NetIQ® eDirectory™ 8.8 SP8

Handbuch der Neuigkeiten

September 2013

Rechtliche Hinweise

Inhalt

Info zu diesem Handbuch und zur Bibliothek

Im *Handbuch der Neuigkeiten* werden Ihnen die neuen Funktionen in NetIQ eDirectory vorgestellt.

Die neueste Version des *Handbuchs der Neuigkeiten in NetIQ eDirectory 8.8 SP8* finden Sie auf der Website NetIQ eDirectory 8.8-Online-Dokumentation.

Zielgruppe

Dieses Handbuch richtet sich an Netzwerkadministratoren.

Weitere Informationen in der Bibliothek

Die Bibliothek enthält folgende Informationsressourcen:

XDASv2-Administrationshandbuch

Beschreibt die Konfiguration und Arbeit mit XDASv2 zur Prüfung von eDirectory und NetIQ Identity Manager.

Installationshandbuch

Beschreibt die Installation von eDirectory. Das Handbuch richtet sich an Netzwerkadministratoren.

Verwaltungshandbuch

Beschreibt die Verwaltung und Konfiguration von eDirectory.

Troubleshooting Guides (Handbücher zur Fehlersuche)

Beschreibt die Behebung von Problemen bei eDirectory.

Anpassungshandbuch für Linux-Plattformen

Beschreibt, wie eDirectory auf Linux-Plattformen mittels Analyse und Feinabstimmung optimiert werden kann, um in allen Bereitstellungen eine bessere Leistung zu erzielen.

Diese Handbücher sind auf der NetIQ eDirectory 8.8-Dokumentationswebsite (https://www.netiq.com/documentation/edir88/) verfügbar.

Informationen zur eDirectory-Verwaltungsfunktion finden Sie im *NetIQ iManager 2.7-Administrationshandbuch* (https://www.netiq.com/documentation/imanager/).

Info zu NetIQ Corporation

NetIQ ist ein globaler Hersteller von Unternehmenssoftware. Unser Blickpunkt liegt auf drei besonderen Herausforderungen, die Sie in Ihrer Umgebung meistern müssen: Änderungen, Komplexität und Risiken. Unser Ziel ist es, Sie dabei zu unterstützen.

Unser Standpunkt

Sich an Änderungen anzupassen und Komplexität und Risiken zu beherrschen ist nichts Neues

Unter den verschiedenen Herausforderungen, denen Sie gegenüberstehen, beeinflussen diese drei Punkte sicherlich am meisten Ihre Möglichkeiten, Ihre physikalischen, virtuellen und Cloud-Umgebungen sicher zu messen, zu überwachen und zu verwalten.

Kritische Geschäftsservices schneller und besser bereitstellen

Wir sind davon überzeugt, dass IT-Organisationen über eine möglichst große Kontrolle verfügen müssen, um eine zeitgerechte und kostenwirksame Servicebereitstellung zu ermöglichen. Der von Änderungen und Komplexität ausgehende, kontinuierliche Druck steigt ständig, weil sich die Unternehmen ständig ändern und die erforderlichen Technologien zur Verwaltung der Änderungen immer komplexer werden.

Unsere Philosophie

Intelligente Lösungen entwickeln, nicht einfach Software

Um zuverlässige Lösungen für die Kontrolle anbieten zu können, stellen wir erst einmal sicher, dass wir das Szenario, in dem Unternehmen wie das Ihre täglich arbeiten, gründlich verstehen. Nur so können wir praxistaugliche, intelligente IT-Lösungen entwickeln, die nachweisbar messbare Ergebnisse liefern. Und das ist für uns wesentlich bereichernder, als einfach eine Software zu verkaufen.

Ihr Erfolg ist unsere Leidenschaft

Ihr Erfolg ist der Wegweiser für unser Geschäft. Wir wissen, dass Sie von der Produktkonzeption bis hin zur Bereitstellung IT-Lösungen benötigen, die richtig funktionieren und nahtlos mit Ihren vorhandenen Investitionen integriert werden können. Sie benötigen fortlaufenden Support, Schulungen nach der Bereitstellung und jemanden, mit dem Sie unkompliziert arbeiten können. Ihr Erfolg ist auch unser Erfolg.

Unsere Lösungen

- Identitäts- und Zugriffsregelung
- Zugriffsverwaltung
- Sicherheitsverwaltung
- System- und Anwendungsverwaltung

- Workload-Management
- Serviceverwaltung

Anfragen an die Verkaufsunterstützung

Bei Fragen zu Produkten, Preisen und Funktionen wenden Sie sich an Ihren Händler vor Ort. Wenn dies nicht möglich ist, wenden Sie sich an unser Verkaufsunterstützungsteam.

Weltweit:	www.netiq.com/about_netiq/officelocations.asp
Vereinigte Staaten und Kanada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Kontakt zum technischen Support

Bei spezifischen Produktproblemen, wenden Sie sich an unseren technischen Support.

Weltweit:	www.netiq.com/support/contactinfo.asp
Nord- und Südamerika:	1-713-418-5555
Europa, Naher Osten und Afrika:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Kontakt zum Dokumentationssupport

Wir möchten Ihnen stets eine nützliche, aussagekräftige Dokumentation an die Hand geben. Wenn Sie uns einen Verbesserungsvorschlag mitteilen möchten, nutzen Sie die Schaltfläche **Kommentar hinzufügen**, die unten auf jeder Seite der unter www.netiq.com/documentation veröffentlichten HTML-Versionen unserer Dokumentation verfügbar ist. Sie können Verbesserungsvorschläge auch per Email an Documentation-Feedback@netiq.com senden. Wir freuen uns auf Ihre Rückmeldung.

