigen muss. Diese Werte werden im `DirXML-SPCachedQuery`-Attribut des Berechtigungsobjekts gespeichert. Sie können die Elemente und Attribute unter dieser Kopfzeile unverändert lassen.

```
<!-- Representation of a DirXML-EntitlementRef within the DirXML
Script and within the operation-data of an operation in an XDS
document. -->
```

Da die DTD Werte für mehr als ein Dokument definiert, ist dieser Abschnitt unter „Representation of a DirXML-EntitlementRef...“ streng genommen kein Bestandteil der Berechtigungsdefinition. Sie können die Elemente und Attribute unter dieser Kopfzeile unverändert lassen.

6.4.4 Erstellen von Berechtigungen mit Designer

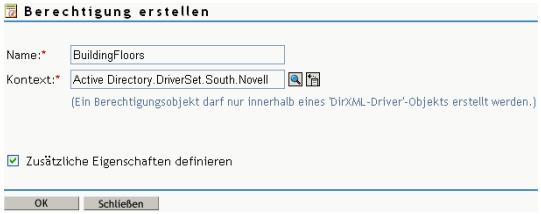
Die Beispiele in Abschnitt 6.4.5, „Erstellen und Bearbeiten von Berechtigungen in iManager“, auf Seite 187 zeigen den eigentlichen XML-Code, der beim Erstellen von Berechtigungen entsteht. Eine wesentlich einfachere Methode, als den Code manuell zu erstellen, bietet jedoch das mit Identity Manager gelieferte Dienstprogramm „Designer“. Nachdem Sie im Modelliermodul von Designer einen Identity Manager-Treiber zu einem Identitätsdepot hinzugefügt haben, können Sie in der Überblicksansicht mit der rechten Maustaste auf den Treiber klicken und den Befehl „Berechtigung hinzufügen“ wählen. Der Assistent für Berechtigungen fragt nach dem gewünschten Berechtigungstyp und führt Sie anschließend durch den Erstellungsvorgang.

Weitere Informationen zur Verwendung des Assistenten für Berechtigungen finden Sie im Designer for Identity Manager 3: Administration Guide (Designer für Identity Manager: Administrationshandbuch).

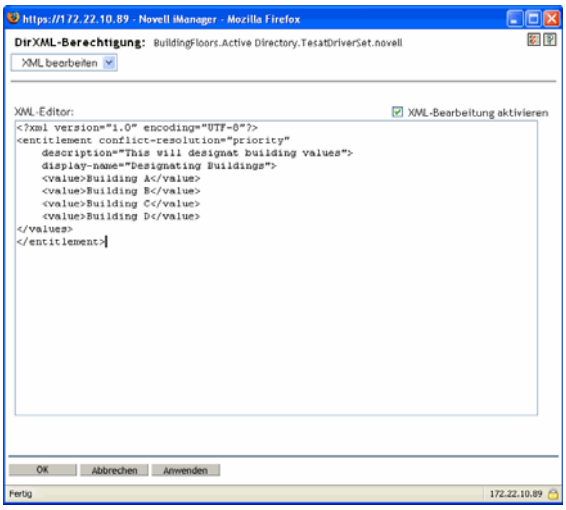
6.4.5 Erstellen und Bearbeiten von Berechtigungen in iManager

Es wird empfohlen, in Designer den Assistenten zum Erstellen von Berechtigungen zu verwenden. Sie haben aber auch die Möglichkeit, Berechtigungen in iManager zu erstellen.

1. Wählen Sie die Option zum Erstellen von Berechtigungen unter „Identity Manager-Dienstprogramme“.
2. Geben Sie auf der Seite „Berechtigung erstellen“ den gewünschten Namen für die Berechtigung ein und suchen Sie mit dem Objekt-Browser das Identity Manager-Treiberobjekt, zu dem die Berechtigung gehört.



3. Wenn die Option „Zusätzliche Eigenschaften definieren“ ausgewählt ist, wird die Seite „XML-Editor“ zum Definieren der gewünschten Elemente der Berechtigung angezeigt.



4. Klicken Sie auf „XML-Bearbeitung aktivieren“, um die Elemente zur Berechtigung hinzuzufügen.

Hinweis: Es wird davon abgeraten, den Namen einer Berechtigung zu ändern. Wenn Sie den Namen der Berechtigung nachträglich ändern, müssen Sie auch alle Verweise in den Richtlinien ändern, in denen die Berechtigung implementiert ist. Der Name der Berechtigung wird in der Richtlinie in den Attributen „Ref“ und „Result“ gespeichert.

6.4.6 Beispielberechtigungen zum leichteren Erstellen eigener Berechtigungen

Sie können zwei Arten von Berechtigungen erstellen: Berechtigungen mit Werten und ohne Werte. Berechtigungen mit Werten beziehen diese Werte aus einer externen Abfrage. Sie können vom Administrator oder frei definiert sein. Nachstehend finden Sie vier Beispiele für die beiden Berechtigungsarten, die Sie erstellen können.

Hinweis: Wenn Sie eine Zeile sehen, die das Kleiner-als-Zeichen (<) nicht enthält, bedeutet dies, dass die Zeile umbrochen wurde und ihr Inhalt eigentlich in einer Zeile und nicht auf zwei (oder drei) Zeilen verteilt angezeigt wird. Denken Sie auch daran, dass es sich hierbei im Gegensatz zur Kontoberechtigung um Beispiele für die Möglichkeiten handelt, die sich Ihnen beim Erstellen der verschiedenen Arten von Berechtigungen mit Werten bieten.

Beispiel 1: Kontoberechtigung: Ohne Werte

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="priority"
    description="This is an Account Entitlement"
    display-name="Account Entitlement"/>
```

In diesem Beispiel lautet der Name der nicht mit Werten belegten Berechtigung „Account“. Daran schließt sich die Zeile mit dem Attribut „conflict-resolution“ und der Standardeinstellung „Priority“ an. In den meisten Fällen bedeutet dies, dass die funktionsbasierte Berechtigung mit der höchsten Priorität den Wert festlegt, wenn die Berechtigung von der Funktion „Funktionsbasierte Berechtigungen“ verwendet wird. (Da es sich hierbei jedoch um ein Beispiel für Berechtigungen ohne Werte handelt, spielen mit Werten belegte Einstellungen keine Rolle. Die Berechtigungsbeschreibung lautet „This is an Account Entitlement“ und der Anzeigename lautet „Account Entitlement“. Diese Informationen genügen, um eine Kontoberechtigung zu erstellen, mit der Sie anschließend in einer Anwendung ein Konto erteilen können.

Der Active Directory-Treiber mit aktivierter Unterstützung für Berechtigungen besitzt eine UserAccount-Berechtigung, die Active Directory zum Erteilen oder Entziehen eines Benutzerkontos verwendet.

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="union"
      description="The User Account entitlement grants or denies an
      account in ActiveDirectory for the user. When granted, the user
      is given an enabled logon account.When revoked, the logon
      account is either disabled or deleted depending on how the drive
      is configured."display-name="User Account Entitlement"
name="UserAccount">
</entitlement>
```

In diesem Beispiel erfolgt die Konfliktlösung über das Attribut „union“, d. h., die Berechtigung kann die zugewiesenen Werte zusammenführen. (Wie bereits erwähnt, sind mit einem Wert belegte Einstellungen für Berechtigungen ohne Wert nicht relevant.) Das Feld „description“ (Beschreibung) erläutert, wofür diese Berechtigung verwendet wird und warum sie erstellt wurde. Diese Informationen sind hilfreich, wenn nachträglich Änderungen an der Berechtigung vorgenommen werden. Der eigentliche Name der Berechtigung lautet „UserAccount“, das Attribut `<display-name>` sorgt jedoch dafür, dass in einem Verwaltungsagenten der Name „User Account Entitlement“ (Benutzerkontoberechtigung) angezeigt wird.

Beispiel 2: Anwendungsabfrageberechtigung: Externe Abfrage

Die in einem Active Directory-Treiber mit Berechtigungsunterstützung enthaltenen Gruppen- und Exchange-Postfach-Berechtigungen liefern Beispiele für Anwendungsabfragen. Verwenden Sie diese Berechtigungsart, wenn Sie zur Ausführung eines Ereignisses externe Informationen aus einem verbundenen System benötigen.

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="union"
   description="The Group Entitlement grants or denies membership in
   a group in Active Directory. The group must be associated with a
   group in the Identity Vault. When revoked, the user is removed from
   the group. The group membership entitlement is not enforced on the
   publisher channel: If a user is added to a controlled group in
   Active Directory by some external tool, the user is not removed by
   the driver. Further, if the entitlement is removed from the user
  object instead of being simply revoked, the driver takes no action."
display-name="Group Membership Entitlement" name="Group">
   <values>
```

```
      <query-app>
         <query-xml>
            <nds dtd-version="2.0">
               <input>
                  <query class-name="Group"
                     scope="subtree">
                     <search-class class-name="Group"/>
                     <read-attr attr-name="Description"/>
                  </query>
               </input>
            </nds>
         </query-xml>
         <result-set>
            <display-name>
                <token-src-dn/>
            </display-name>
            <description>
               <token-attr attr-name="Description"/>
            </description>
            <ent-value>
               <token-association/>
            </ent-value>
         </result-set>
      </query-app>
   </values>
</entitlement>
```

In diesem Beispiel verwendet die Gruppenberechtigung das Attribut „union“ (Zusammenführung) zur Konfliktlösung, wenn die Berechtigung demselben Objekt mehrmals zugewiesen wird. Das Attribut „union“ führt die Berechtigungen der funktionsbasierten Berechtigungsrichtlinien zusammen, sodass die Berechtigung auch dann erteilt wird, wenn eine Richtlinie die Berechtigung entzieht, die andere Richtlinie sie jedoch erteilt.

Die ausführliche Gruppenbeschreibung ist hilfreich, denn sie erklärt den Zweck der Regeln in den Treiberrichtlinien. Diese Beschreibung ist ein gutes Beispiel für die Ausführlichkeit, mit der Sie Berechtigungen definieren sollten.

Der durch das Attribut `<display-name>` definierte Name lautet „Group Membership Entitlement“ (Gruppenmitgliedschaftsberechtigung) und wird in den Verwaltungsagenten angezeigt (z. B. in iManager für funktionsbasierte Berechtigungen). Dieser Name ist der relative eindeutige Name (Relative Distinguished Name, RDN) der Berechtigung. Wenn Sie keinen Anzeigenamen definieren, wird der RDN als Name für die Berechtigung verwendet.

Anhand der anfänglichen Abfragewerte wird der Baum und seine Teilbäume von oben nach unten nach dem Klassennamen „Group“ durchsucht. Diese Werte kommen vom verbundenen Active Directory-Server und die Anwendungsabfrage beginnt beim Tag `<nds>`. Unterhalb des Tags `<query-xml>` nimmt diese Abfrage Daten entgegen mit etwa der folgenden Struktur:

```
<instance class-name="Group" src-dn="o=Blanston,cn=group1">
   <association>o=Blanston,cn=group1</association>
   <attr attr-name="Description"> the description for group1</attr>
</instance>
<instance class-name="Group" src-dn="o=Blanston,cn=group2">
```

```
   <association>o=Blanston,cn=group2</association>
   <attr attr-name="Description"> the description for group2</attr>
</instance>
<instance class-name="Group" src-dn="o=Blanston,cn=group3">
   <association>o=Blanston, cn=group3</association>
   <attr attr-name="Description"> the description for group3</attr>
</instance>
<!-- ... ->
```

Anschließend werden unter dem Tag `<result-set>` die von der Abfrage empfangenen Daten in die verschiedenen Felder eingefügt. In das Feld `<display-name>` wird z. B. `o=Blanston,cn=group1` eingefügt. Das Feld `<description>` erhält `the description for group1` und das Feld `<ent-value>` erhält den Wert `o=Blanston,cn=group1`. Da mehr als eine der vorhandenen Gruppen die Abfragekriterien erfüllt hat, wurden diese Informationen ebenfalls erfasst und als weitere Instanzen dargestellt.

Hinweis: Der Wert für das Verknüpfungsformat ist für jedes externe System eindeutig festgelegt, sodass sich Format und Syntax je nach abgefragtem externen System unterscheiden.

Ein weiteres Beispiel ist die Exchange-Postfach-Berechtigung.

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="union"
  description="The Exchange Mailbox Entitlement grants or denies an
  Exchange mailbox for the user in Microsoft Exchange."
  display-name="Exchange Mailbox Entitlement" name="ExchangeMailbox">
  <values>
      <query-app>
         <query-xml>
            <nds dtd-version="2.0">
               <input>
                  <query class-name="msExchPrivateMDB"
                     dest-dn="CN=Configuration," scope="subtree">
                     <search-class class-name="msExchPrivateMDB"/>
                     <read-attr attr-name="Description"/>
                     <read-attr attr-name="CN"/>
                  </query>
               </input>
            </nds>
          </query-xml>
          <result-set>
            <display-name>
               <token-attr attr-name="CN"/>
            </display-name>
            <description>
               <token-attr attr-name="Description"/>
            </description>
            <ent-value>
              <token-src-dn/>
            </ent-value>
          </result-set>
      </query-app>
```

```
   </values>
</entitlement>
```

In diesem Beispiel verwendet die Exchange-Postfach-Berechtigung das Attribut „union“ (Zusammenführung) zur Konfliktlösung, wenn die Berechtigung demselben Objekt mehrmals zugewiesen wird. Das Attribut „union“ führt die Berechtigungen der funktionsbasierten Berechtigungsrichtlinien zusammen, sodass die Berechtigung auch dann erteilt wird, wenn eine Richtlinie die Berechtigung entzieht, die andere Richtlinie sie jedoch erteilt.

Die Beschreibung gibt an, dass die Berechtigung für den Benutzer in Microsoft Exchange ein Exchange-Postfach erteilt oder dieses entzieht. Damit ist die Aufgabe dieser Berechtigung hinreichend genau beschrieben. Der durch das Attribut „display-name“ definierte Name lautet „Exchange Mailbox Entitlement“ (Exchange-Postfach-Berechtigung) und wird in den Verwaltungsagenten angezeigt (z. B. in iManager für funktionsbasierte Berechtigungen). Dieser Name ist der relative eindeutige Name (Relative Distinguished Name, RDN) der Berechtigung. Wenn Sie keinen Anzeigenamen definieren, wird der RDN als Name für die Berechtigung verwendet.

Anhand der anfänglichen Abfragewerte wird der Container „Configuration“ und seine Teilbäume nach dem Klassennamen von „msExchPrivateMDB“ (ein Funktionsaufruf aus Microsoft Exchange). Diese Werte stammen von der verbundenen Active Directory-Datenbank und die Anwendungsabfrage beginnt beim Tag `<nds>`. Zur Klasse „msExchPrivateMDB“ gibt es in eDirectory kein Gegenstück, sodass Sie sich gut mit Funktionsaufrufen in Microsoft Exchange auskennen müssen, um eine entsprechende Abfrage durchführen zu können. Die Abfrage wird jedoch aufgrund der im Active Directory-Treiber vorgefundenen Regeln und Richtlinien durchgeführt.

Berechtigungsendkonsumenten verwenden die von der Abfrage abgerufenen Daten. So wird beispielsweise der Berechtigungswert („ent-value“) über das Attribut „DirXML-EntitlementRef“ an Identity Manager-Richtlinien übergeben. Der Anzeigename und die beschreibenden Informationen werden von iManager oder der Benutzeranwendung angezeigt und im Attribut „DirXML-SPCachedQuery“ gespeichert.

Beispiel 3: Vom Administrator definierte Berechtigung: Mit Listen

Das dritte Beispiel ist eine vom Administrator definierte Berechtigung, die ein Ereignis zum Erteilen oder Entziehen erstellt, nachdem Sie einen Listeneintrag ausgewählt haben.

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="union"
    description="This will show Administrator-defined Values">
         <display-name="Admin-defined Entitlement"/>
         <values multi-valued="true">
            <value>Building A</value>
            <value>Building B</value>
            <value>Building C</value>
            <value>Building D</value>
            <value>Building E</value>
            <value>Building F</value>
      </values>
</entitlement>
```

In diesem Beispiel lautet der Name der Berechtigung „Admin-defined“ und der Anzeigename ist als „Admin-defined Entitlement“ definiert. (Sie müssen nur dann einen Anzeigenamen angeben, wenn dieser sich vom RDN der Berechtigung unterscheiden soll.) Die Zeile für die Konfliktlösung enthält die Einstellung „union“, d. h., die Berechtigung kann die zugewiesenen Werte zusammenführen.

Die Berechtigungsbeschreibung lautet *This will show Administrator-defined Values*. Das multi-value-Attribut ist auf „true“ eingestellt, d. h., die Berechtigung kann einen Wert auch mehrmals zuweisen. In diesem Beispiel handelt es sich bei den Werten um mit Buchstaben gekennzeichnete Firmengebäude: „Building A“ bis „Building F“. Anschließend können Benutzer oder definierte Aufgabenmanager über einen Berechtigungsclient wie z. B. eine RBE-Aufgabe in iManager oder über die Benutzeranwendung die Gebäudeinformationen angeben, die in eine externe Anwendung wie z. B. Novell eDirectory aufgenommen werden.

Beispiel 4: Vom Administrator definierte Berechtigungen: Ohne Listen

Das vierte Beispiel ist eine vom Administrator definierte Berechtigung, die den Administrator zur Eingabe eines Werts zwingt, bevor die Berechtigung ein Ereignis erteilen oder entziehen kann. Diese Art von Berechtigung können Sie verwenden, wenn Ihnen zum Zeitpunkt der Erstellung noch nicht alle Informationen vorliegen und Sie daher keine Aufgabenliste erstellen können.

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="priority"
    description="There will be no pre-defined list">
    <values multi-valued="false"/>
</entitlement>
```

In diesem Beispiel lautet der Name der Berechtigung „Admin-defined (keine Liste)“ und die Berechtigung verwendet diesen Namen als Anzeigename, weil kein Eintrag für einen Anzeigenamen definiert ist. Auch hier gilt für das Konfliktlösungsattribut die Standardeinstellung „priority“. Dies bedeutet, dass die RBE mit der höchsten Priorität den Wert festlegt, wenn die Berechtigung von der Funktion „Funktionsbasierte Berechtigungen“ verwendet wird. Sie können anschließend über einen Berechtigungsclient wie z. B. eine RBE-Aufgabe in iManager oder über die Benutzeranwendung die Gebäudeinformationen angeben, die in eine externe Anwendung wie z. B. Novell eDirectory aufgenommen werden.

6.4.7 Abschließen der Berechtigungserstellung

Die Beispiele für das Erstellen und Verwenden von Berechtigungen haben die ersten beiden Schritte dieses Verfahrens veranschaulicht (siehe Abschnitt 6.2, „Erstellen von Berechtigungen: Überblick“, auf Seite 174). Schritt 1 beinhaltet das Anlegen einer Checkliste mit den Zielen, die Sie mit den Berechtigungen verfolgen. In Schritt 2 schreiben Sie die Berechtigungen, mit denen die Ziele in der Checkliste umgesetzt werden sollen. Schritt 3, das Erstellen von Richtlinien für den Identity Manager-Treiber, würde den Rahmen dieses Kapitels sprengen. Informationen zum Erstellen und Bearbeiten von Richtlinien finden Sie im *Policy Builder and Driver Customization Guide* (Handbuch zum Richtlinien-Builder und zur Treiberanpassung) und in der Dokumentation zum jeweiligen Identity Manager-Treiber (http://www.novell.com/documentation/idmdrivers/index.html).

Nachdem Sie Berechtigungen erstellt (oder die bei bestimmten Identity Manager-Treibern enthaltenen, vorkonfigurierten Berechtigungen verwendet) haben, müssen Sie diese in Schritt 4 verwalten. Berechtigungen werden durch zwei Pakete oder Agenten verwaltet: über iManager als funktionsbasierte Berechtigungsrichtlinien oder über die Benutzeranwendung bei Workflow-

basierter Bereitstellung. Informationen zu Berechtigungen, die bei der Workflow-basierten Bereitstellung verwendet werden, finden Sie in Abschnitt V: „Entwerfen und Verwalten von Bereitstellungsanforderungen“ im „Identity Manager-Benutzeranwendung: Administrationshandbuch“. Der Rest dieses Kapitels befasst sich mit funktionsbasierten Berechtigungen.

6.5 Verwalten funktionsbasierter Berechtigungen - Überblick

Beim herkömmlichen Verfahren werden Berechtigungen auf verbundenen Systemen treiberspezifisch verwaltet, indem lediglich Treiberkonfigurationsrichtlinien erstellt und bearbeitet werden, z. B. mit dem Richtlinien-Builder. Bei diesem herkömmlichen verteilten Modell kontrollieren häufig unterschiedliche Administratoren die einzelnen Identity Manager-Treiber und verbundenen Systeme. Zudem sind die Geschäftsrichtlinien, die festlegen, ob ein Benutzer Ressourcen eines Systems erhält, in den Konfigurationrichtlinien für die Treiber der jeweils verbundenen Systeme meist “hartkodiert” sind.

Das funktionsbasierte Berechtigungsmodell schafft eine Umgebung, in der ein oder weniger Administratoren befügt sind, die Berechtigungsrichtlinien zu kontrollieren. Ein solcher Administrator muss die Grundlagen von Identity Manager kennen, er benötigt aber keine weit reichenden Identity Manager-, XSLT- oder DirXML-Skript-Kenntnisse, um die Schnittstelle für funktionsbasierte Berechtigungen bedienen zu können.

Mit funktionsbasierten Berechtigungsrichtlinien können Sie Geschäftsressourcen automatisch erteilen oder entziehen, wenn die Kriterien erfüllt sind. Berechtigungen sind wie eine „Eintrittskarte“ für den Zugriff auf eine Ressource. Mit der Eintrittskarte dürfen Sie auf die betreffende Ressource zugreifen, ohne Eintrittskarte wird Ihnen der Zugriff verwehrt. Sie können z. B. Folgendes festlegen: Wenn ein Benutzer die Kriterien 1, 2 und 3 erfüllt, wird der Benutzer bei einer funktionsbasierten Berechtigungsrichtlinie Mitglied der Gruppe H. Erfüllt der Benutzer hingegen die Kriterien 4 und 5, wird er Mitglied der Gruppe I.

Die Vorbereitung zur Verwaltung funktionsbasierter Berechtigungen gliedert sich in drei Schritte:

1. Aktivieren Sie das Attribut „DirXML-EntitlementRef“, des Identity Manager-Treiberobjekts (siehe Abschnitt 6.2.2, „Aktivieren von Berechtigungen bei anderen Identity Manager-Treibern“, auf Seite 176), wenn nicht bereits geschehen.
2. Installieren Sie den Berechtigungs-Service-Treiber (`Entitlement.xml`) wie in Abschnitt 6.6, „Erstellen eines Berechtigungs-Service-Treiberobjekts“, auf Seite 196 beschrieben.
3. Erstellen Sie funktionsbasierte Berechtigungsrichtlinien in iManager, wie in Abschnitt 6.7, „Erstellen von Berechtigungsrichtlinien“, auf Seite 197 beschrieben.

6.5.1 Funktionsweise des Berechtigungs-Service-Treibers

Funktionsbasierte Berechtigungen hängen vom Berechtigungs-Service-Treiber (`Entitlement.xml`) ab. Bei diesem Treiber handelt es sich um einen Service der Engine, der überwacht, ob für Benutzer eine Mitgliedschaft in einer Berechtigungsrichtlinie besteht. Wenn ein Benutzer die dynamischen Mitgliedschaftskriterien einer dynamischen Gruppe in einer

Berechtigungsrichtlinie erfüllt oder ihr statistisch angehört, aktualisiert der Berechtigungs-Service-Treiber im Attribut „DirXML-EntitlementRef“ Informationen zu diesem Benutzerobjekt.

Für die in Abschnitt 6.2.1, „Identity Manager-Treiber mit Vorkonfigurationen, die Berechtigungen unterstützen“, auf Seite 175 aufgelisteten Systeme können Sie Berechtigungen beim Importieren der Identity Manager-Treiberkonfiguration aktivieren. Zu Identity Manager gehören mehrere vorkonfigurierte Treiber, die bereits Berechtigungen und Richtlinien für die Implementierung von Berechtigungen enthalten. Zudem sind diese Treiber so konfiguriert, dass sie den Datenverkehr auf Berechtigungsaktivitäten überwachen. Sie haben dann die Möglichkeit, die bereitgestellten Richtlinien zu überprüfen. Diese Richtlinien unterstützen Berechtigungen, indem sie das Attribut „DirXML-EntitlementRef“ kontrollieren und Berechtigungen erteilen oder entziehen.

Der Berechtigungs-Service-Treiber aktualisiert das Attribut „DirXML-EntitlementRef“ nur, wenn eine der folgenden Situationen eintritt:

- Sie verwenden die Aufgabe „Mitgliedschaft neu bewerten“.
- Sie geben an, in welchem Teil des Baums die Benutzer neu bewertet werden sollen.
- Ein Benutzer wird verschoben.
- Ein Benutzer wird umbenannt.
- Ein beliebiges, für die Mitgliedschaft in einer Berechtigungsrichtlinie verwendetes Attribut wird geändert.

Anhand von Berechtigungsrichtlinien können Sie Berechtigungen auf verbundenen Systemen und Rechte im Identitätsdepot erteilen. Für verbundene Systeme können folgende Berechtigungen vergeben werden:

- Konten
- Mitgliedschaft in Email-Verteilerlisten
- Gruppenmitgliedschaft
- Attribute für die entsprechenden Objekte in verbundenen Systemen, die mit von Ihnen angegebenen Werten belegt sind
- Platzierung
- Andere individuell angepasste Berechtigungen

Einige Optionen, die Sie mithilfe von Berechtigungen erstellen können, werden in den Treiberkonfigurationen veranschaulicht, bei denen die Unterstützung für Berechtigungen aktiviert ist.

Da je Treibersatz ein Berechtigungs-Service-Treiber verwendet wird, kann eine Berechtigungsrichtlinie nur Benutzer verwalten, die sich in einer Lese-/Schreib- oder in einer Masterreproduktion auf dem Server befinden, der dem betreffenden Treibersatz zugeordnet ist.

Die Funktionalität von funktionsbasierten Berechtigungsrichtlinien richtet sich nach Identity Manager. Damit Sie verbundene Systeme verwalten können, müssen die Identity Manager-Treiber installiert und richtig konfiguriert sein, ebenso die Identity Manager-Plugins.

Um mögliche Konflikte zwischen zugewiesenen Berechtigungsrichtlinien und Identity Manager-Treiberkonfigurationen zu vermeiden, sollten Sie Ihre Geschäftsrichtlinien im Auge behalten und darauf achten, wie diese mithilfe von Identity Manager umgesetzt werden. Identity Manager-Berechtigungsrichtlinien und Richtlinien in einer Treiberkonfiguration dürfen sich beim Verwalten von Attributen nicht überschneiden oder zueinander in Konflikt stehen.

6.6 Erstellen eines Berechtigungs-Service-Treiberobjekts

Damit Sie Berechtigungsrichtlinien erstellen können, benötigen Sie ein Berechtigungs-Service-Treiberobjekt. Sie müssen pro Treibersatz eines dieser Objekte erstellen.

Wenn kein solches Objekt vorhanden ist, werden Sie aufgefordert, es zu erstellen, wenn Sie auf die Funktion und Aufgabe „Funktionsbasierte Berechtigungen“ klicken.

1. Überprüfen Sie, ob bereits ein Berechtigungs-Service-Treiber vorhanden ist.

   Klicken Sie in iManager auf *Funktionsbasierte Berechtigungen* > *Funktionsbasierte Berechtigungen* und wählen Sie den Treibersatz aus.

   - Wenn die Seite „Kein Berechtigungs-Service-Treiber“ angezeigt wird, fahren Sie mit Schritt 2 fort, um ein Berechtigungs-Service-Treiberobjekt zu erstellen.
   - Wenn die Seite „Funktionsbasierte Berechtigungen“ mit einer Liste verfügbarer Berechtigungsrichtlinien angezeigt wird, ist bereits ein Berechtigungs-Service-Treiberobjekt vorhanden. In diesem Fall müssen Sie diensen Vorgang nicht durchführen. Fahren Sie fort mit Abschnitt 6.7, „Erstellen von Berechtigungsrichtlinien“, auf Seite 197.

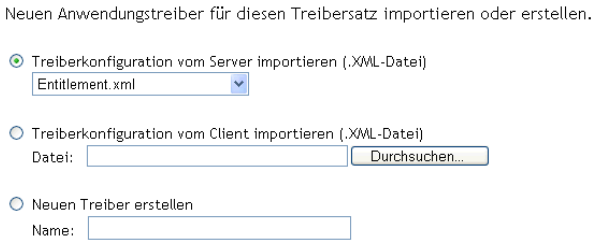
2. Klicken Sie auf der Seite „Kein Berechtigungs-Service-Treiber“ auf *Ja*.

   Der Assistent zum Erstellen von Treibern wird angezeigt.

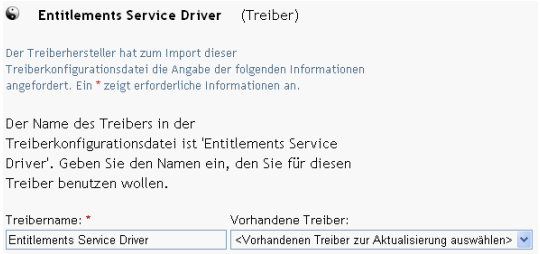
   Sie können auch auf *DirXML-Dienstprogramme* > *Treiber importieren* klicken.

3. Wählen Sie auf der Seite „Assistent zum Erstellen von Treibern“ die Option *In einem vorhandenen Treibersatz* und klicken Sie auf *Weiter*.

4. Wählen Sie im Dropdown-Listenfeld *Treiberkonfiguration vom Server importieren (.XML-Datei)* die Datei *Entitlement.xml* aus.



5. Geben Sie einen Namen für das Berechtigungs-Service-Treiberobjekt ein (oder übernehmen Sie den Standardnamen) und klicken Sie auf *Weiter*.



   Die passende Treiberkonfigurationsdatei wird automatisch ausgewählt. Geben Sie einen Namen für das Treiberobjekt ein oder übernehmen Sie die Vorgabe.

6 Es wird empfohlen, Sicherheitsäquivalenzen zu definieren und Verwaltungsfunktionen auszuschließen. Fügen Sie zu beiden Objekten den Benutzer „Admin“ hinzu und klicken Sie auf *Weiter*.

7 Überprüfen Sie die Zusammenfassung und klicken Sie auf *Fertig stellen*.

Das Treiberschnittstellenmodul für den Berechtigungstreiber wird standardmäßig bei der Installation installiert. Die Konfigurationsdatei des Berechtigungstreibers wird standardmäßig installiert, wenn Sie die Identity Manager-Plugins auf dem iManager-Server installieren.

Nachdem Sie den Assistenten beendet haben, können Sie auf die Plugins für Berechtigungen zugreifen und mit dem Erstellen von funktionsbasierten Berechtigungsrichtlinien für diesen Treibersatz beginnen.

6.7 Erstellen von Berechtigungsrichtlinien

- Abschnitt 6.7.1, „Definieren der Mitgliedschaft für eine Berechtigungsrichtlinie“, auf Seite 198
- Abschnitt 6.7.2, „Auswählen von Berechtigungen für eine Berechtigungsrichtlinie“, auf Seite 199

Zum Erstellen einer Berechtigungsrichtlinie können Sie den mitgelieferten Assistenten verwenden.

1 Stellen Sie sicher, dass Sie den Berechtigungs-Service-Treiber eingerichtet und die erforderlichen Treiberkonfigurationen erstellt haben.

2 Klicken Sie in iManager auf *Funktionsbasierte Berechtigungen* > *Funktionsbasierte Berechtigungen*.

3 Wählen Sie einen Treibersatz aus.

Berechtigungsrichtlinien gelten je Treibersatz.

Die Liste der bereits vorhandenen Berechtigungsrichtlinien wird geöffnet. Diese ähnelt der Liste in der folgenden Abbildung. Wenn Sie zum ersten Mal funktionsbasierte Berechtigungen verwenden, ist die Liste leer.

4 Klicken Sie auf *Neu*.

Der *Assistent für Berechtigungsrichtlinien* wird geöffnet.

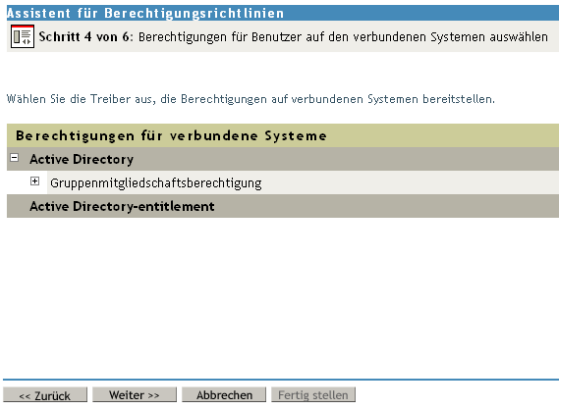
5 Führen Sie Schritt 1 bis 6 des Assistenten durch, um eine Richtlinie zu erstellen. Informationen zu den einzelnen Schritten des Assistenten finden Sie in der Online-Hilfe.

5a Geben Sie in Schritt 1 einen Namen und eine Beschreibung für die Richtlinie ein.

5b Definieren Sie in Schritt 2 den Mitgliederfilter und die Suchparameter.

5c Definieren Sie in Schritt 3 die statischen Mitglieder, indem Sie Mitglieder in die Suchkriterien aufnehmen oder aus ihnen ausschließen.

5d Wählen Sie in Schritt 4 einen Identity Manager-Treiber und stellen Sie die Berechtigungen bereit, die darin aufgenommen werden sollen. Die Berechtigungen haben Sie in Abschnitt 6.4, „Erstellen von Berechtigungen in XML mit iManager“, auf Seite 178 erstellt. Klicken Sie auf *Treiber hinzufügen* und wählen Sie eine hinzuzufügende Berechtigung aus.



5e Suchen Sie in Schritt 5 nach Objekten, für die diese Berechtigungsrichtlinie als Trustee dienen soll.

5f Lesen Sie sich in Schritt 6 die Zusammenfassung durch, um sicherzustellen, dass die Berechtigungsrichtlinie wie von Ihnen gewünscht funktionieren wird. Ist dies der Fall, klicken Sie auf *Fertig stellen*, klicken Sie andernfalls auf *Zurück*.

6 Durch das Erstellen einer Berechtigungsrichtlinie wird der Berechtigungs-Service-Treiber deaktiviert. Klicken Sie auf *Neustart*, um die Sitzung abzuschließen.

6.7.1 Definieren der Mitgliedschaft für eine Berechtigungsrichtlinie

Wie ein Identity Manager-Treiber, kann auch eine Berechtigungsrichtlinie nur Objekte verwalten, die sich in einer Master- oder einer Lese-/Schreibreproduktion auf dem Server befinden, dem sie zugewiesen ist. Jede Berechtigungsrichtlinie wird einem einzelnen Treibersatzobjekt zugeordnet, das einem bestimmten Server zugewiesen wird.

Nur Benutzerobjekte (und andere aus der Klasse „User“ abgeleitete Objekttypen) können Mitglieder einer Berechtigungsrichtlinie sein. Wählen Sie zum Öffnen der Mitgliedschaftsseite in einer Berechtigungsrichtlinie *Funktionsbasierte Berechtigungen* > *Funktionsbasierte Berechtigungen*, markieren Sie in der Liste die Berechtigungsrichtlinie, die Sie bearbeiten möchten, und klicken Sie auf *Bearbeiten*. Klicken Sie im Internet Explorer auf die Registerkarte *Mitgliedschaft*. Wählen Sie in Firefox im Pulldown-Menü den Befehl „Dynamische Mitglieder bearbeiten“.

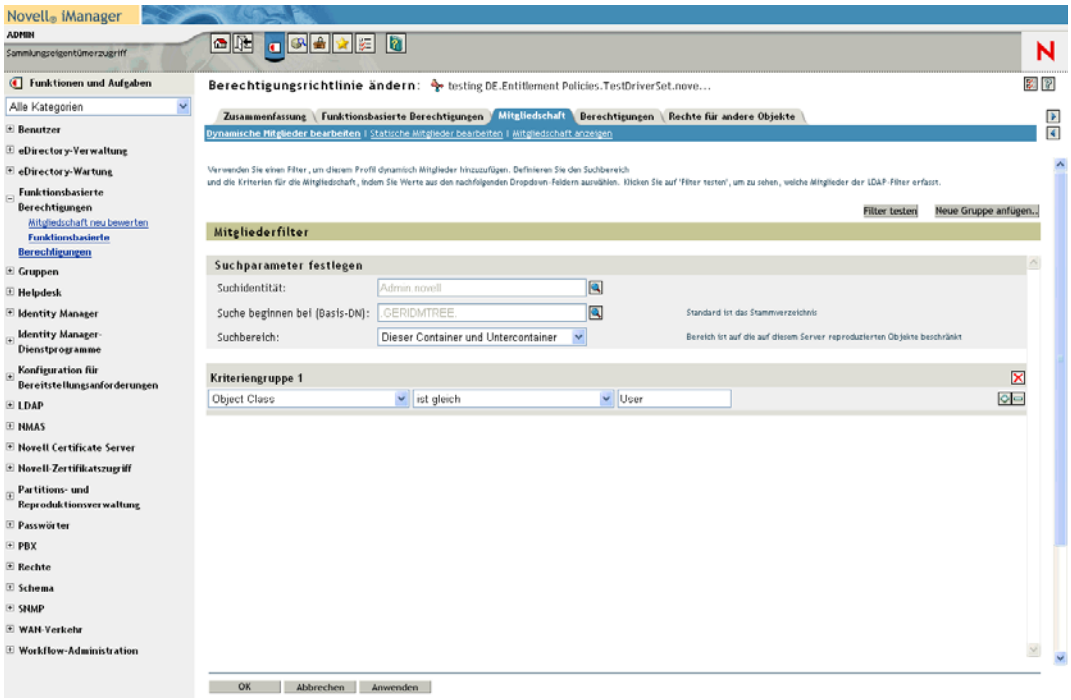
Eine Berechtigungsrichtlinie ist ein dynamisches Gruppenobjekt. Sie können die Mitgliedschaft für eine Berechtigungsrichtlinie dynamisch oder statisch anpassen. Beide Methoden können für dieselbe Berechtigungsrichtlinie eingesetzt werden.

- **Dynamisch:** Sie können Kriterien für eine Mitgliedschaft auf Basis von Attributwerten des Objekts definieren, z. B. dass die Stellenbezeichnung das Wort “Manager” enthalten soll. Die von Ihnen festgelegten Kriterien werden in einen LDAP-Filter konvertiert.

  Benutzer, die die Kriterien erfüllen, werden automatisch Mitglieder der Berechtigungsrichtlinie, ohne dass sie einzeln zur Richtlinie hinzugefügt werden müssen. Die dynamische Mitgliedschaft entspricht einem dynamischen Gruppenobjekt.

  Wenn sich ein Objekt ändert und die Kriterien für die dynamische Mitgliedschaft nicht mehr erfüllt, werden die Berechtigungen automatisch entzogen.

Abbildung 6-2 *Bearbeiten von dynamischen und statischen Mitgliedern*



- **Statisch:** Neben der Einstellung von Kriterien für die dynamische Mitgliedschaft (LDAP-Filter) können Sie bestimmte Benutzer einbeziehen oder ausschließen.

  Sie können Mitglieder statisch einbeziehen, die den Kriterien des Filters nicht entsprechen. Außerdem können Sie Mitglieder ausschließen, die zwar die Kriterien des Filters erfüllen, aber nicht in die Berechtigungsrichtlinie einbezogen werden sollen.

6.7.2 Auswählen von Berechtigungen für eine Berechtigungsrichtlinie

- „Konten auf verbundenen Systemen“ auf Seite 200
- „Mitgliedschaft in Email-Verteilerlisten und NOS-Listen“ auf Seite 201

- „Attributwerte auf verbundenen Systemen“ auf Seite 202

Anhand von Berechtigungen können Sie den Zugriff auf Services auf verbundenen Systemen und auf Rechte im Identitätsdepot erteilen oder entziehen.

Von Ihnen installierte Treiber mit aktivierter Unterstützung für Berechtigungen enthalten eine Reihe von Berechtigungen, die Sie über eine Berechtigungsrichtlinie zuweisen können. Sie können auch eigene Berechtigungen erstellen, die in einer Berechtigungsrichtlinie verwendet werden. Die Berechtigungen, die der Treiber bereitstellen kann, sind untergeordnete Objekte des Treibers, die der Treiberentwickler erstellt, um die Möglichkeiten des Treibers und des verbundenen Systems zu repräsentieren.

Trustee-Rechte auf Objekte im Identitätsdepot werden Mitgliedern der Berechtigungsrichtlinie sofort erteilt. Berechtigungen für verbundene Systeme werden standardmäßig allen Mitgliedern der Berechtigungsrichtlinie erteilt, wenn das nächste Mal ein Attribut für die Mitgliedschaft in einer Berechtigungsrichtlinie geändert, ein Benutzer in einen anderen Container verschoben oder umbenannt wird.

Für verbundene Systeme können folgende Berechtigungen vergeben werden:

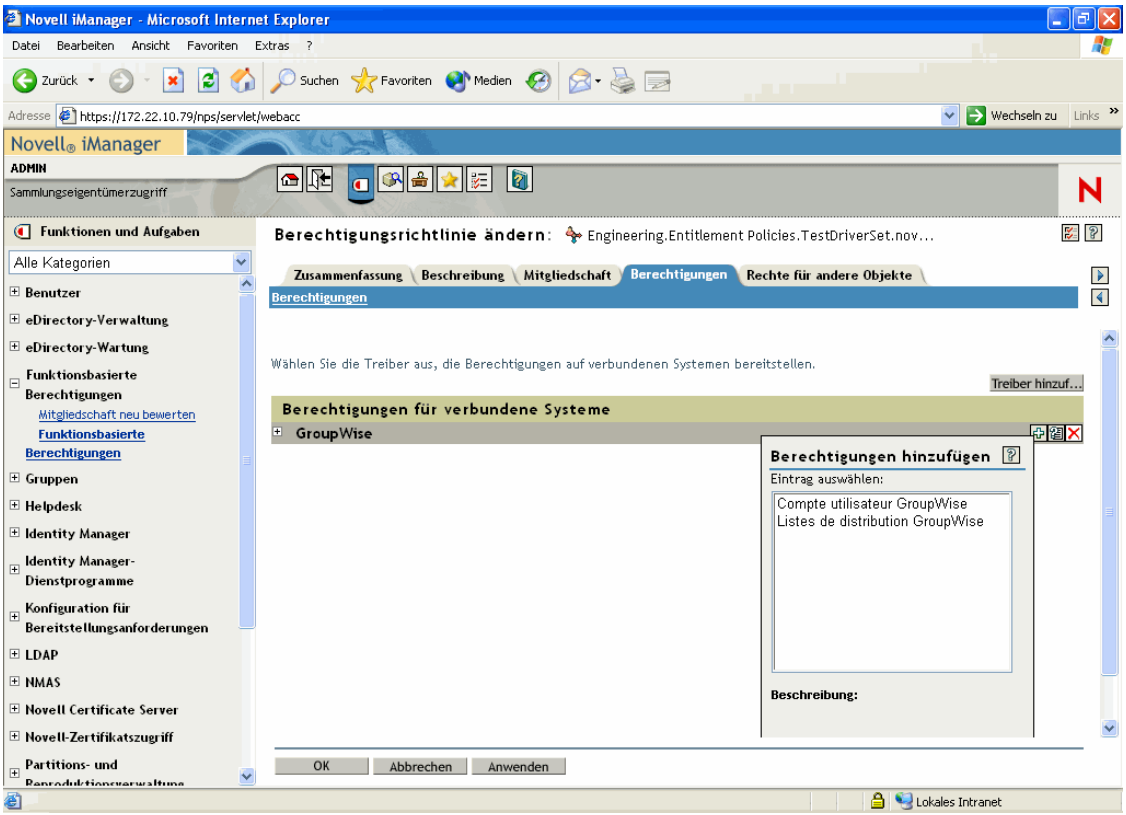
- Konten
- Mitgliedschaft in Email-Verteilerlisten
- Gruppenmitgliedschaft in NOS-Listen
- Attribute für die entsprechenden Objekte in verbundenen Systemen, die mit von Ihnen angegebenen Werten belegt sind
- Andere individuell angepasste Berechtigungen

Konten auf verbundenen Systemen

Öffnen Sie zum Hinzufügen von Berechtigungen zu einer Berechtigungsrichtlinie die Seite „Berechtigungen“ und wählen Sie einen Treiber aus. Die vom Treiber bereitgestellten Berechtigungen werden eingeblendet.

Die folgende Abbildung zeigt beispielsweise zwei Arten von Berechtigungen, die ein GroupWise-Treiber bereitstellt. Beim ersten Eintrag in der Liste handelt es sich um ein GroupWise-Benutzerkonto.

Abbildung 6-3 *Schnittstelle für das Definieren von Berechtigungen*



Mitgliedschaft in Email-Verteilerlisten und NOS-Listen

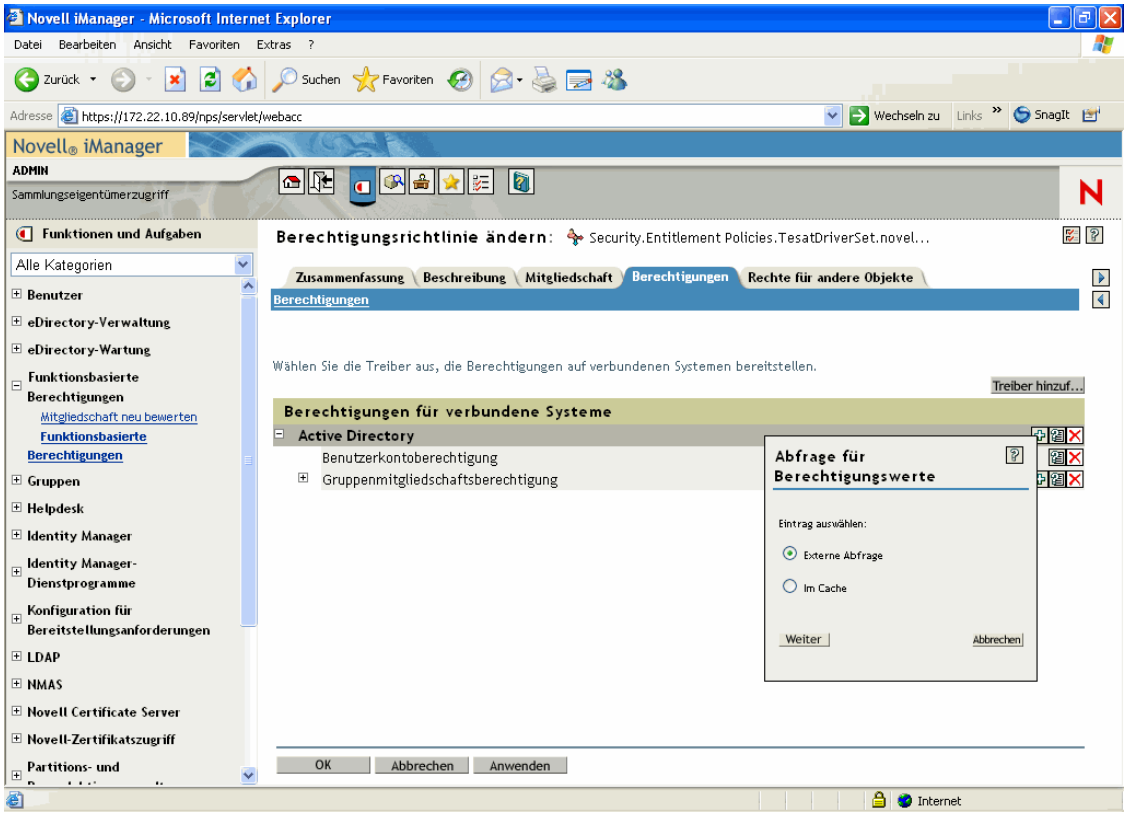
Wählen Sie zum Zuweisen von Mitgliedschaften in Gruppen oder auf verbundenen Systemen in der Liste der vom Treiber bereitgestellten Berechtigungen die Mitgliedschaftsberechtigung aus.

Die folgende Abbildung zeigt ein Beispiel; in dem es sich beim zweiten Eintrag in der Liste um GroupWise-Verteilerlisten handelt.

Abbildung 6-4 *Auswählen von GroupWise-Verteilerlisten*

Wenn Sie in diesem Beispiel *GroupWise-Verteilerlisten* wählen, wird ein Abfragefenster eingeblendet, wie in der folgenden Abbildung gezeigt.

Abbildung 6-5 *Abfrage für Berechtigungen*



In der Schnittstelle „Berechtigungsrichtlinie“ können Sie die Liste der Email-Verteilerlisten oder NOS-Listen abfragen. Nach erfolgter Abfrage können Sie die gecachte Liste anzeigen.

Die Treiber sind so konfiguriert, dass die vollständige Liste ausgegeben wird, damit Sie eine Auswahl aus den Listen treffen können, die auf dem verbundenen System vorhanden sind.

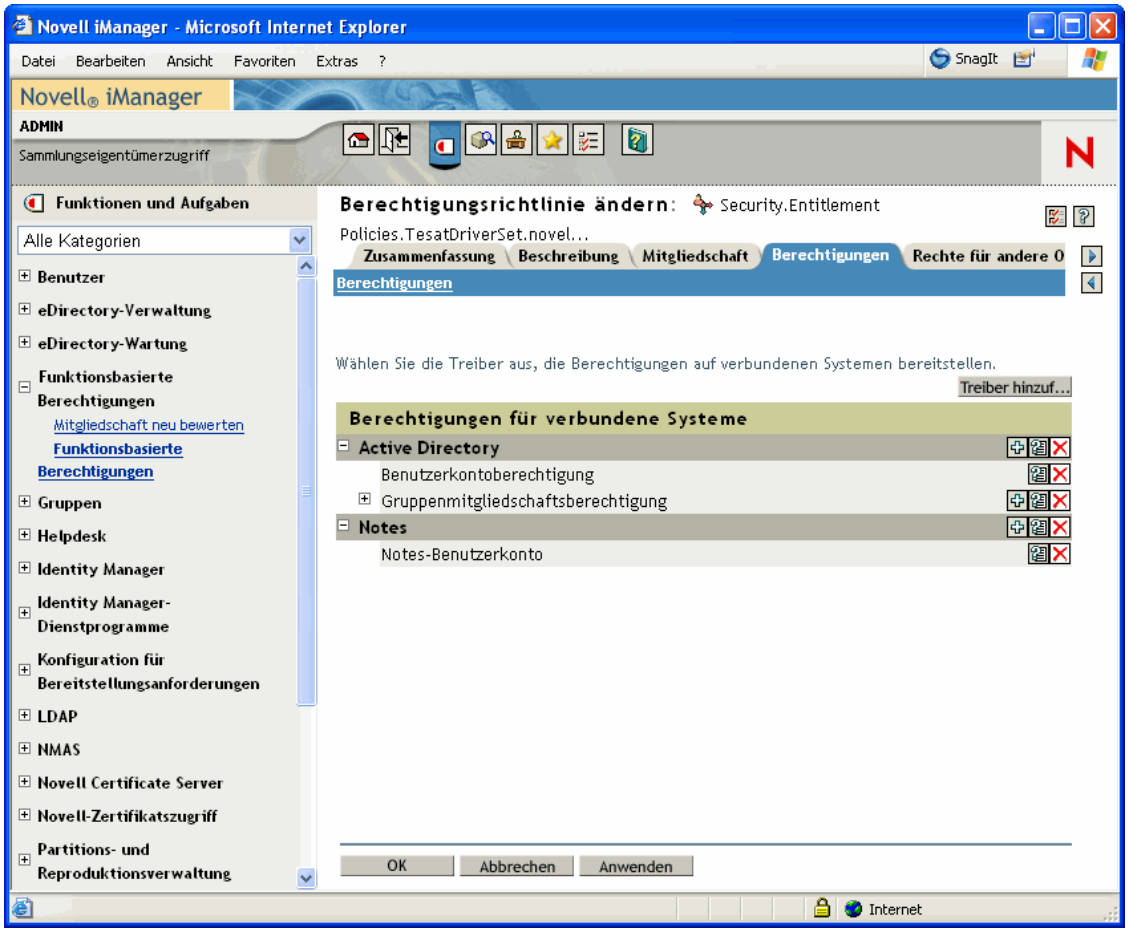
Hinweis: Ein Treiber kann auch so abgeändert werden, dass die Liste auf von Ihnen angegebene Gruppennamen beschränkt und nicht vollständig ausgegeben wird.

Attributwerte auf verbundenen Systemen

Sie können für Benutzerkonten auf verbundenen Systemen Attributwerte zuweisen. Geben Sie hierfür den Wert ein, den die Benutzerkonten erhalten sollen.

Die folgende Abbildung zeigt ein Beispiel für das Hinzufügen eines Attributwerts zu einem Notes-Attribut („Department“).

Abbildung 6-6 *Hinzufügen eines Attributwerts*



6.8 Konfliktlösung zwischen funktionsbasierten Berechtigungsrichtlinien

6.8.1 Konflikte - Überblick

Beim Erstellen von Berechtigungsrichtlinien kann es vorkommen, dass die für einen bestimmten Benutzer geltenden Richtlinien mit der Zuweisung von Berechtigungen an diesen Benutzer in Konflikt stehen.

Nachstehend erfahren Sie, wie sich solche Konflikte lösen lassen. Bei einigen Berechtigungen können Sie die Methode zur Konfliktlösung ändern.

- **Berechtigungen ohne Werte ergänzen sich.** In den meisten Fällen besitzt eine Kontoberechtigung keine Werte. Wenn einem Benutzer mit einer Berechtigungsrichtlinie ein Konto auf einem verbundenen System erteilt wird, erhält der Benutzer ein Konto auf diesem System. Es spielt dabei keine Rolle, ob ein Konflikt mit einer anderen Berechtigungsrichtlinie besteht Es handelt sich bei dem Ergebnis immer um eine Ergänzung.

  Dies trifft immer zu, daher kann die Methode zur Konfliktlösung beim Erteilen von Konten nicht geändert werden.

  Berechtigungen ohne Werte sind mit einem Lichtschalter vergleichbar: Dieser ist entweder ein- oder ausgeschaltet - erteilt oder nicht erteilt.

  Wenn beispielsweise die Berechtigungsrichtlinie „Manager“ einem Benutzer namens Jean Chandler ein Exchange-Konto erteilt, Jean Chandler jedoch von der für das Erteilen von Exchange-Konten zuständigen Berechtigungsrichtlinie „Mail Room Employees“ ausgeschlossen ist, erhält Jean dennoch ein Exchange-Konto.
- **Standardmäßig ergänzen sich Berechtigungen mit Werten im Konfliktfall, Sie können aber auch eine Konfliktlösung nach Priorität vorgeben.** Berechtigungen wie z. B. eine Gruppenmitgliedschaft besitzen eine Liste von Gruppennamen für die Werte oder ein Attribut mit einem Wert. Standardmäßig ergänzen sich diese Berechtigungen.

  Für diese Art der Berechtigungen kann die Methode zur Konfliktlösung ggf. geändert werden.

  In jeder Berechtigung ist eine Einstellung, die die Vorgehensweise bei einem Konflikt festlegt. Jede Art der Berechtigung, die für einen Treiber festgelegt wurde, ist im Manifest separat aufgeführt. Berechtigungen mit Werten verfügen über ein Konfliktlösungsattribut, das für jede Berechtigung getrennt gesetzt wird. Die Standardeinstellung ist `conflict-resolution="priority"`. Der andere mögliche Wert lautet `conflict-resolution="union"`.

  - **conflict-resolution=“union” —** Der Wert “union” bedeutet, dass die Berechtigungen sich ergänzen. Einem Benutzer werden alle Berechtigungen erteilt, die ihm durch die Mitgliedschaft in sämtlichen Richtlinien zustehen. Die abweichenden Berechtigungswerte werden einfach addiert und der Benutzer erhält sie alle.

    Beispiel: Jameel ist Mitglied der Richtlinie „Trade Show Contractors“, die die Mitgliedschaft in der GroupWise-Email-Verteilerliste „Trade Show Mailing List“ erteilt. Er ist jedoch von der Mitgliedschaft in der Richtlinie „Trade Show Managers“, die ebenfalls die Mitgliedschaft in der Email-Verteilerliste „Trade Show Mailing List“ erteilt, ausgeschlossen. In diesem Fall erhält Jameel dennoch die Mitgliedschaft in der Email-Verteilerliste.

    Ein weiteres Beispiel: Consuela wird durch die Richtlinie „Mailroom“ die Mitgliedschaft in der AD-Gruppe „Mailroom Staff“ erteilt. Zudem wird ihr von der Richtlinie „Emergency Volunteers“ die Mitgliedschaft in der AD-Gruppe „Emergency Response“ erteilt. In diesem Fall wird Consuela die Mitgliedschaft in beiden AD-Gruppen erteilt.

    Bei dieser Einstellung spielt die Reihenfolge einer Berechtigungsrichtlinie in der Richtlinienliste keine Rolle.
  - **conflict-resolution=“priority” —** Wenn sich zwei Werte in unterschiedlichen Richtlinien überschneiden oder eine Richtlinie den Benutzer ein- und eine andere ihn ausschließt, bewirkt der Wert “priority”, dass einem Benutzer nur die Berechtigungen aus der Berechtigungsrichtlinie erteilt werden, die in der Liste weiter oben stehen.

Bei den vorgenannten Beispielen fällt das Ergebnis mit dieser Einstellung anders aus.

Jameel beispielsweise erhält keine Mitgliedschaft in „Trade Show Mailing List“, wenn die Richtlinie für die GroupWise-Email-Verteilerliste den Wert “priority” verwendet und die Richtlinie „Trade Show Managers“ in der Liste vor der Richtlinie „Trade Show Contractors“ steht.

Consuela erhält nur die Mitgliedschaft in der Gruppe „Mailroom Staff“, wenn die AD NOS-Gruppenmitgliedschaftsberechtigung den Wert “priority” verwendet und die Richtlinie „Mailroom“ in der Liste vor der Richtlinie „Emergency Volunteers“ steht. Ihr wird keine Mitgliedschaft in der Gruppe „Emergency Response“ erteilt, weil die Konfliktlösung nach Priorität und nicht durch Ergänzung erfolgt.

Diese Funktionalität ist hilfreich, wenn Sie in Ihrer Umgebung funktionsbasierte Berechtigungen verwenden, um Benutzer auf einem anderen System in hierarchischen Strukturen anzuordnen. Dadurch können Sie sicherstellen, dass die Benutzer nur jeweils an einem Ort abgelegt werden und nicht an beiden Orten gleichzeitig.

Beachten Sie, dass diese Einstellung für jede Berechtigung in jedem Treiber einzeln gesetzt werden muss.

Als allgemeine Regel gilt, dass Administrator- oder Managerrichtlinien bei Verwendung der Einstellung “priority” weiter oben in der Liste stehen sollten als Richtlinien für Endbenutzer oder einzelne Mitarbeiter. Gruppen mit enger gefassten Mitgliedschaftskriterien sollten höher als Gruppen mit breiter gefassten Mitgliedschaftskriterien eingeordnet werden.

6.8.2 Ändern der Konfliktlösungsmethode für einzelne Berechtigungen

1 Klicken Sie in iManager auf *Identity Manager > Identity Manager-Überblick* und wählen Sie einen Treibersatz aus.

Eine Seite mit einer grafischen Darstellung aller Treiber des Treibersatzes wird angezeigt.

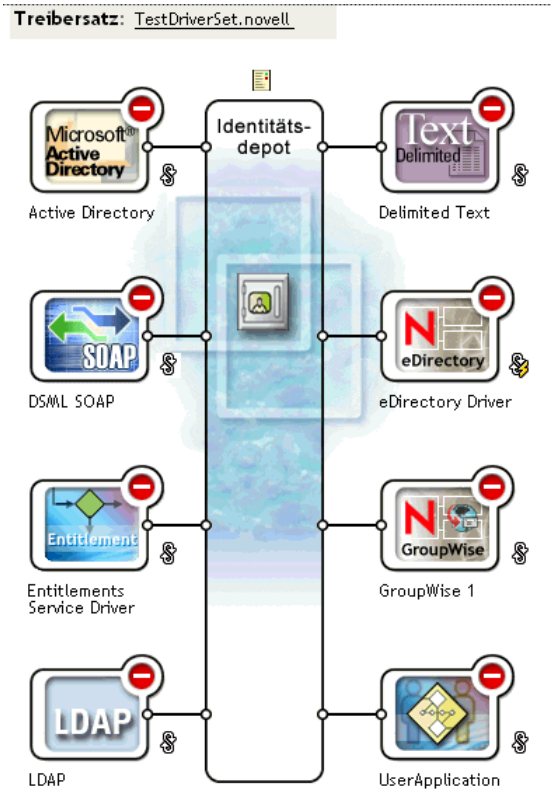
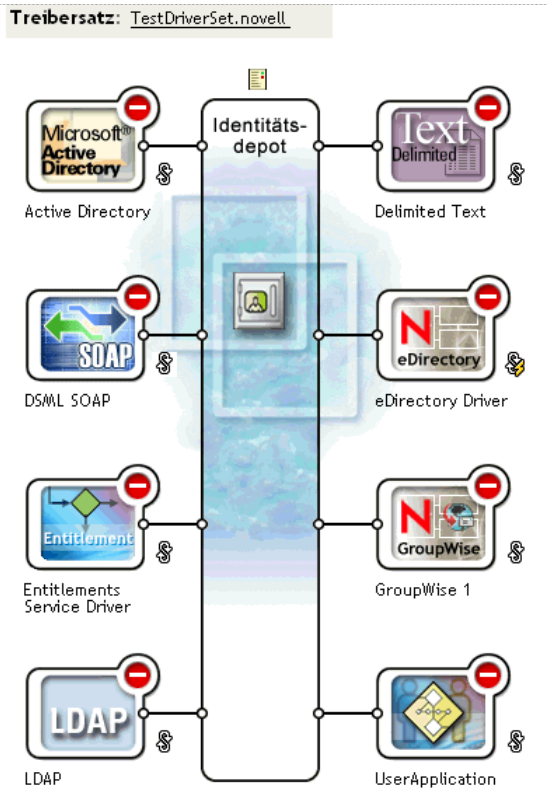


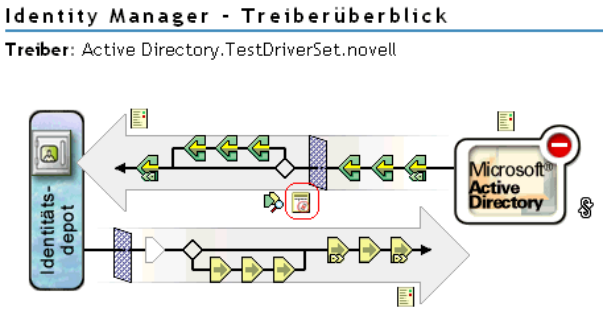
Abbildung 6-7 *Treibersatz*



2 Klicken Sie auf die Schaltfläche für den Treiberstatus und wählen Sie *Treiber anhalten.*

3 Klicken Sie auf das Symbol für den Treiber, der die gewünschte Berechtigung enthält.

Eine Seite mit Symbolen für die Richtlinien des Treibers und für den Treiber selbst wird angezeigt. Klicken Sie in der Mitte der Seite auf das Symbol *Alle Berechtigungen anzeigen* (rot eingekreist).



4 Klicken Sie auf der Seite „Berechtigungen verwalten“ auf den Namen der Berechtigung, um die Berechtigung im XML-Viewer zu öffnen.

5 Aktivieren Sie das Kontrollkästchen *XML-Bearbeitung aktivieren*.

6 Suchen Sie in der XML-Datei nach der Definition der Berechtigung, die Sie ändern möchten.

Hier ein Beispiel für die Zeile, auf die es ankommt:

```
<entitlement conflict-resolution="union" description="Grants
membership to GroupWise Distribution lists" display-name="GroupWise
Distribution Lists" name="gwDistLists">
```

7 Ändern Sie den Wert „conflict-resolution“. Die beiden folgenden Werte sind möglich:

```
conflict-resolution="union"
```

```
conflict-resolution="priority"
```

Informationen zu diesen Werten finden Sie unter „Konfliktlösung zwischen funktionsbasierten Berechtigungsrichtlinien“ auf Seite 203.

8 Klicken Sie auf *Neustart*, um den Berechtigungs-Service-Treiber neu zu starten.

6.8.3 Festlegen der Prioritäten von Berechtigungsrichtlinien

Standardmäßig spielt die Reihenfolge in der Liste der Berechtigungsrichtlinien keine Rolle. Der Grund dafür ist, dass die mit Identity Manager gelieferten Treiberkonfigurationen bei jeder Berechtigung die Einstellung `conflict-resolution="union"` als Methode zur Konfliktlösung verwenden.

Wenn Sie eine der Berechtigungen auf `conflict-resolution="priority"` umstellen, spielt die Reihenfolge in der Liste der Berechtigungsrichtlinien eine Rolle, allerdings nur für die entsprechend geänderten Berechtigungen. Informationen zu diesen Werten finden Sie unter „Konfliktlösung zwischen funktionsbasierten Berechtigungsrichtlinien“ auf Seite 203.

Sie ändern die Reihenfolge der Berechtigungsrichtlinien mittels der Pfeilschaltflächen neben der Liste mit den Berechtigungsrichtlinien. Die Richtlinie, die in der Liste ganz oben steht, hat die höchste Priorität.

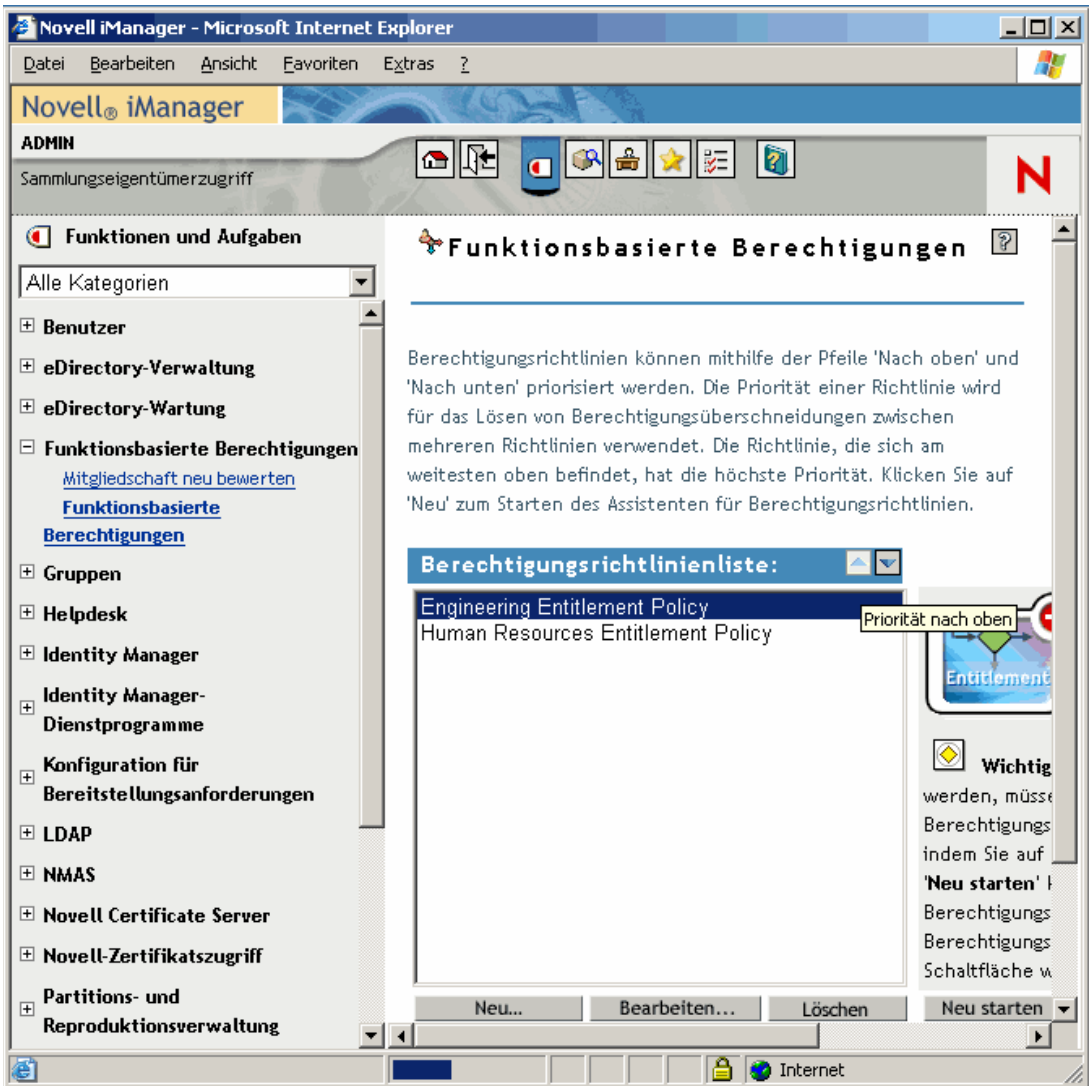
1 Klicken Sie in iManager auf *Funktionsbasierte Berechtigungen* > *Funktionsbasierte Berechtigungen*.

2 Wählen Sie einen Treibersatz aus.

Eine Seite mit einer Liste der Berechtigungsrichtlinien wird angezeigt.

3 Ändern Sie die Priorität der Berechtigungsrichtlinien mittels der Pfeilschaltflächen, mit denen die Richtlinien in der Liste nach oben oder unten verschoben werden können.

Wenn Sie eine Berechtigungsrichtlinie in der Liste weiter nach oben verschieben, erhöht sich ihre Priorität.



4 Klicken Sie auf *Schließen*, um den Treiber neu zu starten.

Die Änderungen an der Priorität werden erst nach einem Neustart des Treibers wirksam.

6.9 Fehlersuche bei funktionsbasierten Berechtigungen

Beachten Sie bei der Fehlersuche die folgenden Punkte:

- Wenn Sie Richtlinien auf der Seite mit der Richtlinienliste durch Klicken auf *Neu*, *Bearbeiten* oder *Entfernen* ändern, wird der *Berechtigungs-Service-Treiber* angehalten. Der Treiber wird erst neu gestartet, wenn Sie auf dieser Seite auf *Neustart* klicken.

  Diese Funktion verhindert, dass der Treiber Berechtigungen in Ihrer Produktionsumgebung erteilt oder entzieht, solange die Änderungen der Richtlinien noch nicht abgeschlossen sind:

- Aus demselben Grund kann der Berechtigungs-Service-Treiber nicht gestartet werden, wenn mehrere Personen gleichzeitig die Berechtigungsrichtlinien zu bearbeiten versuchen.
- Da je Treibersatz ein Berechtigungs-Service-Treiber verwendet wird, kann eine Berechtigungsrichtlinie nur diejenigen Benutzer verwalten, die sich in einer Lese-/Schreib- oder in einer Masterreproduktion auf dem Server befinden, der dem betreffenden Treibersatz zugeordnet ist.

6.10 Berechtigungselemente, die für funktionsbasierte Berechtigungen und für Workflow-basierte Bereitstellungsberechtigungen gelten

Die nachstehenden Informationen beziehen sich nicht auf eine bestimmte Implementierung, sondern auf alle Berechtigungen.

- Abschnitt 6.10.1, „Steuerung der Bedeutung des Erteilens oder Entziehens von Berechtigungen“, auf Seite 210
- Abschnitt 6.10.2, „Verhindern von Datenverlusten“, auf Seite 211
- Abschnitt 6.10.3, „Passwortsynchronisierung und Berechtigungen“, auf Seite 211

6.10.1 Steuerung der Bedeutung des Erteilens oder Entziehens von Berechtigungen

Sie können die Konsequenzen des Erteilens oder Entziehens einer Berechtigung steuern. Jeder Treiber liefert eine Liste der unterstützten Möglichkeiten zur Steuerung der Konsequenzen des “Erteilens” oder “Entziehens.”

Wenn Sie beispielsweise ein GroupWise-Konto hinzufügen, können Sie festlegen, dass „Erteilen“ in Wirklichkeit bedeutet, dem Benutzer das Konto in deaktiviertem Zustand zu erteilen, sodass der Administrator eingreifen muss, bevor der Benutzer auf das Konto zugreifen kann. Sie können das Konto auch aktivieren, dies ist die Standardeinstellung.

Standardmäßig werden in den mitgelieferten Treiberkonfigurationen die Optionen verwendet, bei denen ein Datenverlust am unwahrscheinlichsten ist. So ist beispielsweise die Standardbedeutung von „Entfernen“ bei einem GroupWise-Konto auf “Deaktivieren” eingestellt, damit das Konto nicht verloren geht, wenn der Administrator beim Ändern der Richtlinien einen Fehler macht. Die Identity Manager-Treiberkonfigurationen entziehen beispielsweise auch keine Berechtigungen, die Werte aus einem Benutzerkonto in einem anderen System enthalten. Wenn einem Benutzer die Mitgliedschaft in einer Email-Verteilerliste erteilt wird und der Benutzer später einmal die Kriterien für die Berechtigungsrichtlinie nicht mehr erfüllt, wird er einfach aus der Berechtigungsrichtlinie ausgerschlossen. Die Konten werden deaktiviert, die Gruppenmitgliedschaft und die Attributwerte werden jedoch nicht entfernt. Ein Identity Manager-Experte kann die Treiberkonfigurationen anpassen, wenn Sie andere Ergebnisse wünschen.

Die Interpretation des Entziehens einer Berechtigung ist besonders wichtig, weil funktionsbasierte Berechtigungen die Möglichkeit bieten, in der Produktionsumgebung einer Organisation weitreichende Änderungen durchzuführen, ohne die Ergebnisse vorher testen zu müssen.

Sie können die Einstellungen für das Interpretieren des Erteilens oder Entziehens durch Bearbeiten der Globalkonfigurationswerte eines vorkonfigurierten Treibers ändern. Wenn Sie eine eigene

Konfiguration erstellen, können Sie GCVs hinzufügen, damit das Erteilen und Entziehen von Berechtigungen wunschgemäß interpretiert wird.

6.10.2 Verhindern von Datenverlusten

Funktionsbasierte Berechtigungen bieten die Möglichkeit, auf Basis der Mitgliedschaft in einer Richtlinie weitreichende Änderungen an Berechtigungen wie z. B. Konten durchzuführen. Zugleich bedeutet dies jedoch, dass Fehler beim Ändern von Richtlinien zum Problem werden können. Die mit Identity Manager gelieferten Treiberkonfigurationen verwenden die ungefährlichsten Einstellungen. Sie sollten sich über die Verwendung von GCVs im Klaren sein, um keine Datenverluste zu riskieren.

Wir empfehlen beispielsweise, niemals „delete“ (löschen) als Wert für die GCV zu verwenden, die das Entziehen einer Kontoberechtigung interpretiert.

Als weitere Datenschutzmaßnahme wird der Treiber beim Bearbeiten oder Erstellen von Berechtigungsrichtlinien deaktiviert, damit keine Änderungen wirksam werden, solange Sie die Bearbeitung der Richtlinien noch nicht abgeschlossen haben. Sobald Sie fertig sind, können Sie den Treiber über die Schaltfläche *Neustart* in der Schnittstelle „Berechtigungsrichtlinien“ manuell neu starten. Wenn gleichzeitig ein anderer Benutzer die Berechtigungsrichtlinien bearbeitet und Sie den Berechtigungs-Service-Treiber über die Schaltfläche *Neustart* neu zu starten versuchen, werden Sie ebenso aufgefordert, den Treiber erst dann neu zu starten, wenn der andere Benutzer alle seine Änderungen vorgenommen hat.

6.10.3 Passwortsynchronisierung und Berechtigungen

Die Passwortsynchronisierung wird bei Treibern mit funktionsbasierten Berechtigungen auf die gleiche Weise verwaltet wie bei anderen Treibern (siehe „Passwortsynchronisierung mit verbundenen Systemen“ auf Seite 75).

Sicherheit: Best Practices

7

7.1 Verwenden von SSL

Aktivieren Sie SSL für alle Transportverfahren, für die es zur Verfügung steht. Verwenden Sie SSL für die Kommunikation zwischen der Metaverzeichnis-Engine und dem Remote Loader (siehe Abschnitt 3.2, „Sichere Datentransfers“, auf Seite 47) sowie zwischen der Metaverzeichnis-Engine oder dem Remote Loader und den verbundenen Systemen.

Wenn Sie SSL nicht aktivieren, werden die Daten (z. B. Passwörter) unverschlüsselt gesendet.

7.2 Gesicherter Zugriff

Vergewissern Sie sich, dass der Zugriff auf die Identitätsdepots und die Identity Manager-Objekte sicher ist.

Physische Sicherheit. Schützen Sie den Zugriff auf den physischen Speicherort der Server, auf denen ein Identitätsdepot installiert ist.

Zugriffsrechte. Zum Erstellen von Identity Manager-Objekten und zum Konfigurieren von Treibern sind administrative Rechte erforderlich. Überwachen und kontrollieren Sie, wer Rechte zum Erstellen oder Bearbeiten hat für:

- Einen Identity Manager-Treibersatz
- Einen Identity Manager-Treiber
- Treiberkonfigurationsobjekte (Filter, Formatvorlagen, Richtlinien), insbesondere Richtlinien für den Abruf von Passwörtern oder für die Synchronisierung
- Passwortrichtlinienobjekte (und die iManager-Aufgabe zum Bearbeiten dieser Objekte), da diese steuern, welche Passwörter miteinander synchronisiert und welche Passwortselbstbedienungsoptionen verwendet werden

7.3 Verwalten von Passwörtern

Wenn Sie Daten zwischen verbundenen Systemen austauschen möchten, sollten Sie darauf achten, dass beim Datenaustausch alle sicherheitsrelevanten Aspekte berücksichtigt werden. Dies gilt insbesondere für Passwörter.

- Das Passworthinweisattribut (nsimHint) ist öffentlich zugänglich, damit nicht authentifizierte Benutzer, die ihr Passwort vergessen haben, ihren Passworthinweis lesen können. Passworthinweise tragen dazu bei, die Helpdesk-Anrufe zu reduzieren.

  Aus Sicherheitsgründen werden Passworthinweise überpüft, um sicherzustellen, dass sie nicht das eigentliche Passwort des Benutzers enthalten. Trotzdem kann der Passworthinweis eines Benutzers zu viele Informationen über das Passwort preisgeben.

  So erhöhen Sie bei Verwendung der Passworthinweise die Sicherheit:

  - Gewähren Sie nur auf dem LDAP-Server, der für die Passwortselbstbedienung verwendet wird, den Zugriff auf das nsimHint-Attribut.
  - Machen Sie zur Bedingung, dass Benutzer zuerst Herausforderungsfragen beantworten müssen, bevor sie den Passworthinweis erhalten.
  - Erinnern Sie Benutzer daran, Passworthinweise zu erstellen, aus denen nur sie das Passwort ableiten können. Die Passwortänderungsmeldung in der Passwortrichtlinie bietet dazu eine Möglichkeit. Weitere Informationen hierzu finden Sie unter “Adding a Password Change Message” im Password Management Administration Guide (http://www.novell.com/documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung).

  Falls Sie auf die Passworthinweise verzichten möchten, stellen Sie sicher, dass sie in keiner der Passwortrichtlinien verwendet werden. Wenn Sie das Einrichten von Passworthinweisen verhindern möchten, können Sie noch einen Schritt weitergehen und die Einrichtungsfunktion vollständig entfernen. Eine Beschreibung dieses Vorgangs finden Sie unter “Disabling Password Hint by Removing the Hint Gadget” im Password Management Administration Guide (http://www.novell.com/documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung).
- Herausforderungsfragen sind ebenfalls öffentlich zugänglich, damit nicht authentifizierte Benutzer, die ihr Passwort vergessen haben, sich auf eine andere Art authentifizieren können. Herausforderungsfragen als erforderlich zu definieren erhöht im Rahmen der Selbstbedienung bei vergessenen Passwörtern die Sicherheit, weil ein Benutzer seine Identität durch die korrekte Beantwortung der Fragen beweisen muss, bevor er das vergessene Passwort oder einen Passworthinweis erhält bzw. bevor das Passwort neu eingestellt werden kann.

  Bei Herausforderungsfragen ist die Unbefugtensperre aktiv, d. h., es ist nur eine beschränkte Anzahl fehlerhafter Versuche möglich.

  Dennoch könnte ein Benutzer Herausforderungsfragen erstellen, die Rückschlüsse auf das Passwort ermöglichen. Erinnern Sie Benutzer daran, Herausforderungsfragen und -antworten zu erstellen, aus denen nur sie das Passwort ableiten können. Die Passwortänderungsmeldung in der Passwortrichtlinie bietet dazu eine Möglichkeit. Weitere Informationen hierzu finden Sie unter “Adding a Password Change Message” im Password Management Administration Guide (http://www.novell.com/documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung).

- Aus Sicherheitsgründen sind die Aktionen *Aktuelles Passwort per Email an den Benutzer senden* und *Benutzer darf Passwort zurücksetzen* bei vergessenen Passwörtern nur dann verfügbar, wenn der Benutzer die Herausforderungsfragen beantworten muss.
- In NMAS™ 2.3.4 wurde die Sicherheit von universellen Passwörtern, die von einem Administrator geändert werden, verbessert. Diese Verbesserung funktioniert im Großen und Ganzen genauso wie die Funktion für das NDS®-Passwort.

  Wenn ein Administrator das Passwort eines Benutzers ändert, z. B. beim Erstellen eines neuen Benutzers oder als Reaktion auf einen Helpdesk-Anruf, läuft das Passwort automatisch ab, wenn Sie die entsprechende Einstellung in der Passwortrichtlinie aktiviert haben. Die Einstellung befindet sich in der Passwortrichtlinie unter „Erweiterte Passwortregeln“ und lautet *Anzahl der Tage bis zum Ablaufen des Passworts (0-365)*. Bei dieser speziellen Funktion ist die Anzahl der Tage unwichtig, aber die Einstellung muss aktiviert sein.

7.4 Erstellen von Richtlinien für sichere Passwörter

Passwortrichtlinienobjekte sind öffentlich zugänglich, damit Anwendungen überprüfen können, ob Passwörter regelkonform sind. Dies bedeutet, dass ein nicht authentifizierter Benutzer eine Abfrage in einem Identitätsdepot ausführen kann, um herauszufinden, welche Passwortrichtlinien in Kraft sind. Wenn Ihre Passwortrichtlinien es erfordern, dass Benutzer sichere Passwörter erstellen müssen, sollte dies, wie unter “Create Strong Password Policies” im Password Management Administration Guide (http://www.novell.com/documentation/password_management/index.html) (Administrationshandbuch zur Passwortverwaltung) ausgeführt, kein Risiko darstellen.

Mit der Identity Manager-Passwortsynchronisierung können Sie die Vergabe und Verwaltung von Benutzerpasswörtern vereinfachen und dadurch die Helpdesk-Kosten reduzieren. Die bidirektionale Passwortsynchronisierung ermöglicht eDirectory und verbundenen Systemen, Passwörter auf verschiedene Arten gemeinsam zu nutzen. Dies wird in den Szenarios in Abschnitt 5.8, „Implementierung der Passwortsynchronisierung“, auf Seite 115 beschrieben.

Durch das universelle Passwort und die Passwortrichtlinien können Sie die Verwendung von sicheren Passwörtern erzwingen. Verwenden Sie dazu die erweiterten Passwortregeln in den Passwortrichtlinien. Mit diesen befolgen Sie die in der Softwarebranche gängigen Best Practices für Passwörter.

Sie können beispielsweise festlegen, dass Benutzerpasswörter folgende Regeln einhalten müssen:

- Passwörter müssen eindeutig sein.

  Sie können verhindern, dass Benutzer Passwörter wiederverwenden, und die Anzahl der Passwörter festlegen, die das System für Vergleiche in der Verlaufsliste speichern soll.
- Ein Passwort muss eine Mindestlänge haben.

  Lange Passwörter verwenden zu müssen, ist eine der besten Möglichkeiten, sie sicherer zu machen.
- Ein Passwort muss eine Mindestanzahl an numerischen Zeichen enthalten.

  Wenn sich mindestens ein numerisches Zeichen in einem Passwort befindet, schützt dies vor „Wörterbuchattacken“, bei denen unbefugte Benutzer versuchen, sich durch die Verwendung von Wörtern aus dem Wörterbuch beim System anzumelden.
- Bestimmte Passwörter ausschließen.

Sie können Wörter ausschließen, die Sie als Sicherheitsrisiko ansehen, wie z. B. den Firmennamen, den Standort Ihres Unternehmens bzw. die Wörter „test“ oder „admin“. Obwohl die Ausschlussliste nicht dazu dienen soll, ein komplettes Wörterbuch zu importieren, kann sie relativ lang sein. Bedenken Sie, dass eine lange Ausschlussliste den Anmeldevorgang verlangsamt. Ein besserer Schutz vor Wörterbuchattacken besteht darin, Passwörter mit numerischen Zeichen oder bestimmten Sonderzeichen zu versehen.

Beachten Sie bitte, dass Sie mehrere Passwortrichtlinien erstellen können, wenn Sie in unterschiedlichen Teilen des Baums unterschiedliche Passwortanforderungen festgelegt haben. Eine Passwortrichtlinie kann für einen gesamten Baum, einen Partitionsstammcontainer, einen Container oder sogar einen einzelnen Benutzer gelten. (Es wird zur Vereinfachung der Administration allerdings empfohlen, Passwortrichtlinien so hoch wie möglich im Baum zu definieren.)

Zur Erhöhung der Sicherheit können Sie zusätzlich die Unbefugtensperre einsetzen. Mit dieser eDirectory-Funktion geben Sie an, wie viele fehlerhafte Anmeldeversuche möglich sind, bevor ein Konto gesperrt wird. Diese Einstellung nehmen Sie nicht in der Passwortrichtlinie, sondern am übergeordneten Container vor. Weitere Informationen hierzu finden Sie unter “Managing User Accounts” im *Novell eDirectory 8.7.3 Administration Guide* (http://www.novell.com/documentation/edir873/edir873/data/afxkmdi.html#amm7bjv) (Novell eDirectory 8.7.3 Administrationshandbuch).

7.5 Sicherheit auf verbundenen Systemen

Verbundene Systeme, mit denen Sie Daten synchronisieren, gefährden bei der Speicherung oder Übertragung dieser Daten möglicherweise deren Sicherheit.

Stellen Sie sicher, dass die Systeme, mit denen Sie Passwörter austauschen, die gewünschten Sicherheitsrichtlinien einhalten. Beispielsweise müssen bei LDAP, NIS und Windows Aspekte bezüglich der Sicherheit beachtet werden, bevor Sie für diese Systeme die Passwortsynchronisierung aktivieren können.

Viele Softwarehersteller haben eigene Sicherheitsrichtlinien definiert, die Sie für deren Produkte befolgen sollten.

7.6 Designer für Identity Manager

Bei Verwendung des Designers für Identity Manager sollten Sie Folgendes beachten:

- Überwachen und kontrollieren Sie, wer Rechte zum Erstellen oder Bearbeiten eines Identity Manager-Treibers hat.

  Zum Erstellen von Identity Manager-Objekten und zum Konfigurieren von Treibern sind administrative Rechte erforderlich.
- Bevor Sie ein Administratorpasswort für ein Identitätsdepot an einen technischen Berater vergeben, schränken Sie die Rechte dieses Administrators auf die Bereiche ein, auf die der Berater Zugriff haben muss.
- Löschen Sie die Projektdateien (`.proj`) oder speichern Sie sie in einem Firmenverzeichnis.

  Die `.proj`-Dateien des Designers müssen am firmeninternen Speicherort des Projekts verbleiben. Nach Abschluss des Projekts muss der technische Berater die Dateien der Firma überlassen.
- Wenn Projekt-, Protokoll- und Trace-Dateien nicht mehr benötigt werden, löschen Sie sie.

- Bevor Sie einen Laptop entsorgen oder außer Betrieb nehmen, sollten Sie die Projektdateien auf dessen Festplatte löschen.
- Stellen Sie sicher, dass die Verbindung vom Designer zum Identitätsdepot-Server physisch sicher ist.

  Anderenfalls könnte ein unbefugter Benutzer den Datenverkehr mitverfolgen und firmeninterne bzw. sicherheitsrelevante Daten ausspionieren.
- Wenn Sie Dokumente mit dem Dokumentengenerator erstellen, gehen Sie umsichtig mit diesen Dokumenten um.

  Sie enthalten möglicherweise Passwörter und sicherheitsrelevante Daten in Klartext.
- Wenn der Designer ein eDirectory-Attribut lesen oder schreiben muss, kennzeichnen Sie dieses Attribut nicht als verschlüsselt.

  Der Designer kann verschlüsselte Attribute weder lesen noch schreiben.
- Speichern Sie keine sicherheitsrelevanten Passwörter.

  Zurzeit werden Designer-Projekte nicht verschlüsselt. Passwörter sind lediglich kodiert. Geben Sie deshalb keine Designer-Projekte, die gespeicherte Passwörter haben, zur gemeinsamen Nutzung frei.

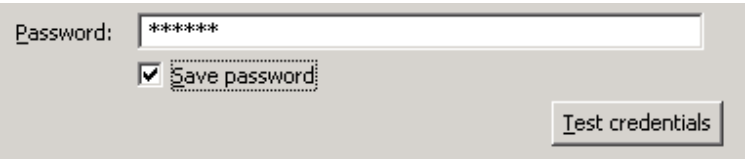
  So speichern Sie ein Passwort für eine Sitzung, aber nicht im Projekt:

  a. Klicken Sie in der erweiterten Überblicksansicht mit der rechten Maustaste auf ein Identitätsdepot.
  b. Wählen Sie „Properties“ (Eigenschaften).
  c. Geben Sie auf der Konfigurationsseite ein Passwort ein und klicken Sie auf *OK*.

     Sie können einmal pro Sitzung ein Passwort eingeben. Wenn Sie das Projekt schließen, geht das Passwort verloren.

  Wenn Sie ein Passwort auf der Festplatte speichern möchten, führen Sie die Schritte 1 bis 3 aus, wählen Sie *Save Password* (Passwort speichern) und klicken Sie auf *OK*.

Abbildung 7-1 *Passwort speichern*



7.7 Best Practices bei der Einrichtung von Sicherheitsmaßnahmen

Befolgen Sie bei der Implementierung von Sicherheitsmaßnahmen die Best Practices der Branche. Blockieren Sie z. B. nicht verwendete Ports auf dem Server.

7.8 Überwachung von Änderungen an sicherheitsrelevanten Daten

- Abschnitt 7.8.1, „Protokollierung von Ereignissen über iManager“, auf Seite 218
- Abschnitt 7.8.2, „Protokollierung von Ereignissen über den Designer“, auf Seite 219

7.8.1 Protokollierung von Ereignissen über iManager

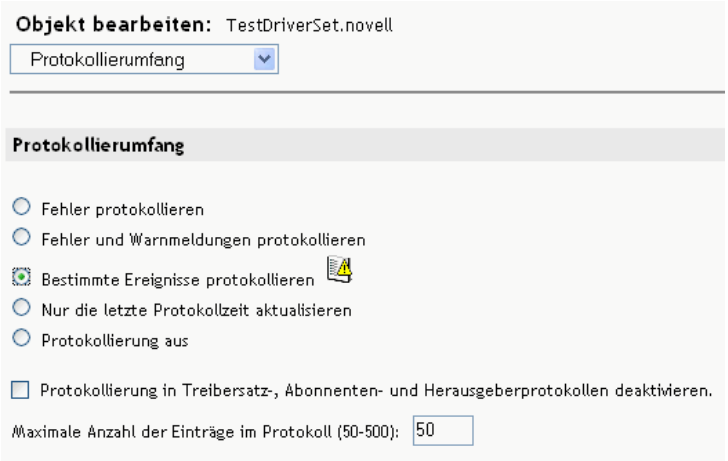
Sie können mit Novell Audit Ereignisse protokollieren, die Sie als wichtig für die Sicherheit erachten. Weitere Informationen zu Novell Audit finden Sie in Kapitel 10, „Protokollierung und Berichterstellung mit Novell Audit“, auf Seite 247.

Beispielsweise können Sie Passwortänderungen für einen bestimmten Identity Manager-Treiber (oder einen Treibersatz) wie folgt protokollieren:

1 Wählen Sie *eDirectory-Administration* > *Objekt bearbeiten* > *Protokollierumfang*.

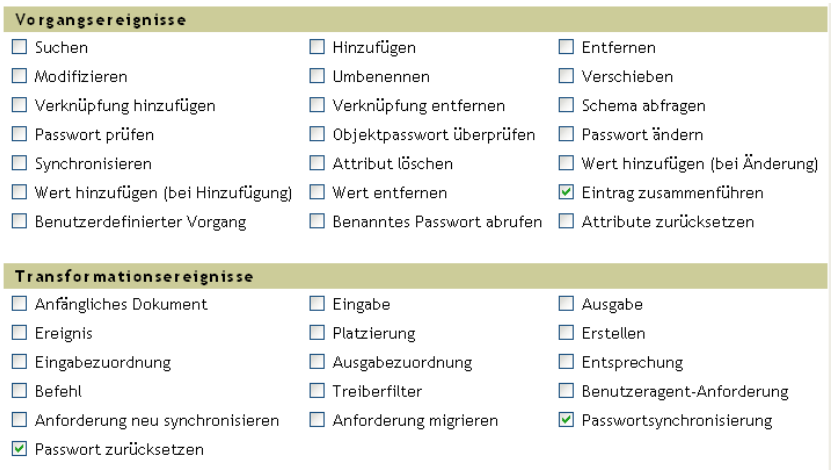
Je nach iManager-Version können Sie die Optionen in einer Dropdown-Liste oder auf einer Registerkarte auswählen.

2 Wählen Sie *Bestimmte Ereignisse protokollieren*.



3 Klicken Sie zum Auswählen bestimmter Ereignisse auf das Symbol für die Protokollereignisse  .

4 Wählen Sie auf der Ereignisseite Folgendes aus:



- Wählen Sie unter „Vorgangsereignisse“ die Option *Passwort ändern*.

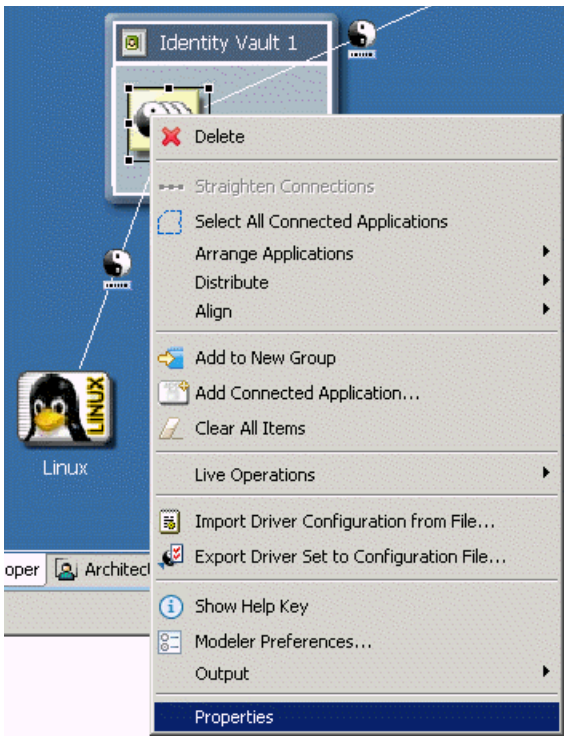
  Mit dieser Option können Sie direkte Änderungen am NDS-Passwort überwachen.
- Wählen Sie unter „Transformationsereignisse“ die Option *Passwort zurücksetzen* und *Passwortsynchronisierung*. Mit diesen zwei Optionen können Ereignisse für das universelle Passwort und das Verteilungspasswort überwacht werden.