Kontakt zur Online-Benutzer-Community

Qmunity, die NetIQ-Online-Community, ist ein Netzwerk zur Zusammenarbeit mit anderen NetIQ-Benutzern und -Experten. Qmunity bietet Ihnen aktuellste Informationen, nützliche Links zu hilfreichen Ressourcen und Kontakt zu NetIQ-Experten, damit Sie über alle Voraussetzungen verfügen, um das meiste aus den IT-Investitionen zu holen, auf die Sie sich verlassen. Weitere Informationen hierzu finden Sie im Internet unter http://community.netiq.com.

1 Service Pack 8 - Funktionen und Verbesserungen

In diesem Kapitel finden Sie einen Überblick über die Funktionen und Verbesserungen in eDirectory 8.8 SP8.

1.1 Verbesserte Skalierbarkeit

eDirectory 8.8 SP8 umfasst die in den folgenden Abschnitten erwähnten Verbesserungen zur Skalierbarkeit, um eine schnellere Datensynchronisierung und Nachrufverarbeitung sowie eine reduzierte Arbeitsspeichernutzung bei der Verarbeitung von Journalereignissen sicherzustellen.

In dieser Version wurden einige Hintergrundprozesse überarbeitet, um sie für große, dynamische Umgebungen anzupassen. Dies umfasst auch die Optimierung der vorhandenen Hintergrundprozesse und die Bereitstellung von Konfigurationsoptionen, um Ihre Systeme Ihrer Umgebung entsprechend anzupassen.

1.1.1 Steuerung der Hintergrundprozesse

Administratoren können die Hintergrundprozesse steuern, indem sie die folgenden Richtlinien "Verzögerungseinstellungen für Hintergrundprozesse" im Fenster "Hintergrundprozesseinstellungen" im NetIQ iMonitor konfigurieren:

- **CPU** - Gibt den maximalen Prozentsatz für die Computerressourcen und die maximale Dauer der Inaktivität desselben Prozesses (Skulker, Tilgung oder Nachruf) an.
- **Hardlimit** - Gibt eine statische Verzögerungseinstellung für die einzelnen Skulker-, Tilgungs- und Nachrufprozesse an.

Informationen zur Konfiguration von Hintergrundprozessen finden Sie im Abschnitt „Konfigurieren von Hintergrundprozessen“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

1.1.2 Skulker-Prozess

Um die Anzahl der Threads zu erhöhen, die für die Reproduktion auf mehreren Servern gleichzeitig erstellt wurden, können Sie den Skulker-Prozess verwenden, um die maximale Anzahl der erstellten Threads festzulegen. Diese Einstellung gilt für alle Partitionen auf einem Server.

Informationen zur Konfiguration des Skulker-Prozesses finden Sie im Abschnitt „Manuelle Konfiguration von Synchronisierungs-Threads“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

1.1.3 Asynchrone Reproduktion

Um die Zeit für die Reproduktion zu verkürzen, werden die folgenden Vorgänge nun parallel ausgeführt:

- Verarbeiten des Änderungs-Caches
- Senden von Paketen an einen Remote-Server

Durch die neue Option **Einstellungen für die asynchrone Ausgangssynchronisierung (Millisekunden)** können Sie nun verhindern, dass der Empfangsserver überlastet wird. Standardmäßig ist diese Option deaktiviert. Die Einstellung ist abhängig von der Umgebung. Wenn Sie diese Option aktivieren, legen Sie sie auf den Wert `100` fest und passen Sie sie anschließend nach oben bzw. unten an, je nach Bedarf.

Informationen zur asynchronen Ausgangssynchronisierung finden Sie im Abschnitt „Konfigurieren der asynchronen Ausgangssynchronisierung“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

1.1.4 Richtlinienbasierte Reproduktion

Administratoren können nun eine Richtlinie (XML-Datei) erstellen, um anzugeben, wie Änderungen reproduziert werden sollen. Dies kann beispielsweise nützlich sein mit einem Reproduktionsring, der über mehrere Speicherorte verteilt wird. Wenn die Richtlinie einen Tippfehler oder eine inkorrekte Syntax enthält, kehrt die Reproduktion zur Standardmethode zurück.

Weitere Informationen finden Sie im Abschnitt „Richtlinienbasierte Reproduktion“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

1.1.5 Nachruf

Ein Nachruf, der generiert wird, weil Objekte gelöscht, umbenannt oder verschoben wurden, wird nun schneller als in früheren Versionen von eDirectory verarbeitet. Beispielsweise erfordert eine Aktualisierung, die früher fünf Zyklen gedauert hat, jetzt möglicherweise nur noch zwei Zyklen.

Der Nachrufprozess kann außerdem jetzt mit dem Skulker-Prozess parallel ausgeführt werden.

1.1.6 Überwachen der Nachrufanzahl und des Änderungscache-Umfangs über iMonitor

iMonitor zeigt die Anzahl der Objekte mit Nachrufen in jedem Zustand an. Außerdem zeigt es die Anzahl der Objekte im Änderungscache einer Partition an, wenn Sie ein Partitionsobjekt über iMonitor auf einem vorhandenen Server anzeigen. Dies ist nützlich für die weitere Überwachung des Status der Synchronisierung und Nachrufverarbeitung.

1.1.7 Verteilte Referenzlinks (Distributed Reference Links, DRL)

Zur Optimierung der Nachrufverarbeitung verwendet eDirectory die folgenden DRL-Attribute nicht mehr:

- `Genutzt durch`
- `Nachruf: Genutzt durch`

1.1.8 Journalereignis-Caching

Das Journalereignissystem wurde geändert, damit Sie eine Kombination aus Arbeitsspeicher und Festplatte zur Beibehaltung von Ereignissen in der Warteschlange verwenden können. Dadurch wird das drastische Wachstum an Arbeitsspeicherverbrauch des NDSD-Prozesses reduziert.