5 Klicken Sie zweimal auf *OK*.

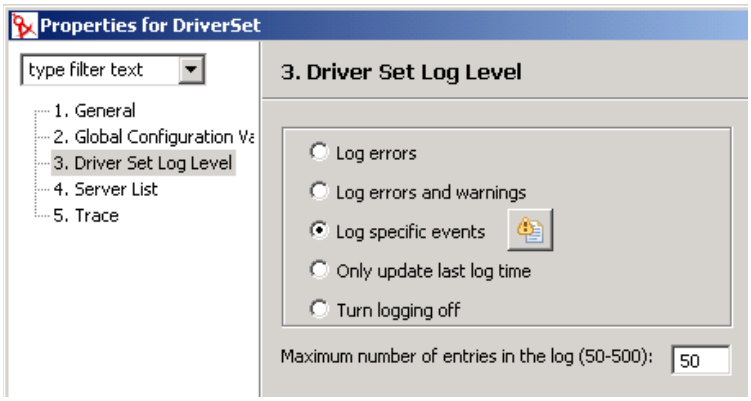
7.8.2 Protokollierung von Ereignissen über den Designer

Sie können Ereignisse für einen Treibersatz oder einen Treiber protokollieren.

Protokollierung von Ereignissen für einen Treibersatz

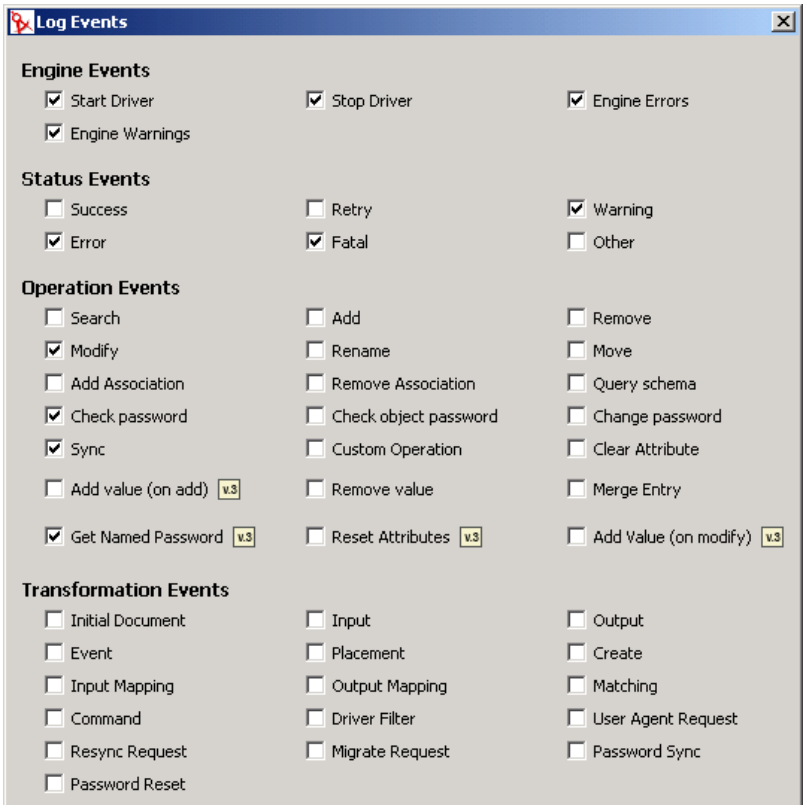


1 Klicken Sie in Designer mit der rechten Maustaste auf einen Treibersatz und wählen Sie *Properties* (Eigenschaften).



2 Wählen Sie *Driver Set Log Level* (Protokollierumfang für Treibersatz) und anschließend *Log Specific Events (Bestimmte Ereignisse protokollieren)*.

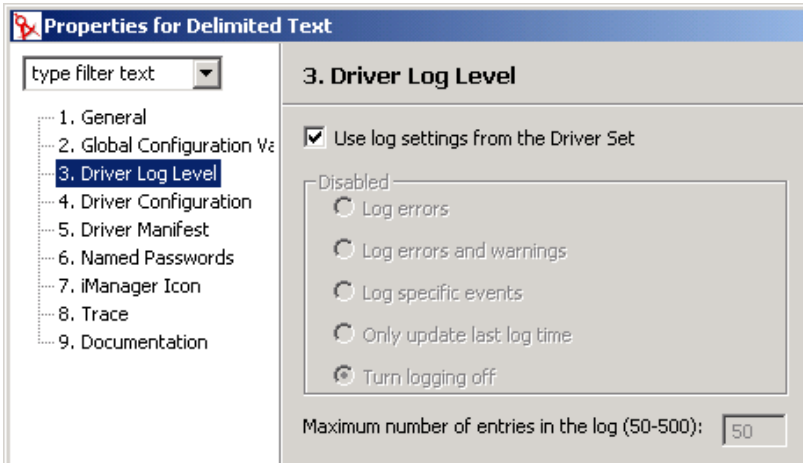
3 Klicken Sie auf das Symbol *Zu protokollierende Ereignisse auswählen*.



4 Wählen Sie die zu protokollierenden Ereignisse aus und klicken Sie anschließend auf *OK*.

Protokollierung von Ereignissen für einen Treiber

1 Klicken Sie in Designer mit der rechten Maustaste auf einen Treiber und wählen Sie *Properties* (Eigenschaften).



2 Wählen Sie *Driver Log Level* (Protokollierumfang für Treiber) und anschließend *Log Specific Events (Bestimmte Ereignisse protokollieren)*.

   Sie können auch die Einstellungen für den Treibersatz akzeptieren und anschließend auf *OK* klicken. Deaktivieren Sie anderenfalls die Option *Use log settings from the Driver Set* (Protokolleinstellungen vom Treibersatz verwenden), wählen Sie *Log specific events* (Bestimmte Ereignisse protokollieren) und klicken Sie anschließend auf *OK*.

3 Klicken Sie auf das Symbol *Zu protokollierende Ereignisse auswählen*.

4 Wählen Sie die zu protokollierenden Ereignisse aus und klicken Sie anschließend auf *OK*.

Verwalten von Engine-Services

8

Die folgenden Treiber werden nur für Services der Metaverzeichnis-Engine verwendet, nicht für externe verbundene Systeme. Diese Treiber werden automatisch bei der Installation von Identity Manager installiert.

8.1 Berechtigungs-Service-Treiber

Weitere Informationen hierzu finden Sie unter Kapitel 6, „Erstellung und Verwendung von Berechtigungen“, auf Seite 173.

8.2 Service-Treiber für manuelle Aufgaben

Der Service-Treiber für manuelle Aufgaben dient dazu, einen oder mehrere Benutzer darüber in Kenntnis zu setzen, dass ein Datenereignis aufgetreten und möglicherweise eine Aktion des Benutzers erforderlich ist. In einem Szenario, in dem es um die Bereitstellung für Mitarbeiter geht, kann das Datenereignis beispielsweise im Erstellen eines neuen Benutzerobjekts und die Aktion des Benutzers in der Zuteilung einer Büronummer durch eine entsprechende Dateneingabe in eDirectory oder in eine Anwendung bestehen. Denkbar sind auch Szenarios, in denen z. B. ein Administrator benachrichtigt wird, dass ein neues Benutzerobjekt erstellt wurde oder ein Benutzer Daten eines Objekts geändert hat usw.

Das Konfigurieren des Service-Treibers für manuelle Aufgaben besteht in der Regel aus dem Konfigurieren zweier separater, aber miteinander verwandter Subsysteme: die Richtlinien und Email-Schablonen des Abonnentenkanals einerseits und die Schablonen und Richtlinien des Webservers auf dem Herausgeberkanal andererseits.

Darüber hinaus müssen Treiberparameter wie z. B. der Name des SMTP-Servers, der Port des Webservers usw. konfiguriert werden.

Dieser Abschnitt umfasst:

8.2.1 Installation

- **Installation:** Der Service-Treiber für manuelle Aufgaben wird bei der Installation der Option *Metaverzeichnis-Server* durch das Installationsprogramm von Identity Manager automatisch installiert.
- **Plattformen:** Der Treiber läuft auf den von Identity Manager und dem Remote Loader unterstützten Plattformen.

- **Aktivierung:** Der Treiber muss nicht separat aktiviert werden. Wenn Sie die Metaverzeichnis-Engine aktivieren, wird dieser Treiber ebenfalls aktiviert.

8.2.2 Überblick

In diesem Abschnitt ist beschrieben, wie sich die verschiedenen Funktionen des Treibers nutzen lassen.

Betriebsarten

Es werden zwei primäre Betriebsarten unterstützt:

- **Direkte Datenanforderung:** Ein Benutzer wird durch eine Email aufgefordert, Daten in eDirectory einzugeben (die eventuell von einer anderen Anwendung verarbeitet werden sollen). Der Email-Empfänger beantwortet die Email, indem er auf eine URL in der Nachricht klickt. Die URL verweist auf einen Webserver, der auf dem Herausgeberkanal des Service-Treibers für manuelle Aufgaben läuft. Der Benutzer interagiert dann mit den dynamischen Webseiten, die der Webserver zur Authentifizierung gegenüber eDirectory™ und zum Eingeben der angeforderten Daten erzeugt.
- **Ereignisbenachrichtigung:** Eine Email wird an einen Benutzer gesendet, ohne dass der Herausgeberkanal daran beteiligt ist. Bei der Email kann es sich nur die Benachrichtigung handeln, dass in eDirectory ein Ereignis eingetreten ist, oder es könnte sich um eine Datenanforderung über eine Methode handeln, die nichts mit dem Webserver des Herausgeberkanals zu tun hat, z. B. Novell iManager, eine andere Anwendung oder eine benutzerdefinierte Schnittstelle.

Beispiel: Email auf dem Abonnentenkanal, Antwort des Webservers auf dem Herausgeberkanal

Im Folgenden ist ein Beispielszenario für einen Bereitstellungsvorgang für einen neuen Mitarbeiter aufgeführt, in dem ihm vom Manager eine Raumnummer zugewiesen wird:

1. In eDirectory wird ein neues Benutzerobjekt erstellt (z. B. vom DirXML-Treiber für das HR-System des Unternehmens).
2. Der Abonnentenkanal des Service-Treibers für manuelle Aufgaben sendet eine SMTP-Nachricht an den Manager des Benutzers sowie an dessen Assistenten. Die SMTP-Nachricht enthält eine URL, die auf den Webserver des Herausgeberkanals verweist. Zusätzlich enthält die URL Datenelemente, die den Benutzer und andere Personen identifizieren, die befugt sind, die angeforderten Daten zu senden.

3. Der Manager oder sein Assistent klickt auf die URL in der Email und in einem Web-Browser wird ein HTML-Formular angezeigt. Der Manager oder sein Assistent führt folgende Schritte aus:
    - Auswahl des DN für das eDirectory-Benutzerobjekt, wodurch der Absender der Email festgelegt wird.
    - Eingabe des eDirectory-Passworts.
    - Eingabe der Raumnummer für den neuen Mitarbeiter.
    - Senden der Raumnummer durch einen Klick auf „Absenden“.
4. Die Raumnummer des neuen Mitarbeiters wird über den Herausgeberkanal des Service-Treibers für manuelle Aufgaben an eDirectory gesendet.

Beispiel: Email auf dem Abonnentenkanal, keine Antwort auf dem Herausgeberkanal

Im Folgenden ist ein Beispielszenario aufgeführt, in dem der Manager eines neuen Mitarbeiters dem Mitarbeiter einen Computer in einem Asset-Management-System zuweist:

1. In eDirectory wird ein neues Benutzerobjekt erstellt (z. B. vom DirXML-Treiber für das HR-System des Unternehmens).
2. Der Abonnentenkanal des Service-Treibers für manuelle Aufgaben sendet eine SMTP-Nachricht an den Manager des Benutzers sowie an dessen Assistenten. Die SMTP-Nachricht enthält Anweisungen für die Dateneingabe im Asset-Management-System.
3. Der Manager oder sein Assistent gibt die Daten im Asset-Management-System ein.
4. (Optional) Die Identifikationsdaten des Computers gelangen über einen DirXML-Treiber für das Asset-Management-System zu eDirectory.

Erstellung von Emails und Webseiten durch den Service-Treiber für manuelle Aufgaben

Emails, HTML-Webseiten und XDS-Dokumente können alle als Dokumente angesehen werden. Der Service-Treiber für manuelle Aufgaben erstellt Dokumente dynamisch, die auf den an den Treiber übermittelten Informationen basieren.

Schablonen sind XML-Dokumente, die häufig verwendete oder feste Teile eines Dokuments enthalten. Zusätzlich enthalten sie Ersetzungs-Token, die angeben, wie die dynamischen oder zu ersetzenden Teile des endgültig zusammengestellten Dokuments angeordnet werden.

Sowohl der Abonnenten- als auch der Herausgeberkanal des Service-Treibers für manuelle Aufgaben erstellen Dokumente anhand von Schablonen. Der Abonnentenkanal erstellt Emails und der Herausgeberkanal erstellt Webseiten und XDS-Dokumente.

Der dynamische Teil eines Dokuments wird über Ersetzungsdaten zur Verfügung gestellt. Ersetzungsdaten auf dem Abonnentenkanal werden von den Abonnentenkanalrichtlinien (z. B. von der Befehlstransformationsrichtlinie) zur Verfügung gestellt. Ersetzungsdaten auf dem Herausgeberkanal werden dem Webserver in Form von HTTP-Daten zur Verfügung gestellt (URL-Daten und HTTP POST-Daten). Der Service-Treiber für manuelle Aufgaben kann automatisch bestimmte, dem Service-Treiber für manuelle Aufgaben bekannte Daten (z. B. die Adresse des Webservers) zur Verfügung stellen.

Die Schablonen werden von XSLT-Formatvorlagen verarbeitet. Diese Formatvorlagen sind nicht zu verwechseln mit Formatvorlagen, die in den Abonnenten- oder Herausgeberkanälen als DirXML-Richtlinien verwendet werden.

Die Ersetzungsdaten werden der XSLT-Formatvorlage als Parameter zur Verfügung gestellt. Nach der Verarbeitung der Formatvorlage wird ein XML-, HTML- oder Textdokument ausgegeben, das als Text einer Email, einer Webseite oder einer Übertragung an DirXML auf dem Herausgeberkanal verwendet wird.

Ersetzungsdaten werden anhand einer URL in einer Email vom Abonnentenkanal an den Herausgeberkanal übergeben. Die URL enthält einen Abfrageteil, in dem die Ersetzungsdatenelemente enthalten sind.

Der Service-Treiber für manuelle Aufgaben enthält im Lieferumfang vordefinierte Formatvorlagen, mit denen Schablonen verarbeitet werden können, um Email-, HTML- und XDS-Dokumente zu erstellen. Wenn zusätzliche Verarbeitungsoptionen gewünscht werden, können weitere benutzerdefinierte Formatvorlagen geschrieben werden.

Es ist auch eine erweiterte Methode für die Erstellung von Dokumenten verfügbar, bei der nur eine XSLT-Formatvorlage und Ersetzungsdaten verwendet werden. Bei dieser Methode werden keine Schablonen einbezogen. In diesem Handbuch wird jedoch angenommen, dass die Methode verwendet wird, bei der Schablonen einbezogen werden, da sie einfacher zu konfigurieren ist und ohne XSLT-Programmierkenntnisse verwaltet werden kann.

Schablonen

In diesem Abschnitt werden Schablonen für die Erstellung von Dokumenten beschrieben, wie sie im Service-Treiber für manuelle Aufgaben verwendet werden.

Schablonen sind XML-Dokumente, die von einer Formatvorlage verarbeitet werden, um ein Ausgabedokument zu erzeugen. Das Ausgabedokument kann in den Formaten XML, HTML oder einfacher Text erzeugt werden (bzw. in jedem anderen Format, das mit XSLT erzeugt werden kann).

Mit Schablonen können auf dem Abonnentenkanal Text für Emails und auf dem Herausgeberkanal dynamische Webseiten und XDS-Dokumente erzeugt werden.

Schablonen enthalten Text, Elemente und Ersetzungs-Token. Ersetzungs-Token werden im Ausgabedokument durch die Daten ersetzt, die der Formatvorlage bei der Verarbeitung der Schablone zur Verfügung gestellt werden.

Im Folgenden werden einige Beispiele für Schablonen aufgeführt, die verschiedenen Zwecken dienen. In den Beispielen sind die Ersetzungs-Token die fett gedruckten Strings zwischen zwei $-Zeichen.

Schablonen können auch Aktionselemente enthalten. Aktionselemente sind Steuerelemente, die von der Formatvorlage, die die Schablone verarbeitet, interpretiert werden. Aktionselemente werden in Anhang F, „Service-Treiber für manuelle Aufgaben: Aktionselemente der Schablone“, auf Seite 329 beschrieben. In den folgenden Beispielen werden auch die Aktionselemente fett gedruckt dargestellt.

Die folgende Beispielschablone wird zur Erzeugung eines HTML-Texts für eine Email verwendet:

```
<html xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head></head>
<body>
Dear $manager$,<p/>
<p>
This message is to inform you that your new employee <b>$given-name$
```

```
$surname$</b> has been hired.
<p>
You need to assign a room number for this individual. Click <a
href="$url$">Here</a> to do this.
</p>
<p>
Thank you,<br/>
HR Department
</p>
</body>
</html>
```

Die folgende Beispielschablone wird zur Erzeugung eines einfachen Texts für eine Email verwendet:

```
<form:text xmlns:form="http://www.novell.com/dirxml/manualtask/form">
Dear $manager$,
This message is to inform you that your new employee $given-name$
$surname$ has been hired.
You need to assign a room number for this individual. Use the following
link to do this:$url$
Thank you,
The HR Department</form:text>
```

Das Element <form:text> ist erforderlich, da Schablonen XML-Dokumente sein müssen. Das Element <form:text> wird bei der Schablonenverarbeitung entfernt.

Die folgende Schablone wird zur Erzeugung eines HTML-Formulars verwendet, das als Webseite zur Dateneingabe verwendet wird.

```
<html  xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head>
<title>Enter room number for $subject-name$</title>
</head>
<body>
    <link href="novdocmain.css" rel="style sheet" type="text/css"/>
    <br/><br/><br/><br/>
    <form class="myform" METHOD="POST" ACTION="$url-base$/
process_template.xsl">
        <table cellpadding="5" cellspacing="10" border="1"
align="center">
          <tr><td>
          <input TYPE="hidden" name="template" value="post_form.xml"/>
          <input TYPE="hidden" name="subject-name" value="$subject-
name$"/>
          <input TYPE="hidden" name="association"
value="$association$"/>
          <input TYPE="hidden" name="response-style sheet"
value="process_template.xsl"/>
          <input TYPE="hidden" name="response-template"
value="post_response.xml"/>
          <input TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"/>
```

```
          <input TYPE="hidden" name="auth-template"
value="auth_response.xml"/>
        <input TYPE="hidden" name="protected-data" value="$protected-
data$"/>
          You are:<br/>          <form:if-single-item name="responder-
dn">
           <input TYPE="hidden" name="responder-dn" value="$responder-
dn$"/>
            $responder-dn$          </form:if-single-item>
<form:if-multiple-items name="responder-dn">            <form:menu
name="responder-dn"/>          </form:if-multiple-items>
        </td></tr>
        <tr><td>
          Enter your password: <br/>
<input name="password" TYPE="password" SIZE="20" MAXLENGTH="40"/>
        </td></tr>
        <tr><td>
          Enter room number for $subject-name$:<br/>
          <input TYPE="text" NAME="room-number" SIZE="20"
MAXLENGTH="20" value="$query:roomNumber$"/>
        </td></tr>
        <tr><td>
          <input TYPE="submit" value="Submit"/> <input TYPE="reset"
value="Clear"/>
        </td></tr>
      </table>
    </form>
  </body>
</html>
```

Die folgende Schablone wird für die Erzeugung eines XDS-Dokuments verwendet:

```
<nds>
  <input>
    <modify class-name="User" src-dn="not-applicable">
      <association>$association$</association>
      <modify-attr attr-name="roomNumber">
        <remove-all-values/>
        <add-value>
          <value>$room-number$</value>
        </add-value>
      </modify-attr>
    </modify>
  </input>
</nds>
```

Ersetzungs-Token

Bei den von $-Zeichen umschlossenen Elementen in den Beispielen handelt es sich um Ersetzungs-Token. Beispielsweise wird das Token $manager$ durch den Namen des Managers ersetzt.

Ersetzungs-Token können entweder in Text- oder in XML-Attributwerten angezeigt werden (siehe im ersten Beispiel den href-Wert innerhalb des Elements <a>).

Ersetzungsdaten

Ersetzungsdaten bestehen aus Strings, die anstelle der Ersetzungs-Token im Ausgabedokument, das aus einer Schablone erzeugt wird, angezeigt werden. Ersetzungsdaten werden entweder von Daten des Abonnentenkanals, HTTP-Daten des Herausgeberkanals oder automatisch vom Treiber zur Verfügung gestellt. Ein zusätzlicher Ersetzungsdatentyp wird von eDirectory über den Identity Manager abgerufen (Abfragedaten). Ersetzungsdaten werden in Anhang D, „Service-Treiber für manuelle Aufgaben: Ersetzungsdaten“, auf Seite 319 genauer beschrieben.

Abonnentenkanaldaten: Es gibt zwei Typen von Ersetzungsdaten für den Abonnentenkanal. Der erste Typ besteht aus den Ersetzungswerten, die in Schablonen zur Email-Erstellung für die Ersetzungs-Token eingesetzt werden. Der zweite Typ wird im Abfrageteil einer URL verwendet, sodass die Daten auf dem Herausgeberkanal verwendet werden können, wenn die URL an den Webserver des Herausgeberkanals übertragen wird.

HTTP-Daten: Ersetzungsdaten werden dem Webserver des Herausgeberkanals in Form von URL-Query-Zeichenkettendaten, HTTP POST-Daten oder beidem zur Verfügung gestellt.

Automatische Daten: Der Service-Treiber für manuelle Aufgaben stellt automatische Daten zur Verfügung. Automatische Datenelemente werden in Anhang E, „Service-Treiber für manuelle Aufgaben: Automatische Ersetzungsdatenelemente“, auf Seite 327 beschrieben.

Abfragedaten: Ersetzungs-Token, die mit „query:“ beginnen, werden als Anforderung aktueller Daten von eDirectory angesehen. Der Teil des Tokens nach „query:“ ist der Name eines eDirectory-Objektattributs. Das abzufragende Objekt wird durch einen der Ersetzungsdatenelemente `association`, `src-dn` oder `src-entry-id` festgelegt. Die Elemente werden in genau dieser Reihenfolge berücksichtigt.

Aktionselemente der Schablone

Aktionselemente sind Namespace-qualifizierte Elemente in der Schablone, die zur einfachen Logiksteuerung oder zur Erstellung von HTML-Elementen für HTML-Formulare verwendet werden. Der zur Qualifizierung der Elemente verwendete Namespace ist http://www.novell.com/dirxml/manualtask/form. In diesem Dokument und in den im Lieferumfang des Service-Treibers für manuelle Aufgaben enthaltenen Beispielschablonen wird das Präfix „form“ verwendet.

Die fett gedruckten Elemente in den Beispielen oben sind Aktionselemente.

Aktionselemente werden ausführlich in Anhang F, „Service-Treiber für manuelle Aufgaben: Aktionselemente der Schablone“, auf Seite 329 beschrieben.

Abonnentenkanal-Emails

Der Abonnentenkanal des Service-Treibers für manuelle Aufgaben ermöglicht den Versand von Emails. Hierzu unterstützt der Treiber ein benutzerdefiniertes XML-Element namens <mail>. Richtlinien auf dem Abonnentenkanal erstellen als Reaktion auf einige eDirectory-Ereignisse (z. B. bei der Erstellung eines Benutzers) ein <mail>-Element. Beispiel für ein <mail>-Element:

```
<mail src-dn="\PERIN-TAO\novell\Provo\Joe">
  <to>JStanley@novell.com</to>
  <cc>carol@novell.com</cc>
  <reply-to>HR@novell.com</reply-to>
  <subject>Room Assignment Needed for: Joe the Intern</subject>
  <message mime-type="text/html">
```

```
    <stylesheet>process_template.xsl</stylesheet>
    <template>html_msg_template.xml</template>
    <replacement-data>
      <item name="manager">JStanley</item>
      <item name="given-name">Joe</item>
      <item name="surname">The Intern</item>
      <url-data>
        <item name="file">process_template.xsl</item>
        <url-query>
          <item name="template">form_template.xml</item>
          <item name="responder-dn" protect="yes">\PERIN-TAO\big-
org\phb</item>
          <item name="responder-dn" protect="yes">\PERIN-TAO\big-
org\carol</item>
          <item name="subject-name">Joe The Intern</item>
        </url-query>
      </url-data>
    </replacement-data>
    <resource cid="css-1">novdocmain.css</resource>
  </message>
  <message mime-type="text/plain">
    <stylesheet>process_text_template.xsl</stylesheet>
    <template>txt_msg_template.xml</template>
    <replacement-data>
      <item name="manager">JStanley</item>
      <item name="given-name">Joe</item>
      <item name="surname">The Intern</item>
      <url-data>
          <item name="file">process_template.xsl</item>
          <url-query>
            <item name="template">form_template.xml</item>
            <item name="responder-dn" protect="yes">\PERIN-TAO\big-
org\phb</item>
            <item name="responder-dn" protect="yes">\PERIN-TAO\big-
org\carol</item>
            <item name="subject-name">Joe The Intern</item>
          </url-query>
        </url-data>
      </replacement-data>
    </message>
  <attachment>HR.gif</attachment>
</mail>
```

Der Abonnentenkanal des Service-Treibers für manuelle Aufgaben verwendet die im <mail>-Element enthaltenen Informationen für die Erstellung einer SMTP-Email. Eine URL kann erstellt und in die Email eingefügt werden, über die der Empfänger die Email beantworten kann. Die URL kann auf den Webserver des Herausgeberkanals oder auf einen beliebigen anderen Webserver verweisen.

Das <mail>-Element und dessen Inhalt werden ausführlich in Anhang G, „Service-Treiber für manuelle Aufgaben: <mail>-Element“, auf Seite 333 beschrieben.

Webserver des Herausgeberkanals

Auf dem Herausgeberkanal des Service-Treibers für manuelle Aufgaben wird ein Webserver ausgeführt, der so konfiguriert ist, dass Benutzer über ihn Daten in eDirectory eingeben können. Der Webserver ist darauf ausgerichtet, mit Emails zu arbeiten, die vom Abonnentenkanal des Service-Treibers für manuelle Aufgaben gesendet werden.

Der Webserver des Herausgeberkanals kann statische Dateien und dynamischen Inhalt verarbeiten. Beispiele für statische Dateien sind u. a. Formatvorlagen und Bilder im .css-Format. Beispiel für dynamischen Inhalt sind Webseiten, die sich basierend auf den in der URL oder HHTP POST-Daten enthaltenen Ersetzungsdaten ändern.

Der Webserver des Herausgeberkanals ist in der Regel so konfiguriert, dass ein Benutzer als Antwort auf eine Email, die vom Abonnentenkanal gesendet wurde, Daten in eDirectory eingeben kann. Eine typische Benutzerinteraktion mit dem Webserver läuft wie folgt ab:

1. Der Benutzer sendet die URL aus der Email über einen Webbrowser an den Webserver. Die URL gibt die Formatvorlage, die Schablone und die Ersetzungsdaten an, die für die Erstellung einer dynamischen Webseite (die üblicherweise ein HTML-Formular enthält) verwendet werden.
2. Der Webserver erstellt eine HTML-Seite, indem er die Schablone mit der Formatvorlage und den Ersetzungsdaten verarbeitet. Die HTML-Seite wird an den Webbrowser des Benutzers als die Ressource zurückgegeben, auf die sich die URL bezieht.
3. Im Browser wird die HTML-Seite angezeigt und der Benutzer gibt die angeforderten Informationen ein.
4. Der Browser sendet eine HTTP POST-Anforderung, die die eingegebenen Informationen und andere Informationen erhält, die von der URL in der Email stammen. Der DN des Benutzers, der die Email beantwortet, und das Benutzerpasswort müssen in den POST-Daten enthalten sein.
5. Der Webserver authentifiziert den Benutzer über dessen DN und das Passwort. Wenn bei der Authentifizierung ein Fehler auftritt, wird als Ergebnis der POST-Anforderung eine Webseite mit einer Fehlermeldung zurückgegeben. Die Fehlermeldung kann über eine in den POST-Daten angegebene Formatvorlage und eine Schablone erstellt werden. Bei erfolgreicher Authentifizierung wird die Verarbeitung fortgesetzt.
6. Der Webserver erstellt mit der in den POST-Daten angegebenen Formatvorlage und Schablone ein XDS-Dokument. Das XDS-Dokument wird auf dem Herausgeberkanal an Identity Manager gesendet.
7. Das Ergebnis der Übertragung des XDS-Dokuments wird zusammen mit der in den POST-Daten angegebenen Formatvorlage und Schablone zur Erstellung einer Webseite verwendet, die dem Benutzer das Ergebnis der Datenübertragung anzeigt. Diese Webseite wird als Ergebnis der POST-Anforderung an den Browser gesendet.

8.2.3 Konfiguration

In diesem Abschnitt wird die Konfiguration der Parameter und Schablonen des Service-Treibers für manuelle Aufgaben beschrieben.

Treibereinstellungen

In diesem Abschnitt werden die Parameter beschrieben, die im Abschnitt „Treibereinstellungen“ in der Benutzeroberfläche des Treiberobjekts angezeigt werden.

Viele dieser Parameter betreffen eigentlich den Webserver des Herausgeberkanals. Sie werden im Bereich für die Treibereinstellungen angezeigt, weil auch der Abonnentenkanal des Service-Treibers für manuelle Aufgaben Zugriff auf sie benötigt.

DN der Dokumentenbasis

Dieser Parameter ist ein eDirectory-DN eines Containerobjekts. Der Service-Treiber für manuelle Aufgaben kann XML-Dokumente (einschließlich XSLT-Formatvorlagen) sowohl von eDirectory als auch von der Festplatte laden. Wenn XML-Dokumente von eDirectory geladen werden sollen, gibt dieser Parameter den Stammcontainer an, aus dem die Dokumente geladen werden.

Von eDirectory geladene Dokumente befinden sich im Attributwert eines eDirectory-Objekts. Wenn nicht explizit angegeben, ist dieses Attribut „XmlData“. Das Attribut kann angegeben werden, indem ein #-Zeichen gefolgt vom Attributnamen an den Namen des Objekts angefügt wird, das das Dokument enthält.

Angenommen, der DN der Dokumentenbasis lautet „novell\Manuelle Aufgaben“ und unter „Manuelle Aufgaben“ befindet sich ein Container namens „Schablonen“.

Wenn sich im Verzeichnis „Schablonen“ ein DirXML-Formatvorlagenobjekt namens „Email_Schablone“ befindet, können folgende Ressourcenkennungen verwendet werden, um auf das XML-Dokument zu verweisen: „Schablonen/Email_Schablone“ oder „Schablonen/Email_Schablone#XmlData“.

Die Ressourcenkennungen können als Ersetzungsdaten, URL-Daten oder HTTP POST-Daten zur Verfügung gestellt werden. Möglicherweise erscheint folgendes Element unterhalb eines Elements vom Typ <message> auf dem Abonnentenkanal:

```
<template>templates/e-mail _template#XmlData</template>
```

Dokumentverzeichnis

Dieser Parameter identifiziert ein Dateisystemverzeichnis, das als Basisverzeichnis für die Auffindung von Ressourcen wie Schablonen, XSLT-Formatvorlagen und anderen Dateiressourcen verwendet wird, die vom Webserver des Herausgeberkanals verarbeitet werden. Beispielwerte:

Windows	c:\Novell\Nds\mt_files
NetWare	SYS:\SYSTEM\mt_files
UNIX	/usr/lib/dirxml/rules/manualtask/mt_files

HTTP-Server verwenden (wahr|falsch)

Dieser Parameter gibt an, ob auf dem Herausgeberkanal ein Webserver ausgeführt werden soll oder nicht. Setzen Sie den Parameter auf „wahr“, wenn der Webserver ausgeführt werden soll, oder auf „falsch“, wenn der Webserver nicht ausgeführt werden soll.

Wenn der Service-Treiber für manuelle Aufgaben nur für das Versenden von Emails ohne Antwort-URL oder mit einer URL verwendet wird, die auf eine andere Anwendung verweist, sollte der HTTP-Server nicht ausgeführt werden, um Systemressourcen zu sparen.

HTTP-IP-Adresse oder -Hostname

Mithilfe dieses Parameters können Sie angeben, welche der lokalen IP-Adressen der Webserver des Herausgeberkanals für die Überwachung von HTTP-Anforderungen verwenden soll.

Wird der Parameter „HTTP-IP-Adresse oder -Hostname“ leer gelassen, überwacht der Webserver des Herausgeberkanals die Standard-IP-Adresse. Dies ist ausreichend für Server mit einer einzelnen IP-Adresse. Bei der Angabe einer IP-Adresse in Punktnotation als Wert für den Parameter überwacht der Webserver des Herausgeberkanals die angegebene Adresse auf HTTP-Anforderungen.

Beachten Sie, dass der für den Parameter „HTTP-IP-Adresse oder -Hostname“ angegebene Wert von der Email-Behandlungsroutine des Abonnentenkanals für die Erstellung von URLs verwendet wird, wenn der Hostname oder die Adresse nicht im Mail-Befehlselement angegeben ist. Wenn der Parameter „HTTP-Server verwenden (wahr|falsch)“ auf „falsch“ gesetzt ist, kann der Parameter „HTTP-IP-Adresse oder -Hostname“ für die Angabe der Adresse oder des Namens eines Webservers verwendet werden, der bei der Erstellung von URLs für Emails verwendet wird.

HTTP-Port

Dieser Parameter ist ein Ganzzahlwert, der angibt, welchen TCP-Port der Webserver des Herausgeberkanals auf eingehende Anforderungen überwachen soll. Wenn für diesen Parameter kein Wert angegeben ist, wird standardmäßig die Portnummer 80 oder 443 überwacht. Dies hängt davon ab, ob SSL für die Webserver-Verbindungen verwendet wird oder nicht.

Wenn der Service-Treiber für manuelle Aufgaben auf dem Identity Manager-Server ausgeführt wird (d. h., er wird nicht unter dem Remote Loader auf einem Remote-Computer ausgeführt), sollte der HTTP-Port nicht auf 80 oder 443 eingestellt werden, da in der Regel iMonitor oder ein anderer Prozess die Ports 80 und 443 verwendet.

Name des KMO

Wenn dieser Parameter nicht leer ist, enthält er den Namen eines eDirectory-Schlüsselmaterialobjekts (Key Material Object, KMO), das das Serverzertifikat und den Schlüssel enthält, die vom Webserver des Herausgeberkanals für SSL verwendet werden.

Wenn dieser Parameter angegeben wird, verwendet der Webserver des Herausgeberkanals SSL für die Verarbeitung von HTTP-Anforderungen.

Dieser Parameter hat Vorrang vor anderen Java*-Keystore-Parametern (siehe unten).

Aus Sicherheitsgründen wird die Verwendung von SSL empfohlen, weil eDirectory-Passwörter bei Verwendung des Webservers des Herausgeberkanals in HTTP POST-Daten übergeben werden.

Name der Keystore-Datei

Dieser Parameter wird zusammen mit „Keystore-Passwort“, „Name des Zertifikats (Schlüsselalias)“ und „Zertifikatspasswort (Schlüsselpasswort)“ für die Angabe einer Java-Keystore-Datei verwendet, die ein Zertifikat und einen Schlüssel enthält, die vom Webserver des Herausgeberkanals für SSL verwendet werden.

Wenn dieser Parameter angegeben wird, verwendet der Webserver des Herausgeberkanals SSL für die Verarbeitung von HTTP-Anforderungen.

Wenn der Parameter „Name des KMO“ einen Wert enthält, werden dieser und ihm zugeordnete Parameter ignoriert.

Aus Sicherheitsgründen wird die Verwendung von SSL empfohlen, weil eDirectory-Passwörter bei Verwendung des Webservers des Herausgeberkanals in HTTP POST-Daten übergeben werden.

Keystore-Passwort

Mit diesem Parameter wird das Passwort für die Java-Keystore-Datei festgelegt, die durch den Parameter „Name der Keystore-Datei“ festgelegt ist.

Name des Zertifikats (Schlüsselalias)

Mit diesem Parameter wird der Name des Zertifikats festgelegt, das in der Java-Keystore-Datei verwendet werden soll, die durch den Parameter „Name der Keystore-Datei“ festgelegt ist.

Zertifikatspasswort (Schlüsselpasswort)

Mit diesem Parameter wird das Passwort für das Zertifikat festgelegt, das durch den Parameter „Name des Zertifikats (Schlüsselalias)“ festgelegt ist.

Abonnenteneinstellungen

In diesem Abschnitt werden die Einstellungen für den Abonnentenkanal beschrieben.

SMTP-Server

Mit diesem Parameter wird der Name des SMTP-Servers festgelegt, den der Abonnentenkanal zum Versenden von Emails verwendet.

SMTP-Kontoname

Wenn für den durch die SMTP-Server-Parameter festgelegten SMTP-Server eine Authentifizierung erforderlich ist, gibt dieser Parameter den für die Authentifizierung zu verwendenden Kontonamen an. Das verwendete Passwort ist das Anwendungspasswort, das den Parametern der Treiberauthentifizierung zugeordnet ist.

Standardmäßige Absenderadresse

Wenn dieser Parameter angegeben wird, besteht er aus der Email-Adresse, die vom Abonnentenkanal als SMTP-Absenderadresse verwendet wird. Wenn dieser Parameter nicht angegeben wird, müssen die <mail>-Elemente, die an den Abonnentenkanal gesendet werden, ein <from>-Element enthalten.

Ein <from>-Element, das unter <mail>-Elementen an den Abonnentenkanal gesendet wird, hat Vorrang vor diesem Parameter.

Zusätzliche Behandlungsroutinen

Wenn dieser Parameter angegeben wird, besteht er aus einer durch Whitespaces getrennten Liste mit Java-Klassennamen. Jeder Klassenname ist eine benutzerdefinierte Klasse, die die Schnittstelle „com.novell.nds.dirxml.driver.manualtask.CommandHandler“ implementiert und ein

benutzerdefiniertes XDS-Element verarbeitet. (Bei der Behandlungsroutine für <mail> handelt es sich um eine integrierte Behandlungsroutine).

Weitere Informationen zu benutzerdefinierten Behandlungsroutinen finden Sie in Anhang I, „Service-Treiber für manuelle Aufgaben: Benutzerdefinierte Element-Behandlungsroutinen auf dem Abonnentenkanal“, auf Seite 351.

Herausgebereinstellungen

In diesem Abschnitt werden die Einstellungen für den Herausgeberkanal beschrieben.

Zusätzliche Servlets

Wenn dieser Parameter angegeben wird, besteht er aus einer durch Whitespaces getrennten Liste mit Java-Klassennamen. Jeder Klassenname ist eine benutzerdefinierte Klasse, die „javax.servlet.http.HttpServer“ erweitert. Benutzerdefinierte Servlets können zur Erweiterung der Funktionalität des Webservers des Herausgeberkanals verwendet werden.

Weitere Informationen zu benutzerdefinierten Servlets finden Sie in Anhang J, „Service-Treiber für manuelle Aufgaben: Benutzerdefinierte Servlets für den Herausgeberkanal“, auf Seite 355.

Abonnentenkanalrichtlinien

Die Konfiguration der Abonnentenkanalrichtlinien hängt davon ab, welchen Zweck eine bestimmte Installation mit dem Service-Treiber für manuelle Aufgaben erfüllen möchte. Es gibt jedoch bestimmte Richtlinien, die von Nutzen sein können.

In der Regel ist die Befehlstransformationsrichtlinie der beste Ort zum Erstellen eines <mail>-Elements, das an den Abonnentenkanal gesendet wird. Die Ursache hierfür ist, dass der Hauptteil der DirXML-Engine-Verarbeitung bereits abgeschlossen ist, wenn Befehle die Befehlstransformationsrichtlinie erreichen. Dies bedeutet, dass die Erstellungsrichtlinien für Add-Ereignisse verarbeitet wurden (wodurch das Einlegen von Vetos für Add-Ereignisse von Objekten ermöglicht wird, die z. B. nicht über alle für die Erstellung einer Email erforderlichen Attribute verfügen). Dies bedeutet auch, dass Modify-Ereignisse für Objekte ohne Verknüpfungen bereits in Add-Ereignisse konvertiert wurden.

Die XSLT-Formatvorlage, die die Email erstellt, fragt eDirectory möglicherweise nach weiteren Informationen ab.

Wenn es sich bei der Email beispielsweise um eine einfache Begrüßungsnachricht an einen neuen Mitarbeiter handelt, enthält der Add-Befehl möglicherweise alle erforderlichen Informationen: Vorname, Nachname und die Internet-Email-Adresse. Dies ist dann der Fall, wenn in der Erstellungsrichtlinie angegeben ist, dass Vorname, Nachname und Internet-Email-Adresse zu den obligatorischen Attributen gehören. Dadurch wird sichergestellt, dass nur Add-Befehle mit den erforderlichen Informationen die Befehlstransformation erreichen können.

Handelt es sich bei der Email jedoch um eine Nachricht an den Manager eines Mitarbeiters, muss die Formatvorlage eDirectory abfragen. Der DN des Managers kann vom Add-Ereignis des Benutzerobjekts des Mitarbeiters zur Verfügung gestellt werden. Die Email-Adresse des Managers muss jedoch abgefragt werden, da diese Information ein Attribut des Benutzerobjekts des Managers ist.

Falls als Ergebnis von Modify-Befehlen für dem Treiber zugeordnete Objekte Email-Benachrichtigungen erzeugt werden, müssen Abfragen für Optionen erstellt werden, die nicht im Modify-Befehl enthalten sind.

Senden von Befehlen an den Abonnentenkanal blockieren

Wenn Emails von anderen Ereignissen als Add-Ereignissen erzeugt werden sollen, muss zugelassen werden, dass Add-Ereignisse für diese zu überwachenden Objekte den Abonnentenkanal erreichen können. Wenn zugelassen wird, dass Add-Ereignisse den Abonnentenkanal erreichen, hat dies die Erzeugung eines Verknüpfungswerts zur Folge, der vom Abonnentenkanal an Identity Manager zurückgegeben wird.

Es ist wichtig, dass für eDirectory-Objekte, die von den Richtlinien des Service-Treibers für manuelle Aufgaben überwacht werden sollen, eine Verknüpfung zum Service-Treiber für manuelle Aufgaben besteht. Nur für Objekte mit einer definierten Verknüpfung werden Ereignisse zum Löschen, Umbenennen und Verschieben an den Treiber weitergeleitet. Darüber hinaus werden Modify-Ereignisse für Objekte ohne eine Verknüpfung nach der Ereignistransformation des Abonnentenkanals in Add-Ereignisse konvertiert.

Alle anderen Befehle (zum Ändern, Verschieben, Umbenennen und Löschen) sollten von der Befehlstransformationsrichtlinie blockiert werden, um zu verhindern, dass sie den Abonnentenkanal erreichen. Der Abonnentenkanal verarbeitet nur <Add>- und <mail>-Befehle. Bei anderen Befehlen gibt der Abonnentenkanal eine Fehlermeldung zurück.

Erzeugen von Emails

Emails werden vom Abonnentenkanal als Antwort auf den Erhalt eines <mail>-Elements gesendet, das die zu sendende Email beschreibt. In Anhang G, „Service-Treiber für manuelle Aufgaben: <mail>-Element“, auf Seite 333 finden Sie eine Beschreibung des <mail>-Elements und dessen Inhalts.

Emails können als Antwort auf ein beliebiges Identity Manager-Ereignis (Hinzufügen, Bearbeiten, Umbenennen, Verschieben, Löschen) erzeugt werden.

Die Ersetzungsdaten, die mit den einem <mail>-Element untergeordneten <message>-Elementen zur Verfügung gestellt werden, hängen von zwei Hauptfaktoren ab:

- Der Schablone, die zur Erzeugung des Nachrichtentext verwendet wurde. Ersetzungselemente, die von der Email-Schablone verwendet werden sollen, werden als untergeordnete Elemente des <replacement-data>-Elements angezeigt.
- Den von den Webseiten-Schablonen auf dem Herausgeberkanal benötigten Informationen, wenn die Email eine Antwort auf dem Herausgeberkanal zur Folge haben soll. Ersetzungselemente, die von den Webseiten-Schablonen verwendet werden sollen, werden als untergeordnete Elemente des <url-query>-Elements angezeigt, das ein untergeordnetes Element von <url-data> ist. Dieses wiederum ist dem <replacement-data>-Element untergeordnet.

Wenn die Email eine URL enthalten soll, die auf den Webserver des Herausgeberkanals verweist und zum Einholen von Informationen von einem Benutzer verwendet wird, müssen die Ersetzungsdaten mindestens ein responder-dn-Element enthalten. Die Werte der responder-dn-Elemente müssen die DNs der Benutzerobjekte der Benutzer sein, an die die Nachricht gesendet wird.

Wenn ein Abfrage-Ersetzungs-Token (siehe Abschnitt , „Ersetzungsdaten“, auf Seite 229) in der Schablone verwendet wird, müssen die Ersetzungsdaten für das <message>-Element ein Element namens „src-dn“ oder „src-entry-id“ oder eine Verknüpfung zum entsprechenden Wert enthalten. Ein Verknüpfungselement kann nur verwendet werden, wenn das abzufragende eDirectory-Objekt bereits über eine Verknüpfung zum Service-Treiber für manuelle Aufgaben verfügt. Die vom Abonnentenkanal für nicht verknüpfte Objekte erzeugte Verknüpfung kann nicht verwendet werden, weil sie zum Zeitpunkt der Abfrage noch nicht in das eDirectory-Objekt geschrieben wurde.

Das <message>-Element kann den MIME-Typ des Nachrichtentexts angeben. Wenn zwar der MIME-Typ, aber keine Formatvorlage angegeben ist (d. h., es ist kein untergeordnetes <stylesheet>-Element von <message> vorhanden), wird einer der zwei Standard-Formatvorlagennamen verwendet. Wenn der MIME-Typ einfacher Text ist, lautet der Standardname der Formatvorlage „process_text_template.xsl“. Bei einem anderen MIME-Typ lautet der Standardname der Formatvorlage „process_template.xsl“.

Email-Schablonen des Abonnentenkanals

Email-Schablonen sind XML-Dokumente, die häufig verwendeten Text und Ersetzungs-Token enthalten. Email-Schablonen werden zur Erzeugung des Texts einer Email verwendet. Allgemeine Informationen zu Schablonen finden Sie in Abschnitt , „Schablonen“, auf Seite 226.

Die in einer Email-Schablone verwendeten Ersetzungs-Token geben die <item>-Elemente vor, die als untergeordnete Elemente des <replacement-data>-Elements zur Verfügung gestellt werden müssen, das von der Abonnentenkanalrichtlinie erstellt wurde, die das <mail>-Element erstellt. Wenn z. B. die Email-Schablone über das Ersetzungs-Token $employee-name$ verfügt, muss ein <item name=“employee-name”>-Element in den Ersetzungsdaten für das <message>-Element vorhanden sein. Wenn das Element mit dem Mitarbeiternamen nicht vorhanden ist, enthält der Nachrichtentext der Email an der Stelle, die das Ersetzungs-Token in der Schablone einnimmt, keinen Text.

Email-Schablonen können zur Generierung von Nachrichtentexten im Format „einfacher Text“, HTML oder XML verwendet werden.

Wenn eine Email-Schablone eine Nachricht mit einfachem, unformatiertem Text generiert, muss diese von einer Formatvorlage verarbeitet werden, in der als Ausgabetyp „einfacher Text“ angegeben ist. Wenn in der Formatvorlage nicht einfacher Text als Ausgabetyp angegeben ist, tritt unerwünschtes XML-Escaping auf. Die Standard-Formatvorlage des Service-Treibers für manuelle Aufgaben, process_text_template.xsl, wird in der Regel zum Verarbeiten von Schablonen verwendet, die ein Ergebnis in einfachem Text ergeben.

Herausgeberkanalrichtlinien

Bei den meisten Implementierungen des Service-Treibers für manuelle Aufgaben sind keine Herausgeberkanalrichtlinien erforderlich. Dies liegt daran, dass die Webseite und die XDS-Schablonen so erstellt werden können, dass sie genau die erforderliche XDS ergeben und nicht mehr anhand der Richtlinien weiterverarbeitet werden müssen.

Wenn Richtlinien erforderlich sind, sind diese sehr genau auf eine Installation zugeschnitten.

Webseitenschablonen des Herausgeberkanals

Webseitenschablonen sind XML-Dokumente, die häufig verwendeten Text und Ersetzungs-Token enthalten. Webseitenschablonen werden zur Generierung von Webseitendokumenten verwendet (in

der Regel HTML-Dokumente). Allgemeine Informationen zu Schablonen finden Sie in Abschnitt , „Schablonen“, auf Seite 226.

Ersetzungs-Token in Webseitenschablonen geben vor, welche Ersetzungsdaten als URL-Abfragedaten auf dem Abonnentenkanal zur Verfügung gestellt werden. Ersetzungsdaten auf dem Herausgeberkanal werden für HTTP GET-Anforderungen von der URL-Query-Zeichenkette und für HTTP POST-Anforderungen von der URL-Query-Zeichenkette und den POST-Daten zur Verfügung gestellt.

Folgendes Szenario ist ein Beispiel für den Fluss der Ersetzungsdaten vom Abonnentenkanal zur Email und anschließend zum Herausgeberkanal.

Der Service-Treiber für manuelle Aufgaben ist so konfiguriert, dass der Manager eines neuen Mitarbeiters aufgefordert wird, dem neuen Mitarbeiter eine Raumnummer zuzuweisen. Der Auslöser für die Email an den Manager ist der <add>-Befehl für ein neues Benutzerobjekt, der von der Befehlstransformationsrichtlinie des Abonnentenkanals verarbeitet wird.

Wenn der Manager in der Email auf die URL klickt, wird eine Webseite im Webbrowser des Managers angezeigt. Die Webseite muss anzeigen, wem der Manager eine Raumnummer zuweist.

Diese Anforderung wird durch das <url-query>-Element auf dem Abonnentenkanal erfüllt, das ein Ersetzungsdatenelement mit dem Namen des neuen Benutzers enthält:

```
<item name=”subject-name”>Joe the Intern</item>
```

Dadurch enthält die URL-Query-Zeichenkette (neben anderen Angaben) “subject-name=Daniel%20ein%20Praktikant”. (Das Zeichen “%20” ist ein URL-kodiertes Leerzeichen).

Wenn der Manager auf die URL in der Email klickt, sendet der Webbrowser des Managers die URL an den Webserver des Herausgeberkanals. Der Webserver erstellt ein Ersetzungsdatenelement namens „subject-name“ mit dem Wert „Daniel ein Praktikant“.

Die ebenfalls durch die URL angegebene Webseitenschablone enthält ein Ersetzungs-Token namens $subject-name$. Wenn die Webseitenschablone von der Formatvorlage verarbeitet wird, um die Webseite zu erstellen, wird das Ersetzungs-Token durch „Daniel ein Praktikant“ ersetzt. Auf diese Weise wird die Webseite an den Mitarbeiter angepasst, dessen Erstellung des Benutzerobjekts das Versenden der Email ausgelöst hat.

Weitere Informationen zu einer ausführlichen Transaktion vom Abonnentenkanal zum Herausgeberkanal finden Sie in Anhang H, „Service-Treiber für manuelle Aufgaben: Datenfluss-Szenario bei Einstellung eines neuen Mitarbeiters“, auf Seite 337.

XDS-Schablonen des Herausgeberkanals

XDS-Schablonen sind XML-Dokumente, die häufig verwendeten Text und Ersetzungs-Token enthalten. XDS-Schablonen werden zur Generierung von XDS-Dokumenten verwendet, die auf dem Herausgeberkanal des Service-Treibers für manuelle Aufgaben an Identity Manager gesendet werden. Allgemeine Informationen zu Schablonen finden Sie im Abschnitt „Überblick“.

Ersetzungs-Token in XDS-Schablonen geben einige Ersetzungsdaten vor, die dem Webserver in Form von Daten in einer HTTP POST-Anforderung zur Verfügung gestellt werden.

Im Folgenden finden Sie ein Beispiel für eine XDS-Schablone:

```
<nds>
  <input>
    <modify class-name="User" src-dn="not-applicable">
      <association>$association$</association>
      <modify-attr attr-name="roomNumber">
        <remove-all-values/>
        <add-value>
          <value>$room-number$</value>
        </add-value>
      </modify-attr>
    </modify>
  </input>
</nds>
```

Die Ersetzungs-Token in der Schablone schreiben vor, dass die HTTP POST-Daten einen Wert für „association“ und „room-number“ zur Verfügung stellen müssen.

In der Regel hat der Wert „association“ seinen Ursprung im Abonnentenkanal. Die Email des Abonnentenkanals würde „association=beliebiger Wert“ in die Query-Zeichenkette der URL platzieren, die in der Email enthalten ist. Die Webseitenschablone, die zur Erzeugung der Webseite verwendet wird, wenn die URL an den Webserver gesendet wird, platziert den Wert „association“ in der Regel in einem versteckten INPUT-Element:

```
<INPUT TYPE="hidden" NAME="association" VALUE="$association$"/>
```

Durch die Platzierung des Werts „association“ als verstecktes INPUT-Element wird das Paar “association=beliebiger Wert” als Teil der HTTP POST-Daten gesendet.

Der Wert „room-number“ wird mithilfe eines INPUT-Elements in die Webseite eingefügt. Dieses Element ist ähnlich wie im folgenden Beispiel:

```
<input TYPE="text" NAME="room-number" SIZE="20" MAXLENGTH="20"/>
```

Wenn der Manager „1234“ eingibt und auf „Senden“ klickt, sendet der Webbrowser „room-number=1234“ als Teil der HTTP POST-Daten.

Anschließend generiert der Webserver ein <item name=“association”>- und ein <item name=“room-number”>-Ersetzungsdatenelement, die bei der Verarbeitung der XDS-Schablone verwendet werden.

Das XDS-Dokument wird durch die Verarbeitung der in den POST-Daten angegebenen XDS-Schablone generiert. Anschließend wird das XDS-Dokument über den Herausgeberkanal des Service-Treibers für manuelle Aufgaben an Identity Manager gesendet.

Trace-Einstellungen

Der Service-Treiber für manuelle Aufgaben gibt Meldungen mit verschiedenen Trace-Stufen aus:

Stufe	Beschreibung der Trace-Meldung
0	Keine Trace-Meldungen

Stufe	Beschreibung der Trace-Meldung
1	Einzeilige Meldungen, die allgemeine Vorgänge protokollieren
2	Keine zusätzlichen Meldungen (DirXML-Engine führt das Tracing für XML-Dokumente auf dieser Stufe und den darüber liegenden Stufen durch)
3	Keine zusätzlichen Meldungen
4	Meldungen im Zusammenhang mit der Dokumenterstellung von Schablonen und Formatvorlagen
5	Dokumente mit Ersetzungsdaten unterliegen dem Tracing

8.2.4 Weitere Informationen

Weitere Informationen zu Einstellungen für den Service-Treiber für manuelle Aufgaben finden Sie in:

- Anhang D, „Service-Treiber für manuelle Aufgaben: Ersetzungsdaten“, auf Seite 319
- Anhang E, „Service-Treiber für manuelle Aufgaben: Automatische Ersetzungsdatenelemente“, auf Seite 327
- Anhang F, „Service-Treiber für manuelle Aufgaben: Aktionselemente der Schablone“, auf Seite 329
- Anhang G, „Service-Treiber für manuelle Aufgaben: <mail>-Element“, auf Seite 333
- Anhang H, „Service-Treiber für manuelle Aufgaben: Datenfluss-Szenario bei Einstellung eines neuen Mitarbeiters“, auf Seite 337
- Anhang I, „Service-Treiber für manuelle Aufgaben: Benutzerdefinierte Element-Behandlungsroutinen auf dem Abonnentenkanal“, auf Seite 351
- Anhang J, „Service-Treiber für manuelle Aufgaben: Benutzerdefinierte Servlets für den Herausgeberkanal“, auf Seite 355

Hochverfügbarkeit

9

Sie können Identity Manager mit gemeinsamer Speichernutzung verwenden, um Hochverfügbarkeit zu gewährleisten. Für die Verwendung von Novell® eDirectory™ und Identity Manager in einer Clusterumgebung sind einige Schritte erforderlich.

Dieser Abschnitt umfasst:

9.1 Konfiguration von eDirectory und Identity Manager zur Verwendung mit der gemeinsamen Speichernutzung unter Linux und UNIX

In diesem Abschnitt wird die Konfiguration von eDirectory und Identity Manager für das Failover in einem Hochverfügbarkeits-Cluster mit gemeinsamer Speichernutzung beschrieben. Dieser Abschnitt enthält allgemeine Informationen zu Hochverfügbarkeits-Clustern mit gemeinsamer Speichernutzung auf einer beliebigen Linux- oder UNIX-Plattform. Die Informationen sind auf keinen speziellen Cluster-Manager zugeschnitten.

Das zugrunde liegende Basiskonzept sieht vor, dass die Zustandsdaten für eDirectory und Identity Manager sich im gemeinsam genutzten Speicher befinden müssen, damit sie für den Clusterknoten verfügbar sind, der zurzeit die Services ausführt. In der Praxis bedeutet dies, dass die eDirectory-Datenablage, die sich in der Regel unter „/var/nds/dib“ befindet, in den gemeinsam genutzten Speicher des Clusters verschoben werden muss. Auch die Statusdaten von Identity Manager befinden sich unter „/var/nds/dib“. Jede eDirectory-Instanz auf den Clusterknoten muss so konfiguriert sein, dass sie die Datenablage des gemeinsamen Speichers verwendet. Auch müssen sich im gemeinsamen Speicher weitere eDirectory-Konfigurationsdaten befinden.

Neben der eDirectory-Datenablage müssen auch die NICI-Daten (Novell International Cryptographic Infrastructure) gemeinsam genutzt werden, damit serverspezifische Schlüssel zwischen den Clusterknoten reproduziert werden. In der Regel empfiehlt es sich, die NICI-Daten nicht in den gemeinsamen Speicher zu verschieben, sondern auf jeden Clusterknoten in den lokalen Speicher zu kopieren. Diese Vorgehensweise ist vorzuziehen, damit die Client-NICI-Funktionalität auf einem Clusterknoten auch dann zur Verfügung steht, wenn sich der Clusterknoten in einem sekundären Zustand befindet und nicht den gemeinsam genutzten Speicher hostet.

In den folgenden Abschnitten wird auf die gemeinsame Nutzung von eDirectory- und NICI-Daten eingegangen. Folgende Bedingungen werden vorausgesetzt:

- Sie verwenden für die Daten und die Konfiguration von NICI, eDirectory und Identity Manager die Standard-Installationsverzeichnisse.

  Die Identity Manager-Daten werden nicht getrennt von eDirectory-Daten behandelt, weil sich die relevanten Identity Manager- und eDirectory-Daten am gleichen Ort befinden.
- Sie sind mit dem Installationsvorgang von eDirectory und Identity Manager vertraut.
- Sie verwenden ein Cluster mit zwei Knoten.

Ein Cluster mit zwei Knoten ist die am weitesten verbreitete Konfiguration, die für Hochverfügbarkeit verwendet wird. Die in diesem Abschnitt beschriebenen Konzepte können jedoch leicht zu einem Cluster mit *n* Knoten erweitert werden.

Dieser Abschnitt umfasst:

9.1.1 Installation von eDirectory

Hinweis: NICI wird als Teil des eDirectory-Installationsvorgangs installiert.

1. Installieren Sie eDirectory auf dem primären Clusterknoten.
2. Konfigurieren Sie eDirectory auf dem primären Clusterknoten. Erstellen Sie auf dem primären Clusterknoten einen neuen Baum oder installieren Sie den Server in einem vorhandenen Baum. Benennen Sie den eDirectory-Server, verwenden Sie hierzu aber nicht den Namen des UNIX-Servers. Verwenden Sie anstelle eines Namens, der für einen Clusterknoten geeignet ist, einen allgemeinen Namen für das Cluster.
3. Installieren Sie auf dem sekundären Clusterknoten dieselbe Version von eDirectory. Konfigurieren Sie eDirectory nicht auf dem sekundären Clusterknoten.

   Der sekundäre Knoten verfügt nicht über einen separaten Baum.

9.1.2 Installation von Identity Manager

1. Installieren Sie Identity Manager über die Metaverzeichnis-Server-Option auf dem primären Clusterknoten.

   Der Installationsvorgang installiert die Identity Manager-Dateien und konfiguriert den eDirectory-Baum für die Verwendung mit Identity Manager.
2. Installieren Sie auf dem zweiten Clusterknoten dieselbe Version von Identity Manager. Verwenden Sie hierzu den Schalter für den sekundären Cluster und geben Sie Folgendes ein:

   ```
   dirxml_platform.bin -DCLUSTER_INSTALL="true"
   ```

   Wählen Sie während der Installation die Metaverzeichnis-Server-Option.

   Wenn der Schalter für den sekundären Cluster verwendet wird, werden die Identity Manager-Dateien installiert, ohne dabei den Versuch zu unternehmen, eine zusätzliche Konfiguration von eDirectory vorzunehmen. Eine Konfiguration ist nicht erforderlich, weil der sekundäre Knoten nicht über einen separaten Baum verfügt.

9.1.3 Gemeinsame Nutzung von NICI-Daten

NICI stellt Verschlüsselungsdienste zur Verfügung, die von eDirectory, Identity Manager und Novell-Client-Anwendungen verwendet werden. Wenn NICI in Verbindung mit eDirectory

verwendet wird, stellt NICI serverspezifische Schlüssel zur Verfügung. Diese serverspezifischen Schlüssel müssen auf allen Clusterknoten, auf denen eDirectory als Clusterdienst ausgeführt wird, identisch sein.

Es gibt zwei Möglichkeiten für die Freigabe von NICI-Daten:

- Die NICI-Daten im gemeinsam genutzten Speicher des Clusters ablegen.

  Der Nachteil dieser Methode liegt darin, dass Anwendungen, die auf NICI angewiesen sind, nur dann auf einem Clusterknoten funktionieren, wenn der Knoten auch den gemeinsam genutzten Speicher hostet.
- Die NICI-Daten vom primären Server in den lokalen Speicher des sekundären Servers kopieren.

So kopieren Sie die NICI-Daten:

1. Benennen Sie /var/novell/nici auf dem sekundären Clusterknoten um (z. B. /var/novell/nici.sav).
2. Kopieren Sie das Verzeichnis /var/novell/nici vom primären Clusterknoten auf den sekundären Clusterknoten.

   Sie können hierzu scp verwenden oder eine tar-Datei des /var/novell/nici-Verzeichnisses auf dem primären Knoten erstellen, sie auf den sekundären Knoten übertragen und dort entpacken.

9.1.4 Freigabe von eDirectory- und Identity Manager-Daten

eDirectory speichert seine Datenablage standardmäßig unter /var/nds/dib. Auch andere Konfigurations- und Statuselemente sind unter /var/nds und in den Unterverzeichnissen gespeichert. Das Standard-Konfigurationsverzeichnis für eDirectory ist /etc. Zur Konfiguration von eDirectory und Identity Manager zur Verwendung mit dem gemeinsamen Speicher in einem Hochverfügbarkeits-Cluster sind die im Folgenden beschriebenen Schritte erforderlich. Es wird vorausgesetzt, dass der gemeinsame Speicher unter /shared gemountet ist.

- „Auf dem primären Knoten“ auf Seite 243
- „Auf dem sekundären Knoten“ auf Seite 244

Auf dem primären Knoten

1. Kopieren Sie den Verzeichnis-Teilbaum /var/nds in /shared/var/nds.
2. Benennen Sie das Verzeichnis /var/nds um (z. B. in /var/nds.sav).

   Es wird empfohlen, in diesem Stadium eine Sicherung zu erstellen. Dadurch können Sie, sofern erforderlich, von vorne beginnen, ohne eDirectory neu installieren zu müssen.
3. Erstellen Sie einen symbolischen Link von /var/nds zu /shared/var/nds (z. B. `ln -s /shared/var/nds /var/nds`).
4. Erstellen Sie folgende symbolische Links:

Link von	Link zu
/shared/var/nds/class16.conf	/etc/class16.conf
/shared/var/nds/class32.conf	/etc/class32.conf

Link von	Link zu
/shared/var/nds/help.conf	/etc/help.conf
/shared/var/nds/ndsimonhealth.conf	/etc/ndsimonhealth.conf
/shared/var/nds/miscicon.conf	/etc/miscicon.conf
/shared/var/nds/ndsimon.conf	/etc/ndsimon.conf
/shared/var/nds/macaddr	/etc/macaddr

5. Erstellen Sie eine Sicherungskopie von /etc/nds.conf.
6. Verschieben Sie /etc/nds.conf in /shared/var/nds.
7. Bearbeiten Sie /shared/var/nds/nds.conf und fügen Sie der Datei folgende Einträge hinzu (überschreiben Sie dabei die aktuellen Einträge für diese Pfadeinstellungen):
   - n4u.nds.dibdir=/shared/var/nds/dib
   - n4u.server.configdir=/shared/var/nds
   - n4u.server.vardir=/shared/var/nds
   - n4u.nds.preferred-server=localhost

   Ersetzen Sie in den folgenden Einträgen „eth0:0“ durch den Schnittstellennamen der vom Cluster gemeinsam genutzten Ethernet-Schnittstelle. Ersetzen Sie des Weiteren „lo“ durch den Schnittstellennamen der localhost-Ethernet-Schnittstelle.
   - n4u.nds.server.interfaces=eth0:0@524,lo@524
   - http.server.interfaces=eth0:0@8008,lo@8008
   - https.server.interfaces=eth0:0@8009,lo@8009
8. Erstellen Sie einen symbolischen Link von /etc/nds.conf zu /shared/var/nds/nds.conf.
9. Starten Sie „ndsd“ und stellen Sie sicher, dass „ndsd“ auf der Basis des gemeinsam genutzten Speichers ausgeführt wird.
10. Halten Sie „ndsd“ an.
11. Platzieren Sie „ndsd“ in der Liste der zu hostenden Ressourcen des Cluster-Managers.
12. Entfernen Sie „ndsd“ aus der Liste der Daemons, die vom Initialisierungsvorgang beim Booten gestartet werden.

Auf dem sekundären Knoten

1. Benennen Sie das Verzeichnis /var/nds um (z. B. in /var/nds.sav). Eine Umbenennung ist nicht zwingend erforderlich, aber wenn Sie Sicherungen erstellen, können Sie an einem Punkt nach der Installation von eDirectory neu beginnen.
2. Erstellen Sie einen symbolischen Link von /var/nds zu /shared/var/nds.
3. Erstellen Sie eine Sicherungskopie von /etc/nds.conf.
4. Entfernen Sie /etc/nds.conf.
5. Erstellen Sie einen symbolischen Link von /etc/nds.conf zu /shared/var/nds/nds.conf.
6. Platzieren Sie „ndsd“ in der Liste der zu hostenden Ressourcen des Cluster-Managers.
7. Entfernen Sie „ndsd“ aus der Liste der Daemons, die vom Initialisierungsvorgang beim Booten gestartet werden.

Wenn die Schritte für den primären und den sekundären Knoten abgeschlossen sind, starten Sie die Clusterdienste. eDirectory und Identity Manager werden nun auf dem primären Knoten ausgeführt.

9.1.5 Aspekte hinsichtlich des Identity Manager-Treibers

Die meisten Identity Manager-Treiber können in einer Clusterkonfiguration ausgeführt werden. Die folgenden Aspekte müssen jedoch beachtet werden:

- Auf jedem Clusterknoten müssen die Programmdateien des Treibers (.jar-Dateien und/oder freigegebene Objekte) installiert sein.
- Wenn der Treiber auf demselben Server ausgeführt werden muss wie die Anwendung, die der Treiber unterstützt, muss auch die Anwendung so konfiguriert werden, dass sie als Teil der Clusterdienste ausgeführt wird.
- Wenn der Treiber über einen konfigurierbaren Ablageort für treiberspezifische Zustandsdaten verfügt, muss sich dieser Ablageort im gemeinsam genutzten Speicher des Clusters befinden.

  Ein Beispiel hierfür ist der LDAP-Treiber bei der Verwendung ohne ein Änderungsprotokoll oder der JDBC-Treiber bei der Verwendung im auslöserfreien Modus.
- Wenn Konfigurationsdaten des Treibers außerhalb von eDirectory gespeichert sind, müssen sich die Konfigurationsdaten im gemeinsam genutzten Speicher befinden oder auf jeden Clusterknoten dupliziert werden. Ein Beispiel hierfür sind die Verzeichnisse für die Schablonen des Treibers für manuelle Aufgaben.

9.2 Fallstudie für SuSE Linux

Eine Beschreibung für die Ausführung von Identity Manager mit einem gemeinsam genutzten Speicher und SuSE LINUX Enterprise Server 8 finden Sie in TID10093317 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm).

Protokollierung und Berichterstellung mit Novell Audit

10

Identity Manager kann mit Novell® Audit zur Revision und Berichterstellung verwendet werden.

10.1 Überblick

Novell Audit besteht aus mehreren Modulen, die Funktionen zum Überwachen, zur Protokollierung, zur Berichterstellung und zur Benachrichtigung zur Verfügung stellen. Durch die Integration mit Novell Audit bietet Identity Manager detaillierte Informationen zum aktuellen und vergangenen Status der Treiber- und Engine-Aktivitäten. Diese Informationen werden von mehreren vorkonfigurierten Berichten, Standard-Benachrichtigungsservices und benutzerdefinierten Datenprotokollierungen zur Verfügung gestellt.

Sie können Identity Manager-Ereignisse in Echtzeit überwachen, E-Mail-Benachrichtigungen für ein beliebiges Identity Manager-Ereignis versenden und mit Novell Audit Berichte der Identity Manager-Aktivität generieren.

Die an Novell Audit gesendeten Meldungstypen werden über Plugins gesteuert, die denen des Berichts- und Benachrichtigungsservices (RNS) ähneln. Diesen Plugins werden zusätzliche Stufen hinzugefügt, damit Sie die zu protokollierenden Vorgangs- und Debug-Informationstypen wie „status“, „add entry“ (Eintrag hinzufügen) und „search“ (Suchen) auswählen können.

Berichts- und Benachrichtigungsservice

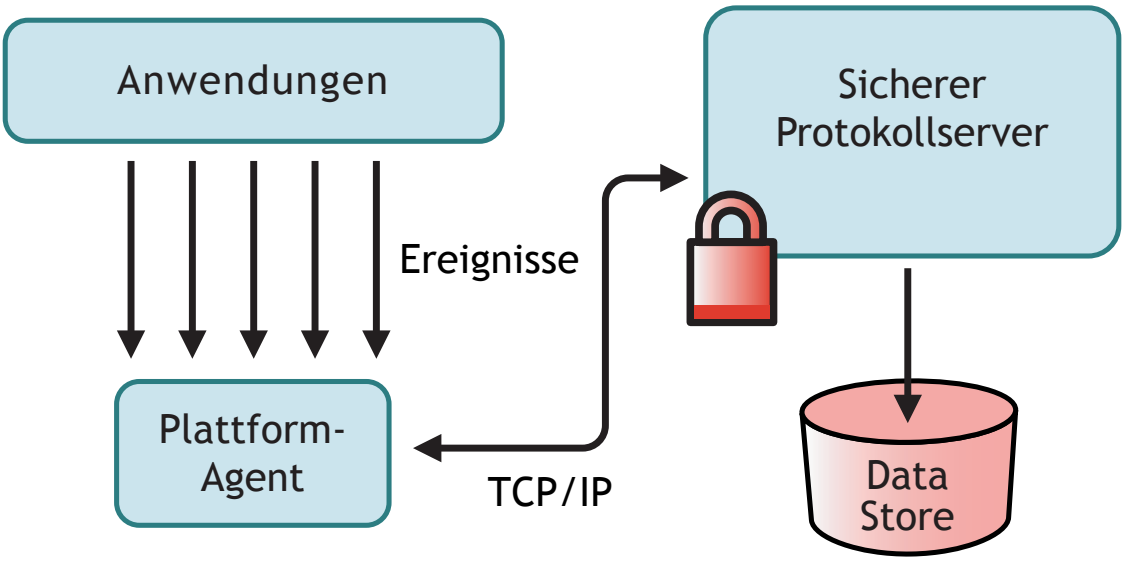
Der Berichts- und Benachrichtigungsservice (RNS) ist veraltet, auch wenn die Metaverzeichnis-Engine weiterhin RNS-Funktionen verarbeitet, wenn Sie RNS verwenden. Es wird ein Wechsel zu Novell Audit empfohlen, weil Novell Audit die von RNS zur Verfügung gestellte Funktionalität erweitert. Außerdem wird RNS in einer zukünftigen Version von Identity Manager möglicherweise nicht mehr unterstützt. Eine RNS-Dokumentation finden Sie im *DirXML 1.1a-Administration Guide* (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html) (DirXML 1.1a Administrationshandbuch).

10.2 Novell Audit

Novell Audit ist ein zentralisierter, plattformübergreifender Protokollservice, der Protokolldaten von mehreren Anwendungen in einem zentralen Datenspeicher speichern kann. Nach der Protokollierung von Ereignisdaten können Sie basierend auf den protokollierten Ereignissen Benachrichtigungen auslösen und detaillierte Berichte und benutzerdefinierte Abfragen ausführen.

Die folgende Abbildung bietet eine Übersicht über die Architektur von Novell Audit:

Abbildung 10-1 *Übersicht über die Architektur*



In dieser Abbildung ist Identity Manager eine der Anwendungen, die den Platform Agent (Plattformagent) verwenden, um dem Novell Audit Secure Logging Server (sicherer Protokollserver) Ereignisse zu melden.

10.3 Einrichten von Novell Audit

Wie im Überblick beschrieben, besteht Novell Audit aus zwei Hauptkomponenten:

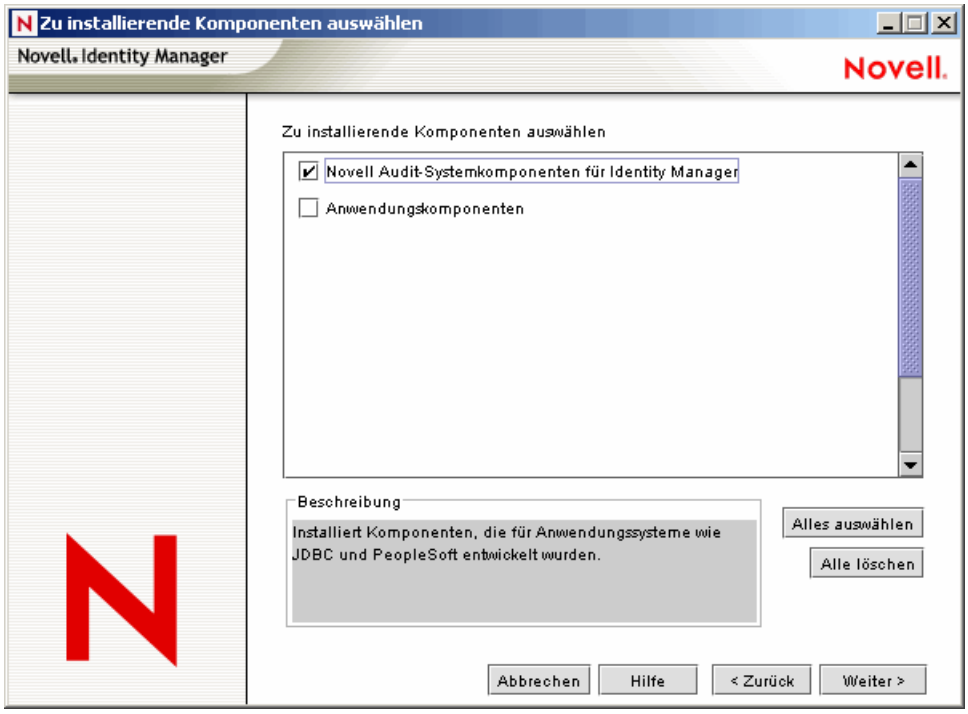
- Plattformagent
- Sicherer Protokollserver

Der Plattformagent ist die Komponente, die mit Identity Manager ausgeführt wird, um Ereignisse an den sicheren Protokollserver zu kommunizieren. Die Komponente wird zusammen mit Identity Manager installiert. Der sichere Protokollserver ist die Komponente, die Ereignisdaten von Identity Manager und anderen Anwendungen empfängt. Sie wird separat von Identity Manager als Teil von Novell Audit 1.0.3. installiert.

10.3.1 Einrichten des Plattformagenten

Der Plattformagent wird installiert, indem Sie während der Installation die Novell Audit-Systemkomponenten für Identity Manager auswählen.

Abbildung 10-2 *Installation von Identity Manager*



Der Plattformagent kann während der Installation von Identity Manager oder zu einem späteren Zeitpunkt installiert werden.

Hinweis: Wenn Sie den Plattformagenten nach dem Start der Metaverzeichnis-Engine installieren, muss Identity Manager neu gestartet werden, bevor eine Verbindung zwischen dem Plattformagenten und Identity Manager hergestellt wird. Identity Manager versucht nur beim Start, eine Verbindung zum Plattformagenten herzustellen.

Konfigurieren Sie den Plattformagenten nach der Installation und führen Sie hierzu folgende Schritte aus:

1. Öffnen Sie die Novell Audit-Konfigurationsdatei (`logevent.cfg`) in einem Texteditor. Der Standard-Ablageort für diese Datei ist:

Betriebssystem	Pfad
NetWare®	`sys:\etc\logevent.cfg`
Windows	*`windows_directory`*`\logevent.cfg`
Linux\Solaris	`/etc/logevent.conf`

2. Geben Sie als Wert des LogHost-Parameters die IP-Adresse oder den DNS-Namen Ihres sicheren Protokollservers an.

3 Starten Sie Identity Manager neu.

10.3.2 Einrichten des sicheren Protokollservers

Hinweis: Der Novell Audit Secure Logging Server ist nicht im Lieferumfang von Identity Manager enthalten. Der sichere Protokollserver ist Teil von Novell Audit 1.0.3. Weitere Informationen zum Herunterladen von Novell Audit 1.0.3 finden Sie auf der Produktseite von Novell Audit (http://www.novell.com/products/nsureaudit).

Der sichere Protokollserver kann auf NetWare 5.1 oder höher, Windows* NT 4.0, Windows 2000 Server, Windows 2003 Server, Solaris* 8 oder 9 und verschiedenen Versionen von Linux*, einschließlich SuSE® Enterprise Linux Server 8 und SuSE 9.0, ausgeführt werden.

Der sichere Protokollserver kann Ereignisse in MySQL*, Oracle*, Microsoft* SQL Server, Java*-Anwendungen und verschiedenen anderen Ablageorten, einschließlich eines Flatfiles, protokollieren. Novell Audit umfasst eine eigene Anwendung, Novell Audit Report, für die Abfrage von Datenbanken nach Ereignisdaten. Zur Verwendung dieses Werkzeugs für die erweiterte Berichterstellung ist eine Datenablage mit einer ODBC-Schnittstelle erforderlich.

Für jede Plattform ist eine Kurzanleitung mit Installationsanweisungen für den sicheren Protokollserver verfügbar, die in Novell Audit 1.0.3 enthalten ist. Die Kurzanleitungen und der *Novell Audit 1.0.3 Administration Guide* (Novell Audit 1.0.3 Administrationshandbuch) können auch im Internet auf der Website zur Audit Novell-Dokumentation (http://www.novell.com/documentation/nsureaudit) angezeigt werden.

10.4 Konfiguration der Protokollierung

In Identity Manager können Sie die zu protokollierenden Ereignisse konfigurieren, indem Sie mehrere vordefinierte Stufen verwenden oder jedes zu protokollierende Ereignis einzeln auswählen. Auch Änderungen an den Konfigurationseinstellungen werden protokolliert.

Benutzerdefinierte Ereignisse, die in Abschnitt 10.4.2, „Benutzerdefinierte Ereignisse“, auf Seite 256 erläutert sind, werden bei aktivierter Protokollierung immer protokolliert und nie von der Metaverzeichnis-Engine gefiltert.

Die Protokollierung wird für einen Treibersatz oder für einen einzelnen Treiber konfiguriert. Treiber können die Konfiguration der Protokollierung vom Treibersatz erben. Weitere Informationen zu den eDirectory™-Attributen, die Protokolldaten enthalten, finden Sie in Abschnitt 10.4.3, „eDirectory-Objekte“, auf Seite 258.

In der Standardeinstellung werden nur kritische und benutzerdefinierte Ereignisse protokolliert.

10.4.1 Auswahl der zu protokollierenden Ereignisse

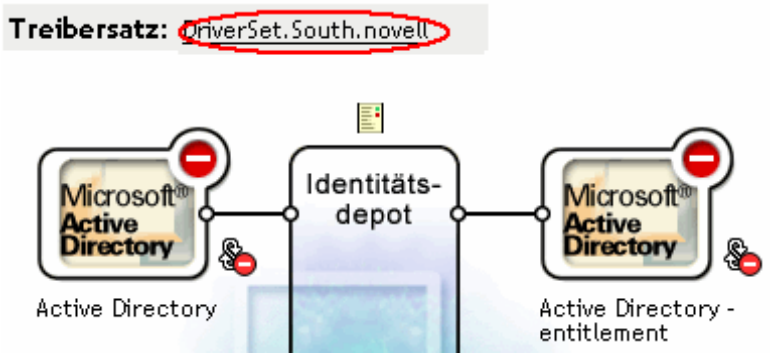
Sie können Ereignisse für einen Treibersatz oder für einen bestimmten Treiber auswählen.

Protokollierung von Ereignissen für den Treibersatz:

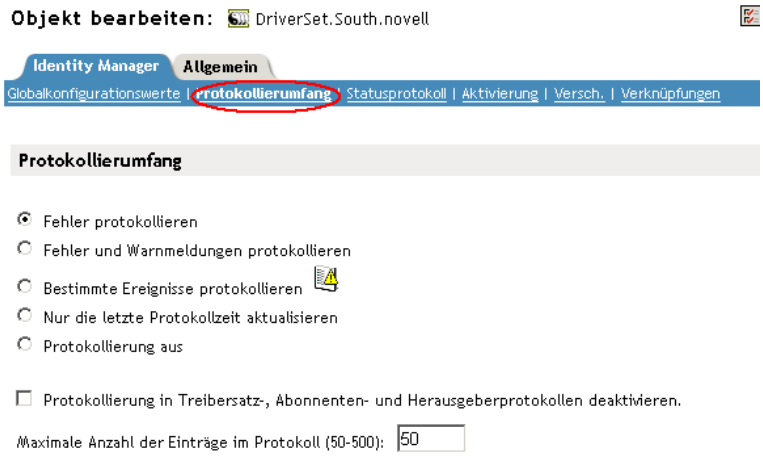
1 Wählen Sie in iManager *Identity Manager* > *Identity Manager-Überblick* und klicken Sie auf *Weiter*.

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

3 Klicken Sie auf den Namen des Treibersatzes. Die Seite „Objekt bearbeiten“ wird angezeigt.



4 Wählen Sie *Protokollierumfang* auf der Registerkarte *Identity Manager*.



5 Wählen Sie die passende Protokollierungsoption für Ihre Umgebung.

Option	Beschreibung
Fehler protokollieren	Dies ist der Standard-Protokollierumfang. Mit dieser Option werden alle Ereignisse mit dem Status „Error“ (Fehler) sowie benutzerdefinierte Ereignisse protokolliert. Wenn diese Option ausgewählt ist, empfangen Sie nur Ereignisse mit der Dezimal-ID 196646, bei denen im ersten Textfeld eine Fehlermeldung gespeichert ist.
Fehler und Warnmeldungen protokollieren	Durch diese Option werden alle Ereignisse mit dem Status „Error“ (Fehler) oder „Warning“ (Warnmeldung) sowie benutzerdefinierte Ereignisse protokolliert. Wenn diese Option ausgewählt ist, empfangen Sie nur Ereignisse mit den Dezimal-IDs 196646 und 196647, bei denen im ersten Textfeld eine Fehler- oder Warnmeldung gespeichert ist.

Option	Beschreibung
Bestimmte Ereignisse protokollieren	Mit dieser Option können Sie bestimmte zu protokollierende Ereignisse in einer Liste auswählen. Klicken Sie auf das Symbol , um Ereignisse auszuwählen. Benutzerdefinierte Ereignisse werden immer protokolliert. Wenn Sie außer Fehler- oder Warnmeldungen auch andere Ereignisse protokollieren möchten, müssen Sie diese in dieser Liste auswählen. Bei Auswahl dieser Option müssen Sie auch Fehler und Warnhinweise auswählen, wenn Sie diese weiterhin protokollieren möchten. Eine Liste aller verfügbaren Ereignisse finden Sie unter „Identity Manager-Ereignisse“ auf Seite 254.
Nur die letzte Protokollzeit aktualisieren	Es werden nur benutzerdefinierte Ereignisse protokolliert. Wenn ein Ereignis auftritt, wird die letzte Protokollierungszeit aktualisiert, sodass Sie die Uhrzeit und das Datum des letzten Fehlers im Statusprotokoll einsehen können.
Protokollierung aus	Es werden nur benutzerdefinierte Ereignisse protokolliert.
Protokollierung in Treibersatz-, Abonnenten- und Herausgeberprotokollen deaktivieren	Mit dieser Option wird die Protokollierung im Treibersatzobjektprotokoll und in den Abonnenten- und Herausgeberprotokollen deaktiviert.
Maximale Anzahl der Einträge im Protokoll	Mit dieser Einstellung können Sie die maximale Anzahl der Einträge festlegen, die in den Statusprotokollen protokolliert werden sollen. Weitere Informationen finden Sie in Abschnitt 10.7.2, „Anzeigen von Statusprotokollen“, auf Seite 263.

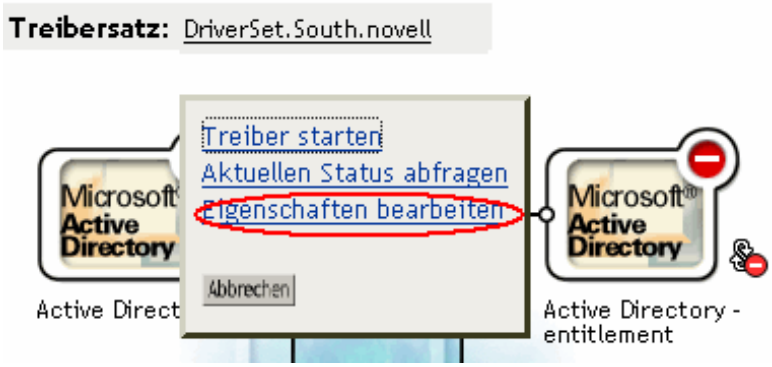
6 Klicken Sie nach Auswahl der zu protokollierenden Ereignisse auf *OK*.

Protokollierung von Ereignissen für den Treiber:

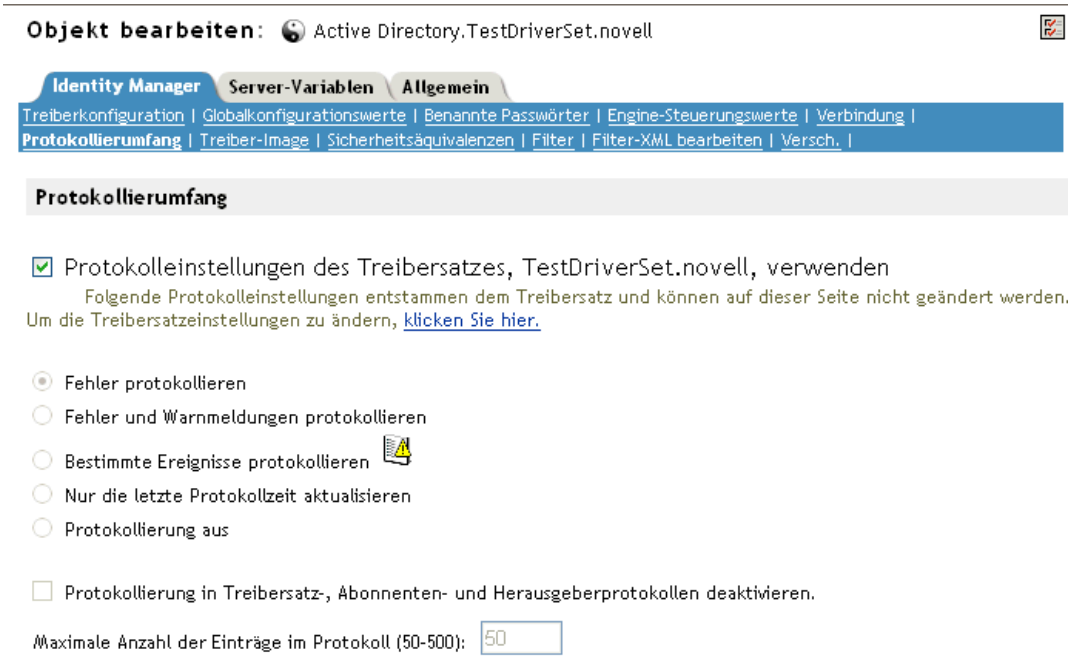
1 Wählen Sie in iManager *Identity Manager* > *Identity Manager-Überblick* und klicken Sie auf *Weiter*.

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

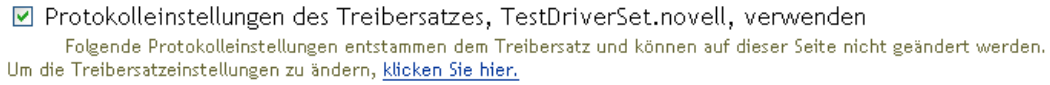
3 Klicken Sie auf die obere rechte Ecke des Treibersymbols und wählen Sie anschließend *Eigenschaften bearbeiten*.



4 Wählen Sie *Protokollierumfang* auf der Registerkarte *Identity Manager*.



5 (Optional) In der Standardeinstellung ist das Treiberobjekt so konfiguriert, dass es die Protokolleinstellungen vom Treibersatzobjekt erbt. Wenn Sie nur protokollierte Ereignisse für diesen Treiber auswählen möchten, deaktivieren Sie die Option „Protokolleinstellungen des Treibersatzes verwenden“.



6 Wählen Sie die passende Protokollierungsoption für Ihre Umgebung.

Option	Beschreibung
Fehler protokollieren	Dies ist der Standard-Protokollierumfang. Mit dieser Option werden alle Ereignisse mit dem Status „Error“ (Fehler) sowie benutzerdefinierte Ereignisse protokolliert. Wenn diese Option ausgewählt ist, empfangen Sie nur Ereignisse mit der Dezimal-ID 196646, bei denen im ersten Textfeld eine Fehlermeldung gespeichert ist.
Fehler und Warnmeldungen protokollieren	Durch diese Option werden alle Ereignisse mit dem Status „Error“ (Fehler) oder „Warning“ (Warnmeldung) sowie benutzerdefinierte Ereignisse protokolliert. Wenn diese Option ausgewählt ist, empfangen Sie nur Ereignisse mit den Dezimal-IDs 196646 und 196647, bei denen im ersten Textfeld eine Fehler- oder Warnmeldung gespeichert ist.

Option	Beschreibung
Bestimmte Ereignisse protokollieren	Mit dieser Option können Sie bestimmte zu protokollierende Ereignisse in einer Liste auswählen. Klicken Sie auf das Symbol  , um Ereignisse auszuwählen. Benutzerdefinierte Ereignisse werden immer protokolliert. Wenn Sie außer Fehler- oder Warnmeldungen auch andere Ereignisse protokollieren möchten, müssen Sie diese in dieser Liste auswählen. Bei Auswahl dieser Option müssen Sie auch Fehler und Warnhinweise auswählen, wenn Sie diese weiterhin protokollieren möchten. Eine Liste aller verfügbaren Ereignisse finden Sie unter „Identity Manager-Ereignisse“ auf Seite 254.
Nur die letzte Protokollzeit aktualisieren	Es werden nur benutzerdefinierte Ereignisse protokolliert. Wenn ein Ereignis auftritt, wird die letzte Protokollierungszeit aktualisiert, sodass Sie die Uhrzeit und das Datum des letzten Fehlers im Statusprotokoll einsehen können.
Protokollierung aus	Es werden nur benutzerdefinierte Ereignisse protokolliert.
Protokollierung in Treibersatz-, Abonnenten- und Herausgeberprotokollen deaktivieren	Mit dieser Option wird die Protokollierung im Treibersatzobjektprotokoll und in den Abonnenten- und Herausgeberprotokollen deaktiviert.
Maximale Anzahl der Einträge im Protokoll	Mit dieser Einstellung können Sie die maximale Anzahl der Einträge festlegen, die in den Statusprotokollen protokolliert werden sollen. Weitere Informationen finden Sie in Abschnitt 10.7.2, „Anzeigen von Statusprotokollen“, auf Seite 263.

7 Klicken Sie nach Auswahl der zu protokollierenden Ereignisse auf *OK*.

Identity Manager-Ereignisse

Eine Liste aller Ereignisse, die von Identity Manager protokolliert werden, finden Sie in Anhang C, „Identity Manager - Ereignisse und Berichte“, auf Seite 289.

Ereignisse beim Starten oder Anhalten des Treibers

Identity Manager kann bei jedem Starten oder Anhalten des Treibers ein Ereignis generieren. Die folgende Tabelle enthält Details zu diesen Ereignissen:

Tabelle 10-1 *Ereignisse beim Starten oder Anhalten des Treibers*

Ereignis	Protokollierumfang	Informationen
EV_LOG_DRIVER_START	LOG_INFO	Wenn Sie die Treiberstarts protokollieren möchten, müssen Sie die Option *Bestimmte Ereignisse protokollieren* verwenden und das entsprechende Ereignis auswählen.

Ereignis	Protokollierumfang	Informationen
EV_LOG_DRIVER_STOP	LOG_WARNING	Wenn Sie protokollieren möchten, wenn ein Treiber angehalten wird, wählen Sie *Fehler und Warnmeldungen protokollieren* oder verwenden Sie die Option *Bestimmte Ereignisse protokollieren* und wählen Sie das entsprechende Ereignis aus.

Weitere Informationen zum Erstellen von Novell Audit-Benachrichtigungen basierend auf diesen Ereignissen finden Sie in Abschnitt 10.6, „Senden von Benachrichtigungen bei Eintritt eines Ereignisses“, auf Seite 260.

Fehler- und Warnereignisse

Identity Manager generiert beim Auftreten eines Fehlers oder eines Warnhinweises ein Ereignis. Die folgende Tabelle enthält Details zu diesen Ereignissen:

Tabelle 10-2 *Fehler- und Warnereignisse*

Ereignis	Protokollierumfang	Informationen
DirXML_Error	LOG_ERROR	Alle Identity Manager-Fehler protokollieren dieses Ereignis. Der aufgefundene Fehlercode wird im Ereignis gespeichert. Wenn Sie Fehler protokollieren möchten, wählen Sie *Fehler protokollieren*, *Fehler und Warnmeldungen protokollieren* oder verwenden Sie die Option *Bestimmte Ereignisse protokollieren* und wählen Sie das entsprechende Ereignis aus.
DirXML_Warning	LOG_WARNING	Alle Identity Manager-Warnhinweise protokollieren dieses Ereignis. Der aufgefundene Code des Warnhinweises wird im Ereignis gespeichert. Wenn Sie Warnhinweise protokollieren möchten, wählen Sie *Fehler und Warnmeldungen protokollieren* oder verwenden Sie die Option *Bestimmte Ereignisse protokollieren* und wählen Sie das entsprechende Ereignis aus.

Weitere Informationen zum Erstellen von Novell Audit-Benachrichtigungen basierend auf diesen Ereignissen finden Sie in Abschnitt 10.6, „Senden von Benachrichtigungen bei Eintritt eines Ereignisses“, auf Seite 260.