Verbesserungen für Journalereignisse:

- **Caching**

  Wenn die Journalereignis-Warteschlange über einen bestimmten Punkt im Arbeitsspeicher (32 MB = max. 8 x 4 MB-Blöcke) hinaus wächst, beginnt eDirectory damit, einen Cache auf der Festplatte zu verwenden.

- **Variablen**

  Journalereignisse enthalten die folgenden Variablen, die Benutzer konfigurieren können:

  - NDSD_EVENT_DISK_CACHE
  - NDSD_EVENT_DISK_CACHE_DIR

- **Komprimierung**

  Eine verbesserte Komprimierung minimiert die Datenmenge auf der Festplatte. Das Komprimierungsverhältnis liegt bei ungefähr 20:1.

1.1.9 Unterstützung für Solid State Disks (SSD)

Diese Version unterstützt Enterprise-SSD für verbesserte E/A-Vorgänge.

1.1.10 Advanced Referral Costing (ARC)

In dieser Version ist ARC standardmäßig aktiviert.

Weitere Informationen finden Sie im Abschnitt „Advanced Referral Costing“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

1.1.11 Intervall für die Anmeldeaktualisierung

Durch die neue Option "Intervall für die Deaktivierung der Anmeldeaktualisierung" können Administratoren ein Zeitintervall (in Sekunden) angeben, innerhalb dessen eDirectory die Anmeldeattribute nicht aktualisiert.

HINWEIS: Diese Option gilt nur für Anmeldungen bei NetIQ Directory Services (NDS).

Weitere Informationen finden Sie im Abschnitt „Steuerung und Konfiguration des DS-Agenten“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

1.2 LDAP-Verbesserungen

Diese Version enthält die folgenden LDAP-Verbesserungen:

1.2.1 Zulassende Änderungssteuerung

Anhand dieser Option können Sie den aktuellen LDAP-Bearbeitungsvorgang erweitern. Wenn Sie versuchen, ein nicht vorhandenes Attribut zu löschen oder einem bereits vorhandenen Attribut einen Wert hinzuzufügen, dann wird der Vorgang ohne Anzeige einer Fehlermeldung ausgeführt.

Weitere Informationen finden Sie im Abschnitt „Konfiguration der zulassenden Änderungssteuerung“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

1.2.2 Unterstützung für generalisierte Zeit

Die Option "Unterstützung für generalisierte Zeit" ermöglicht Ihnen die Anzeige der Zeit im Format `YYYYMMDDHHmmSS.0Z`.

Beachten Sie, dass `0Z` die Unterstützung für Sekundenbruchteile bezeichnet wie von Active Directory unterstützt. Da eDirectory die Anzeige von Sekundenbruchteilen nicht unterstützt, wird durch diese Option *0* angezeigt, um zu verhindern, dass die Funktion in einer gleichzeitig bestehenden Umgebung außer Kraft gesetzt wird.

Weitere Informationen finden Sie im Abschnitt „Konfiguration der Unterstützung für generalisierte Zeit“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

1.2.3 Steuerung der Teilbaumlöschung

Diese Version unterstützt die Steuerung der Teilbaumlöschung, durch das die Löschung von Containerobjekten zugelassen wird. Früher konnten nur Blattobjekte gelöscht werden. Die Steuerung der Teilbaumlöschung unterstützt jedoch nicht die Löschung von Partitionscontainern.

1.3 IPv6-Unterstützung

Diese Version unterstützt sowohl IPv4-Netzwerke als auch IPv6-Netzwerke. Standardmäßig wird IPv6 bei der Installation von eDirectory automatisch aktiviert. Wenn Sie von einer früheren Version von eDirectory aus aufrüsten, müssen Sie die IPv6-Unterstützung manuell aktivieren.

eDirectory 8.8 SP8 unterstützt die folgenden IPv6-Modi:

- Dual-Stack
- Tunnelung
- Reines IPv6

eDirectory 8.8 SP8 unterstützt nicht die folgenden IPv6-Adresstypen:

- Lokale Linkadressen
- IPv4-zugeordnete IPv6-Adressen
- IPv4-kompatible IPv6-Adressen

eDirectory 8.8 SP8 unterstützt die folgenden Adressierungsformate:

- [::]
- [::1
- [2015::12]
- [2015::12]:524

1.4 Revisionsverbesserungen

Diese Version verbessert die XDAS-Revision durch Unterstützung der Client-IP-Adresse in Ereignissen.

2 Unterstützte Plattformen für die eDirectory-Installation

eDirectory 8.8 SP8 ist eine plattformübergreifende Version, die die Stabilität von eDirectory verbessern soll.

2.1 Veraltete Plattformen

eDirectory 8.8 SP8 unterstützt folgende Plattformen nicht:

- NetWare
- 32- und 64-Bit-eDirectory auf Solaris
- 32-Bit-eDirectory auf AIX
- 32-Bit-eDirectory auf Linux
- 32-Bit-eDirectory auf Windows

2.2 Linux

Sie müssen eDirectory auf einer der folgenden Plattformen installieren:

- SLES 11 SP1, SP2 und SP3 64-Bit
- SLES 10 SP4 64-Bit
- RHEL 5.7, 5.8 und 5.9
- RHEL 6.2, 6.3 und 6.4

Sie können diese Betriebssysteme im virtuellen Modus auf folgenden Hypervisoren ausführen:

- VMware ESXi
- Xen (auf SLES 10 und SLES 11 und deren Support Packs)

  HINWEIS: eDirectory 8.8 SP8 wird von einem SLES 10 XEN-Virtualisierungsdienst unterstützt, der das SLES 10-Gastbetriebssystem ausführt. Die folgenden Aktualisierungen sind auf der NetIQ-Aktualisierungs-Website (https://update.novell.com) verfügbar:

  - SUSE-Linux-Enterprise-Server-X86_64-10-0-20061011-020434
  - SLES10-Aktualisierungen

Weitere Informationen zur Registrierung und Aktualisierung von SUSE Linux Enterprise 10 finden Sie im Abschnitt Registrieren von SUSE Linux Enterprise im NetIQ Customer Center (http://www.suse.com/products/register.html). Vergewissern Sie sich nach der Installation der neuesten Aktualisierung, dass die Mindest-Patch-Stufe der installierten Aktualisierung "3.0.2_09763-0.8" lautet.