Remote Loader-Ereignisse

Folgende Ereignisse werden vom Remote Loader protokolliert:

Tabelle 10-3 *Remote Loader-Ereignisse*

Ereignis	Protokollierumfang	Informationen
Remote Loader Start (Start von Remote Loader)	LOG_INFO	Wenn Sie das Starten des Remote Loader protokollieren möchten, müssen Sie die Option *Bestimmte Ereignisse protokollieren* verwenden und das entsprechende Ereignis auswählen.
Remote Loader Stop (Anhalten des Remote Loader)	LOG_INFO	Wenn Sie das Anhalten des Remote Loader protokollieren möchten, müssen Sie die Option *Bestimmte Ereignisse protokollieren* verwenden und das entsprechende Ereignis auswählen.
Remote Loader Connection Established (Remote Loader-Verbindung hergestellt)	LOG_INFO	Wenn Sie protokollieren möchten, wenn Remote Loader-Verbindungen hergestellt werden, müssen Sie die Option *Bestimmte Ereignisse protokollieren* verwenden und das entsprechende Ereignis auswählen.
Remote Loader Connection Dropped (Remote Loader-Verbindung unterbrochen)	LOG_INFO	Wenn Sie protokollieren möchten, wenn Remote Loader-Verbindungen unterbrochen werden, müssen Sie die Option *Bestimmte Ereignisse protokollieren* verwenden und das entsprechende Ereignis auswählen.

Weitere Informationen zum Erstellen von Novell Audit-Benachrichtigungen basierend auf diesen Ereignissen finden Sie in Abschnitt 10.6, „Senden von Benachrichtigungen bei Eintritt eines Ereignisses“, auf Seite 260.

10.4.2 Benutzerdefinierte Ereignisse

Mit Identity Manager können Sie eigene Ereignisse konfigurieren, die in Novell Audit protokolliert werden sollen. Ereignisse können über eine Aktion im Richtlinien-Builder oder innerhalb einer Formatvorlage protokolliert werden. Alle Informationen, auf die Sie bei der Definition von Richtlinien zugreifen können, können protokolliert werden.

Ereignis-IDs

Die Ereignis-IDs zwischen 1000 und 1999 sind für benutzerdefinierte Ereignisse bestimmt. Geben Sie bei der Definition Ihrer eigenen Ereignisse einen Wert an, der innerhalb dieses Bereichs liegt. In Novell Audit ist diese ID mit der Anwendungs-ID 003 für Identity Manager kombiniert.

Protokollierumfang

Mithilfe des Protokollierumfangs können Sie Ereignisse nach dem protokollierten Ereignistyp gruppieren. Es sind folgende vordefinierte Protokollierumfänge verfügbar:

Tabelle 10-4 *Protokollierumfang*

Protokollierumfang	Beschreibung
Notfallereignisse protokollieren (log-emergency)	Ereignisse, die dazu führen, dass die Metaverzeichnis-Engine oder der Treiber heruntergefahren wird.
Warnmeldungen protokollieren (log-alert)	Ereignisse, die eine sofortige Aufmerksamkeit erfordern.
Kritische Ereignisse protokollieren (log-critical)	Ereignisse, die zu einer Störung von Teilen der Metaverzeichnis-Engine oder des Treibers führen.
Fehler protokollieren (log-error)	Ereignisse, die Fehler beschreiben, die von der Metaverzeichnis-Engine oder dem Treiber behoben werden können.
Warnhinweise protokollieren (log-warning)	Negative Ereignisse, die kein Problem darstellen.
Hinweise protokollieren (log-notice)	Positive oder negative Ereignisse, mit deren Hilfe ein Administrator die Verwendung und den Betrieb verstehen bzw. verbessern kann.
Informationen protokollieren (log-info)	Positive Ereignisse beliebiger Bedeutung.
Fehlersuche protokollieren (log-debug)	Ereignisse, die für den Support oder Techniker relevant sind, um für den Betrieb der Metaverzeichnis-Engine oder des Treibers eine Fehlersuche durchzuführen.

Generieren von Ereignissen mithilfe des Richtlinien-Builders

Im Richtlinien-Builder werden Ereignisse durch Auswahl der Aktion *Ereignis generieren* protokolliert.

1. Wählen Sie vor der Generierung des Ereignisses die einzuhaltende Bedingung aus und wählen Sie die Aktion *Ereignis generieren*.
2. Geben Sie eine Ereignis-ID an.
3. Wählen Sie einen Protokollierumfang.
4. Klicken Sie auf das Symbol neben dem Feld *Zeichenketten eingeben*, um den Benannte-Zeichenkette-Builder zu starten.
5. Verwenden Sie den Benannte-Zeichenkette-Builder zum Erstellen benannter Zeichenketten für die benutzerdefinierten Datenfelder:

6. Klicken Sie auf *OK*, um zum Richtlinien-Builder zurückzukehren und mit der Erstellung Ihrer Richtlinie fortzufahren.

Weitere Informationen zur Konfiguration einer Richtlinie für die Protokollierung von Ereignissen finden Sie unter “Generate Event” im *Policy Builder and Driver Customization Guide* (Handbuch zum Richtlinien-Builder und zur Treiberanpassung).

Generieren von Ereignissen mithilfe von Statusdokumenten

Statusdokumente, die mithilfe von Formatvorlagen unter Verwendung des Elements <xsl:message> generiert wurden, werden an Novell Audit gesendet. Sie enthalten eine Ereignis-ID, die dem Level-Attribut des Statusdokuments entspricht, wie in der folgenden Tabelle angegeben:

Tabelle 10-5 *Statusdokumente*

Status-Level	Status-Ereignis-ID
Success (Ordnungsgemäß durchgeführt)	EV_LOG_STATUS_SUCCESS (1)
Retry (Wiederholen)	EV_LOG_STATUS_RETRY (2)
Warning (Warnhinweis)	EV_LOG_STATUS_WARNING (3)
Error (Fehler)	EV_LOG_STATUS_ERROR (4)
Fatal (Schwerwiegend)	EV_LOG_STATUS_FATAL (5)
Benutzerdefiniert	EV_LOG_STATUS_OTHER (6)

Im folgenden Beispiel wird ein Novell Audit-Ereignis 0x004 und value1=7777 mit der Ebene EV_LOG_STATUS_ERROR generiert:

```
<xsl:message>
   <status level="error" text1="This would be text1" value="7777">This
data would be in the blob and in text 2, since no value is specified
for text2 in the attributes.</status>
</xsl:message>
```

Im folgenden Beispiel wird ein Novell Audit-Ereignis 0x004 und value1=7778 mit der Ebene EV_LOG_STATUS_ERROR generiert:

```
<xsl:message>
   <status level="error" text1="This would be text1" text2="This would
be text2" value1="7778">This data would be in the blob only for this
case, since a value for text2 is specified in the attributes.</status>
</xsl:message>
```

10.4.3 eDirectory-Objekte

Dieser Abschnitt enthält Details zu den Novell eDirectory-Attributen, die Protokolldaten speichern. Es ist nicht notwendig, diese Attribute direkt zu ändern, weil diese Objekte entsprechend Ihrer Auswahl in iManager automatisch konfiguriert werden.

Die Identity Manager-Ereignisse, die Sie protokollieren möchten, sind im DirXML-LogEvent-Attribut des Treibersatzobjekts oder des Treiberobjekts gespeichert. Das Attribut ist eine mehrwertige Ganzzahl. Jeder Wert identifiziert eine zu protokollierende Ereignis-ID.

Vor der Protokollierung eines Ereignisses gleicht die Engine den aktuellen Ereignistyp mit dem Inhalt dieses Attributs ab. Auf diese Weise wird ermittelt, ob ein Ereignis zu protokollieren ist oder nicht.

Bei früheren Versionen von Identity Manager wurde das DirXML-DriverTraceLevel-Attribut zum Einrichten des Protokollierumfangs verwendet. Der Protokollierumfang wurde für jedes Treiberobjekt angegeben, da die Vererbung nicht unterstützt wurde. In den Nachfolgeversionen von Identity Manager 2 können Treiberobjekte diese Informationen vom Treibersatzobjekt erben. Das DirXML-DriverTraceLevel-Attribut eines Treiberobjekts hat bei der Ermittlung der Protokolleinstellungen die höchste Priorität. Wenn ein Treiberobjekt kein DirXML-DriverTraceLevel-Attribut enthält, verwendet die Engine die Protokolleinstellungen des übergeordneten Treibersatzobjekts.

10.5 Abfragen und Berichterstellung

Novell Audit bietet zwei Werkzeuge für Abfragen auf Ereignisse in der Novell Audit-Datenbank: das Novell Audit iManager-Plugin und Novell Audit Report (LReport).

Das Novell Audit iManager-Plugin ist eine webbasierte JDBC-Anwendung für Datenbankabfragen, mit der Sie unter Verwendung von Dropdown-Listen und Makros auf einfache Art Abfragen erstellen und speichern können.

Novell Audit Report ist eine Windows-basierte ODBC-konforme Anwendung, mit der man über SQL-Anweisungen oder über Crystal Decisions Reports Oracle- und MySQL-Datenspeicher abfragen kann (oder jede andere Datenbank, die ODBC-Treiber unterstützt).

Befolgen Sie die Anweisungen im *Novell Audit Administration Guide* (Novell Audit Administrationshandbuch), wenn Sie auf das Novell Audit iManager-Plugin zugreifen oder Novell Audit Report einrichten möchten. Dieses Handbuch ist auf der Novell Audit-Website (http://www.novell.com/documentation/nsureaudit) verfügbar.

10.5.1 Identity Manager-Berichte

Identity Manager enthält eine Reihe von Crystal Decisions Reports (*.rpt), die das Sammeln von Informationen zu den gängigen Operationen in Identity Manager vereinfachen. Diese Berichte befinden sich auf der Installations-CD von Identity Manager.

Nachdem Sie Novell Audit Report konfiguriert haben, können diese Berichte neben den anderen benutzerdefinierten Abfragen und Berichte ausgeführt werden. Unter Working with Reports in Novell Audit Report (http://www.novell.com/documentation/nsureaudit/nsureaudit/data/alsn2fj.html) im *Novell Audit 1.0.3 Administration Guide* (Novell Audit 1.0.3 Administrationshandbuch) finden Sie Informationen darüber, wie diese Berichte in Novell Audit Report eingesetzt werden können. Beispiele dieser Berichte finden Sie in Abschnitt C.11, „Berichte“, auf Seite 310 im Anhang C, „Identity Manager - Ereignisse und Berichte“, auf Seite 289.

10.5.2 Anzeigen von Identity Manager-Ereignissen

1 Klicken Sie im Novell Audit Report-Arbeitsbereich auf die Registerkarte *Events* und erweitern Sie den Ordner *DirXML*.

Diese Liste enthält alle vordefinierten Identity Manager-Ereignisse. Doppelklicken Sie auf ein Ereignis in der Liste, um die Ereigniseigenschaften anzuzeigen.

2. Wenn Sie ein Identity Manager-Ereignis abfragen möchten, klicken Sie im Arbeitsbereich mit der rechten Maustaste auf das Ereignis und wählen Sie *Define Query*.
3. Der Abfrageexperte wird geöffnet. Geben Sie einen Zeitrahmen an und bestätigen Sie das Ereignis.
4. Sie führen die Abfrage aus, indem Sie im Arbeitsbereich die Registerkarte *Query* auswählen, mit der rechten Maustaste auf den Abfragenamen klicken und anschließend *Run* auswählen.

Abfragen können aber mithilfe von SQL-Anweisungen erstellt werden. Alle Identity Manager-Ereignisse haben eine dezimale Ereignis-ID, deren gültige Werte zwischen 109608 und 262144 liegen.

10.6 Senden von Benachrichtigungen bei Eintritt eines Ereignisses

Novell Audit bietet die Möglichkeit, Benachrichtigungen zu senden, wenn ein bestimmtes Ereignis eintritt bzw. nicht eintritt. Benachrichtigungen werden infolge eines Ereignisses oder mehrerer Ereignisse und auf Grund von mit den Ereignissen verbundenen Werten gesendet. Benachrichtigungen können an jeden beliebigen Protokollierungskanal gesendet werden, d. h. Sie können Benachrichtigungen an eine Datenbank, eine Java-Anwendung, ein SNMP-Management-System o. ä senden.

Weitere Informationen zum Erstellen von Benachrichtigungen finden Sie unter "Configuring Filters and Event Notifications" im *Novell Audit 1.0.3 Administration Guide* (http://www.novell.com/documentation/nsureaudit/nsureaudit/data/al0lg08.html#al0lg08) (Novell Audit 1.0.3 Administrationshandbuch).

10.7 Verwenden von Statusprotokollen

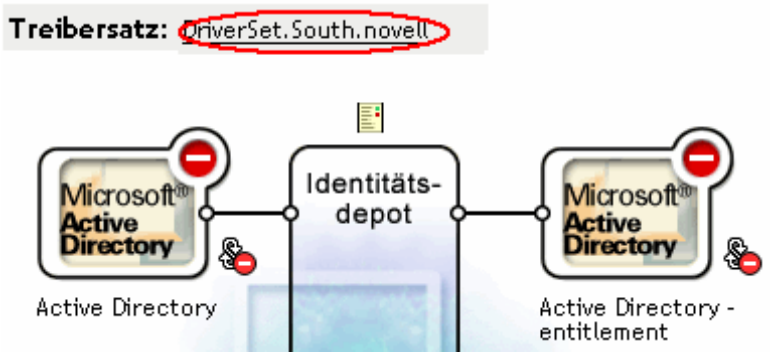
Zusätzlich zu der von Novell Audit bereitgestellten Funktionalität protokolliert Identity Manager eine bestimmte Anzahl von Ereignissen für das Treibersatzobjekt und das Treiberobjekt. Diese Statusprotokolle bieten eine Übersicht über die zuletzt ausgeführten Identity Manager-Aktivitäten. Hat das Protokoll die festgelegte Maximalgröße erreicht, wird die ältere Hälfte des Protokolls entfernt, um Platz zur Protokollierung neuer Ereignisse zu schaffen. Deshalb sollte zur Protokollierung von Ereignissen, die Sie über einen längeren Zeitraum aufbewahren möchten, Novell Audit oder der Berichts- und Benachrichtigungsservice verwendet werden.

10.7.1 Einstellen der maximalen Protokollgröße

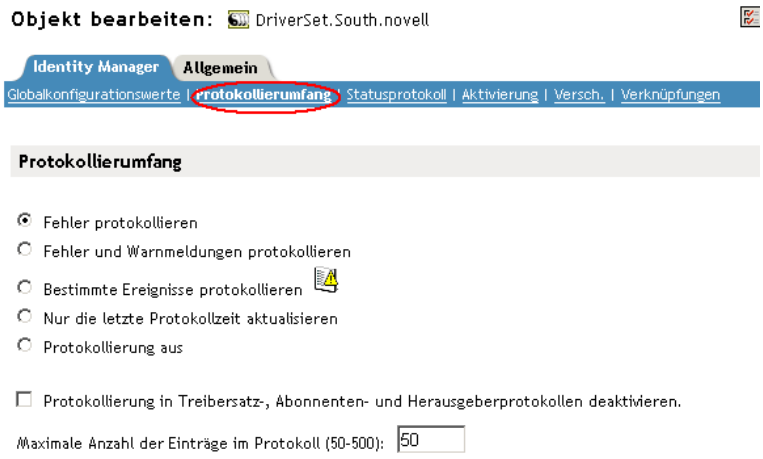
Statusprotokolle können so konfiguriert werden, dass sie zwischen 50 und 500 Ereignisse aufnehmen können. Diese Einstellung kann für das Treibersatzobjekt vorgenommen werden, sodass alle Treiber im Satz dieselbe Einstellung verwenden, oder für jeden Treiber einzeln konfiguriert werden. Es besteht keine Abhängigkeit zwischen der maximalen Protokollgröße und den Ereignissen, die Sie protokollieren möchten. So können Sie beispielsweise die zu protokollierenden Ereignisse auf Treibersatzebene konfigurieren und dann für jeden Treiber im Treibersatz eine individuelle Protokollgröße angeben.

Protokollgröße auf Treibersatzebene definieren

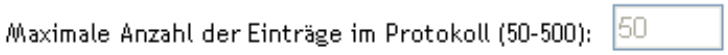
1. Wählen Sie in iManager *Identity Manager* > *Identity Manager-Überblick* und klicken Sie auf *Weiter*.
2. Wählen Sie das Treibersatzobjekt aus und klicken Sie auf *Suchen*.
3. Klicken Sie auf den Namen des Treibersatzes. Die Seite „Objekt bearbeiten“ wird angezeigt.



4. Wählen Sie *Protokollierumfang* auf der Registerkarte *Identity Manager*.



5. Geben Sie die maximale Protokollgröße im Feld *Maximale Anzahl der Einträge im Protokoll* an:

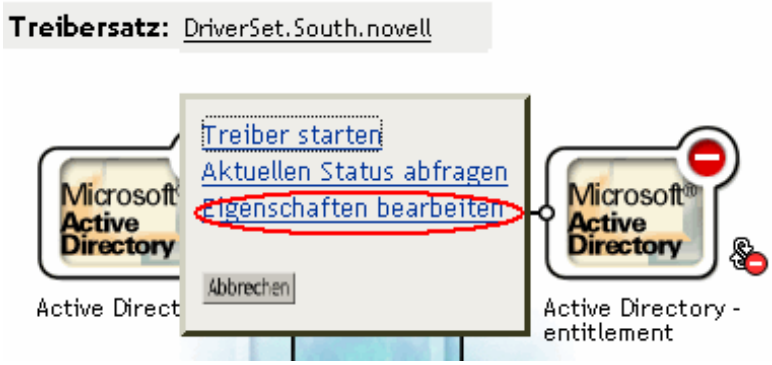


6. Wenn Sie die Einstellung vorgenommen haben, klicken Sie auf *OK*.

Protokollgröße für einen Treiber definieren

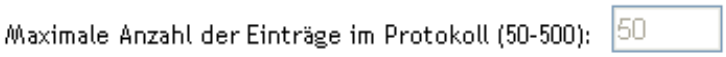
1. Wählen Sie in iManager *Identity Manager* > *Identity Manager-Überblick* und klicken Sie auf *Weiter*.
2. Wählen Sie das Treibersatzobjekt aus und klicken Sie auf *Suchen*.

3 Klicken Sie auf die obere rechte Ecke des Treibersymbols und wählen Sie anschließend *Eigenschaften bearbeiten*.



4 Wählen Sie *Protokollierumfang* auf der Registerkarte *Identity Manager*.

5 Geben Sie die maximale Protokollgröße im Feld *Maximale Anzahl der Einträge im Protokoll* an:



6 Wenn Sie die Einstellung vorgenommen haben, klicken Sie auf *OK*.

10.7.2 Anzeigen von Statusprotokollen

Einträge im Statusprotokoll werden in iManager in Form eines Statusprotokollsymbols  dargestellt. An den Stellen, an denen Sie dieses Symbol in iManager sehen, können Sie ein Kurzzeitprotokoll anzeigen. Folgende Statusprotokolle sind verfügbar:

- Für den Treibersatz.
- Auf dem Herausgeberkanal für jeden Treiber im Satz.
- Auf dem Abonnentenkanal für jeden Treiber im Satz.

Die Statusprotokolle für den Herausgeber- und den Abonnentenkanal protokollieren kanalspezifische Meldungen, die vom Treiber generiert werden, z. B. ein Vorgangsveto für ein nicht verknüpftes Objekt.

Das Statusprotokoll für den Treibersatz enthält nur von der Engine generierte Meldungen, z. B. Statusänderungen für Treiber im Treibersatz. Alle Engine-Meldungen werden protokolliert.

DirXML-Befehlszeilenprogramm

A

Dieses Dienstprogramm und sowie mehrere Skripts werden im Rahmen der Installation von Identity Manager auf allen Plattformen installiert. Das Befehlszeilenprogramm befindet sich in folgenden Speicherorten:

- Windows: `\Novell\Nds\dxcmd.bat`
- NetWare: `sys:\system\dxcmd.ncf`
- UNIX: `/usr/bin/dxcmd`

Das DirXML-Befehlszeilenprogramm kann auf zwei Arten verwendet werden.

A.1 Interaktiver Modus

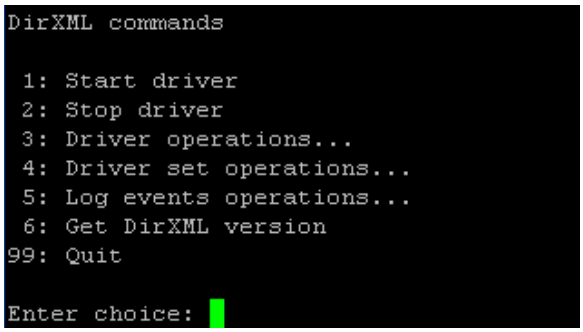
Der interaktive Modus bietet eine Textschnittstelle zur Verwendung des DirXML-Befehlszeilenprogramms.

1. Geben Sie an der Konsole `dxcmd` ein.
2. Geben Sie den Namen eines Benutzers ein, der über ausreichende Rechte für die Identity Manager-Objekte verfügt.

   Beispiel: admin.novell
3. Geben Sie das Passwort des angegebenen Benutzers an.

   Beispiel: novell

   Abbildung A-1 *DXCMD-Befehle*

4. Geben Sie die Nummer des Befehls ein, den Sie ausführen möchten.

   Tabelle A-1 auf Seite 266 enthält eine Liste der Optionen und der verfügbaren Funktionalität.
5. Geben Sie „99“ ein, um das Programm zu beenden.

Hinweis: Wenn Sie eDirectory™ 8.8 auf Unix/Linux verwenden, müssen Sie die Parameter „-host“ und „-port“ angeben. Beispiel: `dxcmd -host 10.0.0.1 -port 524`. Werden keine Parameter angegeben, tritt ein jclient-Fehler auf.

```
novell.jclient.JCException: connect (to address) 111 UNKNOWN ERROR
```

Standardmäßig überwacht eDirectory 8.8 nicht localhost. Das DirXML-Befehlszeilenprogramm muss die Server-IP-Adresse oder den Hostnamen und den Port auflösen, damit eine Authentifizierung möglich ist.

Tabelle A-1 *Optionen des interaktiven Modus*

Option	Beschreibung
1: Start driver	Startet den Treiber. Gibt es mehr als einen Treiber, wird jeder Treiber mit einer Nummer aufgelistet. Geben Sie die Nummer des Treibers ein, den Sie starten möchten.
2: Stop driver	Stoppt den Treiber. Gibt es mehr als einen Treiber, wird jeder Treiber mit einer Nummer aufgelistet. Geben Sie die Nummer des Treibers ein, den Sie stoppen möchten.
3: Driver operations...	Listet die für den Treiber verfügbaren Vorgänge auf. Gibt es mehr als einen Treiber, wird jeder Treiber mit einer Nummer aufgelistet. Geben Sie die Nummer des Treibers ein, dessen verfügbare Vorgänge Sie sehen möchten. Die verfügbaren Vorgänge finden Sie in Tabelle A-2 auf Seite 267.
4: Driver set operations...	Listet die für den Treibersatz verfügbaren Vorgänge auf. • 1: Treibersatz mit Server verknüpfen • 2: Verknüpfung von Treibersatz mit Server lösen • 99: Exit
5: Log events operations...	Listet die zum Protokollieren von Ereignissen mit Novell Audit verfügbaren Vorgänge auf. Eine Beschreibung dieser Optionen finden Sie in Tabelle A-5 auf Seite 273 .
6: Get DirXML version	Gibt die installierte Version von Identity Manager an.
99: Quit	Beendet das DirXML-Befehlszeilenprogramm.

Abbildung A-2 *Treiberoptionen*

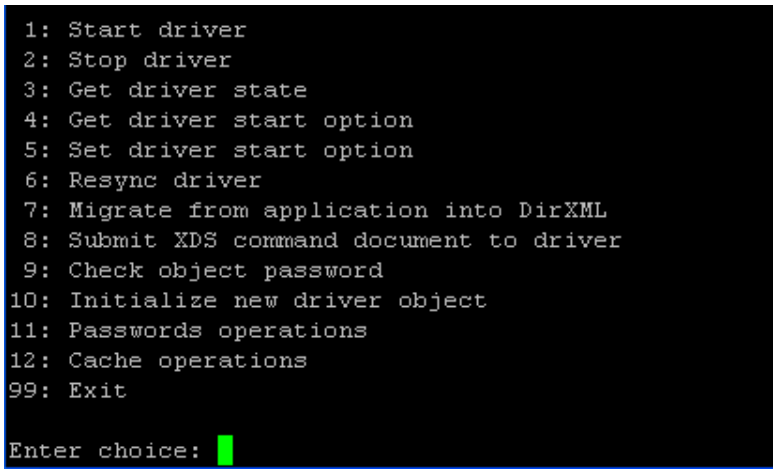


Tabelle A-2 *Treiberoptionen*

Vorgang	Beschreibung
1: Start driver	Startet den Treiber.
2: Stop driver	Stoppt den Treiber.
3: Get driver state	Gibt den Status des Treibers an. • 0 - Treiber wird angehalten • 1 - Treiber wird gestartet • 2 - Treiber wird ausgeführt • 3 - Treiber wird angehalten
4: Get driver start option	Gibt die aktuelle Treiberstartoption an. • 1 - Deaktiviert • 2 - Manuell • 3 - Automatisch
5: Set driver start option	Ändert die Startoption des Treibers. • 1 - Deaktiviert • 2 - Manuell • 3 - Automatisch • 99 - Beenden

Vorgang	Beschreibung
6: Resync driver	Erzwingt eine Neusynchronisierung des Treibers. Sie werden aufgefordert, ein Zeitintervall für die Neusynchronisierung anzugeben. *Do you want to specify a minimum time for resync? (Möchten Sie ein Zeitintervall für die Neusynchronisierung angeben?) (yes/no) (ja/nein)* Wenn Sie „yes“ eingeben, müssen Sie anschließend Datum und Uhrzeit der Neusynchronisierung angeben. *Enter a date/time (format 9/27/05 3:27 PM) > (Geben Sie ein Datum/eine Uhrzeit ein [Format 9/27/05 3:27 PM])* Wenn Sie „no“ eingeben, wird die Neusynchronisierung sofort ausgeführt.
7: Migrate from application into DirXML	Verarbeitet ein XML-Dokument, das einen Abfragebefehl enthält. *Enter filename of XDS query document: (Geben Sie den Dateinamen des XDS-Abfragedokuments ein)* Erstellen Sie an Hand der Novell nds.dtd (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html) das XML-Dokument, das einen Abfragebefehl enthält. Beispiele: NetWare: `sys:\files\query.xml` Windows: `c:\files\query.xml` Linux: `/files/query.xml`

Vorgang	Beschreibung
8: Submit XDS command document to driver	Verarbeitet ein XDS-Befehlsdokument. *Enter filename of XDS command document: (Geben Sie den Dateinamen des XDS-Befehlsdokuments ein)* Beispiele: NetWare: `sys:\files\user.xml` Windows: `c:\files\user.xml` Linux: `/files/user.xml` *Enter name of file for response: (Geben Sie den Namen der Datei für Antworten ein)* Beispiele: NetWare: `sys:\files\user.log` Windows: `c:\files\user.log` Linux: `/files/user.log`
9: Check object password	Überprüft, ob ein Objektpasswort im verbundenen System einem Treiber zugeordnet ist. Es stimmt mit dem eDirectory-Passwort des Objekts überein (Verteilungspasswort, wird mit dem universellen Passwort verwendet). Enter user name: (Benutzernamen eingeben)
10: Initialize new driver object	Führt eine interne Initialisierung der Daten für ein neues Treiberobjekt aus. Dies dient nur zu Testzwecken.
11: Passwords operations	Es gibt neun Passwortoptionen. Eine Beschreibung dieser Optionen finden Sie in Tabelle A-3 auf Seite 270 .
12: Cache operations	Es gibt fünf Cache-Vorgänge. Eine Beschreibung dieser Optionen finden Sie in Tabelle A-4 auf Seite 272.
99: Exit	Beendet die Treiberoptionen.

Abbildung A-3 *Passwortvorgänge*

Tabelle A-3 *Passwortvorgänge*

Vorgang	Beschreibung
1: Set shim password	Legt das Anwendungspasswort fest. Dies ist das Passwort des Benutzerkontos, das Sie zur Authentifizierung beim verbundenen System verwenden.
2: Clear shim password	Löscht das Anwendungspasswort.
3: Set Remote Loader password	Mit dem Remote Loader-Passwort wird der Zugriff auf die Remote Loader-Instanz kontrolliert. Weitere Informationen finden Sie in Kapitel 3, „Einrichten eines verbundenen Systems“, auf Seite 45. Geben Sie das Remote Loader-Passwort ein und bestätigen Sie es durch eine erneute Eingabe.
4: Clear Remote Loader password	Löscht das Remote Loader-Passwort, damit kein Remote Loader-Passwort für das Treiberobjekt festgelegt ist.
5: Set named password	Ermöglicht das Speichern eines Passworts oder anderer sicherheitsrelevanter Daten auf dem Treiber. Weitere Informationen finden Sie in Abschnitt 2.9, „Verwenden benannter Passwörter“, auf Seite 28. Es müssen vier Angaben gemacht werden: • Enter password name: (Geben Sie den Passwortnamen ein) • Enter password description: (Geben Sie die Passwortbeschreibung ein) • Enter password: (Passwort eingeben) • Confirm password (Passwort bestätigen)

Vorgang	Beschreibung
6: Clear named passwords (Benannte Passwörter löschen)	Löscht ein angegebenes benanntes Passwort oder alle benannten Passwörter, die auf dem Treiberobjekt gespeichert sind. Do you want to clear all named passwords? (Möchten Sie alle benannten Passwörter löschen?) (yes/no): Wenn Sie „yes“ eingeben, werden alle benannten Passwörter gelöscht. Wenn Sie „no“ eingeben, werden Sie dazu aufgefordert, den Namen des zu löschenden Passworts anzugeben.
7: List named passwords	Listet alle benannten Passwörter, die auf dem Treiberobjekt gespeichert sind. Es werden der Passwortname und die Passwortbeschreibung aufgelistet.
8: Get passwords state	Gibt an, ob ein Passwort festgelegt wurde für: • Driver Object password: (Treiberobjektpasswort) • Application password: (Anwendungspasswort) • Remote loader password: (Remote Loader-Passwort) Mit dem dxcmd-Dienstprogramm kann das Anwendungspasswort und das Remote Loader-Passwort festgelegt werden. Das Treiberobjektpasswort kann mit diesem Dienstprogramm nicht eingerichtet werden. Es zeigt aber an, ob es festgelegt wurde oder nicht.
99: Exit	Beendet das aktuelle Menü. Sie gelangen zurück zu den Treiberoptionen.

Abbildung A-4 *Cache-Vorgänge*

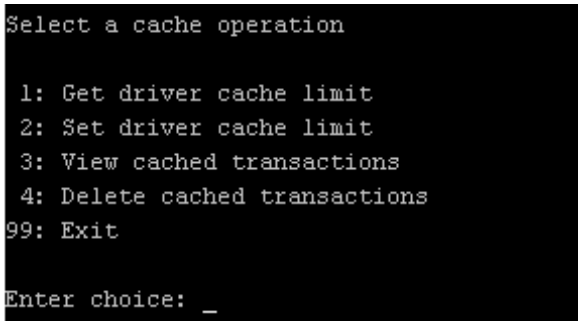


Tabelle A-4 *Cache-Vorgänge*

Vorgang	Beschreibung
1: Get driver cache limit	Gibt die aktuelle Cache-Größe für den Treiber an.
2: Set driver cache limit	Legt die Treiber-Cache-Größe in Kilobyte fest (0 für unbegrenzt).
3: View cached transactions	Es wird eine Textdatei mit den Ereignissen erstellt, die im Cache gespeichert sind. Sie können die Anzahl der anzuzeigenden Transaktionen auswählen. • Enter option token (default=0): (Geben Sie das Options-Token an [Standard=0]) • Enter maximum transactions records to return (default=1): (Geben Sie die maximale Anzahl der Transaktionsdatensätze ein, die zurückzugeben sind [Standard=1]) • Enter name of file for response: (Geben Sie den Namen der Datei für Antworten ein)
4: Delete cached transactions	Löscht die im Cache gespeicherten Transaktionen. • Enter position token (default=0): (Geben Sie das Positions-Token an [Standard=0]): • Enter event-id value of first transaction record to delete (optional): (Geben Sie die Ereignis-ID des ersten zu löschenden Transaktionsdatensatzes ein [optional]): • Enter number of transaction records to delete (default=1): (Geben Sie die Anzahl der Transaktionsdatensätze ein, die zu löschen sind [Standard=1]:
99: Exit	Beendet das aktuelle Menü. Sie gelangen zurück zu den Treiberoptionen.

Abbildung A-5 *Protokollereignisvorgänge*

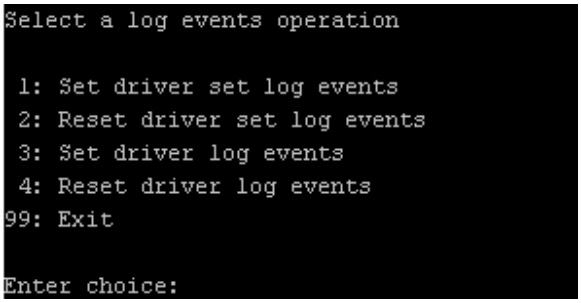


Tabelle A-5 *Protokollereignisvorgänge*

Vorgang	Beschreibung
1: Set driver set log events	Ermöglicht das Protokollieren von Treibersatzereignissen mit Novell Audit. Sie können 49 Ereignistypen zum Protokollieren auswählen. Eine Liste dieser Optionen finden Sie in Tabelle A-6 auf Seite 273. Geben Sie die Nummer des Ereignistyps ein, den Sie protokollieren möchten. Wenn Sie die Ereignistypen ausgewählt haben, geben Sie „99“ ein, um die Auswahl zu bestätigen.
2: Reset driver set log events	Setzt alle Protokollereignisoptionen zurück.
3: Set driver log events	Ermöglicht das Protokollieren von Treiberereignissen mit Novell Audit. Sie können 49 Ereignistypen zum Protokollieren auswählen. Eine Liste dieser Optionen finden Sie in Tabelle A-6 auf Seite 273. Geben Sie die Nummer des Ereignistyps ein, den Sie protokollieren möchten. Wenn Sie die Ereignistypen ausgewählt haben, geben Sie „99“ ein, um die Auswahl zu bestätigen.
4: Reset driver log events	Setzt alle Protokollereignisoptionen zurück.
99: Exit	Beendet das Menü für Protokollereignisvorgänge.

Tabelle A-6 *Protokollereignisse für Treibersätze und Treiber*

Optionen
1: Status success (Status: Erfolgreich)
2: Status retry (Status: Wiederholen)
3: Status warning (Status: Warnmeldung)
4: Status error (Statusfehler)
5: Status fatal (Status: Gravierend)
6: Status other (Status: Sonstiges)
7: Query elements (Elemente vom Typ 'Abfragen')
8: Add elements (Elemente vom Typ 'Hinzufügen')
9: Remove elements (Elemente vom Typ 'Entfernen')
10: Modify elements (Elemente vom Typ 'Ändern')
11: Rename elements (Elemente vom Typ 'Umbenennen')
12: Move elements (Elemente vom Typ 'Verschieben')
13: Add-association elements (Elemente vom Typ 'Verknüpfung hinzufügen')

Optionen
14: Remove-association elements (Elemente vom Typ 'Verknüpfung entfernen')
15: Query-schema elements (Elemente vom Typ 'Schema abfragen')
16: Check-password elements (Elemente vom Typ 'Passwort überprüfen')
17: Check-object-password elements (Elemente vom Typ 'Objektpasswort überprüfen')
18: Modify-password elements (Elemente vom Typ 'Passwort ändern')
19: Sync elements (Elemente vom Typ 'Synchronisieren')
20: Pre-transformed XDS document from shim (Vortransformiertes XDS-Dokument vom Schnittstellenmodul)
21: Post input transformation XDS document (XDS-Dokument vom Typ 'Nach Eingabetransformation')
22: Post output transformation XDS document (XDS-Dokument vom Typ 'Nach Ausgabetransformation')
23: Post event transformation XDS document (XDS-Dokument vom Typ 'Nach Ereignistransformation')
24: Post placement transformation XDS document (XDS-Dokument vom Typ 'Nach Platzierungstransformation')
25: Post create transformation XDS document (XDS-Dokument vom Typ 'Nach Erstellungstransformation')
26: Post mapping transformation <inbound> XDS document (XDS-Dokument vom Typ 'Nach Zuordnungstransformation' [eingehend])
27: Post mapping transformation <outbound> XDS document (XDS-Dokument vom Typ 'Nach Zuordnungstransformation' [ausgehend])
28: Post matching transformation XDS document (XDS-Dokument vom Typ 'Nach Entsprechungstransformation')
29: Post command transformation XDS document (XDS-Dokument vom Typ 'Nach Befehlstransformation')
30: Post-filtered XDS document <Publisher> (XDS-Dokument vom Typ 'Nach Filterung' [Herausgeber])
31: User agent XDS command document (XDS-Befehlsdokument vom Typ 'Benutzeragent')
32: Driver resync request (Anforderung auf Neusynchronisierung des Treibers)
33: Driver migrate from application (Treiber migrieren von Anwendung)
34: Driver start (Treiber starten)
35: Driver stop (Treiber stoppen)
36: Password sync (Passwortsynchronisierung)
37: Password request (Passwortanforderung)
38: Engine error (Engine-Fehler)
39: Engine warning (Engine-Warnhinweis)
40: Add attribute (Attribut hinzufügen)
41: Clear attribute (Attribut löschen)

Optionen
42: Add value (Wert hinzufügen)
43: Remove value (Wert entfernen)
44: Merge entire (Einträge zusammenführen)
45: Get named password (Benanntes Passwort abrufen)
46: Unknown (Unbekannt)
47: Unknown (Unbekannt)
48: User defined IDs (Benutzerdefinierte IDs)
99: Accept checked items (Markierte Elemente akzeptieren)

A.2 Befehlszeilenmodus

Der Befehlszeilenmodus ermöglicht Ihnen die Verwendung von Skript- oder Stapeldateien. In Tabelle A-7 auf Seite 275 sind die verschiedenen Optionen aufgelistet.

Sie müssen bei der Verwendung der Befehlszeilenoptionen entscheiden, welche Elemente Sie benötigen, und diese dann in einem Befehl zusammenfassen.

Beispiel: `dxcmd -user admin.headquarters -host 10.0.0.1 -password n0vell -start test.driverset.headquarters`

Mit diesem Befehl wird der Treiber gestartet.

Tabelle A-7 *Befehlszeilenoptionen*

Option	Beschreibung
Konfiguration	
-user <Benutzername>	Geben Sie den Namen eines Benutzers mit administrativen Rechten für die Treiber an, die Sie testen möchten.
-host <Hostname oder IP-Adresse>	Geben Sie die IP-Adresse des Servers an, auf dem der Treiber installiert ist.
-password <Benutzerpasswort>	Geben Sie das Passwort des angegebenen Benutzers an.
-port <Portnummer>	Geben Sie eine Portnummer an, wenn der Standardport nicht verwendet wird.
-q <automatischer Modus>	Bei der Ausführung eines Befehls werden sehr wenige Informationen angezeigt.
-v <ausführlicher Modus>	Bei der Ausführung eines Befehls werden ausführliche Informationen angezeigt.
-? <diese Nachricht anzeigen>	Zeigt das Hilfemenü an.
-help <diese Nachricht anzeigen>	Zeigt das Hilfemenü an.

Option	Beschreibung
Aktionen	
-start <Treiber-DN>	Startet den Treiber.
-stop <Treiber-DN>	Stoppt den Treiber.
-getstate <Treiber-DN>	Gibt den Status des Treibers an („wird ausgeführt“ oder „angehalten“).
-getstartoption <Treiber-DN>	Gibt die Startoption des Treibers an.
-setstartoption <Treiber-DN> <disabled|manual|auto> <resync|noresync>	Dient zum Festlegen der Startoptionen für den Treiber, wenn der Server neu gestartet wird. Legt zudem fest, ob die Objekte neu synchronisiert werden müssen, wenn der Treiber neu startet.
-getcachelimit <Treiber-DN>	Gibt das Cache-Limit für den Treiber an.
-setcachelimit <Treiber-DN> <0 oder positive Ganzzahl>	Legt das Cache-Limit für den Treiber fest.
-migrateapp <Treiber-DN> <Dateiname>	Verarbeitet ein XML-Dokument, das einen Abfragebefehl enthält. Erstellen Sie an Hand der Novell nds.dtd (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html) das XML-Dokument, das einen Abfragebefehl enthält.
-setshimpassword <Treiber-DN> <Passwort>	Legt das Anwendungspasswort fest. Dies ist das Passwort des Benutzerkontos, das Sie zur Authentifizierung beim verbundenen System verwenden.
-clearshimpassword <Treiber-DN> <Passwort>	Löscht das Anwendungspasswort.
-setremoteloaderpassword <Treiber-DN> <Passwort>	Legt das Remote Loader-Passwort fest. Mit dem Remote Loader-Passwort wird der Zugriff auf die Remote Loader-Instanz kontrolliert. Weitere Informationen finden Sie in Kapitel 3, „Einrichten eines verbundenen Systems“, auf Seite 45.
<clearremoteloaderpassword <Treiber-DN>	Löscht das Remote Loader-Passwort.

Option	Beschreibung
-sendcommand <Treiber-DN> <Eingabedatein-ame> <Ausgabedateiname>	Verarbeitet ein XDS-Befehlsdokument. Geben Sie das XDS-Befehlsdokument als Eing-abedatei an. Beispiele: NetWare: `sys:\files\user.xml` Windows: `c:\files\user.xml` Linux: `/files/user.log` Geben Sie den Namen der Ausgabedatei an, die die Ergebnisse enthalten soll. Beispiele: NetWare: `sys:\files\user.log` Windows: `c:\files\user.log` Linux: `/files/user.log`
-setlogevents <dn> <Ganzzahl ...>	Legt die mit Novell Audit zu protokollierenden Ereignisse für den Treiber fest. Die Ganzzahl ist die Option für das zu protokollierende Ereignis. Tabelle A-6 auf Seite 273 enthält die für diesen Vorgang gültigen Ganzzahlen.
-clearlogevents <DN>	Löscht alle mit Novell Audit protokollierten Ereign-isse für den Treiber.
-setdriverset <Treibersatz-DN>	Verknüpft einen Treibersatz mit dem Server.
-cleardriverset	Löscht die Verknüpfung zwischen Treiber und Server.
-getversion	Gibt die installierte Version von Identity Manager an.
-initdriver object <DN>	Führt eine interne Initialisierung der Daten für ein neues Treiberobjekt aus. Dies dient nur zu Testzwecken.
-setnamedpassword <Treiber-DN> <Name> <Passwort> [Beschreibung]	Legt benannte Passwörter für das Treiberobjekt fest. Geben Sie den Namen, das Passwort und die Beschreibung des benannten Passworts an.
-clearnamedpassword <Treiber-DN> <Name>	Löscht ein angegebenes benanntes Passwort.
-clearallnamedpaswords <Treiber-DN>	Löscht alle benannten Passwörter, die für einen bestimmten Treiber festgelegt wurden.

Konfigurationsoptionen für einen Remote Loader

B

Mit den in der folgenden Tabelle aufgeführten Optionen können Sie einen Remote Loader konfigurieren.

Tabelle B-1 *Remote Loader-Optionen*

Option	Kurzform	Parameter	Beschreibung
address		IP-Adresse	Dieser Parameter ist optional. Er gibt an, dass der Remote Loader eine bestimmte lokale IP-Adresse überwacht. Dies ist hilfreich, wenn der Server, der den Remote Loader hostet, mehrere IP-Adressen hat und der Remote Loader nur eine dieser Adressen überwachen soll. Die folgenden drei Optionen sind verfügbar: address=*Adressnummer* address='localhost' Diesen Parameter nicht verwenden. Wenn Sie den Parameter „-address“ nicht verwenden, überwacht der Remote Loader alle lokalen IP-Adressen. Beispiel: address=137.65.134.83
-class	-cl	Java-Klassenname	Gibt den Java-Klassennamen des zu hostenden Identity Manager-Anwendungsschnittstellenmoduls an. Einen Java-Treiber können Sie beispielsweise mit einer der folgenden Optionen angeben: -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim Java verwendet zum Lesen von Zertifikaten einen Keystore. Die Optionen „-class“ und „-module“ schließen sich gegenseitig aus. Eine Liste der Java-Klassennamen finden Sie in Tabelle B-2 auf Seite 286.

Option	Kurzform	Parameter	Beschreibung
-commandport	-cp	Portnummer	Gibt den TCP/IP-Port an, der von der Remote Loader-Instanz zu Steuerungszwecken verwendet wird. Wenn die Remote Loader-Instanz ein Anwendungsschnittstellenmodul hostet, ist der Befehls-Port der Port, über den eine andere Remote Loader-Instanz mit der Instanz kommuniziert, die das Schnittstellenmodul hostet. Wenn die Remote Loader-Instanz einen Befehl an eine Instanz sendet, die ein Anwendungsschnittstellenmodul hostet, ist der Befehls-Port der Port, der von der Host-Instanz überwacht wird. Wenn kein Port angegeben ist, wird standardmäßig Befehls-Port 8000 verwendet. Durch die Angabe unterschiedlicher Verbindungs- und Befehls-Ports können auf dem Server, auf dem unterschiedliche Treiberinstanzen gehostet werden, mehrere Instanzen des Remote Loader ausgeführt werden. Beispiel: -commandport 8001 -cp 8001
-config	kein	Dateiname	Gibt eine Konfigurationsdatei an. Die Konfigurationsdatei kann bis auf `config` beliebige Befehlszeilenoptionen enthalten. Die an der Befehlszeile angegebenen Optionen haben Vorrang vor den in der Konfigurationsdatei angegebenen Optionen. Beispiel: -config config.txt
-connection	-conn	Zeichenkette für die Verbindungskonfiguration	Gibt die Verbindungsparameter für die Verbindung zum Metaverzeichnis-Server an, auf dem das Identity Manager-Remote-Schnittstellenmodul ausgeführt wird. Die Standardverbindungsmethode für den Remote Loader ist TCP/IP mit SSL. Der TCP/IP-Standardport für diese Verbindung ist 8090. Es können mehrere Instanzen des Remote Loader auf demselben Server ausgeführt werden. Jede Instanz des Remote Loader hostet eine separate Anwendungsschnittstellenmodulinstanz des Identity Manager. Sie unterscheiden mehrere Instanzen des Remote Loader voneinander, indem Sie für jede Remote Loader-Instanz unterschiedliche Verbindungs- und Befehls-Ports angeben. Beispiel: -connection "port=8091 rootfile=server1.pem" -conn "port=8091 rootfile=server1.pem"

Option	Kurzform	Parameter	Beschreibung
-description	-desc	Kurzbeschreibung	Geben Sie eine kurze Beschreibungszeichenkette (z. B. SAP) an, die für den Titel des Trace-Fensters und für die Novell® Audit-Protokollierung verwendet wird. Beispiel: -description SAP -desc SAP Die Remote Loader-Konsole schreibt lange Formen in die Konfigurationsdateien. Sie können entweder eine lange Form (z. B. -description) oder eine kurze Form (z. B. -desc) verwenden.
-help	-?	kein	Zeigt Hilfe-Informationen an. Beispiel: -help -?
-java	-j	kein	Gibt an, dass für eine Java-Schnittstellenmodulinstanz Passwörter festgelegt werden müssen. Diese Option ist nur in Verbindung mit der Option „setpasswords“ hilfreich. Wenn „-class“ mit „-setpasswords“ angegeben wird, ist diese Option nicht erforderlich.
-javadebugport	-jdp	Portnummer	Gibt an, dass die Remote Loader-Instanz das Java-Debugging auf dem angegebenen Port aktivieren soll. Dies ist hilfreich für Entwickler von Identity Manager-Anwendungsschnittstellenmodulen. Beispiel: -javadebugport 8080 -jdp 8080
Keystore			Bedingte Parameter. Wird nur für Identity Manager-Anwendungsschnittstellenmodule in JAR-Dateien verwendet. Gibt den Dateinamen des Java-Keystores an, der das Herkunftsverbürgungszertifikat des Herausgebers des Zertifikats enthält, das vom Remote-Schnittstellenmodul verwendet wird. Dies ist in der Regel die Zertifizierungsstelle des eDirectory™-Baums, der das Remote-Schnittstellenmodul hostet. Wenn Sie SSL ausführen und den Remote Loader für die Kommunikation mit einem Java-Treiber benötigen, geben Sie ein Schlüssel/Wert-Paar ein: `keystore='`*`keystorename`*`' storepass='`*`passwort`*`'`

Option	Kurzform	Parameter	Beschreibung
-module	-m	Modulname	Gibt das Modul an, in dem das zu hostende Identity Manager-Anwendungsschnittstellenmodul enthalten ist. Bei einem nativen Treiber können Sie beispielsweise eine der folgenden Optionen angeben: -module "c:\Novell\Remote-Loader\Exchange5Shim.dll" -m "c:\Novell\Remote-Loader\Exchange5Shim.dll" oder: -module "usr/lib/dirxml/NISDriverShim.so" -m "usr/lib/dirxml/NISDriverShim.so" Die Option „-module“ verwendet ein rootfile-Zertifikat. Die Optionen „-module“ und „-class“ schließen sich gegenseitig aus.
-password	-p	Passwort	Gibt das Passwort für die Befehlsauthentifizierung an. Dieses Passwort muss dasselbe Passwort sein, das mit `setpasswords` für die Loader-Instanz angegeben wurde, die Ziel der Befehle ist. Wenn eine Befehlsoption (beispielsweise „unload“ oder „tracechange“) angegeben und die `-password`-Option nicht angegeben ist, wird der Benutzer aufgefordert, das Passwort des Loaders einzugeben, auf den sich der Befehl bezieht. Beispiel: -password novell4 -p novell4
port		Dezimale Portnummer	Ein obligatorischer Parameter. Er gibt den TCP/IP-Port an, den der Remote Loader auf Verbindungen vom Remote-Schnittstellenmodul überwacht. Beispiel: port=8090
rootfile			Ein bedingter Parameter. Wenn Sie SSL ausführen und den Remote Loader für die Kommunikation mit einem nativen Treiber benötigen, geben Sie Folgendes ein: `rootfile='trusted certname'`

Option	Kurzform	Parameter	Beschreibung
-service	-serv	Kein Parameter oder install/ uninstall	Zum Installieren einer Instanz als Dienst wird das Argument „install“ zusammen mit den zum Hosten eines Anwendungsschnittstellenmoduls erforderlichen Argumenten verwendet. Die verwendeten Argumente müssen z. B. „-module“ und können „-connection“, „-commandport“ usw. enthalten. Mit dieser Option wird der Win32-Dienst installiert, aber nicht gestartet. Zum Deinstallieren einer als Dienst ausgeführten Instanz wird das Argument „uninstall“ zusammen mit den zum Hosten eines Anwendungsschnittstellenmoduls erforderlichen Argumenten verwendet. Die Variante ohne Argument wird an der Befehlszeile nur für eine Instanz verwendet, die als Win32-Dienst ausgeführt wird. Dies wird beim Installieren einer Instanz als Dienst automatisch eingerichtet. Beispiel: -service install -serv uninstall Diese Option ist nicht für „rdxml“ oder den Java Remote Loader verfügbar.
-setpasswords	-sp	Passwort Passwort	Gibt das Passwort der Remote Loader-Instanz und das Passwort des Identity Manager-Treiberobjekts des Remote-Schnittstellenmoduls an, mit dem der Remote Loader kommuniziert. Das erste Passwort im Argument ist das Passwort für den Remote Loader. Das zweite Passwort in den optionalen Argumenten ist das Passwort für das Identity Manager-Treiberobjekt, das mit dem Remote-Schnittstellenmodul auf dem Metaverzeichnis-Server verknüpft ist. Es müssen entweder beide oder keine Passwörter angegeben werden. Wenn kein Passwort angegeben wird, fordert der Remote Loader zur Eingabe der Passwörter auf. Dies ist eine Konfigurationsoption. Mithilfe dieser Option wird die Remote Loader-Instanz mit den angegebenen Passwörtern konfiguriert. Es wird jedoch weder ein Identity Manager-Anwendungsschnittstellenmodul geladen noch mit anderen Loader-Instanzen kommuniziert. Beispiel: -setpasswords novell4 staccato3 -sp novell4 staccato3

Option	Kurzform	Parameter	Beschreibung
-storepass		Keystore-Passwort	Wird nur für Identity Manager-Anwendungsschnittstellenmodule in JAR-Dateien verwendet. Gibt das Passwort für den Java-Keystore an, der im Parameter „keystore“ festgelegt ist. Beispiel: storepass=MeinPasswort Diese Option gilt nur für den Java Remote Loader.
-trace	-t	Ganzzahl	Gibt die Trace-Stufe an. Diese Option wird nur beim Hosten eines Anwendungsschnittstellenmoduls verwendet. Die Trace-Stufen entsprechen den auf dem Metaverzeichnis-Server verwendeten Trace-Stufen. Beispiel: -trace 3 -t 3
-tracechange	-tc	Ganzzahl	Weist eine Remote Loader-Instanz an, die ein Anwendungsschnittstellenmodul hostet, ihre Trace-Stufe zu ändern. Die Trace-Stufen entsprechen den auf dem Metaverzeichnis-Server verwendeten Trace-Stufen. Beispiel: -tracechange 1 -tc 1
-tracefile	-tf	Dateiname	Gibt eine Datei an, in die die Trace-Meldungen geschrieben werden sollen. Trace-Meldungen werden in die Datei geschrieben, wenn die Trace-Stufe größer als Null ist. Trace-Meldungen werden auch bei geschlossenem Trace-Fenster in die Datei geschrieben. Beispiel: -tracefile c:\temp\trace.txt -tf c:\temp\trace.txt
-tracefilechange	-tfc	Keine oder „Dateiname“	Weist eine Remote Loader-Instanz, die ein Anwendungsschnittstellenmodul hostet, an, eine Trace-Datei zu verwenden, oder eine bereits geöffnete Datei zu schließen und eine neue zu verwenden. Wenn diese Option ohne Argumente verwendet wird, schließt die Host-Instanz alle geöffneten Trace-Dateien. Beispiel: -tracefilechange c:\temp\newtrace.txt tfc c:\temp\newtrace.txt

Option	Kurzform	Parameter	Beschreibung
-tracefilemax	-tfm	Größe	Gibt die Maximalgröße an, die die Trace-Datei auf der Festplatte belegen darf. Bei Angabe dieser Option wird die Trace-Datei mit dem Namen verwendet, der mit der Option „tracefile“ angegeben wurde, sowie bis zu neun zusätzliche Rollover-Dateien. Die Rollover-Dateien werden benannt, indem an den Namen der Haupt-Trace-Datei “*_n*” angehängt wird, wobei 1 bis 9 gültige Werte für n sind. Der Parameter für die Größe gibt die Anzahl der Byte an. Geben Sie die Größe mithilfe der Erweiterungen K, M oder G für Kilobyte, Megabyte oder Gigabyte an. Wenn die Trace-Datei beim Starten des Remote Loader größer als das angegebene Maximum ist, dann behält die Trace-Datei diese Größe bei, bis das Rollover über alle 10 Dateien ausgeführt wurde. Beispiel: -tracefilemax 1000M -tfm 1000M In diesem Beispiel darf die Trace-Datei nicht größer als 1 GB sein.
-unload	-u	kein	Entlädt die Remote Loader-Instanz. Wenn der Remote Loader als Win32-Dienst ausgeführt wird, wird der Dienst durch diese Option gestoppt. Beispiel: -unload -u
-window	-w	on/off	Öffnet oder schließt das Trace-Fenster in einer Remote Loader-Instanz. Beispiel: -window on -w off Diese Option ist nur auf Windows-Plattformen verfügbar. Sie ist nicht für den Java Remote Loader verfügbar.

Option	Kurzform	Parameter	Beschreibung
-wizard	-wiz	kein	Startet den Konfigurationsassistenten. Wenn Sie „dirxml_remote.exe“ ohne Befehlszeilenparameter ausführen, wird auch der Assistent gestartet. Diese Option ist hilfreich, wenn zudem eine Konfigurationsdatei angegeben ist. In diesem Fall wird der Assistent mit den Werten aus der Konfigurationsdatei gestartet und die Konfiguration kann mithilfe des Assistenten geändert werden, ohne die Konfigurationsdatei direkt bearbeiten zu müssen. Beispiel: -wizard -wiz Diese Option ist nur auf Windows-Plattformen verfügbar. Sie ist nicht für den Java Remote Loader verfügbar.

Tabelle B-2 *Java-Klassennamen*

Java-Klassenname	Treiber
com.novell.nds.dirxml.driver.avaya.PBXDriverShim	Avaya PBX-Treiber
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	Treiber für Text mit Begrenzungszeichen
com.novell.nds.dirxml.driver.nds.DriverShimImpl	eDirectory-Treiber
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	Treiber für den Berechtigungsservice
com.novell.gw.dirxml.driver.gw.GWdriverShim	GroupWise-Treiber
com.novell.nds.dirxml.jdbc.JDBCDriverShim	JDBC-Treiber
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	LDAP-Treiber
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	Loopback-Treiber
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	Treiber für manuelle Aufgaben
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	NIS-Treiber
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes-Treiber
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft-Treiber
com.novell.nds.dirxml.driver.SAPShim.SAPDriverShim	SAP HR-Treiber
com.novell.nds.dirxml.driver.sapusershim.SAPDriverShim	Treiber für die SAP-Benutzerverwaltung
com.novell.nds.dirxml.driver.sifagent.SIFShim	SIF-Treiber
com.novell.nds.dirxml.driver.soap.SOAPDriver	SOAP-Treiber
com.novell.idm.driver.ComposerDriverShim	Benutzeranwendung

Java-Klassenname	Treiber
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	Treiber für Remedy ARS

Identity Manager - Ereignisse und Berichte

C

Dieser Abschnitt enthält eine Liste aller Novell® Audit-Ereignisse, die von Identity Manager protokolliert werden. Hier finden Sie auch Beispiele für die Berichte, die mit Novell Audit erzeugt werden können. In Abschnitt C.11, „Berichte“, auf Seite 310 finden Sie die Beispielberichte.

Jedes Ereignis enthält folgende Informationen: EventID, Description, Originator Title, Target Title, Subtarget Title, Text1 Title, Text2 Title, Text3 Title, Value1 Title, Value1 Type, Value2 Title, Value2 Type, Value3 Title, Value3 Type, Group Title, Group Type, Data Title, Data Type und Display Schema.

In den nachfolgenden Tabellen sind die Ereignisse folgender Komponenten aufgelistet.

C.1 Engine-Ereignisse

Die Tabellen enthalten die Engine-Ereignisse, die mit Novell Audit protokolliert werden können.

Tabelle C-1 *Engine-Ereignis-Felder: Originator Title, Target Title und Subtarget Title*

EventID	Description	Originator Title	Target Title	Subtarget Title
30001	Status Success	Channel	src-dn (dest-dn)	Level
30002	Status Retry	Channel	src-dn (dest-dn)	Level
30003	Status Warning	Channel	src-dn (dest-dn)	Level
30004	Status Error	Channel	src-dn (dest-dn)	Level
30005	Status Fatal	Channel	src-dn (dest-dn)	Level
30006	Status Other	Channel	src-dn (dest-dn)	Level

EventID	Description	Originator Title	Target Title	Subtarget Title
30007	Search	Channel	dest-dn oder association	Scope
30008	Add Entry	Channel	dest-dn oder association	Attribute name
30009	Delete Entry	Channel	dest-dn oder association	Attribute name
3000A	Modify Entry	Channel	dest-dn oder association	Attribute name
3000B	Rename Entry	Channel	dest-dn oder association	Object type
3000C	Move Entry	Channel	dest-dn oder association	Move Destination
3000D	Add Association	Channel	dest-dn	Attribute name
3000E	Remove Association	Channel		Attribute name
3000F	Query Schema	Channel		
30010	Check Password	Channel	Driver	
30011	Check Object Password	Channel	dest-dn oder association	
30012	Change Password	Channel	dest-dn oder association	
30013	Sync	Channel	dest-dn oder association	Attribute name
30014	Input XML Document	Channel		Attribute name
30015	Input Transformation Document	Channel		
30016	Output Transformation Document	Channel		
30017	Event Transformation Document	Channel		
30018	Placement Rule Transformation Document	Channel		
30019	Create Rule Transformation Document	Channel		
3001A	Input Mapping Rule Transformation Document	Channel		
3001B	Output Mapping Rule Transformation Document	Channel		

EventID	Description	Originator Title	Target Title	Subtarget Title
3001C	Matching Rule Transformation Document	Channel		
3001D	Command Transformation Document	Channel		
3001E	Publisher Filter Transformation Document	Channel		
3001F	User Agent Request	Channel		
30020	Resync Driver	Channel	Driver	
30021	Migrate	Channel	Association	Attribute name
30022	Driver Start	Driver Set	Driver	
30023	Driver Stop	Driver Stop	Driver	
30024	Password Sync	Channel	Object	Attribute name
30025	Password Reset	Channel	dest-dn oder association	Attribute name
30026	DirXML Error	Channel	Object	
30027	DirXML Warning	Channel	Object	
30028	Custom Operation	Channel		
30029	Clear Attribute	Channel	dest-dn oder association	Attribute name
3002A	Add Value - Modify Entry	Channel	dest-dn oder association	Attribute name
3002B	Remove Value	Channel	dest-dn oder association	Attribute name
3002C	Merge Entries	Channel	Object	Attribute name
3002D	Get Named Password	Driver oder Channel	Object	
3002E	Reset Attributes	Channel	Object	Channel
3002F	Add Value - Add Entry	Channel	dest-dn oder association	Attribute name

Tabelle C-2 *Engine-Ereignis-Felder: Text1 Title, Text2 Title und Text3 Title*

EventID	Description	Text1 Title	Text2 Title	Text3 Title
30001	Status Success	Type	Status Document	Event ID
30002	Status Retry	Type	Status Document	Event ID
30003	Status Warning	Type	Status Document	Event ID
30004	Status Error	Type	Status Document	Event ID
30005	Status Fatal	Type	Status Document	Event ID

EventID	Description	Text1 Title	Text2 Title	Text3 Title
30006	Status Other	Type	Status Document	Event ID
30007	Search	Object type		Event ID
30008	Add Entry	Object type	src-dn	Event ID
30009	Delete Entry	Object type	src-dn	Event ID
3000A	Modify Entry	Object type	src-dn	Event ID
3000B	Rename Entry	New name	src-dn	Event ID
3000C	Move Entry	Move Association	src-dn	Event ID
3000D	Add Association	Association		Event ID
3000E	Remove Association	Association		Event ID
3000F	Query Schema			Event ID
30010	Check Password			
30011	Check Object Password			Event ID
30012	Change Password	Object type	src-dn	Event ID
30013	Sync	Object type	association	Type
30014	Input XML Document			Warning message
30015	Input Transformation Document			Warning message
30016	Output Transformation Document			Warning message
30017	Event Transformation Document			Warning message
30018	Placement Rule Transformation Document			Warning message
30019	Create Rule Transformation Document			Warning message
3001A	Input Mapping Rule Transformation Document			Warning message
3001B	Output Mapping Rule Transformation Document			Warning message
3001C	Matching Rule Transformation Document			Warning message
3001D	Command Transformation Document			Warning message
3001E	Publisher Filter Transformation Document			Warning message
3001F	User Agent Request			

EventID	Description	Text1 Title	Text2 Title	Text3 Title
30020	Resync Driver			Error message
30021	Migrate	Object type		Warning message
30022	Driver Start			Driver message
30023	Driver Stop			Driver message
30024	Password Sync			
30025	Password Reset		src-dn	
30026	DirXML Error	Error Message		
30027	DirXML Warning	Warning message		
30028	Custom Operation			
30029	Clear Attribute		src-dn	Event ID
3002A	Add Value - Modify Entry	Value	src-dn	Event ID
3002B	Remove Value	Value	src-dn	Event ID
3002C	Merge Entries	Object type	Channel	Association
3002D	Get Named Password	Password Name		Event ID
3002E	Reset Attributes			
3002F	Add Value - Add Entry	Value	src-dn	Event ID

Tabelle C-3 *Engine-Ereignis-Felder: Value1 Title, Value2 Title und Value3 Title*

EventID	Description	Value1 Title	Value2 Title	Value3 Title
30001	Status Success			
30002	Status Retry			
30003	Status Warning			
30004	Status Error			
30005	Status Fatal			
30006	Status Other			
30007	Search			Result
30008	Add Entry			Result
30009	Delete Entry			Result
3000A	Modify Entry			Result
3000B	Rename Entry			Result
3000C	Move Entry			Result
3000D	Add Association			Result

EventID	Description	Value1 Title	Value2 Title	Value3 Title
3000E	Remove Association			Result
3000F	Query Schema			Result
30010	Check Password			
30011	Check Object Password			
30012	Change Password			Result
30013	Sync			Result
30014	Input XML Document			
30015	Input Transformation Document			
30016	Output Transformation Document			
30017	Event Transformation Document			
30018	Placement Rule Transformation Document			
30019	Create Rule Transformation Document			
3001A	Input Mapping Rule Transformation Document			
3001B	Output Mapping Rule Transformation Document			
3001C	Matching Rule Transformation Document			
3001D	Command Transformation Document			
3001E	Publisher Filter Transformation Document			
3001F	User Agent Request			Result
30020	Resync Driver			Result
30021	Migrate			
30022	Driver Start	State		
30023	Driver Stop	State		
30024	Password Sync			Result
30025	Password Reset			
30026	DirXML Error	Code		
30027	DirXML Warning	Code		

EventID	Description	Value1 Title	Value2 Title	Value3 Title
30028	Custom Operation			
30029	Clear Attribute			Result
3002A	Add Value - Modify Entry			Result
3002B	Remove Value			Result
3002C	Merge Entries			
3002D	Get Named Password			Result
3002E	Reset Attributes			
3002F	Add Value - Add Entry			Result

Tabelle C-4 *Engine-Ereignis-Felder: Data Type und Triggers*

EventID	Description	Data Type	Triggers
30001	Status Success	XML Document	Viele verschiedene Ereignisse können das Ereignis „Status: Success“ („Status: Erfolgreich“) auslösen. Es bedeutet in der Regel, dass ein Vorgang erfolgreich ausgeführt wurde.
30002	Status Retry	XML Document	Viele verschiedene Ereignisse können das Ereignis „Status: Retry“ („Status: Wiederholen“) auslösen. Es bedeutet, dass ein Vorgang nicht abgeschlossen wurde und zu einem späteren Zeitpunkt erneut ausgeführt werden muss.
30003	Status Warning	XML Document	Viele verschiedene Ereignisse können das Ereignis „Status: Warning“ („Status: Warnmeldung“) auslösen. Es bedeutet in der Regel, dass ein Vorgang abgeschlossen wurde, aber geringfügige Probleme auftraten.
30004	Status Error	XML Document	Viele verschiedene Ereignisse können das Ereignis „Status: Error“ („Status: Fehler“) auslösen. Es bedeutet in der Regel, dass ein Vorgang nicht erfolgreich ausgeführt wurde.

EventID	Description	Data Type	Triggers
30005	Status Fatal	XML Document	Viele verschiedene Ereignisse können das Ereignis „Status: Fatal“ („Status: Gravierend“) auslösen. Es bedeutet in der Regel, dass ein Vorgang nicht abgeschlossen wurde und die Engine oder der Treiber nicht mit der Verarbeitung fortfahren konnte.
30006	Status Other	XML Document	Jedes Statusdokument mit einem anderen Level als den fünf zuvor definierten erzeugt das Ereignis „Status: Other“ („Status: Sonstiges“). Diese Ereignisse können nur in einer Formatvorlage oder einer Regel generiert werden.
30007	Search	XML Document	Tritt auf, wenn ein Abfragedokument an die IDM-Engine oder den IDM-Treiber gesendet wird.
30008	Add Entry	XML Document	Tritt auf, wenn ein Objekt hinzugefügt wird.
30009	Delete Entry	XML Document	Tritt auf, wenn ein Objekt gelöscht wird.
3000A	Modify Entry	XML Document	Tritt auf, wenn ein Objekt geändert wird.
3000B	Rename Entry	XML Document	Tritt auf, wenn ein Objekt umbenannt wird.
3000C	Move Entry	XML Document	Tritt auf, wenn ein Objekt verschoben wird.
3000D	Add Association	XML Document	Tritt auf, wenn eine Verknüpfung hinzugefügt wird. Dies ist bei Hinzufügevorgängen oder Entsprechungen der Fall.
3000E	Remove Association	XML Document	Wenn ein Objekt gelöscht wird, tritt kein Ereignis zum Entfernen einer Verknüpfung auf. Das Ereignis tritt auf, wenn ein Benutzerobjekt in der getrennten Anwendung gelöscht und der Löschvorgang dann in eine Änderung konvertiert wird, bei der die Verknüpfung entfernt wird.
3000F	Query Schema	XML Document	Tritt auf, wenn ein Vorgang zum Abfragen eines Schemas an die IDM-Engine oder den IDM-Treiber gesendet wird.
30010	Check Password		Manuelle Funktion, die über iManager initiiert wird.

EventID	Description	Data Type	Triggers
30011	Check Object Password	XML Document	Tritt auf, wenn eine Anforderung zum Überprüfen des Passworts eines Objekts gestellt wird. Dies gilt nicht für Treiber.
30012	Change Password	XML Document	Tritt auf, wenn eine Anforderung zum Ändern des Treiberpasworts gestellt wird.
30013	Sync	XML Document	Tritt auf, wenn ein Synchronisierungsereignis angefordert wird.
30014	Input XML Document	XML Document	Wird immer dann generiert, wenn von der Engine oder dem Treiber ein Eingabedokument erstellt wird.
30015	Input Transformation Document	XML Document	Wird nach der Verarbeitung der Eingabetransformationsrichtlinien generiert. Ermöglicht dem Benutzer die Durchsicht des transformierten Dokuments.
30016	Output Transformation Document	XML Document	Wird nach der Verarbeitung der Ausgabetransformationsrichtlinien generiert. Ermöglicht dem Benutzer die Durchsicht des transformierten Dokuments.
30017	Event Transformation Document	XML Document	Wird nach der Verarbeitung der Ereignistransformationsrichtlinien generiert. Ermöglicht dem Benutzer die Durchsicht des transformierten Dokuments.
30018	Placement Rule Transformation Document	XML Document	Wird nach der Verarbeitung der Richtlinien für Platzierungsregeln generiert. Ermöglicht dem Benutzer die Durchsicht des transformierten Dokuments.
30019	Create Rule Transformation Document	XML Document	Wird nach der Verarbeitung der Regelerstellungsrichtlinien generiert. Ermöglicht dem Benutzer die Durchsicht des transformierten Dokuments.
3001A	Input Mapping Rule Transformation Document	XML Document	Wird nach der Verarbeitung der Schema-Zuordnungsregeln generiert, die das Dokument in ein eDirectory-Schema konvertieren.
3001B	Output Mapping Rule Transformation Document	XML Document	Wird nach der Verarbeitung der Schema-Zuordnungsregeln generiert, die das Dokument in das Anwendungsschema konvertieren.

EventID	Description	Data Type	Triggers
3001C	Matching Rule Transformation Document	XML Document	Wird nach der Verarbeitung der Richtlinien für Übereinstimmungsregeln generiert. Ermöglicht dem Benutzer die Durchsicht des transformierten Dokuments.
3001D	Command Transformation Document	XML Document	Wird nach der Verarbeitung der Befehlstransformationsrichtlinien generiert. Ermöglicht dem Benutzer die Durchsicht des transformierten Dokuments.
3001E	Publisher Filter Transformation Document	XML Document	Wird nach der Verarbeitung des Benachrichtigungsfilters auf dem Herausgeberkanal generiert. Ermöglicht dem Benutzer die Durchsicht des transformierten Dokuments.
3001F	User Agent Request	XML Document	Tritt auf, wenn ein XDS-Befehlsdokument vom Typ „Benutzeragent“ auf dem Abonnentenkanal an den Treiber gesendet wird.
30020	Resync Driver		Tritt auf, wenn eine Anforderung zu einer erneuten Synchronisierung gestellt wird.
30021	Migrate		Tritt auf, wenn eine Migrierungsanforderung gestellt wird.
30022	Driver Start	XML Document	Tritt auf, wenn ein Treiber gestartet wird.
30023	Driver Stop	XML Document	Tritt auf, wenn ein Treiber angehalten wird.
30024	Password Sync		Wird generiert, wenn das einfache Passwort oder das Verteilungspasswort für ein Objekt festgelegt wird.
30025	Password Reset		Wird generiert, wenn das Passwort der verbundenen Anwendung nach einer fehlerhaften Passwortsynchronisierung zurückgesetzt wird.
30026	DirXML Error		Wird generiert, wenn die Engine einen internen Fehler ausgibt.
30027	DirXML Warning		Wird generiert, wenn die Engine eine interne Warnmeldung ausgibt.

EventID	Description	Data Type	Triggers
30028	Custom Operation	XML Document	Tritt auf, wenn es in einem Eingabedokument einen unbekannten Vorgang gibt. Beispiele für bekannte Vorgänge sind „add“ „delete“ und „modify“.
30029	Clear Attribute		Tritt auf, wenn ein Änderungsvorgang ein Element vom Typ „remove-all-value“-enthält.
3002A	Add Value - Modify Entry	Value	Tritt auf, wenn bei der Änderung eines Objekts ein Wert hinzugefügt wird.
3002B	Remove Value	Value	Tritt auf, wenn ein Änderungsvorgang ein Element vom Typ „remove-value“ enthält.
3002C	Merge Entries	XML Document	Tritt auf, wenn zwei Objekte zusammengeführt werden.
3002D	Get Named Password	XML Document	Wird beim Vorgang „Get Named Password“ („Benanntes Passwort abrufen“) generiert.
3002E	Reset Attributes	XML Document	Tritt auf, wenn ein Ereignis zum Zurücksetzen eines Dokuments an den Herausgeber- oder Abonnentenkanal gesendet wird.
3002F	Add Value - Add Entry	Value	Tritt auf, wenn beim Erstellen eines Objekts ein Wert hinzugefügt wird.

C.2 Serverereignisse

Die Tabellen enthalten die Serverereignisse, die mit Novell Audit protokolliert werden können.

Tabelle C-5 *Serverereignis-Felder: Originator Title, Target Title und Subtarget Title*

EventID	Description	Originator Title	Target Title	Subtarget Title
307D0	Config:Log Events	Server	Driver	Attribute name
307D1	Config:Driver Cache Limit	Server	Driver	Attribute name
307D2	Config:Driver Set	Server	Server	Attribute name
307D3	Config:Driver Start Option	Server	Driver	Attribute name
307D4	Driver Resync	Server	Driver	
307D5	Migrate Application Server	Server	Driver	

EventID	Description	Originator Title	Target Title	Subtarget Title
307D6	Shim Password Set	Server	Driver	Attribute name
307D7	Keyed Password Set	Server	Driver	
307D8	Remote Loader Password Set	Server	Driver	Attribute name

Tabelle C-6 *Serverereignis-Felder: Text1 Title, Text2 Title und Text3 Title*

EventID	Description	Text1 Title	Text2 Title	Text3 Title
307D0	Config:Log Events			Operation
307D1	Config:Driver Cache Limit			
307D2	Config:Driver Set	Driver Set	Type	
307D3	Config:Driver Start Option			Message
307D4	Driver Resync			
307D5	Migrate Applica-tion Server			
307D6	Shim Password Set			
307D7	Keyed Password Set		Type	
307D8	Remote Loader Password Set			

Tabelle C-7 *Serverereignis-Felder: Value1 Title, Value2 Title und Value3 Title*

EventID	Description	Value1 Title	Value2 Title	Value3 Title
307D0	Config:Log Events			Result
307D1	Config:Driver Cache Limit	Limit		Result
307D2	Config:Driver Set			Result
307D3	Config:Driver Start Option	Start option		Result
307D4	Driver Resync			Result
307D5	Migrate Applica-tion Server			Result
307D6	Shim Password Set		Version	Result

EventID	Description	Value1 Title	Value2 Title	Value3 Title
307D7	Keyed Password Set			Result
307D8	Remote Loader Password Set		Version	Result

Tabelle C-8 *Serverereignis-Felder: Data Type und Triggers*

EventID	Description	Data Type	Triggers
307D0	Config:Log Events	Input buffer	Tritt auf, wenn das Attribut zur Ereignisprotokollierung für das Treiber- oder Treibersatzobjekt geändert wird.
307D1	Config:Driver Cache Limit		Tritt auf, wenn das Treiber-Cache-Limit-Attribut für ein Treiberobjekt geändert wird.
307D2	Config:Driver Set	Input buffer	Tritt auf, wenn die Treibersatz/Server-Verknüpfung geändert wird.
307D3	Config:Driver Start Option	Input buffer	Tritt auf, wenn die Treiber-Startoption für ein Treiberobjekt geändert wird.
307D4	Driver Resync		Tritt auf, wenn für einen Treiber eine Neusynchronisierung erteilt wird.
307D5	Migrate Application Server	XML Document	Tritt auf, wenn die Migration des Anwendungsservers ausgeführt wird.
307D6	Shim Password Set		Tritt auf, wenn das Anwendungspasswort festgelegt wird.
307D7	Keyed Password Set		
307D8	Remote Loader Password Set		Tritt auf, wenn das Remote Loader-Passwort festgelegt wird.

C.3 Remote Loader-Ereignisse

Die Tabelle enthält die Remote Loader-Ereignisse, die mit Novell Audit protokolliert werden können.

Tabelle C-9 *Remote Loader-Ereignis-Felder: Originator Title, Target Title und Subtarget Title*

EventID	Description	Originator Title	Triggers
30BB8	Remote Loader Start	Instance	Tritt auf, wenn Remote Loader gestartet wird.
30BB9	Remote Loader Stop	Instance	Tritt auf, wenn der Remote Loader gestoppt wird.

EventID	Description	Originator Title	Triggers
30BBA	Remote Loader Connection Established	Instance	Tritt auf, wenn die Remote Loader-Verbindung hergestellt wird.
30BBB	Remote Loader Connection Dropped	Instance	Tritt auf, wenn die Remote Loader-Verbindung unterbrochen wird.

C.4 Detail-Portlets

Tabelle C-10 *Detail-Portlet-Felder: Originator Title, Target Title und Subtarget Title*

EventID	Description	Originator Title	Target Title	Subtarget Title
31400	Delete_Entity	User Name	Entity DN	Entity Definition
31401	Update_Entity	User Name	Entity DN	Entity Definition

Tabelle C-11 *Detail-Portlet-Felder: Group Title, Group Type und Triggers*

EventID	Description	Group Title	Group Type	Triggers
31400	Delete_Entity	Group Number	Number	Tritt auf, wenn ein Objekt gelöscht wird.
31401	Update_Entity	Group Number	Number	Tritt auf, wenn ein Objekt geändert wird.

C.5 Portlet „Passwort ändern“

Tabelle C-12 *Felder des Portlets „Passwort ändern“: Originator Title, Target Title und Text3 Title*

EventID	Description	Originator Title	Target Title	Text3 Title
31420	Change_Password_Failure	Initiator ID	Target DN	Error Message
31421	Change_Password_Success	Initiator ID	Target DN	

Tabelle C-13 *Felder des Portlets „Passwort ändern“: Value3 Title, Value3 Type und Triggers*

EventID	Description	Value3 Title	Value3 Type	Triggers
31420	Change_Password_Failure	Error Number	Boolean	Tritt auf, wenn bei einer Passwortänderung ein Fehler auftritt.
31421	Change_Password_Success			Tritt auf, wenn eine Passwortänderung erfolgreich ist.

C.6 Portlets „Passwort vergessen“ und „Passwort ändern“

Tabelle C-14 *Felder der Portlets „Passwort vergessen“ und „Passwort ändern“: Originator Title, Target Title und Text3 Title*

EventID	Description	Originator Title	Target Title	Text3 Title
31420	Forgot_Password_Change_Failure	Initiator ID	Target DN	Error Message
31421	Forgot_Password_Change_Success	Initiator ID	Target DN	

Tabelle C-15 *Felder der Portlets „Passwort vergessen“ und „Passwort ändern“: Value3 Title, Value3 Type und Group Title*

EventID	Description	Value3 Title	Value3 Type	Group Title
31420	Forgot_Password_Change_Failure	Error Number	Boolean	Group Number
31421	Forgot_Password_Change_Success			Group Number

Tabelle C-16 *Felder der Portlets „Passwort vergessen“ und „Passwort ändern“: Group Type und Triggers*

EventID	Description	Group Type	Triggers
31420	Forgot_Password_Change_Failure	Number	Tritt auf, wenn bei einer Änderung ein Fehler auftritt.
31421	Forgot_Password_Change_Success	Number	Tritt auf, wenn eine Änderung erfolgreich ist.

C.7 Portlet „Suchliste“

Tabelle C-17 *Felder des Portlets „Suchliste: Originator Title, Target Title und Group Title*

EventID	Description	Originator Title	Target Title	Group Title
31430	Search_Request	User ID	Search Key	User ID
31431	Search_Saved	User ID	Search Key	User ID

Tabelle C-18 *Felder des Portlets „Suchliste: Group Type, Data Title und Data Type*

EventID	Description	Group Type	Data Title	Data Type
31430	Search_Request	Number	Search XML	String

EventID	Description	Group Type	Data Title	Data Type
31431	Search_Saved	Number	Search XML	String

Tabelle C-19 *Felder des Portlets „Suchliste: Triggers*

EventID	Description	Triggers
31430	Search_Request	Tritt auf, wenn ein Benutzer eine Suchanforderung ausführt.
31431	Search_Saved	Tritt auf, wenn der Benutzer „Meine gespeicherten Suchvorgänge“ auswählt.

C.8 Portlet „Erstellen“

Tabelle C-20 *Felder des Portlets „Erstellen“: Originator Title, Target Title und Subtarget Title*

EventID	Description	Originator Title	Target Title	Subtarget Title
31440	Create_Entity	User Name	Entity DN	Entity Definition

Tabelle C-21 *Felder des Portlets „Erstellen“: Triggers*

Event ID	Description	Triggers
31440	Create_Entity	Tritt auf, wenn ein Objekt erstellt wird.

C.9 Sicherheitskontext

Die Tabellen enthalten die Sicherheitsereignisse, die mit Novell Audit protokolliert werden können.

Tabelle C-22 *Sicherheitskontext - Felder: Originator Title, Target Title und Text1 Title*

EventID	Description	Originator Title	Target Title	Text1 Title
31540	Create_Proxy_Definition_Success	Initiator ID	Definition	Detail
31541	Create_Proxy_Definition_Failure	Initiator ID	Definition	Detail
31542	Update_Proxy_Definition_Success	Initiator ID	Definition	Detail
31543	Update_Proxy_Definition_Failure	Initiator ID	Definition	Detail
31544	Delete_Proxy_Definition_Success	Initiator ID	Definition	Detail
31545	Delete_Proxy_Definition_Failure	Initiator ID	Definition	Detail
31546	Create_Delegatee_Definition_Success	Initiator ID	Definition	Detail
31547	Create_Delegatee_Definition_Failure	Initiator ID	Definition	Detail
31548	Update_Delegatee_Definition_Success	Initiator ID	Definition	Detail

EventID	Description	Originator Title	Target Title	Text1 Title
31549	Update_Delegatee_Definition_Failure	Initiator ID	Definition	Detail
3154A	Delete_Delegatee_Definition_Success	Initiator ID	Definition	Detail
3154B	Delete_Delegatee_Definition_Failure	Initiator ID	Definition	Detail
3154C	Create_Availability_Success	Initiator ID	Target	
3154D	Create_Availability_Failure	Initiator ID	Target	Detail
3154E	Delete_Availability_Success	Initiator ID	Target	Detail
3154F	Delete_Availability_Failure	Initiator ID	Target	Detail

Tabelle C-23 *Sicherheitskontext - Felder: Text3 Title, Data Title und Data Type*

EventID	Description	Text3 Title	Data Title	Data Type
31540	Create_Proxy_Definition_Success			
31541	Create_Proxy_Definition_Failure	Error Message	stacktrace	String
31542	Update_Proxy_Definition_Success			
31543	Update_Proxy_Definition_Failure	Error Message	stacktrace	String
31544	Delete_Proxy_Definition_Success			
31545	Delete_Proxy_Definition_Failure	Error Message	stacktrace	String
31546	Create_Delegatee_Definition_Success			
31547	Create_Delegatee_Definition_Failure	Error Message	stacktrace	String
31548	Update_Delegatee_Definition_Success			
31549	Update_Delegatee_Definition_Failure	Error Message	stacktrace	String
3154A	Delete_Delegatee_Definition_Success			
3154B	Delete_Delegatee_Definition_Failure	Error Message	stacktrace	String
3154C	Create_Availability_Success			
3154D	Create_Availability_Failure	Error Message	stacktrace	String
3154E	Delete_Availability_Success			
3154F	Delete_Availability_Failure	Error Message	stacktrace	String

Tabelle C-24 *Sicherheitskontext - Felder: Triggers*

EventID	Description	Triggers
31540	Create_Proxy_Definition_Success	Tritt bei erfolgreicher Erstellung der Vertretungsdefinition auf.
31541	Create_Proxy_Definition_Failure	Tritt bei fehlerhafter Erstellung der Vertretungsdefinition auf.

EventID	Description	Triggers
31542	Update_Proxy_Definition_Success	Tritt bei erfolgreicher Aktualisierung der Vertretungsdefinition auf.
31543	Update_Proxy_Definition_Failure	Tritt bei fehlerhafter Aktualisierung der Vertretungsdefinition auf.
31544	Delete_Proxy_Definition_Success	Tritt bei erfolgreichem Löschen der Vertretungsdefinition auf.
31545	Delete_Proxy_Definition_Failure	Tritt bei fehlerhaftem Löschen der Vertretungsdefinition auf.
31546	Create_Delegatee_Definition_Success	Tritt bei erfolgreicher Erstellung der Delegiertendefinition auf.
31547	Create_Delegatee_Definition_Failure	Tritt bei fehlerhafter Erstellung der Delegiertendefinition auf.
31548	Update_Delegatee_Definition_Success	Tritt bei erfolgreicher Aktualisierung der Delegiertendefinition auf.
31549	Update_Delegatee_Definition_Failure	Tritt bei fehlerhafter Aktualisierung der Delegiertendefinition auf.
3154A	Delete_Delegatee_Definition_Success	Tritt bei erfolgreichem Löschen der Delegiertendefinition auf.
3154B	Delete_Delegatee_Definition_Failure	Tritt bei fehlerhaftem Löschen der Delegiertendefinition auf.
3154C	Create_Availability_Success	Tritt bei erfolgreicher Erstellung des Verfügbarkeitsstatus auf.
3154D	Create_Availability_Failure	Tritt bei fehlerhafter Erstellung des Verfügbarkeitsstatus auf.
3154E	Delete_Availability_Success	Tritt bei erfolgreichem Löschen des Verfügbarkeitsstatus auf.
3154F	Delete_Availability_Failure	Tritt bei fehlerhaftem Löschen des Verfügbarkeitsstatus auf.

C.10 Workflow

Die Tabellen enthalten die Benutzeranwendungsereignisse, die mit Novell Audit protokolliert werden können.

Tabelle C-25 *Workflow-Felder: Originator Title, Target Title und Subtarget Title*

EventID	Description	Originator Title	Target Title	Subtarget Title
31520	Workflow_Error	Initiator ID		
31521	Workflow_Started	Initiator ID		
31522	Workflow_Forwarded	Initiator ID	Recipient	Process Name
31523	Workflow_Reassigned	Initiator ID	Recipient	Process Name

EventID	Description	Originator Title	Target Title	Subtarget Title
31524	Workflow_Approved	Initiator ID	Recipient	Process Name
31525	Workflow_Refused	Initiator ID	Recipient	Process Name
31526	Workflow_Ended	Initiator ID	Recipient	Process Name
31527	Workflow_Claimed	Initiator ID	Recipient	Process Name
31528	Workflow_Unclaimed	Initiator ID	Recipient	Process Name
31529	Workflow_Denied	Initiator ID	Recipient	Process Name
3152A	Workflow_Completed	Initiator ID	Recipient	Process Name
3152B	Workflow_Timedout	Initiator ID	Recipient	Process Name
3152C	User_Message	Initiator ID	Author	
3152D	Provision_Error	Initiator ID	Recipient	Process Name
3152E	Provision_Submitted	Initiator ID	Recipient	Process Name
3152F	Provision_Success	Initiator ID	Recipient	Process Name
31530	Provision_Failure	Initiator ID	Recipient	Process Name
31531	Provision_Granted	Initiator ID	Recipient	Process Name
31532	Provision_Revoked	Initiator ID	Recipient	Process Name
31533	Workflow_Retracted	Initiator ID	Recipient	Process Name

Tabelle C-26 *Workflow-Felder: Text1 Title, Text2 Title und Text3 Title*

EventID	Description	Text1 Title	Text2 Title	Text3 Title
31520	Workflow_Error	Activity	Process ID	Error Message
31521	Workflow_Started	Activity	Process ID	
31522	Workflow_Forwarded	Activity	Process ID	
31523	Workflow_Reassigned	Activity	Process ID	
31524	Workflow_Approved	Activity	Process ID	Secondary User
31525	Workflow_Refused	Activity	Process ID	Secondary User
31526	Workflow_Ended	Activity	Process ID	
31527	Workflow_Claimed	Activity	Process ID	Secondary User
31528	Workflow_Unclaimed	Activity	Process ID	Secondary User
31529	Workflow_Denied	Activity	Process ID	Secondary User
3152A	Workflow_Completed	Activity	Process ID	
3152B	Workflow_Timedout	Activity	Process ID	
3152C	User_Message		Message	

EventID	Description	Text1 Title	Text2 Title	Text3 Title
3152D	Provision_Error	Activity	Process ID	Error Message
3152E	Provision_Submitted	Activity	Process ID	
3152F	Provision_Success	Activity	Process ID	
31530	Provision_Failure	Activity	Process ID	
31531	Provision_Granted	Activity	Process ID	
31532	Provision_Revoked	Activity	Process ID	
31533	Workflow_Retracted	Activity	Process ID	Secondary User

Tabelle C-27 *Workflow-Felder: Value3 Title, Value3 Type und Data Title*

EventID	Description	Value3 Title	Value3 Type	Data Title
31520	Workflow_Error	Error Number	Boolean	stacktrace
31521	Workflow_Started			
31522	Workflow_Forwarded			
31523	Workflow_Reassigned			
31524	Workflow_Approved			Secondary User Type
31525	Workflow_Refused			Secondary User Type
31526	Workflow_Ended			
31527	Workflow_Claimed			Secondary User Type
31528	Workflow_Unclaimed			Secondary User Type
31529	Workflow_Denied			Secondary User Type
3152A	Workflow_Completed			
3152B	Workflow_Timedout			
3152C	User_Message			
3152D	Provision_Error	Error Number	Boolean	stacktrace
3152E	Provision_Submitted			
3152F	Provision_Success			
31530	Provision_Failure			
31531	Provision_Granted			
31532	Provision_Revoked			

EventID	Description	Value3 Title	Value3 Type	Data Title
31533	Workflow_Retracted			Secondary User Type

Tabelle C-28 *Workflow-Felder: Data Type und Triggers*

EventID	Description	Data Type	Triggers
31520	Workflow_Error	String	Viele Elemente können dieses Ereignis auslösen.
31521	Workflow_Started		Tritt auf, wenn der Workflow gestartet wird.
31522	Workflow_Forwarded		Tritt auf, wenn der Workflow weitergeleitet wird.
31523	Workflow_Reassigned		Tritt auf, wenn der Workflow neu zugeordnet wird.
31524	Workflow_Approved	String	Tritt auf, wenn der Workflow genehmigt wird.
31525	Workflow_Refused	String	Tritt auf, wenn der Workflow abgelehnt wird.
31526	Workflow_Ended		Tritt auf, wenn der Workflow beendet wird.
31527	Workflow_Claimed	String	Tritt auf, wenn der Workflow beansprucht wird.
31528	Workflow_Unclaimed	String	
31529	Workflow_Denied	String	Tritt auf, wenn der Workflow zurückgewiesen wird.
3152A	Workflow_Completed		Tritt auf, wenn der Workflow abgeschlossen wird.
3152B	Workflow_Timedout		Tritt auf, wenn es beim Workflow eine Zeitüberschreitung gibt.
3152C	User_Message		
3152D	Provision_Error	String	Viele Elemente können dieses Ereignis auslösen.
3152E	Provision_Submitted		
3152F	Provision_Success		
31530	Provision_Failure		
31531	Provision_Granted		
31532	Provision_Revoked		
31533	Workflow_Retracted	String	Tritt auf, wenn der Workflow zurückgezogen wird.