- Windows Server 2008 R2 Virtualisierung mit Hyper-V

Informationen zu der auf Ihrem System installierten Version von SUSE Linux finden Sie in der Datei `/etc/SuSE-release`.

Stellen Sie sicher, dass auf Red Hat-Systemen die neuesten glibc-Patches von Red Hat Errata (http://rhn.redhat.com/errata) angewendet werden. Die erforderliche Mindestversion der glibc-Bibliothek lautet 2.1.

2.3 Windows

Sie müssen eDirectory auf einer der folgenden Plattformen installieren:

- Windows Server 2008 (x64) (Standard/Enterprise/Data Center Edition) und Service Packs
- Windows Server 2008 R2 (Standard/Enterprise/Data Center Edition) und Service Packs
- Windows 2012-Server

WICHTIG

- Zur Installation von eDirectory 8.8 SP8 auf Windows Server 2008 R2 ist ein Konto mit Verwaltungsrechten erforderlich.
- Windows-Desktopversionen werden nicht unterstützt.

3 Verbesserungen für die Installation und Aufrüstung

In diesem Kapitel werden die neuen Funktionen und Verbesserungen für die Installation und Aufrüstung von NetIQ eDirectory 8.8 beschrieben.

In der folgenden Tabelle sind die neuen Funktionen aufgeführt und die Plattformen angegeben, auf denen diese unterstützt werden.

Funktion	Linux	Windows
Mehrere Paketformate für die Installation von eDirectory 8.8	✓	✗
Installation am benutzerdefinierten Speicherort für Anwendungsdateien	✓	✓
Installation am benutzerdefinierten Speicherort für Datendateien	✓	✓
Installation am benutzerdefinierten Speicherort für Konfigurationsdateien	✓	✗
Nicht-Root-Installation	✓	✗
Verbesserte Unterstützung für Installationen auf hochverfügbaren Clustern	✓	✓
FHS-Konformität	✓	✗
LSB-Konformität	✓	✗
Serverzustandsüberprüfungen	✓	✓
SecretStore-Integration	✓	✓
Installation der eDirectory-Instrumentation	✓	✓

Dieses Kapitel enthält die folgenden Informationen:

- Abschnitt 3.7, „SecretStore-Integration mit eDirectory“, auf Seite 28
- Abschnitt 3.8, „Installation der eDirectory-Instrumentation“, auf Seite 29
- Abschnitt 3.9, „Weiterführende Informationen“, auf Seite 29

3.1 Mehrere Paketformate für die Installation von eDirectory 8.8

Unter Linux können Sie aus verschiedenen Dateiformaten auswählen, wenn Sie eDirectory 8.8 auf Ihrem Host installieren. Die Dateiformate sind in der nachfolgenden Tabelle aufgeführt.

Benutzertyp und Speicherort für die Installation	Linux
Root-Benutzer	
Standardstandort	RPM
Benutzerdefinierter Speicherort	Tarball-Datei
Nicht-Root-Benutzer	
Benutzerdefinierter Speicherort	Tarball-Datei

Weitere Informationen zur Installation mit Tarball-Dateien finden Sie im *NetIQ eDirectory 8.8 SP8-Installationshandbuch*.

3.2 Installieren von eDirectory 8.8 an einem benutzerdefinierten Speicherort

eDirectory 8.8 bietet Ihnen die Flexibilität, die Anwendung, Daten und Konfigurationsdateien an einem Speicherort Ihrer Wahl zu installieren.

In einem der Szenarien zur Installation von eDirectory 8.8 an einem benutzerdefinierten Speicherort ist auf Ihrem Host bereits eine ältere Version von eDirectory installiert und Sie möchten eDirectory 8.8 zunächst testen, bevor Sie auf diese Version aufrüsten. Auf diese Weise können Sie Ihre vorhandene eDirectory-Einrichtung weiterhin unterbrechungsfrei ausführen und gleichzeitig diese neue Version testen. Anschließend können Sie entscheiden, ob Sie die vorhandene Version behalten oder auf eDirectory 8.8 aufrüsten möchten.

HINWEIS: SLP und der SNMP-Unteragent sind an den Standardspeicherorten installiert.

In diesem Abschnitt wird erklärt, wie die verschiedenen Dateien an einem benutzerdefinierten Speicherort installiert werden:

- Abschnitt 3.2.1, „Angabe eines benutzerdefinierten Speicherorts für Anwendungsdateien“, auf Seite 21
- Abschnitt 3.2.2, „Angabe eines benutzerdefinierten Speicherorts für Datendateien“, auf Seite 21
- Abschnitt 3.2.3, „Angabe eines benutzerdefinierten Speicherorts für Konfigurationsdateien“, auf Seite 21

3.2.1 Angabe eines benutzerdefinierten Speicherorts für Anwendungsdateien

Bei der Installation von eDirectory können Sie Ihre Anwendungsdateien an einem Speicherort Ihrer Wahl installieren.