C.11 Berichte

Im Folgenden finden Sie Beispiele für Novell Audit-Berichte. Es können folgende Berichte ausgeführt werden:

- Administrative Action Report
- Historical Approval Flow Report
- Resource Provisioning Report
- Specific User Audit Trail
- Specific User Provisioning
- User Provisioning

Abbildung C-1 *Administrative Action Report*

Novell® Audit Report for Identity Manager

Administrative Action Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 5

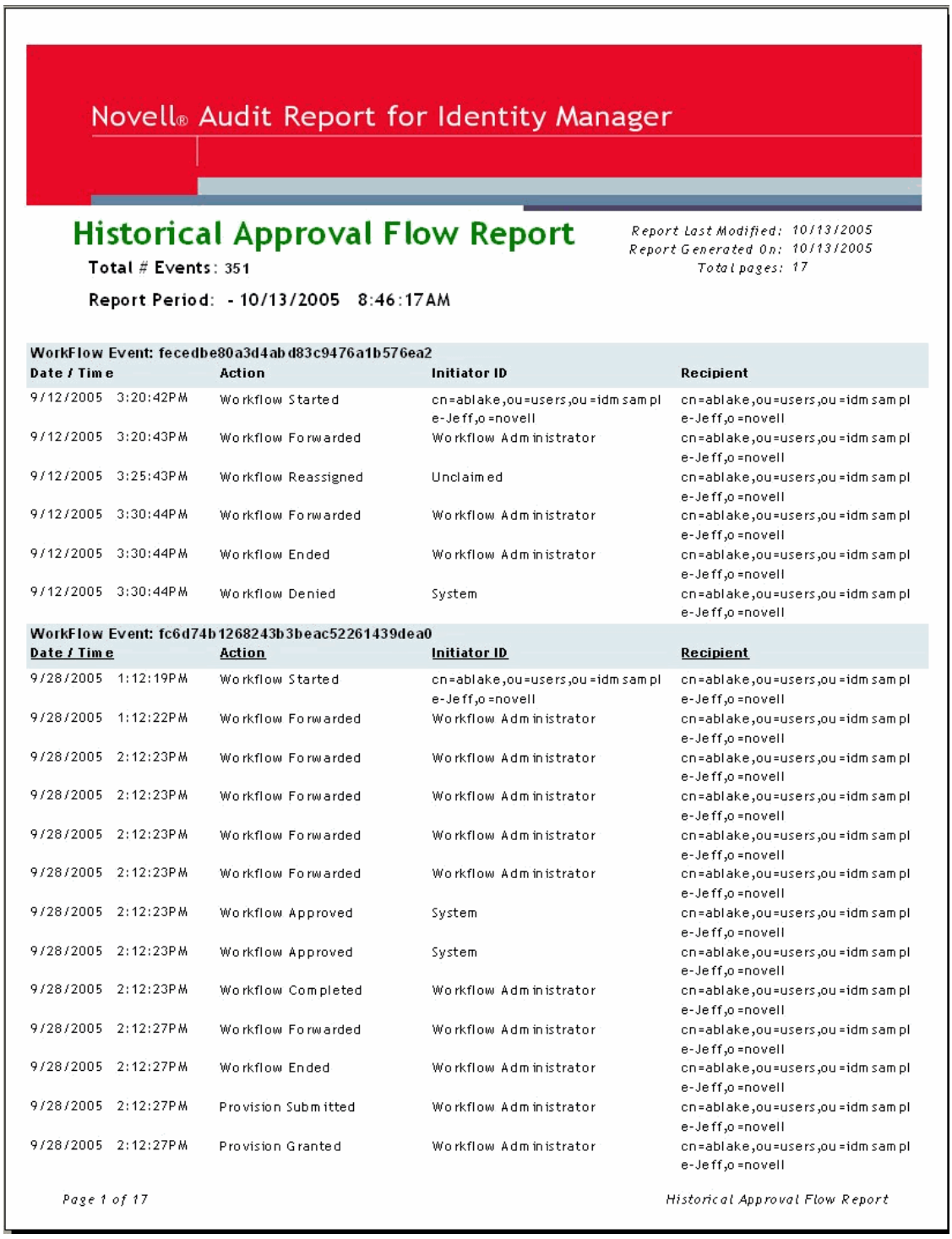
Total # Events: 121

Report Period: - 10/13/2005 8:43:50AM

Date / Time	Administrator	Subject	Action
8/18/2005 5:45:17PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:07:40PM	cn=admin,ou=idmsample-cts10,o=novell	cn=testCreateUser11,ou=users,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:09:05PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:12:50PM	cn=admin,ou=idmsample-cts10,o=novell	cn=testCreateUser11,ou=users,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:13:39PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/23/2005 4:56:39PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Deleted
8/31/2005 12:01:55PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:02:18PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 12:19:07PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:19:31PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 12:27:58PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:28:22PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 2:59:39PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 3:24:30PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 8:11:59PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=testCreateUser,ou=users,ou=idmsample-Jeff,o=novell	Entity Deleted
8/31/2005 8:12:23PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-Jeff,o=novell	Entity Deleted
8/31/2005 8:12:55PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=admin,ou=idmsample-Jeff,o=novell	Entity Updated
8/31/2005 8:13:03PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=admin,ou=idmsample-Jeff,o=novell	Entity Updated
9/1/2005 10:29:53AM	cn=admin,ou=idmsample-Jeff,o=novell	cn=aa,ou=users,ou=idmsample-Jeff,o=novell	Entity Deleted
9/1/2005 11:31:45AM	cn=admin,ou=idmsample,o=novell	cn=asoprano,ou=users,ou=idmsample,o=novell	Entity Created

Page 1 of 5 Administrative Action Report

Abbildung C-2 *Historical Approval Flow Report*



Novell® Audit Report for Identity Manager

Historical Approval Flow Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 17

Total # Events: 351

Report Period: - 10/13/2005 8:46:17AM

WorkFlow Event: fecedbe80a3d4abd83c9476a1b576ea2

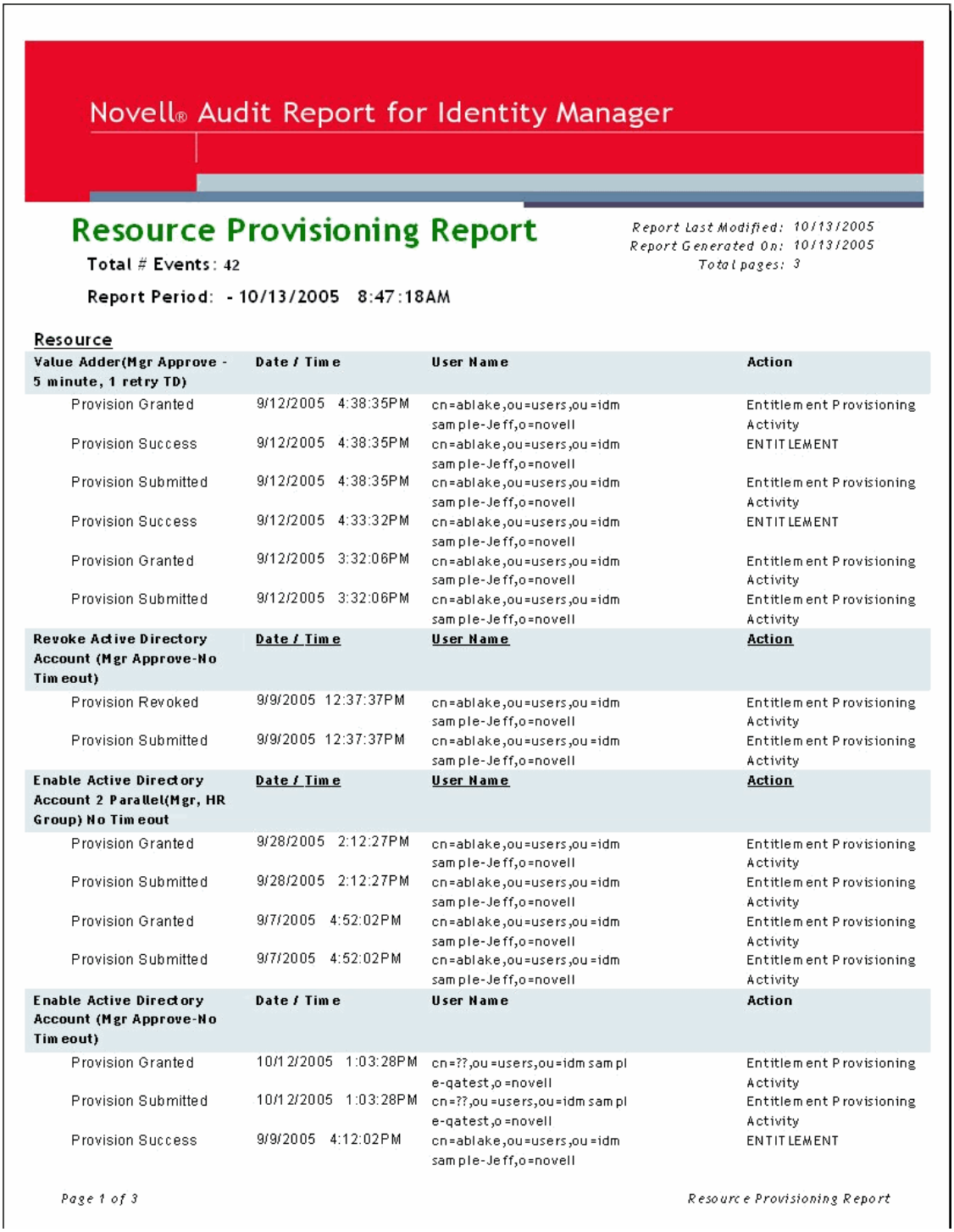
Date / Time	Action	Initiator ID	Recipient
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Denied	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

WorkFlow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID	Recipient
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Approved	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Approved	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

Page 1 of 17 Historical Approval Flow Report

Abbildung C-3 *Resource Provisioning Report*



Novell® Audit Report for Identity Manager

Resource Provisioning Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 3

Total # Events: 42

Report Period: - 10/13/2005 8:47:18AM

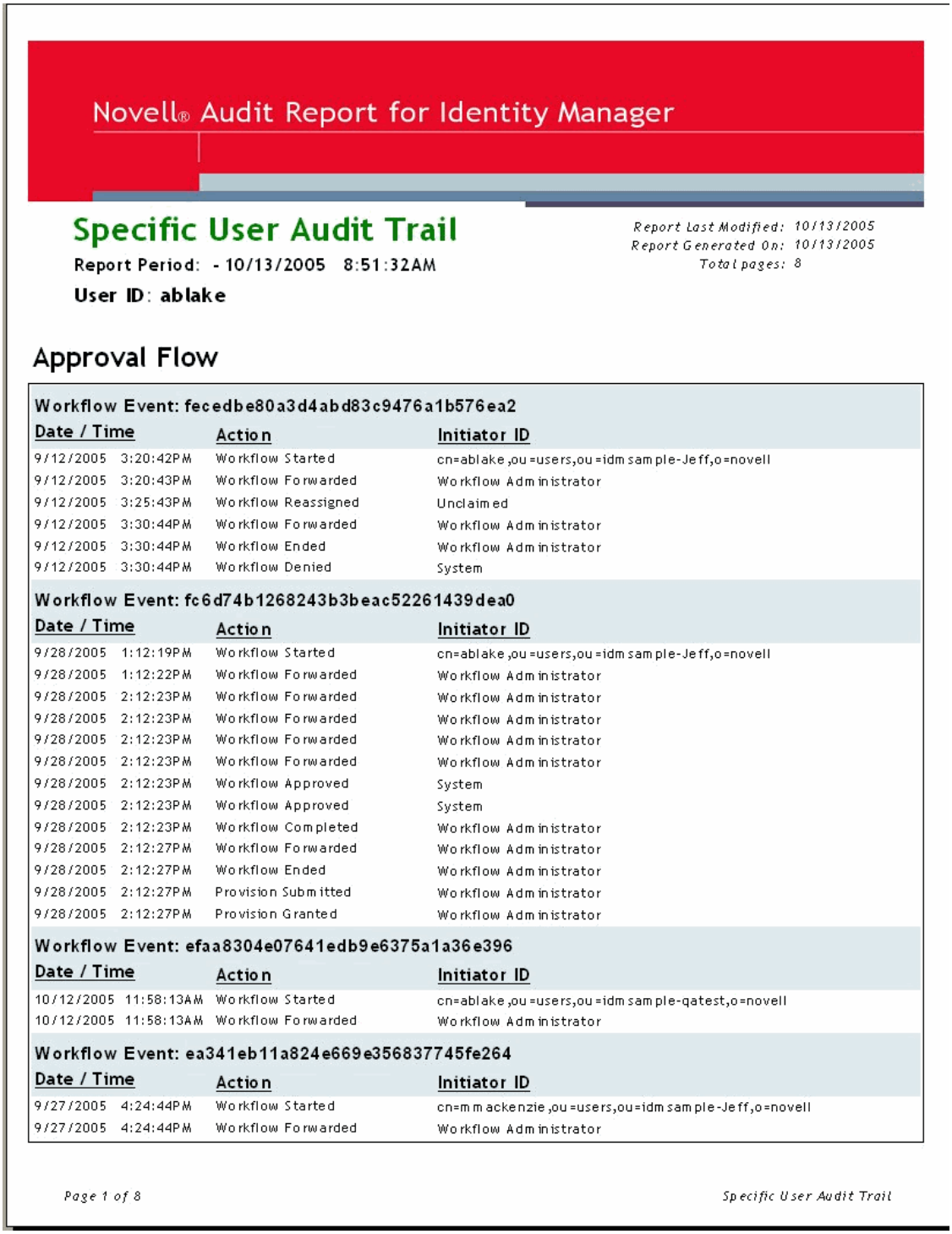
Resource

Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Date / Time	User Name	Action
Provision Granted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Revoke Active Directory Account (Mgr Approve-No Timeout)	**Date / Time**	**User Name**	**Action**
Provision Revoked	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	**Date / Time**	**User Name**	**Action**
Provision Granted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Granted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Enable Active Directory Account (Mgr Approve-No Timeout)	**Date / Time**	**User Name**	**Action**
Provision Granted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idm sample-qatest,o=novell	Entitlement Provisioning Activity
Provision Submitted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idm sample-qatest,o=novell	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT

Page 1 of 3

Resource Provisioning Report

Abbildung C-4 *Specific User Audit Trail 1*



Novell® Audit Report for Identity Manager

Specific User Audit Trail

Report Period: - 10/13/2005 8:51:32AM

User ID: ablake

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 8

Approval Flow

Workflow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Denied	System

Workflow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator

Workflow Event: efaa8304e07641edb9e6375a1a36e396

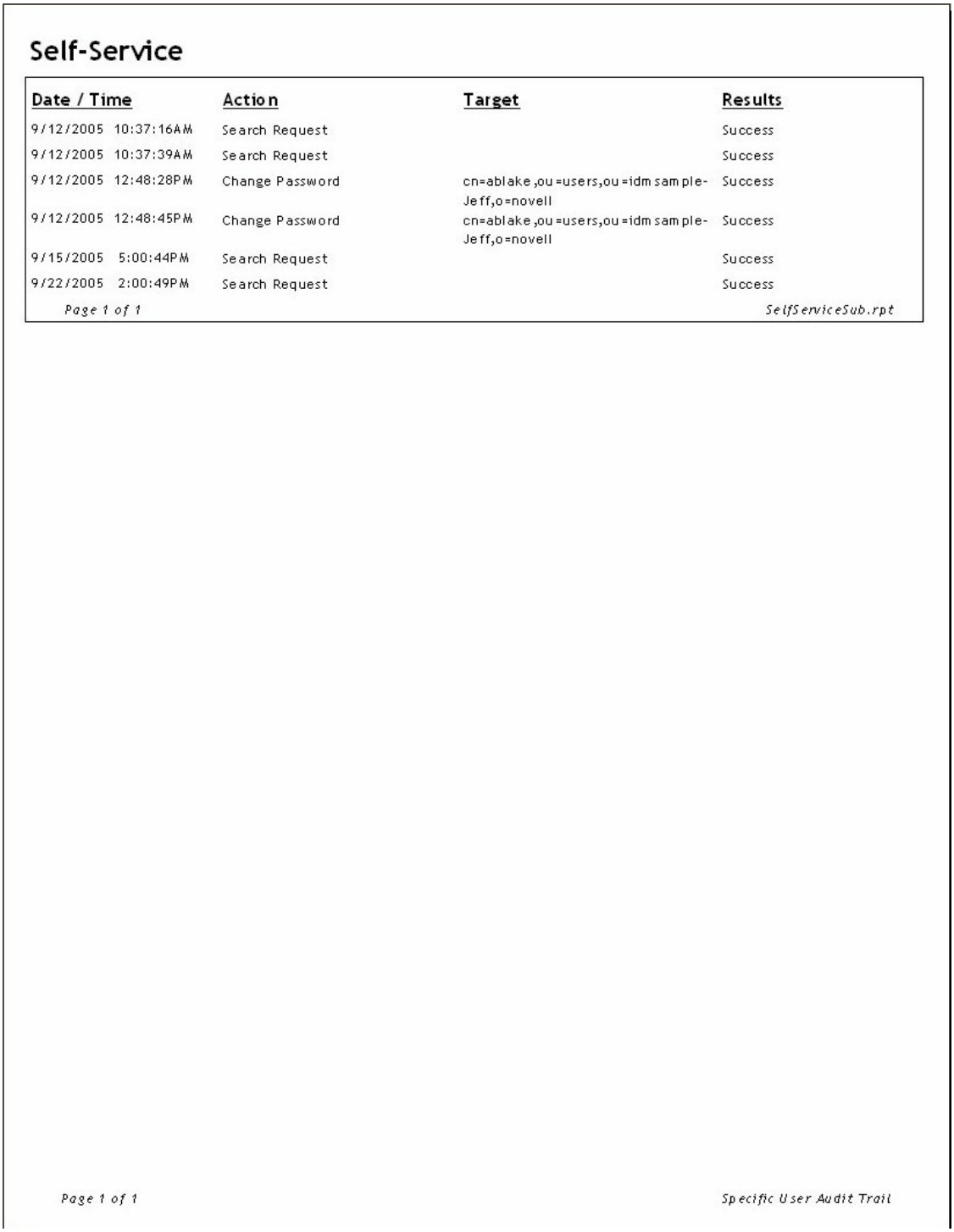
Date / Time	Action	Initiator ID
10/12/2005 11:58:13AM	Workflow Started	cn=ablake,ou=users,ou=idmsample-qatest,o=novell
10/12/2005 11:58:13AM	Workflow Forwarded	Workflow Administrator

Workflow Event: ea341eb11a824e669e356837745fe264

Date / Time	Action	Initiator ID
9/27/2005 4:24:44PM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample-Jeff,o=novell
9/27/2005 4:24:44PM	Workflow Forwarded	Workflow Administrator

Page 1 of 8 *Specific User Audit Trail*

Abbildung C-5 *Specific User Audit Trail 2*



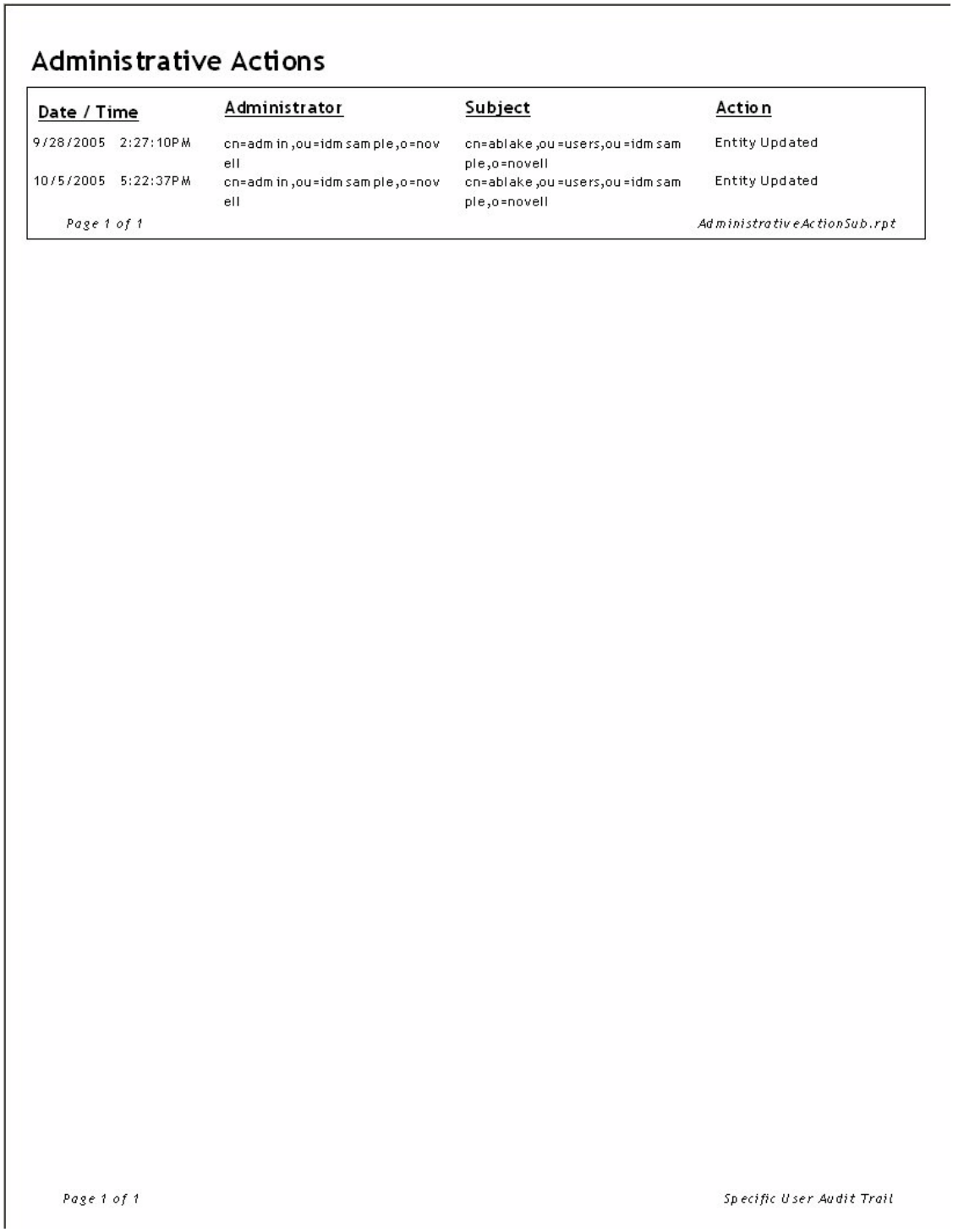
Self-Service

Date / Time	Action	Target	Results
9/12/2005 10:37:16AM	Search Request		Success
9/12/2005 10:37:39AM	Search Request		Success
9/12/2005 12:48:28PM	Change Password	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Success
9/12/2005 12:48:45PM	Change Password	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Success
9/15/2005 5:00:44PM	Search Request		Success
9/22/2005 2:00:49PM	Search Request		Success

Page 1 of 1 *SelfServiceSub.rpt*

Page 1 of 1 *Specific User Audit Trail*

Abbildung C-6 *Specific User Audit Trail 3*



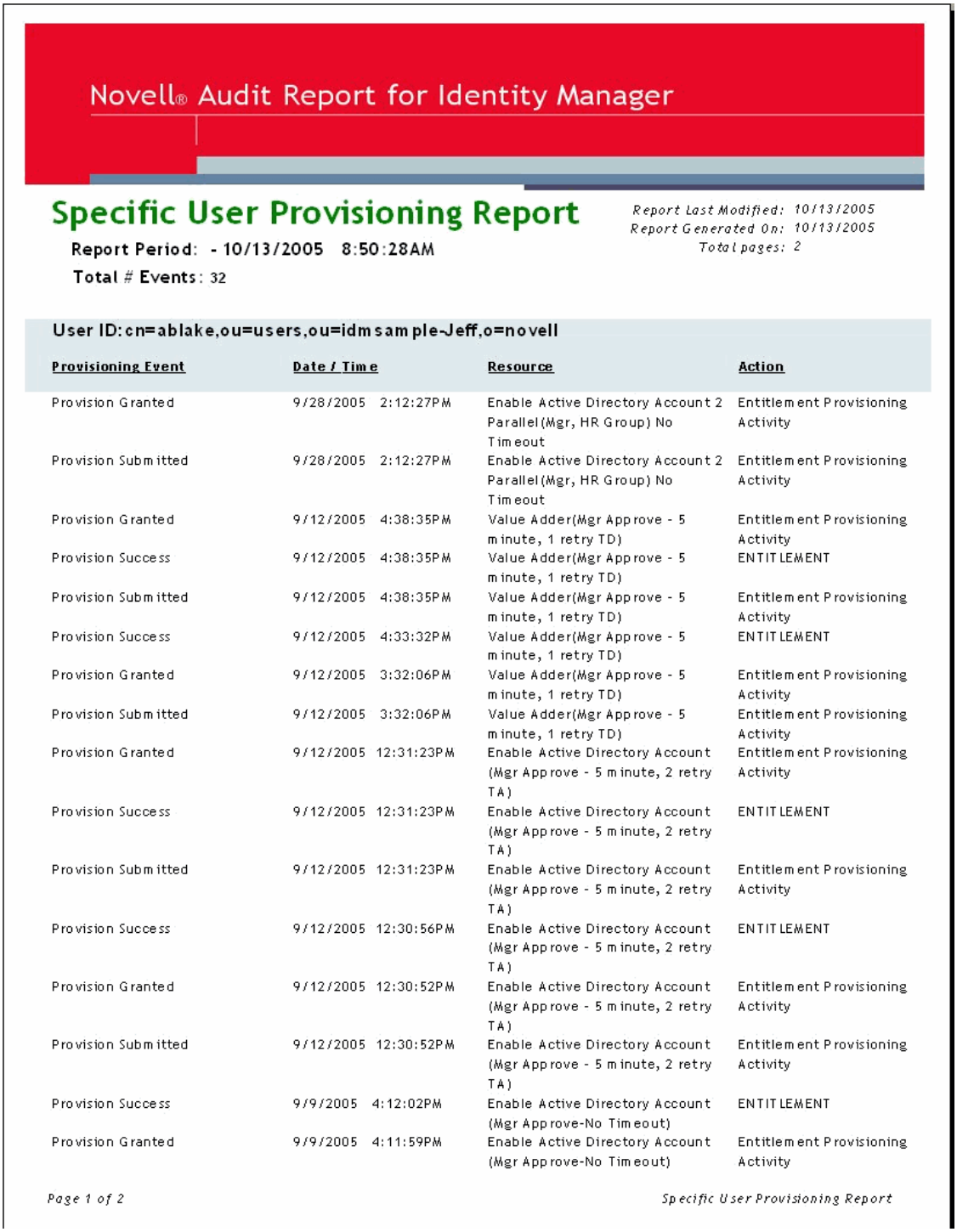
Administrative Actions

Date / Time	Administrator	Subject	Action
9/28/2005 2:27:10PM	cn=admin,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell	Entity Updated
10/5/2005 5:22:37PM	cn=admin,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell	Entity Updated

Page 1 of 1 *AdministrativeActionSub.rpt*

Page 1 of 1 *Specific User Audit Trail*

Abbildung C-7 *Specific User Provisioning Report*



Novell® Audit Report for Identity Manager

Specific User Provisioning Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 2

Report Period: - 10/13/2005 8:50:28AM

Total # Events: 32

User ID: cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

Provisioning Event	Date / Time	Resource	Action
Provision Granted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Granted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Granted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Submitted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:30:56PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Granted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	Enable Active Directory Account (Mgr Approve-No Timeout)	ENTITLEMENT
Provision Granted	9/9/2005 4:11:59PM	Enable Active Directory Account (Mgr Approve-No Timeout)	Entitlement Provisioning Activity

Page 1 of 2 *Specific User Provisioning Report*

Abbildung C-8 *User Provisioning Report*

Novell® Audit Report for Identity Manager

User Provisioning Report

Total # Events: 42

Report Period: - 10/13/2005 8:54:20AM

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 3

User

cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Date / Time	Resource	Action
Provision Granted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Granted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Granted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Submitted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:30:56PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Granted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	Enable Active Directory Account (Mgr Approve-No Timeout)	ENTITLEMENT
Provision Granted	9/9/2005 4:11:59PM	Enable Active Directory Account (Mgr Approve-No Timeout)	Entitlement Provisioning Activity

Page 1 of 3

User Provisioning Report

Service-Treiber für manuelle Aufgaben: Ersetzungsdaten

D

Ersetzungsdaten sind Teil von XML-Dokumenten, die als Schablonen zum Erstellen von Emails, Webseiten und XDS-Dokumenten verwendet werden. Die eigentliche Ersetzung erfolgt durch die Verarbeitung des Schablonendokuments mit einer XSLT-Formatvorlage, die die Ersetzung als Teil der Erstellung des Ausgabedokuments durchführt.

Ersetzungsdaten werden dem Service-Treiber für manuelle Aufgaben durch verschiedene Mechanismen auf dem Abonnenten- und Herausgeberkanal zur Verfügung gestellt.

Abonnentenkanal

- Die Ersetzungsdaten werden als Teil des <mail>-Elements zur Verfügung gestellt.
- Ein Teil der Ersetzungsdaten wird möglicherweise in Form von URL-Daten zur Verfügung gestellt. Wenn URL-Daten zur Verfügung gestellt werden, werden sie verarbeitet, vervollständigt und durch automatische Datenelemente ersetzt (siehe Anhang E, „Service-Treiber für manuelle Aufgaben: Automatische Ersetzungsdatenelemente“, auf Seite 327).
- Wenn im <mail>-Element angegeben ist, dass ein Wert für „association“ gebildet werden soll (d. h., das <mail>-Element verfügt über ein „src-dn“-Attribut), wird ein automatisches Datenelement namens “association” zu den Ersetzungsdaten hinzugefügt.

Herausgeberkanal

- Ersetzungsdaten werden in den HTTP URL-Daten und den HTTP POST-Daten zur Verfügung gestellt.
- Bevor die Ersetzungsdaten zur Schablonenverarbeitung verwendet werden, erhalten sie automatische URL-Ersetzungsdatenelemente.

Ersetzungsdaten liegen bei der Schablonenverarbeitung als XML-Dokument vor. Das Ersetzungsdatendokument wird an die Formatvorlage weitergeleitet, die die Schablone als Parameter namens „replacement-data“ verarbeitet. Das XML-Dokument wird direkt von der Formatvorlage verarbeitet, wenn keine Schablone verwendet wird.

D.1 Datensicherheit

Datenelemente werden über eine vom Abonnentenkanal versendete URL vom Abonnentenkanal an den Herausgeberkanal weitergeleitet. Eine Änderung der Datenelemente in der URL stellt eine Sicherheitsbedrohung dar. Wenn z. B. die „responder-dn“-Werte in der vom Abonnentenkanal zur Verfügung gestellten URL in der URL, die an den Webserver des Herausgeberkanals weitergeleitet wird, durch den DN eines anderen Benutzers ersetzt werden, könnte dadurch ein unbefugter Benutzer Daten in eDirectory ändern.

Damit sichergestellt ist, dass die Daten in der übertragenen URL den ursprünglichen Daten vom Abonnentenkanal entsprechen, werden geschützte Daten bereitgestellt. Geschützte Daten sind Daten, die aus Gründen der Sicherheit nicht geändert werden können. Diese Daten sind je nach Konfiguration unterschiedlich, enthalten aber immer Datenelemente vom Typ „responder-dn“ sowie Elemente, die den eDirectory-Objekten entsprechen, deren Werte geändert werden müssen.

Datenelemente werden durch Verschlüsselung der Originalwerte geschützt. Diese verschlüsselten Werte werden anschließend in einer URL-Query-Zeichenkette platziert. Wenn der Webserver des Herausgeberkanals die verschlüsselten Werte empfängt, entschlüsselt der Herausgeberkanal die Werte und vergleicht sie mit den unverschlüsselten Datenelementen, die von einer HTTP GET- oder HTTP POST-Anforderung zur Verfügung gestellt werden.

Wenn eine Instanz eines Datenelements in den verschlüsselten Daten enthalten ist, muss ein unverschlüsselter Datenelementwert einem der verschlüsselten Datenelementwerte entsprechen. Wenn der unverschlüsselte Datenelementwert keinem der verschlüsselten Datenelementwerte entspricht, wird die HTTP-Anforderung vom Webserver des Herausgeberkanals zurückgewiesen.

Darüber hinaus werden alle HTTP POST-Anforderungen zurückgewiesen, die keine geschützten Daten enthalten.

Beispiel

In einer HTTP POST-Anforderung verwendet der Webserver des Herausgeberkanals die unverschlüsselten POST-Daten namens „responder-dn“ zur Überprüfung des Passworts, das in den POST-Daten enthalten ist. Diese Überprüfung dient der Authentifizierung des antwortenden Benutzers anhand seines eDirectory-Objekts.

Angenommen, der Inhalt des <url-query>-Elements des Abonnentenkanals enthält die folgenden zwei Datenelemente:

```
<item name="responder-dn" protect="yes">\PERIN-TAO\novell\phb</item>

<item name="responder-dn" protect="yes">\PERIN-TAO\novell\carol</item>
```

Die vom Abonnentenkanal erzeugte URL enthält dann in den geschützten Daten beide „responder-dn“-Werte.

Angenommen, ein böswilliger Benutzer erhält diese URL, die per Email versendet wurde. Er verwendet die URL zum Abrufen des HTML-Formulars, über das die Benutzer die Daten eines eDirectory-Objekts ändern können.

Der böswillige Benutzer verwendet in der HTTP POST-Anforderung, die an den Webserver gesendet wird, als unverschlüsselten „responder-dn“-Wert seinen DN von eDirectory (responder-dn=\PERIN-TAO\novell\wally). Des Weiteren überträgt er auch sein eigenes Passwort in den POST-Daten, damit die Authentifizierung durch den Webserver erfolgreich verläuft.

Wenn die HTTP POST-Daten jedoch beim Webserver des Herausgeberkanals eingehen, wird der Wert „\PERIN-TAO\novell\wally“ in den verschlüsselten geschützten Daten nicht gefunden und die POST-Anforderung wird zurückgewiesen.

D.2 XML-Elemente

Im Folgenden werden die Elemente erläutert, aus denen ein Ersetzungsdatendokument besteht. Wenn für ein Element keine XML-Attribute beschrieben werden, sind diese für das entsprechende Attribut nicht zulässig.

D.2.1 <replacement-data>

Das Element <replacement-data> kann an folgenden Stellen angezeigt werden:

1. Als untergeordnetes Element des <message>-Elements unterhalb eines <mail>-Elements des Abonnentenkanals.

   Der Service-Treiber für manuelle Aufgaben verarbeitet das zur Verfügung gestellte <replacement-data>-Element zu einem eigenständigen <replacement-data>-Element, das bei der Schablonenverarbeitung verwendet wird. Das Element wird wie folgt verarbeitet:

   a. Wurde für das umschließende <mail>-Element ein association-Wert erstellt, wird den Ersetzungsdaten ein <item name="association">-Element hinzugefügt. Der Wert des erstellten Elements ist der association-Wert, der an Identity Manager zurückgegeben wird.

   b. Verfügt das <replacement-data>-Element über ein untergeordnetes <url-data>-Element, wird das <url-data>-Element durch verschiedene <item>-Elemente ersetzt, die erstellte URL-Daten enthalten. Siehe „<url-data>“ und „<url-query>“.

2. Als eigenständiges Element auf oberster Ebene eines Ersetzungsdatendokuments, das zur Erstellung eines Dokuments anhand einer Formatvorlage auf dem Abonnenten- oder Herausgeberkanal verwendet wird.

D.2.2 <item>

Das <item>-Element kann den Elementen <replacement-data>, <url-data> oder <url-query> untergeordnet sein. Der Inhalt des <item>-Elements ist der Text, der beim Austauschen der Ersetzungs-Token in Schablonen verwendet wird. <item>-Elemente werden immer mithilfe des „name“-Attributs benannt.

<item>-Attribute

name: Der Wert dieses Attributs gibt den Namen an, unter dem sich die Ersetzungs-Token auf das Attribut beziehen. Wenn z. B. der Wert des „name“-Attributs „manager“ ist, wird das Ersetzungs-Token $manager$ durch den im Element <item name="manager"> enthaltenen Wert ersetzt. Die Verwendung des „name“-Attributs ist obligatorisch.

protect: Bei <item>-Elementen, die untergeordnete Elemente des <url-query>-Elements sind, gibt dieses Attribut an, ob das Element in der URL-Query-Zeichenkette (siehe <url-query>) zum Abschnitt mit den geschützten Daten hinzugefügt werden soll. Wenn das „protect“-Attribut vorhanden ist, muss es auf den Wert „yes“ gesetzt sein.

Vordefinierte <item>-Namen

Bestimmte <item>-Elemente haben entweder auf dem Abonnenten- oder dem Herausgeberkanal (oder auf beiden Kanälen) eine vordefinierte Bedeutung.

template: Der Herausgeberkanal verarbeitet den Wert des „template“-Elements als Namen des Schablonendokuments, das bei der Generierung einer Antwort auf eine HTTP GET-Anforderung verwendet werden soll.

Der Wert wird in den URL-Query-Daten platziert, wenn <item name="template"> auf dem Abonnentenkanal als untergeordnetes Element des <url-query>-Elements angezeigt wird. Auf diese Weise wird der Name des Schablonendokuments, das bei der Beantwortung der HTTP GET-Anforderung verwendet werden soll, an den Webserver des Herausgeberkanals übergeben.

responder-dn: Der Herausgeberkanal verwendet den Wert des „responder-dn“-item-Elements in den HTTP POST-Daten als den DN des eDirectory-Objekts, anhand dessen das in den HTTP POST-Daten enthaltene Passwort bestätigt wird.

Der Webserver weist alle HTTP POST-Anforderungen zurück, die keinen Wert für „responder-dn“ und „password“ enthalten. Darüber hinaus wird die Anforderung zurückgewiesen, wenn in den HTTP POST-Daten kein item-Element vom Typ „protected-data“ vorhanden ist.

Der Abonnentenkanal stellt ein oder mehrere Elemente vom Typ <item name=“responder-dn” protect=“yes”> unter dem <url-query>-Element zur Verfügung. Da die „responder-dn“-item-Elemente zur Benutzerauthentifizierung verwendet werden, müssen sie geschützt werden.

password: Dieses Element wird dem Webserver des Herausgeberkanals über HTTP POST-Daten zur Verfügung gestellt. Dieses item-Element beinhaltet das Passwort, das anhand des eDirectory-Objekts überprüft wird, das durch das „responder-dn“-item-Element in den POST-Daten festgelegt ist. Das item-Element „password“ wird in der Regel in das HTML-Formular eingegeben, mit dem die HTTP POST-Anforderung erzeugt wird.

Beispiel:

```
<INPUT TYPE= "password" NAME="password" SIZE="20" MAXLENGTH="40"/>
```

response-template: Dieses Element wird dem Webserver über HTTP POST-Daten zur Verfügung gestellt. Mit ihm wird die Webseite generiert, die als Antwort auf die POST-Anforderung verwendet wird. Das Element wird in der Regel als verstecktes „INPUT“-Element in das HTML-Formular angegeben, mit dem die HTTP POST-Anforderung erzeugt wird.

Beispiel:

```
<INPUT TYPE="hidden" NAME="response-template" VALUE="post_form.xml"/>
```

response-stylesheet: Dieses Element wird dem Webserver über HTTP POST-Daten zur Verfügung gestellt. Mit ihm wird die Webseite generiert, die als Antwort auf die POST-Anforderung verwendet wird. Das Element wird in der Regel als verstecktes „INPUT“-Element in dem HTML-Formular angegeben, mit dem die HTTP POST-Anforderung erzeugt wird.

Beispiel:

```
<INPUT TYPE="hidden" NAME="response-stylesheet"
VALUE="process_template.xsl"/>
```

auth-template: Dieses Element wird dem Webserver über HTTP POST-Daten zur Verfügung gestellt. Es wird zur Generierung der Webseite bereitgestellt, die als Antwort auf die POST-Anforderung erzeugt wird, wenn bei der Authentifizierung des Benutzers ein Fehler auftritt. Das item-Element „auth-template“ wird in der Regel als verstecktes „INPUT“-Element in das HTML-Formular angegeben, mit dem die HTTP POST-Anforderung erzeugt wird.

Beispiel:

```
<INPUT TYPE="hidden" NAME="auth-template" VALUE="auth_response.xml"/>
```

auth-stylesheet: Dieses Element wird dem Webserver über HTTP POST-Daten zur Verfügung gestellt. Es wird zur Generierung der Webseite bereitgestellt, die als Antwort auf die POST-

Anforderung erzeugt wird, wenn bei der Authentifizierung des Benutzers ein Fehler auftritt. Das item-Element „auth-template“ wird in der Regel als verstecktes „INPUT“-Element in das HTML-Formular angegeben, mit dem die HTTP POST-Anforderung erzeugt wird.

Beispiel:

```
<INPUT TYPE="hidden" NAME="auth-stylesheet"
VALUE="process_template.xsl"/>
```

protected-data: Das item-Element „protected-data“ enthält die vom Abonnentenkanal erstellten verschlüsselten Daten. Auf dem Abonnentenkanal wird dieses item-Element automatisch zur Verfügung gestellt.

Auf dem Herausgeberkanal wird das item-Element „protected-data“ für eine HTTP GET-Anforderung von der URL-Query-Zeichenkette und für eine HTTP POST-Anforderung von den POST-Daten zur Verfügung gestellt.

Es wird in der Regel von der HTTP GET-Anforderung an die Webseite übergeben. Dort wird die HTTP POST-Anforderung über ein Ersetzungs-Token in der Schablone generiert, die zur Erstellung der Antwort auf HTTP GET verwendet wird.

Beispiel:

```
<INPUT TYPE="hidden" NAME="protected-data" VALUE="$protected-data$"/>
```

D.2.3 <url-data>

Auf dem Abonnentenkanal ist das Element <url-data> dem Element <replacement-data> untergeordnet, das sich unterhalb des <message>-Elements befindet. Es enthält <item>-Elemente, die zur Erzeugung der URL und verwandter Datenelemente der Schablone zur Verfügung gestellt werden, die zur Erstellung der Email verwendet wird. Es enthält außerdem das <url-query>-Element.

URLs bestehen aus fünf Teilen, die der Service-Treiber für manuelle Aufgaben verwenden kann:

1. Ein Schema wie http, https oder ftp.
2. Ein Host wie z. B. www.novell.com oder 192.168.0.1.
3. Eine Portnummer. Hierbei handelt es sich um einen Doppelpunkt gefolgt von einer Ganzzahl, z. B. :80 oder :8180.
4. Eine Datei- oder Ressourcenangabe. Dies ist in der Regel ein Dateiname, der Pfadangaben enthalten kann, z. B. stylesheets/process_template.xsl.
5. Eine Query-Zeichenkette. Hierbei handelt es sich um eine Sammlung von Name/Wert-Paaren, die durch &-Zeichen voneinander getrennt sind, z. B. template=form_template.xml&protected-data=AabABJKEL=.

Vordefinierte <item>-Namen unter <url-data>

<item>-Elemente unterhalb des <url-data>-Elements werden ignoriert, sofern sie nicht zu den nachfolgend aufgeführten Typen gehören. Alle diese Elemente sind optional.

file: Dieses Element gibt den Dateiteil der URL an. Wenn es mit dem Webserver des Herausgeberkanals verwendet wird, gibt das item-Element „file“ die Formatvorlage an, mit der die HTML-Startseite erstellt werden soll, die beim Aufruf der URL angezeigt wird. Wenn es nicht auf dem Webserver des Herausgeberkanals, sondern auf einem anderen Server verwendet wird, gibt das item-Element „file“ den Namen der Ressource an, auf die die URL verweist.

Ist dieses file-Element nicht vorhanden, wird standardmäßig auf process_template.xsl verwiesen.

scheme: Optionales item-Element unterhalb des <url-data>-Elements. Sofern vorhanden, gibt es das URL-Schema an (z. B. http oder ftp). Dieses item-Element wird in der Regel nur verwendet, wenn die URL nicht auf den Webserver des Herausgeberkanals, sondern auf einen anderen Server verweist.

Wenn das „scheme“-Element nicht vorhanden ist, wird je nach Konfiguration des Webservers des Herausgeberkanals standardmäßig auf http oder https als URL-Schema verwiesen.

host: Optionales item-Element unterhalb des <url-data>-Elements. Sofern vorhanden, gibt es den URL-Host an. Dieses item-Element wird in der Regel nur verwendet, wenn die URL nicht auf den Webserver des Herausgeberkanals, sondern auf einen anderen Server verweist.

Wenn das „host“-item-Element nicht angezeigt wird, wird der URL-Host standardmäßig auf die IP-Adresse des Servers gesetzt, auf dem der Service-Treiber für manuelle Aufgaben ausgeführt wird (d. h. auf die IP-Adresse des Webservers des Herausgeberkanals).

port: Optionales item-Element unterhalb des <url-data>-Elements. Sofern vorhanden, gibt es den Port für die URL an. Dieses item-Element wird in der Regel nur verwendet, wenn die URL nicht auf den Webserver des Herausgeberkanals, sondern auf einen anderen Server verweist.

Wenn das „port“-item-Element nicht vorhanden ist, wird der URL-Port standardmäßig auf den Port gesetzt, auf dem der Webserver des Herausgeberkanals ausgeführt wird.

D.2.4 <url-query>

Das <url-query>-Element ist dem <url-data>-Element untergeordnet. Es enthält <item>-Elemente, die zur Erzeugung des Abfrageteils der URL verwendet werden, die per Email versendet wird.

Alle item-Elemente, die dem <url-query>-Element untergeordnet sind, werden in der Form name=“value” in die Query-Zeichenkette eingefügt, wobei „name“ der Wert des Namensattributs des <item>-Elements und „value“ der Inhalt des <item>-Elements ist.

Item-Elemente, die unterhalb des Elements <url-query> angezeigt werden, verfügen möglicherweise über ein „protect“-Attribut mit dem Wert „yes“. Ist dies der Fall, sind die Namen und Werte von „item“ verschlüsselt und werden innerhalb eines generierten Name/Wert-Paars in der URL-Query-Zeichenkette platziert. Der Name des generierten Werts lautet „protected-data“. Der Wert ist das mit Base64 kodierte und verschlüsselte Name/Wert-Paar (oder mehrere Paare für mehrwertige Attribute).

Durch das Schützen von Daten wird sichergestellt, dass die Daten nicht geändert werden können, wenn die URL an den Webserver des Herausgeberkanals gesendet wird. Die „responder-dn“-Datenelemente sollten z. B. geschützt werden, um sicherzustellen, dass eDirectory-Daten nur von Benutzern geändert werden können, die befugt sind, die Email zu beantworten.

Wenn die erzeugte URL auf dem Webserver des Herausgeberkanals verwendet werden soll, muss das <url-query>-Element mindestens ein Element vom Typ <item name=“responder-dn”

protect=“yes”> enthalten. Anderenfalls weist der Webserver die resultierende HTTP POST-Anforderung zurück.

Service-Treiber für manuelle Aufgaben: Automatische Ersetzungsdatenelemente

E

Der Service-Treiber für manuelle Aufgaben stellt bestimmte Ersetzungsdatenelemente zur Verfügung. In diesem Abschnitt werden diese Datenelemente beschrieben.

E.1 Automatische Ersetzungsdaten auf dem Abonnentenkanal

Während der Verarbeitung auf dem Abonnentenkanal werden automatisch folgende Datenelemente zu „replacement-data“-Dokumenten hinzugefügt:

association: Ein Element vom Typ <item name=”association”> wird zum „replacement-data“-Dokument hinzugefügt, wenn das <mail>-Element über ein untergeordnetes <association>-Element verfügt oder wenn der Abonnentenkanal ein <add-association>-Element zurückgibt. Der Inhalt des <item>-Elements ist der „association“-Wert des eDirectory-Objekts, das der verarbeiteten Email zugeordnet ist. Da der Wert für „association“ dem eDirectory-Objekt möglicherweise noch nicht hinzugefügt wurde, kann er nicht für Abfragen verwendet werden.

url: Der Inhalt des <item>-Elements ist die vollständige URL, die in der Email zu verwenden ist. Auf dem Abonnentenkanal wird das „url“-item-Element aus den folgenden item-Elementen unterhalb des <url-data>-Elements erstellt: aus „scheme“, „host“, „port“, „file“ und den item-Elementen unterhalb des <url-query>-Elements. Wenn „scheme“, „host“ oder „port“ nicht gefunden werden, werden die Standardwerte verwendet. Die Standardwerte werden anhand der Konfiguration des Webservers des Herausgeberkanals ermittelt.

url-base: Der Inhalt des <item>-Elements ist der Teil der generierten URL ohne die Ressourcenangabe („file“) und ohne den Query-String.

url-query: Der Inhalt des <item>-Elements ist eine URL-Query-Zeichenkette, die aus den <item>-Elementen unter dem <url-query>-Element generiert wird.

url-file: Der Inhalt des <item>-Elements ist die Ressourcenangabe für die URL.

protected-data: Der Inhalt des <item>-Elements ist ein verschlüsseltes Formular mit Name/Wert-Paaren aus den <item>-Elementen unter dem <url-query>-Element. Nur <item>-Elemente, bei denen das „protect“-Attribut auf “yes” gesetzt ist, werden zum „protected-data“-Element hinzugefügt. Weitere Informationen zu geschützten Daten finden Sie in Anhang D, „Service-Treiber für manuelle Aufgaben: Ersetzungsdaten“, auf Seite 319.

E.2 Automatische Ersetzungsdaten auf dem Herausgeberkanal

Während der Verarbeitung auf dem Webserver des Herausgeberkanals werden automatisch folgende Datenelemente zu „replacement-data“-Dokumenten hinzugefügt:

post-status: Der Webserver des Herausgeberkanals erstellt während der Verarbeitung einer HTTP POST-Anforderung ein Element vom Typ <item name="post-status"> und fügt es zum „replacement-data"-Dokument hinzu. Bei einer HTTP POST-Anforderung an den Webserver handelt es sich um eine Anforderung zur Übertragung eines XDS-Dokuments an Identity Manager. Identity Manager gibt als Ergebnis der XDS-Übertragung ein Statusdokument zurück. Der Inhalt des <item name="post-status">-Elements ist der Wert des Level-Attributs des <status>-Elements, das von Identity Manager als Ergebnis der Übertragung an Identity Manager zurückgegeben wird.

Das item-Element „post-status" wird in der Regel bei der Erstellung der Webseite verwendet, die als Ergebnis der HTTP POST-Anforderung zurückgegeben wird.

post-status-message: Der Webserver des Herausgeberkanals erstellt während der Verarbeitung einer HTTP POST-Anforderung ein Element vom Typ <item name="post-status-message"> und fügt es zum „replacement-data"-Dokument hinzu. Bei einer HTTP POST-Anforderung an den Webserver handelt es sich um eine Anforderung zur Übertragung eines XDS-Dokuments an Identity Manager. Identity Manager gibt als Ergebnis der XDS-Übertragung ein Statusdokument zurück. Der Inhalt des <item name="post-status-message">-Elements ist der Inhalt des <status>-Elements, das von Identity Manager als Ergebnis der Übertragung an Identity Manager zurückgegeben wird. Das item-Element „post-status-message" wird nur erstellt, wenn das von Identity Manager zurückgegebene <status>-Element über Inhalt verfügt.

Das item-Element „post-status-message" wird in der Regel bei der Erstellung der Webseite verwendet, die als Ergebnis der HTTP POST-Anforderung zurückgegeben wird.

url: Der Webserver des Herausgeberkanals erstellt während der Verarbeitung von HTTP GET- und HTTP POST-Anforderungen ein Element vom Typ <item name="url"> und fügt es dem „replacement-data"-Dokument hinzu. Das <item>-Element wird hinzugefügt, bevor Dokumente anhand des „replacement-data"-Dokuments erstellt werden. Schema, Host und Port der URL werden durch die Webserver-Konfiguration festgelegt.

url-base: Der Webserver des Herausgeberkanals erstellt während der Verarbeitung von HTTP GET- und HTTP POST-Anforderungen ein Element vom Typ <item name="url-base"> und fügt es zum „replacement-data"-Dokument hinzu. Das <item>-Element wird hinzugefügt, bevor Dokumente anhand des „replacement-data"-Dokuments erstellt werden. Der Inhalt des <item>-Elements „url-base" auf dem Herausgeberkanal und der Inhalt des <item>-Elements „url" sind identisch.

Service-Treiber für manuelle Aufgaben: Aktionselemente der Schablone

F

Aktionselemente sind Namespace-qualifizierte Elemente in einem Schablonendokument, die zur einfachen Logiksteuerung oder zur Erstellung von HTML-Elementen für HTML-Formulare verwendet werden. Der zur Qualifizierung der Elemente verwendete Namespace ist http://www.novell.com/dirxml/manualtask/form. In diesem Dokument und in den im Lieferumfang des Service-Treibers für manuelle Aufgaben enthaltenen Beispielschablonen wird das Präfix „form“ verwendet.

Alle Aktionselemente, auf die in diesem Abschnitt nicht speziell eingegangen wird, werden bei der Schablonenverarbeitung von der Formatvorlage entfernt (sofern die Formatvorlage nicht benutzerdefiniert ist). Durch dieses Verhalten wird z. B. die Verwendung eines „form:text“-Elements für die Daten einer Email mit einfachem Text ermöglicht, wodurch die Schablone zu gültiger XML wird.

F.1 <form:input>

Das <form:input>-Element wird zur Erzeugung von einem oder mehreren HTML INPUT-Elementen verwendet, sofern ein oder mehrere Ersetzungsdatenelemente vorhanden sind. Die Anzahl der erstellten INPUT-Elemente entspricht der Anzahl der Ersetzungsdatenelemente mit dem Namen, der durch das Namensattribut des Elements <form:input> angegeben wird.

Attribute

Name: Über dieses Attribut wird der Name der Ersetzungsdatenelemente festgelegt, die zur Erstellung der INPUT-Elemente verwendet werden. Der Attributwert wird als Wert des Namensattributs des erstellten INPUT-Elements verwendet.

„type“ oder „TYPE“: Dieses Attribut gibt den Wert des Attributs „type“ der erstellten INPUT-Elemente an.

value: Wenn der Wert des Attributs „value“ gleich “yes” ist, wird den erstellten INPUT-Elementen mit dem Stringwert des Ersetzungsdatenelements ein Attribut vom Typ „value“ hinzugefügt. Wenn der Wert des Attributs ungleich “yes” ist, wird der Inhalt der erstellten INPUT-Elemente auf den Stringwert des Ersetzungsdatenelements gesetzt.

Beispiel

```
<form:input name="responder-dn" TYPE="hidden" value="yes"/>
```

erstellt ein oder mehrere INPUT-Elemente mit einer ähnlichen Struktur wie

```
<INPUT name="responder-dn" TYPE="hidden" value="\PERIN-
TAO\novell\phb"/>
```

F.2 <form:if-item-exists>

Das <form:if-item-exists>-Element wird für die bedingte Dateneingabe in das Ausgabedokument verwendet. Der Inhalt des <form:if-item-exists>-Elements wird nur verarbeitet, wenn das angegebene Element Teil der Ersetzungsdaten ist.

Attribute

Name: Gibt den Namen des Ersetzungsdatenelements an. Wenn ein oder mehrere Beispiele des Ersetzungsdatenelements vorhanden sind, werden die Inhalte des <form:if-item-exists>-Elements verarbeitet.

Beispiel

```
<form:if-item-exists name="post-status-message">
      <tr>
        <td>
          Status message was: $post-status-message$
        </td>
      </tr>
</form:if-item-exists>
```

In diesem Beispiel wird nur dann eine Zeile in eine HTML-Tabelle eingefügt, wenn ein Ersetzungsdatenelement namens „post-status-message“ vorhanden ist.

F.3 <form:if-multiple-items>

Das „form:if-multiple-items“ Element wird für die bedingte Dateneingabe in das Ausgabedokument verwendet. Der Inhalt von „form:if-multiple-items“ wird nur verarbeitet, wenn das angegebene Element mehrmals in den Ersetzungsdaten vorhanden ist.

Attribute

name: Gibt den Namen des Ersetzungsdatenelements an. Wenn das Ersetzungsdatenelement mehrmals vorhanden ist, wird der Inhalt von „form:if-multiple-items“ verarbeitet.

Beispiel

```
<form:if-multiple-items name="responder-dn">
    <form:menu name="responder-dn"/>
</form:if-multiple-items>
```

In diesem Beispiel wird ein HTML SELECT-Element (siehe <form:menu>) erzeugt, wenn mehrere Ersetzungsdatenelemente namens „responder-dn“ vorhanden sind.

F.4 <form:if-single-item>

Das „form:if-single-item“-Element wird für die bedingte Dateneingabe in das Ausgabedokument verwendet. Der Inhalt des „form:if-item-exists“-Elements wird nur verarbeitet, wenn das angegebene Element genau einmal in den Ersetzungsdaten vorhanden ist.

Attribute

name: Gibt den Namen des Ersetzungsdatenelements an. Der Inhalt des „form:if-single-item“-Elements wird nur verarbeitet, wenn das angegebene Element genau einmal in den Ersetzungsdaten vorhanden ist.

Beispiel

```
<form:if-single-item name="responder-dn">
  <input TYPE="hidden" name="responder-dn" value="$responder-dn$"/>
  $responder-dn$
</form:if-single-item>
```

In diesem Beispiel wird in das Ausgabedokument ein HTML INPUT-Element und Platzhaltertext eingefügt, wenn in den Ersetzungsdaten das Ersetzungsdatenelement “responder-dn” genau einmal vorhanden ist.

F.5 <form:menu>

Das „form:menu“-Element wird zur Erzeugung eines HTML SELECT-Elements mit mindestens einem untergeordneten Element vom Typ „OPTION“ verwendet. Das erste untergeordnete „OPTION“-Element ist „OPTION selected“.

Attribute

name: Gibt den Namen des Ersetzungsdatenelements an. Wenn das genannte item-Element in den Ersetzungsdaten vorhanden ist, wird im Ausgabedokument ein HTML SELECT-Element erstellt. Für jede Instanz des Ersetzungsdatenelements in den Ersetzungsdaten wird als untergeordnetes Element des „SELECT“-Elements ein HTML OPTION-Element erstellt.

Beispiel

```
<form:menu name="responder-dn"/>
```

Die aus diesem Beispiel resultierenden HTML-Elemente sehen wie folgt aus:

```
<SELECT name="responder-dn">
    <OPTION selected>\PERIN-TAO\big-org\php</OPTION>
    <OPTION>\PERIN-TAO\big-org\carol</OPTION>
</SELECT>
```

Service-Treiber für manuelle Aufgaben: <mail>-Element

G

In diesem Abschnitt werden das <mail>-Element und dessen Inhalt ausführlich beschrieben. Wenn bei einem Element keine Attribute aufgeführt sind, sind für das entsprechende Element keine Attribute definiert.

G.1 <mail>

Im <mail>-Element und seinem Inhalt werden die Daten beschrieben, die zur Erstellung einer SMTP-Nachricht erforderlich sind.

<mail>-Attribute

src-dn: Enthält den DN-Wert des eDirectory-Objekts, das die Email auslöst. Dieses Attribut ist erforderlich, wenn die Objektdaten als Antwort auf die Email über den Webserver des Herausgeberkanals geändert werden sollen.

G.2 <to>

Das <to>-Element ist dem <mail>-Element untergeordnet. Die Email-Adressen der Hauptempfänger der SMTP-Nachricht sind in einem oder mehreren <to>-Elementen enthalten. Mindestens ein <to>-Element ist obligatorisch. Alle <to>-Elemente können nur jeweils eine Email-Adresse enthalten.

G.3 <cc>

Das <cc>-Element ist dem <mail>-Element untergeordnet. Es können keine oder mehrere <cc>-Elemente vorhanden sein, in denen die Email-Adressen der Empfänger enthalten sind, die im cc-Feld der SMTP-Nachricht aufgeführt werden. Das <cc>-Element ist optional. Alle <cc>-Elemente können nur jeweils eine Email-Adresse enthalten.

G.4 <bcc>

Das <bcc>-Element ist dem <mail>-Element untergeordnet. Es können keine oder mehrere <bcc>-Elemente vorhanden sein, in denen die Email-Adressen der Empfänger enthalten sind, die im bcc-Feld der SMTP-Nachricht aufgeführt werden. Das <bcc>-Element ist optional. Alle <bcc>-Elemente können nur jeweils eine Email-Adresse enthalten.

G.5 <from>

Das <from>-Element ist dem <mail>-Element untergeordnet. Das <from>-Element enthält die Email-Adresse des Absenders der Email. Das <from>-Element ist optional. Wenn das <from>-Element nicht vorhanden ist, wird die standardmäßige Absenderadresse verwendet, die über die Parameter des Service-Treibers für manuelle Aufgaben zur Verfügung gestellt wird.

G.6 <reply-to>

Das <reply-to>-Element ist dem <mail>-Element untergeordnet. Das <reply-to>-Element enthält die Email-Adresse der Entität, an die die Antworten auf die SMTP-Nachricht adressiert werden. Das <reply-to>-Element ist optional.

G.7 <subject>

Das <subject>-Element ist dem <mail>-Element untergeordnet. Anhand seines Inhalts wird der Betreff der SMTP-Nachricht festgelegt. Das <subject>-Element ist nicht obligatorisch, seine Verwendung wird jedoch aus nahe liegenden Gründen empfohlen.

G.8 <message>

Das <message>-Element ist dem <mail>-Element untergeordnet. Anhand seines Inhalts wird der Nachrichtentext der SMTP-Nachricht erstellt. Mindestens ein <message>-Element ist obligatorisch. Möglicherweise werden mehrere <message>-Elemente zur Verfügung gestellt, wenn eine SMTP-Nachricht mit alternativen Darstellungen des Nachrichtentexts erstellt wird (z. B. einfacher Text und HTML oder Englisch und eine weitere Sprache).

<message>-Attribute

mime-type: In diesem optionalen Attribut wird der MIME-Typ des Nachrichtentexts festgelegt, der durch das <message>-Element erzeugt wird (z. B. text/plain oder text/html). Ist dieses Attribut nicht vorhanden, versucht der Treiber, den MIME-Typ automatisch zu ermitteln.

Email-Clients können zur besten Darstellung für die Anzeige den MIME-Typ verwenden, sofern eine SMTP-Nachricht über alternative Darstellungen verfügt.

language: Dieses optionale Attribut legt die Sprache fest, in der der Nachrichtentext durch das <message>-Element erzeugt wird. Der Wert sollte die SMTP-Spezifikation berücksichtigen. Wenn das Attribut nicht vorhanden ist, wird der Standardwert für die Sprache angegeben.

Email-Clients können zur besten Darstellung für die Anzeige die Sprachangabe verwenden, sofern eine SMTP-Nachricht über alternative Darstellungen verfügt.

G.9 <stylesheet>

Das <stylesheet>-Element ist dem <message>-Element untergeordnet. Das <stylesheet>-Element enthält den Namen einer XSLT-Formatvorlage, die zur Erstellung des Nachrichtentexts verwendet wird. Wenn das <stylesheet>-Element nicht vorhanden ist, wird „process_template.xsl“ als Formatvorlage verwendet.

G.10 <template>

Das <template>-Element ist dem <message>-Element untergeordnet. Das <template>-Element enthält den Namen eines XML-Dokuments, das zur Erstellung des Nachrichtentexts verwendet wird. Wenn das <template>-Element nicht vorhanden ist, wird das Dokument mit den Ersetzungsdaten von der Formatvorlage der Nachricht verarbeitet, um den Nachrichtentext zu erstellen.

G.11 <filename>

Das <filename>-Element ist dem <attachment>-Element untergeordnet. Das <filename>-Element enthält einen Dateinamen. Anhand des Werts für „filename“ wird einer erstellten Anlage ein Dateiname zugewiesen.

G.12 <replacement-data>

Das <replacement-data>-Element ist dem <message>-Element untergeordnet. Der Inhalt des Elements wird von der Formatvorlage, die die Schablone verarbeitet, als Parameter verwendet. Wenn keine Schablone vorhanden ist, wird es direkt von der Formatvorlage der Nachricht verarbeitet. Die Inhalte des <replacement-data>-Elements werden in Anhang D, „Service-Treiber für manuelle Aufgaben: Ersetzungsdaten“, auf Seite 319 und Anhang E, „Service-Treiber für manuelle Aufgaben: Automatische Ersetzungsdatenelemente“, auf Seite 327 beschrieben.

G.13 <resource>

Das <resource>-Element ist dem <message>-Element untergeordnet. Sein Inhalt wird als der Name einer Datei behandelt, die in die SMTP-Nachricht als Ressource für den Nachrichtentext integriert werden soll. Beispielsweise könnte eine .css-Formatvorlage für einen HTML-Nachrichtentext als Ressource zur Verfügung gestellt werden.

<resource>-Attribute

cid: In diesem Attribut wird die Content-ID angegeben, die verwendet wird, um auf die Ressource in URLs im Nachrichtentext zu verweisen. Wenn beispielsweise eine .css-Formatvorlage als Ressource dient, nimmt das Attribut „cid“ möglicherweise den Wert „css-1“ an. Im HTML-Nachrichtentext kann mittels des folgenden Elements auf die .css-Formatvorlage verwiesen werden:

```
<link href="cid:css-1" rel="style sheet" type="text/css">
```

G.14 <attachment>

Das <attachment>-Element ist dem <mail>-Element untergeordnet. Sein Inhalt kann mit dem Inhalt des <message>-Elements identisch sein oder einen Dateinamen enthalten. Dem <mail>-Element können keine oder mehrere <attachment>-Elemente untergeordnet sein.

<attachment>-Attribute

mime-type: Dieses optionale Attribut gibt den MIME-Typ der Anlage an. Ist dieses Attribut nicht vorhanden, versucht der Treiber, den MIME-Typ automatisch zu ermitteln.

language: Dieses optionale Attribut gibt die Sprache der Anlage an. Wenn das Attribut nicht vorhanden ist, wird der Standardwert für die Sprache angegeben.

Service-Treiber für manuelle Aufgaben: Datenfluss-Szenario bei Einstellung eines neuen Mitarbeiters

H

In diesem Abschnitt wird anhand eines Beispiels detailliert der Datenfluss beschrieben. In dem Beispiel wird durch die Einstellung eines neuen Mitarbeiters eine Email an den Manager des Mitarbeiters gesendet. In dieser Email wird der Manager aufgefordert, dem Mitarbeiter über eine in der Email enthaltene URL eine Raumnummer zuzuweisen.

Der Service-Treiber für manuelle Aufgaben muss für das Beispielszenario wie folgt konfiguriert werden:

H.1 Konfiguration des Abonnentenkanals

Filter

Klasse: User

Attribute: „Given Name“, „manager“, „Surname“

Richtlinien

Erstellungsrichtlinie: Obligatorische Attribute sind „Given Name“, „manager“ und „Surname“.

Befehlstransformationsrichtlinie: Konvertiert das <add>- in das <mail>-Element.

H.2 Konfiguration des Herausgeberkanals

Filter

Klasse: User

Attribute: „roomNumber“

Richtlinien

Keine.

H.3 Beschreibung des Datenflusses

In der folgenden Liste sind „responder-dn“ und „association“ die wichtigsten Datenelemente, die am Prozess beteiligt sind. Das Element „responder-dn“ wird zur Authentifizierung des Benutzers

verwendet, der die Daten über den Webserver eingibt. Das item-Element „association“ gibt das eDirectory-Objekt an, dessen Daten zu ändern sind.

1. Das Unternehmen stellt einen neuen Mitarbeiter ein. Die Daten des neuen Mitarbeiters werden in das HR-System des Unternehmens eingegeben.
2. Der Identity Manager-Treiber für das HR-System erstellt ein neues Benutzerobjekt in eDirectory. Zu den Benutzerattributen gehören „Given Name“, „Surname“ und „manager“.
3. An den Abonnentenkanal des Service-Treibers für manuelle Aufgaben wird für das neue Benutzerobjekt folgendes <add>-Ereignis übertragen:

```
<nds dtdversion="1.1" ndsversion="8.6">
  <input>
    <add class-name="User" src-dn="\PERIN-TAO\novell\Provo\Joe"
src-entry-id="281002" timestamp="1023314433#2">
      <add-attr attr-name="Surname">
        <value type="string">the Intern</value>
      <add-attr>
      <add-attr attr-name="Given Name">
        <value type="string">Joe</value>
      <add-attr>
      <add-attr attr-name="manager">
        <value type="dn">\PERIN-TAO\novell\Provo\phb</value>
      <add-attr>
    </add>
  </input>
</nds>
```

   a. Die Richtlinie zur Abonnenten-Befehlsumwandlung verwendet den „manager DN“-Wert, um eDirectory nach der Email-Adresse des Managers und den DN seines Assistenten abzufragen.
   b. Wenn der Manager einen Assistenten hat, erstellt die Abonnenten-Befehlsumwandlung eine Abfrage an eDirectory nach der Email-Adresse seines Assistenten.
   c. Die Abonnenten-Befehlsumwandlung erstellt ein <mail>-Element und ersetzt das <add>-Befehlselement durch das <mail>-Element. Im folgenden Beispiel sind Ersetzungsdatenelemente fett gedruckt.

```
<nds dtdversion="1.1" ndsversion="8.6">
  <input>
    <mail src-dn="\PERIN-TAO\novell\Provo\Joe">
      <to>phb@company.com</to>
      <cc>carol@company.com</cc>
      <bcc>HR@company.com</bcc>
      <reply-to>HR@company.com</reply-to>
      <subject>Room Assignment Needed for: Joe the Intern</
subject>
      <message mime-type="text/html">
        <stylesheet>process_template.xsl</stylesheet>
        <template>html_msg_template.xml</template>
        <replacement-data>
          <item name="manager">JStanley</item>          <item
name="given-name">Joe</item>          <item name="surname">the
Intern</item>
```

```
          <url-data>
            <item name="file">process_template.xsl</item>
            <url-query>
         <item name="template">form_template.xml</item>
<item name="responder-dn" protect="yes">\PERIN-
TAO\novell\Provo\phb</item>              <item name="responder-
dn" protect="yes">\PERIN-TAO\novell\Provo\carol</item>
<item name="subject-name">Joe the Intern</item>
            </url-query>
          </url-data>
        </replacement-data>
        <resource cid="css-1">novdocmain.css</resource>
      </message>
    </mail>
  </input>
</nds>
```

d. Der Abonnentenkanal des Service-Treibers für manuelle Aufgaben empfängt das <mail>-Element von Nsure™ Identity Manager.

e. Der Abonnentenkanal erzeugt einen „association“-Wert, weil das <mail>-Element über ein „src-dn“-Attribut verfügt.

f. Der Abonnentenkanal erzeugt anhand der Daten des <mail>-Elements ein Ersetzungsdatendokument, das zur Generierung der Email verwendet wird. Im Abfrageteil der URL (der Teil, der dem ?-Zeichen folgt und fett gedruckt ist) sind verschiedene Datenelemente enthalten. Der Webserver des Herausgeberkanals verwendet diese Datenelemente, wenn die URL als HTTP GET-Anforderung an den Webserver übertragen wird.

```
<replacement-data>
  <item name="manager">JStanley</item>
  <item name="given-name">Joe</item>
  <item name="surname">the Intern</item>
  <item name="template">form_template.xml</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\phb</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\carol</
item>
  <item name="subject-name">Joe the Intern</item>
  <item name="association">1671b2:ee4246a561:-
7fff:192.168.0.1</item>
  <item name="url-base">https://192.168.0.1:8180</item>
  <item name="url-file">process_template.xsl</item>
  <item name="protected-data">
rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAARbAA
1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFMAAlw
YXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ4cH
VyAAJbQqzzF/gGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAfgAEAAAA
uMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn+3+fE6SphHr3Hgjli4Jp3rUk
H7y6dXvcu7iq21Vs+9o6iZVzljTIJX/jjRrVZlR5JOuRNhk8JHFZ8FhgsmiIAH
/Fs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z/DBR13pIAobMpWY
kMaz4+G9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7zOU9Uvd9qXtaE2rR0
AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="url-
query">template=form_template.xml&amp;responder-dn=%5CPERIN-
```

```
TAO%5Cnovell%5Cprovo%5Cphb&amp;responder-dn=%5CPERIN-
TAO%5Cnovell%5Cprovo%5Ccarol&amp;subject-
name=Joe+the+Intern&amp;association=1671b2%3Aee4246a561%3A-
7fff%3A192.168.0.1&amp;protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAf
gAEAAAAuMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn%2B3%2BfE6SphHr3Hg
jli4Jp3rUkH7y6dXvcu7iq21Vs%2B9o6iZVzljTIJX%2FjjRrVZlR5JouRNhk8J
HFZ8FhgsmiIAH%2FFs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z%
2FDBR13pIAobMpWYkMaz4%2BG9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7
zOU9Uvd9qXtaE2rR0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="url">
https://192.168.0.1:8180/
process_template.xsl?template=form_template.xml&amp;responder-
dn=%5CPERIN-TAO%5Cnovell%5CProvo%5Cphb&amp;responder-
dn=%5CPERIN-TAO%5Cnovell%5Cprovo%5Ccarol&amp;subject-
name=Joe+the+Intern&amp;association=1671b2%3Aee4246a561%3A-
7fff%3A192.168.0.1&amp;protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAf
gAEAAAAuMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn%2B3%2BfE6SphHr3Hg
jli4Jp3rUkH7y6dXvcu7iq21Vs%2B9o6iZVzljTIJX%2FjjRrVZlR5JouRNhk8J
HFZ8FhgsmiIAH%2FFs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z%
2FDBR13pIAobMpWYkMaz4%2BG9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7
zOU9Uvd9qXtaE2rR0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREV
</item>
</replacement-data>
```

g. Der Abonnentenkanal verarbeitet die Datei „html_msg_template.xml“ mit der Datei „process_template.xsl“. Das Ersetzungsdatendokument wird als Parameter an die Formatvorlage übergeben. Im Folgenden finden Sie das Dokument „html_msg_template.xml“. Die Ersetzungs-Token sind fett gedruckt. Die Ersetzungs-Token werden durch die Werte der zugehörigen <item>-Elemente aus dem Ersetzungsdatendokument ersetzt.

```
<html xmlns:form="http://www.novell.com/dirxml/manualtask/
form">
  <head>
  </head>
  <body>
    <link href="cid:css-1" rel="style sheet" type="text/css"/>
    <p>
    Dear $manager$,
    </p>
    <p>
    This message is to inform you that your new employee
<b>$given-name$ $surname$</b> has been hired.
    </p>
    <p>
    Please assign a room number for this individual. Click <a
```

```
href="$url$">Here</a> to do this.
    </p>
    <p>
    Thank you,<br/>
    HR<br/>
    HR Department
    </p>
  </body>
</html>
```

Im Folgenden ist die erzeugte Email abgebildet. Die Ersetzungs-Token wurden durch die Werte der zugehörigen <item>-Elemente aus dem Ersetzungsdatendokument ersetzt.

```
<html>
  <head>
<META http-equiv="Content-Type" content="text/html;
charset=UTF-8">
  </head>
  <body>
    <link href="cid:css-1" rel="style sheet" type="text/css">
    <p>
    Dear J Stanley,
    </p>
    <p>
    This message is to inform you that your new employee <b>Joe
the Intern</b> has been hired.
    </p>
    <p>
    Please assign a room number for this individual. Click <a
href="https://192.168.0.1:8180/
process_template.xsl?template=form_template.xml&responder-
dn=%5CPERIN-TAO%5Cnovell%5CProvo%5Cphb&responder-dn=%5CPERIN-
TAO%5Cnovell%5CProvo%5Ccarol&subject-
name=Joe+the+Intern&association=45f0e3%3Aee45e07709%3A-
7fff%3A192.168.0.1&protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG%2BO3BAgEKdXE
AfgAEAAAAuMU%2FSoFRkebvh2d5SqalF91ttjRY5lyyW5%2B%2FFIfOuDdYikYi
DbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY%2Bi4VoVjUSXS3a8fiXB8moM
dPtLJ%2FGyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL
%2FeFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlP
S0iWzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT">Here</a> to
do this.
    </p>
    <p>
    Thank you,<br>
    HR<br>
    HR Department
    </p>
  </body>
</html>
```

h. Die SMTP-Email wird an den Manager und seinen Assistenten gesendet.

i. Der Abonnentenkanal gibt ein XML-Dokument mit einem <status>-Element und einem <add-association>-Element an Identity Manager zurück.

4. Der Manager öffnet die Email und klickt auf den Link “hier”.

5. Der Webbrowser des Managers sendet die URL als eine HTTP GET-Anforderung an den Webserver des Herausgeberkanals.

   a. Der Webserver erzeugt das folgende Ersetzungsdatendokument. Die meisten Datenelemente stammen aus dem Abfrageteil der URL. Ausnahmen hiervon sind die automatisch generierten item-Elemente „url“ und „url-base“.

```
<replacement-data>
  <item name="association">45f0e3:ee45e07709:-
7fff:192.168.0.1</item>
  <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="template">form_template.xml</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\phb</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\carol</
item>
  <item name="subject-name">Joe the Intern</item>
  <item name="url-base">https://192.168.0.1:8180</item>
  <item name="url">https://192.168.0.1:8180</item>
</replacement-data>
```

   Der Webserver verarbeitet das Dokument „form_templates.xml“ mit der Formatvorlage „process_template.xsl“. Die Ersetzungs-Token und Aktionselemente sind fett gedruckt. Beachten Sie, dass viele Datenelemente in versteckten INPUT-Elemente platziert sind, sodass die Datenelemente als Teil der HTML POST-Daten an den Webserver weitergeleitet werden.

   Darüber hinaus ist ein Ersetzungs-Token $query:roomNumber$ vorhanden, das den aktuellen Wert des „roomNumber“-Attributs des Mitarbeiters abruft (sofern verfügbar).

```
<html  xmlns:form="http://www.novell.com/dirxml/manualtask/
form">
  <head>
    <title>Enter room number for $subject-name$</title>
  </head>
  <body>
    <link href="novdocmain.css" rel="style sheet" type="text/
css"/>
    <br/><br/><br/><br/>
```

```
    <form class="myform" METHOD="POST" ACTION="$url-base$/
process_template.xsl">
        <table cellpadding="5" cellspacing="10" border="1"
align="center">
          <tr><td>
          <input TYPE="hidden" name="template"
value="post_form.xml"/>
          <input TYPE="hidden" name="subject-name"
value="$subject-name$"/>
          <input TYPE="hidden" name="association"
value="$association$"/>
          <input TYPE="hidden" name="response-style sheet"
value="process_template.xsl"/>
          <input TYPE="hidden" name="response-template"
value="post_response.xml"/>
          <input TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"/>
          <input TYPE="hidden" name="auth-template"
value="auth_response.xml"/>
          <input TYPE="hidden" name="protected-data"
value="$protected-data$"/>
          <form:if-single-item name="responder-dn">
            You are:<br/>
            <input TYPE="hidden" name="responder-dn"
value="$responder-dn$"/>
            $responder-dn$
         </form:if-single-item>        <form:if-multiple-items
name="responder-dn">
            Indicate your identity:<br/>
           <form:menu name="responder-dn"/>         </form:if-
multiple-items>
        </td></tr>
        <tr><td>
          Enter your password: <br/><input name="password"
TYPE="password" SIZE="20" MAXLENGTH="40"/>
        </td></tr>
        <tr><td>
          Enter room number for $subject-name$:<br/>
          <input TYPE="text" NAME="room-number" SIZE="20"
MAXLENGTH="20" value="$query:roomNumber$"/>
        </td></tr>
        <tr><td>
          <input TYPE="submit" value="Submit"/> <input
TYPE="reset" value="Clear"/>
        </td></tr>
      </table>
    </form>
  </body>
</html>
```

Die resultierende HTML-Seite sieht wie folgt aus:

```
<html>
  <head>
```

```
<META http-equiv="Content-Type" content="text/html;
charset=UTF-8">
    <title>Enter room number for Joe the Intern</title>
  </head>
  <body>
    <link href="novdocmain.css" rel="style sheet" type="text/
css">
    <br><br><br><br>
<form class="myform" METHOD="POST" ACTION="https://
192.168.0.1:8180/process_template.xsl">
<table cellpadding="5" cellspacing="10" border="1"
align="center">
<tr>
<td>
    <input TYPE="hidden" name="template" value="post_form.xml">
    <input TYPE="hidden" name="subject-name" value="Joe the
Intern">
    <input TYPE="hidden" name="association"
value="45f0e3:ee45e07709:-7fff:192.168.0.1">
    <input TYPE="hidden" name="response-style sheet"
value="process_template.xsl">
    <input TYPE="hidden" name="response-template"
value="post_response.xml">
    <input TYPE="hidden" name="auth-style sheet"
value="process_template.xsl">
    <input TYPE="hidden" name="auth-template"
value="auth_response.xml">
    <input TYPE="hidden" name="protected-data"
value="rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHAC
AARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AA
J4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FIfOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT">
    Indicate your identity:<br>
    <SELECT name="responder-dn">
        <OPTION selected>\PERIN-TAO\novell\Provo\phb</OPTION>
        <OPTION>\PERIN-TAO\novell\Provo\carol</OPTION>
    </SELECT>
</td>
</tr>
<tr>
<td>
    Enter your password: <br>
    <input name="password" TYPE="password" SIZE="20"
MAXLENGTH="40">
</td>
</tr>
<tr>
```

```
<td>
    Enter room number for Joe the Intern:<br>
    <input TYPE="text" NAME="room-number" SIZE="20"
MAXLENGTH="20" value="">
</td>
</tr>
<tr>
<td>
    <input TYPE="submit" value="Submit"> <input TYPE="reset"
value="Clear">
</td>
</tr>
</table>
</form>
</body>
</html>
```

b. Der Manager wählt seinen eDirectory-DN im Menü der Webseite aus, gibt sein Passwort ein, weist dem neuen Mitarbeiter eine Raumnummer zu und klickt auf „Senden“.

c. Der Webbrowser sendet eine HTTP POST-Anforderung an den Webserver.

d. Der Webserver erzeugt aus den POST-Daten das folgende Ersetzungsdatendokument. Beachten Sie die Daten, die in den versteckten <INPUT>-Elementen platziert waren. Die vom Manager in das Formular eingegebenen Daten sind fett gedruckt.

```
<replacement-data>  <item name="room-number">cubicle 1234</
item>
  <item name="template">post_form.xml</item>
  <item name="response-template">post_response.xml</item>
  <item name="auth-template">auth_response.xml</item>
  <item name="association">45f0e3:ee45e07709:-
7fff:192.168.0.1</item>
  <item name="password" is-sensitive="true"><!-content
suppressed ?</item>
  <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\phb</item>
  <item name="auth-style sheet">process_template.xsl</item>
  <item name="response-style sheet">process_template.xsl</item>
  <item name="subject-name">Joe the Intern</item>
  <item name="url-base">https://192.168.0.1:8180</item>
  <item name="url">https://192.168.0.1:8180</item>
</replacement-data>
```

e. Der Webserver überprüft, ob der Wert des item-Elements „responder-dn“ mit dem „responder-dn“-Wert in den geschützten Daten übereinstimmt. Wenn die Werte nicht identisch sind, bricht der Webserver die Anforderung ab. Wenn die Werte identisch sind, wird die Verarbeitung fortgesetzt.

f. Der Webserver sendet die XDS-Anforderung <check-object-password> auf dem Herausgeberkanal an Identity Manager, um den Benutzer zu authentifizieren, der die HTTP POST-Anforderung sendet.

```
<nds dtdversion="1.0" ndsversion="8.6">
  <source>
    <product build="20020606_0824" instance="Manual Task
Service Driver" version="1.1a">DirXML Manual Task Service
Driver</product>
    <contact>Novell, Inc.</contact>
  </source>
  <input>
    <check-object-password dest-dn="\PERIN-
TAO\novell\Provo\phb" event-id="chkpwd">
      <password><!-- content suppressed --></password>
    </check-object-password>
  </input>
</nds>
```

g. Identity Manager gibt <status level=”success”> zurück. Wenn Identity Manager einen anderen Status als „success“ (erfolgreich) zurückgibt, wird anhand der durch das Datenelement „auth_template“ festgelegten Schablonen und der durch das Datenelement „auth_stylesheet“ festgelegten Formatvorlage eine Webseite erzeugt, die als Ergebnis der POST-Anforderung zurückgegeben wird.

h. Der Webserver verarbeitet die Schablone „post_form.xml“ mit der Formatvorlage „process_template.xsl“ und erstellt ein XDS-Dokument. Die Ersetzungs-Token sind fett gedruckt.

```
<nds>
  <input>
    <modify class-name="User" src-dn="not-applicable" event-
id=”wfmod”>
      <association>$association$</association>
      <modify-attr attr-name="roomNumber">
        <remove-all-values/>
        <add-value>
          <value>$room-number$</value>
        </add-value>
      </modify-attr>
    </modify>
  </input>
</nds>
```

i. Der Herausgeberkanal sendet das erstellte XDS-Dokument an Identity Manager.

```
<nds>
  <input>
    <modify class-name="User" src-dn="not-applicable" event-
```

```
id=”wfmod”>
      <association>45f0e3:ee45e07709:-7fff:192.168.0.1</
association>
      <modify-attr attr-name="roomNumber">
        <remove-all-values/>
        <add-value>
          <value>cubicle 1234</value>
        </add-value>
      </modify-attr>
    </modify>
  </input>
</nds>
```

j. Identity Manager gibt ein Ergebnisdokument zurück.

```
<nds dtdversion="1.1" ndsversion="8.6">
  <source>
    <product version="2.0">Identity Manager</product>
    <contact>Novell, Inc.</contact>
  </source>
  <output>
    <status event-id="wfmod" level="success"></status>
  </output>
</nds>
```

k. Der Webserver fügt dem Ersetzungsdatendokument das item-Element „post-status“ (und möglicherweise das item-Element „post-status-message“) hinzu. Das hinzugefügte Datenelement ist fett gedruckt:

```
<replacement-data>
  <item name="room-number">cubicle 1234</item>
  <item name="template">post_form.xml</item>
  <item name="response-template">post_response.xml</item>
  <item name="auth-template">auth_response.xml</item>
  <item name="association">45f0e3:ee45e07709:-
7fff:192.168.0.1</item>
  <item name="password" is-sensitive=”true”><!-content
suppressed ?</item>
  <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\phb</item>
  <item name="auth-style sheet">process_template.xsl</item>
  <item name="response-style sheet">process_template.xsl</item>
  <item name="subject-name">Joe the Intern</item>
```

```
  <item name="url-base">https://192.168.0.1:8180</item>
  <item name="url">https://192.168.0.1:8180</item>
  <status event-id="" level="success"></status>  <item
name="post-status">success</item>
</replacement-data>
```

l. Der Webserver verarbeitet die Schablone „post_response.xml“ mit der Formatvorlage „process_template.xsl“. Die Ersetzungs-Token und Aktionselemente sind fett gedruckt.

```
<htm xmlns:form="http://www.novell.com/dirxml/manualtask/form">
  <head>
    <title>Result of post for $subject-name$</title>
  </head>
  <body>
    <link href="novdocmain.css" rel="style sheet" type="text/
css"/>
    <br/><br/><br/><br/>
    <table class="formtable" cellpadding="5" cellspacing="20"
border="1" align="center">
      <tr>
        <td>
          DirXML reported status = $post-status$
        </td>
      </tr><form:if-item-exists name="post-status-message">
      <tr>
        <td>
          Status message was: $post-status-message$
        </td>
      </tr></form:if-item-exists>
    </table>
  </body>
</html>
```

m. Die resultierende Webseite wird als Ergebnis der HTTP POST-Anforderung zurückgegeben. In der Tabelle ist keine zweite Zeile vorhanden, weil das Datenelement „post-status-message“, auf das das Element <form:if-item-exists> verweist, im Ersetzungsdatendokument nicht vorhanden ist.

```
<html>
  <head>
<META http-equiv="Content-Type" content="text/html;
charset=UTF-8">
    <title>Result of post for Joe the Intern</title>
  </head>
  <body>
    <link href="novdocmain.css" rel="style sheet" type="text/
css">
    <br><br><br><br>
    <table class="formtable" cellpadding="5" cellspacing="20"
border="1" align="center">
      <tr>
        <td>
          DirXML reported status = success
        </td>
```

```
      </tr>
    </table>
  </body>
</html>
```

Service-Treiber für manuelle Aufgaben: Benutzerdefinierte Element-Behandlungsroutinen auf dem Abonnentenkanal

Der Treiber bietet einen Erweiterungsmechanismus, der zum Versenden von Benachrichtigungen an Benutzer nicht SMTP (Simplified Mail Transport Protocol), sondern andere Methoden verwendet. Es ist z. B. möglich, dass ein Kunde Benachrichtigungen mit MAPI (Messaging Application Programming Interface), nicht aber mit SMTP versenden muss.

Wenn Sie nicht SMTP, sondern einen anderen Mechanismus zum Versenden von Benachrichtigungen verwenden möchten, müssen Sie eine Java-Klasse für die Verarbeitung eines benutzerdefinierten XML-Elements schreiben, das auf dem Abonnentenkanal des Treibers übertragen wird.

Die benutzerdefinierte Java-Element-Behandlungsroutine muss die Java-Schnittstelle „com.novell.nds.dirxml.driver.manualtask.CommandHandler“ implementieren. Der Name der benutzerdefinierten Elementklasse ist in den Konfigurationsparametern des Abonnentenkanals unter „Zusätzliche Behandlungsroutinen“ festgelegt.

Wenn der Abonnentenkanal ein Befehlselement findet, prüft er dessen Tabelle mit den Behandlungsroutinen. Wenn er eine Behandlungsroutine für die Verarbeitung des Befehlselements findet, wird es an die Behandlungsroutine weitergeleitet. Die Behandlungsroutine führt die erforderliche Verarbeitung aus.

Im Treiber sind zwei Element-Behandlungsroutinen integriert: jeweils eine Behandlungsroutine für <mail>- und <add>-Elemente.

Der Autor der benutzerdefinierten Behandlungsroutine kann das benutzerdefinierte Befehlselement nach Bedarf definieren. Das <mail>-Element kann als Vorlage zur Konfiguration des benutzerdefinierten Befehlselements verwendet werden.

Die benutzerdefinierten Elemente werden anhand von Richtlinien auf dem Abonnentenkanal auf die gleiche Weise erstellt wie das <mail>-Element.

Die Dokumentation für „com.novell.nds.dirxml.driver.manualtask.CommandHandler“ und viele weitere Utility- und Support-Klassen finden Sie in den Javadocs, die im Lieferumfang des Treibers enthalten sind. Die Javadocs befinden sich im Distributions-Image in der Datei „manual_task_docs.zip“.

I.1 Erstellen von URLs zur Verwendung mit dem Webserver des Herausgeberkanals

Zur sicheren Verwendung des Herausgeberkanal-Webservers des Treibers ist es erforderlich, dass zur Erstellung der URL, die in die Benachrichtigung eingefügt werden soll, Utility-Klassen verwendet werden. Für diese Aufgabe ist „com.novell.nds.dirxml.driver.manualtask.URLData“ geeignet.

Der Beispielcode in „SampleCommandHandler.java“ veranschaulicht diesen Prozess.

I.2 Erstellen von Nachrichtendokumenten anhand von Formatvorlagen und Schablonendokumenten

Es bietet sich an, dieselbe Methode zur Erstellung von Dokumenten zu verwenden wie die SMTP-Behandlungsroutine. Bei dieser Methode handelt es sich um eine Kombination aus Formatvorlagen, Schablonendokumenten und Ersetzungsdaten. Sie müssen hierzu die Formatvorlagen und Schablonendokumente abrufen und den Formatvorlagen-Prozessor per Programm aufrufen.

Der Beispielcode in „SampleCommandHandler.java“ veranschaulicht diesen Prozess.

I.3 SampleCommandHandler.java

Quellcode für ein Beispiel einer benutzerdefinierten Befehls-Behandlungsroutine ist im Lieferumfang des Treibers enthalten. Der Quellcode befindet sich im Distributions-Image in der Datei „manual_task_docs.zip“.

Die Behandlungsroutine ist in der Klasse „com.novell.nds.dirxml.driver.manualtask.samples.SampleCommandHandler“ implementiert.

Die Beispiel-Behandlungsroutine generiert lediglich ein Dokument, das auf Formatvorlagen und Schablonen basiert, und schreibt das Ergebnisdokument in eine Datei.

I.3.1 Kompilieren der SampleCommandHandler-Klasse

Sie können zum Kompilieren der SampleCommandHandler-Klasse jeden beliebigen Java-2-Compiler verwenden. Sie müssen „nxsl.jar“, „dirxml.jar“, „collections.jar“ und „ManualTaskServiceBase.jar“ im Klassenpfad des Java-Compilers ablegen.

I.3.2 Austesten der SampleCommandHandler-Klasse

Importieren Sie die Konfiguration zum Raumnummer-Beispiel für den Treiber.

Kompilieren Sie die SampleCommandHandler-Klasse und legen Sie die resultierende Klassendatei in einer .jar-Datei ab. Speichern Sie die .jar-Datei im DirXML.jar-Dateiverzeichnis für die Plattform, auf der Sie den Treiber ausführen.

Fügen Sie unter dem <subscriber-options>-Element das folgende XML-Element hinzu, das sich in den Treiberparametern im XML-Abschnitt der Treibereigenschaften befindet:

```
<output-path display-name="Sample Output Path"></output-path>
```

Bearbeiten Sie die Treiberparameter. Geben Sie in dem item-Element mit der Bezeichnung „Sample Output Path“ ein Pfad zu dem Verzeichnis an, in das der SampleCommandHandler die erstellten Dokumente schreiben soll. Fügen Sie zum Element mit der Bezeichnung „Zusätzliche Behandlungsroutinen“ die Zeichenkette „com.novell.nds.dirxml.driver.manualtask.samples.SampleCommandHandler“ hinzu.

Ersetzen Sie die Befehlstransformationsrichtlinie des Abonnentenkanals durch das Dokument „CommandXform.xsl“, das sich in demselben Verzeichnis befindet wie die Datei „SampleCommandHandler.java“.

Erstellen Sie ein Benutzerobjekt und fügen Sie diesem einen Managerverweis hinzu. Wenn der Manager über einen Wert für die „Email-Adresse“ verfügt, wird ein <sample>-Befehlselement an den Abonnentenkanal gesendet und der SampleCommandHandler schreibt eine Datei in das von Ihnen zuvor angegebene Verzeichnis.

Service-Treiber für manuelle Aufgaben: Benutzerdefinierte Servlets für den Herausgeberkanal

J

Der Treiber bietet einen Erweiterungsmechanismus, über den dem Webserver des Herausgeberkanals zusätzliche Funktionen hinzugefügt werden können. Benutzerdefinierte Servlets können vom Herausgeberkanal geladen werden, indem der Name der Servletklassen im Treiberkonfigurationselement mit der Bezeichnung „Zusätzliche Servlets“ angegeben wird.

J.1 Verwendung des Herausgeberkanals

Wenn ein benutzerdefiniertes Servlet Daten an Identity Manager übertragen muss, muss das Servlet hierfür den Herausgeberkanal des Treibers verwenden. Die Klassen „com.novell.nds.dirxml.driver.manualtask.ServletRegistrar“ und „com.novell.nds.dirxml.driver.manualtask.PublisherData“ vereinfachen dies. Der Beispielcode in „SampleServlet.java“ veranschaulicht diesen Prozess.

J.2 Authentifizierung

Ein benutzerdefiniertes Servlet muss Benutzer authentifizieren, die Informationen senden. Der Beispielcode in „SampleServlet.java“ veranschaulicht diesen Prozess. Bei diesem Typ der Authentifizierung anhand des <check-object-password>-Elements werden jedoch keine eDirectory™-Rechte überprüft. Änderungen, die auf dem Herausgeberkanal gesendet werden, sind zulässig, wenn das Treiberobjekt über die erforderlichen Rechte zur Durchführung der Änderungen verfügt. Es ist dabei unwesentlich, ob der Benutzer, der die Änderungen sendet, über diese Rechte verfügt oder nicht.

Bei Verwendung einer URL, die von einer Befehls-Behandlungsroutine auf dem Abonnentenkanal erzeugt wurde, müssen Sie zur Bestätigung der URL die Klasse „com.novell.nds.dirxml.driver.manualtask.URLData“ verwenden. Auf diese Weise wird sichergestellt, dass das Datenelement „responder-dn“ nicht unerlaubt geändert wurde. Weitere Informationen hierzu finden Sie in den Javadocs.

J.3 SampleServlet.java

Quellcode für ein Beispiel-Servlet ist im Lieferumfang des Treibers enthalten. Der Quellcode befindet sich im Distributions-Image in der Datei „manualtask_driver_docs.zip“.

Das Servlet ist in der Klasse „com.novell.nds.dirxml.driver.manualtask.samples.SampleServlet“ implementiert.

Das Beispiel-Servlet akzeptiert eine HTTP GET-Anforderung für alle Ressourcen mit der Endung „.sample“. Die Query-Zeichenkette der HTTP URL muss die item-Elemente „dest-dn“, „attr-name“ und „value“ enthalten.

Das Servlet authentifiziert den Benutzer und sendet anschließend über den Herausgeberkanal des Treibers eine Änderungsanforderung an Identity Manager.

J.3.1 Kompilieren der SampleServlet-Klasse

Sie können zum Kompilieren der SampleServlet-Klasse jeden beliebigen Java-2-Compiler verwenden. Sie müssen „nxsl.jar“, „dirxml.jar“, „collections.jar“ und „ManualTaskServiceBase.jar“ im Klassenpfad des Java-Compilers ablegen.

J.3.2 Austesten der SampleServlet-Klasse

Importieren Sie die Konfiguration zum Raumnummer-Beispiel für den Treiber.

Kompilieren Sie die SampleServlet-Klasse und platzieren Sie die resultierende Klassendatei in eine .jar-Datei. Speichern Sie die .jar-Datei im DirXML.jar-Dateiverzeichnis für die Plattform, auf der Sie den Treiber ausführen.

Bearbeiten Sie die Treiberparameter. Fügen Sie zum Element mit der Bezeichnung „Zusätzliche Behandlungsroutinen“ die Zeichenkette „com.novell.nds.dirxml.driver.manualtask.samples.SampleServlet“ hinzu.

Fügen Sie zum Filter des Herausgeberkanals „Telefonnummer“ hinzu.

Senden Sie die folgende URL in einem Browser (in der Annahme, dass der Browser auf demselben Computer ausgeführt wird wie der Treiber):

https:localhost:8180/1.sample?dest-dn=username.container&attr-name=Telefonnummer&value=5551212

Ersetzen Sie *username.container* durch den DN eines Benutzers in Ihrem Baum.