Linux

Zur Installation von eDirectory 8.8 an einem benutzerdefinierten Speicherort können Sie die Tarball-Installationsdatei verwenden und eDirectory 8.8 an einem Speicherort Ihrer Wahl entpacken.

Windows

Sie konnten bereits vor eDirectory 8.8 einen benutzerdefinierten Speicherort für die Anwendungsdateien während der Installation über den Assistenten angeben.

3.2.2 Angabe eines benutzerdefinierten Speicherorts für Datendateien

Bei der Konfiguration von eDirectory können Sie die Datendateien an einem Speicherort Ihrer Wahl speichern. Die Datendateien enthalten die Verzeichnisse `data`, `dib` und `log`.

Linux

Zur Konfiguration der Datendateien an einem benutzerdefinierten Speicherort können Sie entweder die Option `-d` oder die Option `-D` des ndsconfig-Dienstprogramms verwenden.

Option	Beschreibung
-d *benutzerdefinierter_Speicherort*	Erstellt das `DIB`-Verzeichnis (DIB ist die eDirectory-Datenbank) im angegebenen Pfad. **HINWEIS:** Diese Option war auch bereits vor eDirectory 8.8 verfügbar.
-D *benutzerdefinierter_Speicherort*	Erstellt die Verzeichnisse `data` (enthält Daten wie die PIDs und Socket-IDs), `dib` und `log` im angegebenen Pfad.

Windows

Unter Windows würden Sie aufgefordert werden, den DIB-Pfad während der Installation einzugeben. Geben Sie einen Pfad Ihrer Wahl ein.

3.2.3 Angabe eines benutzerdefinierten Speicherorts für Konfigurationsdateien

Bei der Konfiguration von eDirectory können Sie den Pfad auswählen, in dem Sie Ihre Konfigurationsdateien speichern möchten.

Linux

Zur Konfiguration der Konfigurationsdatei `nds.conf` an einem anderen Speicherort können Sie die Option `--config-file` des ndsconfig-Dienstprogramms verwenden.

Gehen Sie folgendermaßen vor, um die anderen Konfigurationsdateien (wie `modules.conf`, `ndsimon.conf` und `ice.conf`) an einem anderen Speicherort zu installieren:

1. Kopieren Sie alle Konfigurationsdateien an den neuen Speicherort.
2. Legen Sie den neuen Speicherort fest, indem Sie Folgendes eingeben:

   ```
   ndsconfig set n4u.nds.configdir benutzerdefinierter_Speicherort
   ```

Windows

Sie können keinen benutzerdefinierten Speicherort für die Konfigurationsdateien unter Windows angeben.

3.3 Nicht-Root-Installation

eDirectory 8.8 und höher unterstützt die Installation und Konfiguration von eDirectory-Servern durch einen Nicht-Root-Benutzer. Frühere Versionen von eDirectory konnten nur durch einen Root-Benutzer installiert und konfiguriert werden, wobei nur eine einzelne Instanz von eDirectory auf einem Host ausgeführt wurde.

Bei eDirectory 8.8 oder höher kann jeder Nicht-Root-Benutzer einen Tarball-Build zur Installation von eDirectory verwenden. Es können mehrere Instanzen von binären eDirectory-Installationen vom selben Benutzer oder von verschiedenen Benutzern vorhanden sein. Doch auch für Nicht-Root-Benutzer-Installationen können die Dienste auf Systemebene wie Novell International Cryptographic Infrastructure (NICI), SNMP und SLP nur mit den Root-Berechtigungen installiert werden. NICI ist eine obligatorische Komponente und SNMP und SLP sind optionale Komponenten für die eDirectory-Funktionalität. Außerdem kann bei einer Paketinstallation nur eine einzelne Instanz vom Root-Benutzer installiert werden.

Nach der Installation kann ein Nicht-Root-Benutzer eDirectory-Serverinstanzen konfigurieren, indem er seine individuelle Tarball-Installation verwendet oder eine binäre Installation. Dies bedeutet, dass mehrere Instanzen von eDirectory-Servern auf einem einzelnen Host ausgeführt werden können, weil jeder Benutzer, ob Root- oder Nicht-Root-Benutzer, verschiedene eDirectory-Serverinstanzen auf einem einzelnen Host konfigurieren kann, indem er entweder eine Paketinstallation oder eine Tarball-Installation verwendet. Weitere Details zur Funktion für mehrere Instanzen finden Sie in den Abschnitten „Mehrere Instanzen“ und „Aufrüsten mehrerer Instanzen“ im *NetIQ eDirectory 8.8 SP8-Installationshandbuch*.

Die Nicht-Root-Installation und -Konfiguration gilt nur für Linux-Plattformen. Weitere Informationen zur Nicht-Root-Installation und -Konfiguration finden Sie im Abschnitt „Installation von eDirectory 8.8 durch Nicht-Root-Benutzer“ im *NetIQ eDirectory 8.8 SP8-Installationshandbuch*.

3.4 Verbesserte Unterstützung für Installationen in hochverfügbaren Clustern

eDirectory 8.8 SP8 vereinfacht die Installation und Verwaltung von eDirectory sowohl in Linux- als auch in Windows-Clustern, wodurch die Clustering-Unterstützung verbessert und die hohe Verfügbarkeit ermöglicht wird. eDirectory bietet auch eine hohe Verfügbarkeit über die Reproduktionssynchronisierung, die mit dem Clustering kombiniert werden kann, um eine höhere Verfügbarkeitsstufe zu erzielen.

Weitere Informationen zur Installation von eDirectory in Clustern finden Sie im *NetIQ eDirectory 8.8 SP8-Installationshandbuch*.

3.5 Kompatibilität mit Standards

eDirectory 8.8 ist kompatibel mit den folgenden Standards:

- Abschnitt 3.5.1, „FHS-Kompatibilität“, auf Seite 23
- Abschnitt 3.5.2, „LSB-Kompatibilität“, auf Seite 24

3.5.1 FHS-Kompatibilität

Um Dateikonflikte mit anderen Produktanwendungsdateien zu vermeiden, befolgt eDirectory 8.8 den Filesystem Hierarchy Standard (FHS). Diese Funktion ist nur unter Linux verfügbar.

eDirectory folgt dieser Verzeichnisstruktur nur dann, wenn Sie es am Standardspeicherort installiert haben. Wenn Sie einen benutzerdefinierten Speicherort gewählt haben, dann wäre die Verzeichnisstruktur *benutzerdefinierter_Speicherort*/*Standardpfad*.

Beispiel: Wenn Sie eDirectory im Verzeichnis `eDir88` installiert haben, würde dieselbe Verzeichnisstruktur im Verzeichnis `eDir88` befolgt werden. Die man-Seiten würden dann im Verzeichnis `/eDir88/opt/novell/man` installiert werden.

In der folgenden Tabelle ist die Änderung in der Verzeichnisstruktur aufgeführt:

Im Verzeichnis gespeicherte Dateitypen	Verzeichnisname und -pfad
Ausführbare Binärdateien und statische Shell-Skripts	`/opt/novell/eDirectory/bin`
Ausführbare Binärdateien für Root-Benutzer	`/opt/novell/eDirectory/sbin`
Statische oder dynamische Bibliotheksbinärdateien	`/opt/novell/eDirectory/lib`
Konfigurationsdateien	`/etc/opt/novell/eDirectory/conf`
Dynamische Schreib/Lese- und Laufzeitdaten wie DIB	`/var/opt/novell/eDirectory/data`
Protokolldateien	`/var/opt/novell/eDirectory/log`
Linux man-Seiten	`/opt/novell/man`

Umgebungsvariablen exportieren

Bei der FHS-Implementierung in eDirectory 8.8 müssen Sie die Umgebungsvariablen des Pfads aktualisieren und exportieren. Dadurch entstehen die folgenden Probleme:

- Sie müssen sich alle exportierten Pfade merken, weil Sie diese Pfade bei jedem Öffnen einer Shell exportieren und die Dienstprogramme verwenden müssen.
- Wenn Sie mehr als einen Satz von Binärdateien verwenden möchten, müssen Sie mehr als eine Shell öffnen oder Sie müssen die Festlegung der Pfade aufheben und diese häufig neu für den anderen Satz von Binärdateien festlegen.

Zur Behebung des oben genannten Problems können Sie das Skript `/opt/novell/eDirectory/bin/ndspath` wie folgt verwenden:

- Fügen Sie das ndspath-Skript dem Dienstprogramm als Präfix hinzu und führen Sie das gewünschte Dienstprogramm wie folgt aus:

  ```
  custom_location/opt/novell/eDirectory/bin/ndspath utility_name_with_parameters
  ```

- Exportieren Sie die Pfade in der aktuellen Shell wie folgt:

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

- Nach Eingabe des oben genannten Befehls führen Sie die Dienstprogramme genauso aus wie immer. Rufen Sie das Skript in Ihrem profile-, bashrc- oder ähnlichen Skripts aus. Daher können Sie damit beginnen, die Dienstprogramme direkt zu verwenden, sobald Sie sich anmelden oder eine neue Shell öffnen.

3.5.2 LSB-Kompatibilität

eDirectory 8.8 ist nun kompatibel mit Linux Standard Base (LSB). LSB empfiehlt auch die FHS-Kompatibilität. Alle eDirectory-Pakete in Linux weisen das Präfix *novell* auf. Beispiel: `NDSserv` ist nun `novell-NDSserv`.

3.6 Serverzustandsüberprüfungen

eDirectory 8.8 führt Serverzustandsüberprüfungen ein, anhand derer Sie vor der Aufrüstung herausfinden können, ob sich Ihr Server in einem funktionsfähigen Zustand befindet.

Die Serverzustandsüberprüfungen werden bei jeder Aufrüstung standardmäßig und vor der eigentlichen Paketaufrüstung ausgeführt. Sie können jedoch auch das Diagnosetool "ndscheck" für die Zustandsüberprüfung ausführen.

3.6.1 Notwendigkeit der Zustandsüberprüfungen

In früheren Versionen von eDirectory wurde bei der Aufrüstung der Zustand des Servers nicht überprüft, bevor mit der Aufrüstung fortgefahren wurde. Wenn der Zustand instabil war, trat bei dem Aufrüstungsvorgang ein Fehler auf und eDirectory befand sich in einem inkonsistenten Zustand. In einigen Fällen konnten Sie möglicherweise kein Rollback zu den Einstellungen vor der Aufrüstung durchführen.

Dieses neue Tool zur Zustandsüberprüfung behebt dieses Problem und Sie können sicherstellen, dass Ihr Server bereit für die Aufrüstung ist.

3.6.2 Wann ist ein Server in einem funktionsfähigen Zustand?

Das Dienstprogramm für Serverzustandsüberprüfungen führt bestimmte Zustandsüberprüfungen durch, um sicherzustellen, dass der Baum fehlerfrei ist. Der Zustand des Baums wird als fehlerfrei erklärt, wenn alle Zustandsüberprüfungen erfolgreich abgeschlossen wurden.

3.6.3 Durchführen von Zustandsüberprüfungen

Sie können Serverzustandsüberprüfungen auf zwei Arten durchführen:

- „Mit der Aufrüstung“, auf Seite 25
- „Als eigenständiges Dienstprogramm“, auf Seite 25

HINWEIS: Sie brauchen Administratorrechte zur Ausführung des Dienstprogramms für Zustandsüberprüfungen. Das mindestens erforderliche Recht, das zur Ausführung des Dienstprogramms festgelegt werden kann, ist das Recht "Öffentlich". Mit dem Recht "Öffentlich" sind jedoch einige der NetWare Core Protocol (NCP)-Objekte und Partitionsinformationen nicht verfügbar.

Mit der Aufrüstung

Die Zustandsüberprüfungen werden standardmäßig bei jeder Aufrüstung von eDirectory durchgeführt.

Linux

Bei jeder Aufrüstung werden die Zustandsüberprüfungen standardmäßig vor dem Start der eigentlichen Aufrüstung durchgeführt.

Zum Überspringen der standardmäßigen Zustandsüberprüfungen können Sie die Option "-j" mit dem Dienstprogramm "nds-install" verwenden.

Windows

Die Serverzustandsüberprüfungen werden als Teil des Installationsassistenten durchgeführt. Sie können nach der Aufforderung die Zustandsüberprüfungen aktivieren bzw. deaktivieren.

Als eigenständiges Dienstprogramm

Sie können die Serverzustandsüberprüfungen jederzeit als eigenständiges Dienstprogramm ausführen. In der folgenden Tabelle werden die Dienstprogramme für die Zustandsüberprüfung erklärt.

Tabelle 3-1 *Diensprogramme für die Zustandsüberprüfung*

Plattform	Dienstprogramm-Name
Linux	ndscheck Syntax: `ndscheck -h hostname:port -a admin_FDN -F logfile_path --config-file configuration_file_name_and_path` **HINWEIS:** Sie können entweder `-h` oder `--config-file` angeben, doch nicht beide Optionen.
Windows	ndscheck

3.6.4 Arten der Zustandsüberprüfung

Wenn Sie das ndscheck-Dienstprogramm aufrüsten oder ausführen, werden die folgenden Arten von Zustandsüberprüfungen durchgeführt:

- Basis-Serverzustand
- Zustand der Partitionen und Reproduktionen

Wenn Sie das ndscheck-Dienstprogramm ausführen, werden die Ergebnisse der Zustandsüberprüfungen am Bildschirm angezeigt und in der Datei `ndscheck.log` protokolliert. Weitere Informationen zu den Protokolldateien finden Sie unter Abschnitt 3.6.6, „Protokolldateien“, auf Seite 28.

Wenn die Zustandsüberprüfungen als Teil der Aufrüstung durchgeführt werden, dann werden Sie nach den Zustandsüberprüfungen entweder dazu aufgefordert, den Aufrüstungsprozess fortzusetzen, oder der Vorgang wird abgebrochen, je nach Schweregrad des Fehlers. Die Details zu den Fehlern sind unter Abschnitt 3.6.5, „Kategorisierung des Zustands“, auf Seite 27 beschrieben.

Basis-Serverzustand

Dies ist die erste Phase der Zustandsüberprüfung. Das Dienstprogramm für die Zustandsüberprüfung prüft Folgendes:

1. Der eDirectory-Dienst ist aktiv. Die DIB ist geöffnet und kann einige Basisinformationen des Baums wie den Baumnamen lesen.
2. Der Server überwacht auf den entsprechenden Portnummern.

   Für LDAP werden die TCP- und SSL-Portnummern abgerufen und es wird geprüft, ob der Server auf diesen Ports überwacht.

   Auf ähnliche Weise werden die HTTP- und HTTPS-Portnummern abgerufen und es wird geprüft, ob der Server auf diesen Ports überwacht.

Zustand der Partitionen und Reproduktionen

Nach der Überprüfung des Basisserverzustands wird im nächsten Schritt der Zustand der Partitionen und Reproduktionen wie folgt geprüft:

1. Überprüft den Zustand der Reproduktionen der lokalen Partitionen.

2. Liest den Reproduktionsring aller Partitionen auf dem Server und prüft, ob alle Server im Reproduktionsring aktiv sind und ob sich alle Reproduktionen im Zustand "EIN" befinden.
3. Überprüft die Zeitsynchronisierung aller Server im Reproduktionsring. Dadurch wird der Zeitunterschied zwischen den Servern angezeigt.

3.6.5 Kategorisierung des Zustands

Auf Basis der bei der Überprüfung des Zustands eines Servers gefundenen Fehler können drei Zustandskategorien unterschieden werden. Der Status der Zustandsüberprüfungen wird in einer Protokolldatei protokolliert. Weitere Informationen hierzu finden Sie in Abschnitt 3.6.6, „Protokolldateien“, auf Seite 28.

Die drei Zustandskategorien lauten Normal, Warnhinweis und Kritisch.

Normal

Der Serverzustand ist normal, wenn alle Zustandsüberprüfungen erfolgreich durchgeführt wurden.

Die Aufrüstung wird ohne Unterbrechung fortgesetzt.

Warnhinweis

Der Serverzustand befindet sich in der Kategorie "Warnung", wenn bei der Zustandsüberprüfung geringfügige Fehler gefunden wurden.

Wenn die Zustandsüberprüfung als Teil der Aufrüstung ausgeführt wird, werden Sie aufgefordert, entweder den Vorgang abzubrechen oder ihn fortzusetzen.

Warnungen treten normalerweise in den folgenden Szenarien auf:

1. Server überwacht nicht auf LDAP- und HTTP-Ports, entweder normal, sicher oder beides.
2. Die Nicht-Masterserver im Reproduktionsring können nicht kontaktiert werden.
3. Die Server im Reproduktionsring sind nicht synchronisiert.

Kritisch

Der Serverzustand ist kritisch, wenn bei der Zustandsüberprüfung kritische Fehler gefunden wurden.

Wenn die Zustandsüberprüfung als Teil der Aufrüstung ausgeführt wird, wird der Aufrüstungsvorgang abgebrochen.

Der kritische Status tritt normalerweise in den folgenden Fällen auf:

1. Die DIB kann nicht gelesen oder geöffnet werden. Die DIB ist möglicherweise gesperrt oder beschädigt.
2. Die Server im Reproduktionsring können alle nicht kontaktiert werden.
3. Die lokalen Partitionen sind beschäftigt.
4. Die Reproduktion befindet sich nicht im Zustand "EIN".

3.6.6 Protokolldateien

Jeder Vorgang der Serverzustandsüberprüfung, unabhängig davon, ob sie mit der Aufrüstung oder als eigenständiges Dienstprogramm ausgeführt wird, hält den Status des Zustands in einer Protokolldatei fest.

Der Inhalt der Protokolldatei ähnelt den Meldungen, die während der Überprüfungen am Bildschirm angezeigt werden.

Die Protokolldatei der Zustandsüberprüfung enthält Folgendes:

- Status der Zustandsüberprüfung (normal, Warnung oder kritisch).
- URLs zur NetIQ-Support-Site.

In der folgenden Tabelle finden Sie die Speicherorte für die Protokolldatei auf den verschiedenen Plattformen:

Tabelle 3-2 *Speicherorte der Protokolldatei für die Zustandsüberprüfung*

Plattform	Name der Protokolldatei	Standort der Protokolldatei
Linux	`ndscheck.log`	Hängt von dem Speicherort ab, den Sie mit dem Dienstprogramm `ndscheck -F` angegeben haben. Wenn Sie die Option `-F` nicht verwendet haben, wird der Speicherort der Datei `ndscheck.log` von den anderen Optionen bestimmt, die Sie an der ndscheck-Befehlszeile wie folgt verwendet haben: 1. Wenn Sie die Option `-h` verwendet haben, wird die Datei `ndscheck.log` im Basisverzeichnis des Benutzers gespeichert. 2. Wenn Sie die Option `--config-file` verwendet haben, wird die Datei `ndscheck.log` im Protokollverzeichnis der Serverinstanz gespeichert. Sie können auch eine Instanz aus der Liste mehrerer Instanzen auswählen.
Windows	`ndscheck.log`	*`Installationsverzeichnis`*

3.7 SecretStore-Integration mit eDirectory

eDirectory 8.8 stellt Ihnen eine Option zur Konfiguration von Novell SecretStore 3.4 während der eDirectory-Konfiguration zur Verfügung. Vor eDirectory 8.8 mussten Sie SecretStore manuell installieren.

SecretStore ist eine einfache und sichere Passwortverwaltungslösung. Damit können Sie eine einzelne Authentifizierung bei eDirectory für den Zugriff auf die meisten Linux-, Windows-, Web- und Mainframe-Anwendungen verwenden.

Nach der Authentifizierung bei eDirectory speichern SecretStore-fähige Anwendungen die entsprechenden Anmeldeberechtigungsnachweise und rufen sie ab. Durch die Verwendung von SecretStore müssen Sie sich nicht mehr die vielen verschiedenen Passwörter merken, die für den Zugriff auf passwortgeschützte Anwendungen, Websites und Mainframes erforderlich sind, oder diese synchronisieren.

Zur Konfiguration von SecretStore 3.4 zusammen mit eDirectory können sie folgendermaßen vorgehen:

- **Linux:**

  Verwenden Sie den Parameter `ndsconfig add -m ss`. Hier ist `ss` ein optionaler Parameter, der SecretStore bezeichnet. Wenn Sie den Modulnamen nicht angeben, werden alle Module installiert. Wenn Sie SecretStore nicht konfigurieren möchten, können Sie den Wert `no_ss` an diese Option anhängen und `-m no_ss` angeben.

- **Windows:**

  Bei der Installation von eDirectory ist eine Option verfügbar, mit der Sie angeben können, ob das SecretStore-Modul konfiguriert werden soll. Die Option ist standardmäßig aktiviert.

Weitere Informationen zur Verwendung von SecretStore finden Sie im *Novell SecretStore 3.4-Verwaltungshandbuch* (https://www.netiq.com/documentation/secretstore34/).

3.8 Installation der eDirectory-Instrumentation

Früher war die eDirectory-Instrumentation ein Teil von Novell Audit. Ab der eDirectory-Version 8.8 SP3 muss die eDirectory-Instrumentation separat installiert werden.

Detaillierte Informationen zur Installation, Konfiguration und Deinstallation der eDirectory-Instrumentation finden Sie im Abschnitt "eDirectory-Instrumentation" im *NetIQ eDirectory 8.8 SP8-Installationshandbuch*.

3.9 Weiterführende Informationen

In den folgenden Handbüchern finden Sie weitere Informationen zu den in diesem Kapitel behandelten Funktionen:

- *NetIQ eDirectory 8.8 SP8-Installationshandbuch*
- *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*
- Unter Linux: man-Seiten `nds-install`, `ndsconfig` und `ndscheck`

4 NICI-Datensicherung und -Wiederherstellung

Novell International Cryptography Infrastructure (NICI) speichert Schlüssel und Benutzerdaten im Dateisystem sowie in system- und benutzerspezifischen Verzeichnissen und Dateien. Diese Verzeichnisse und Dateien werden geschützt, indem entsprechende Berechtigungen anhand der im Betriebssystem vorhandenen Methode dafür festgelegt werden. Dies erfolgt über das NICI-Installationsprogramm.

Durch die Deinstallation von NICI auf dem System werden die System- oder Benutzerverzeichnisse und -dateien nicht entfernt. Daher sollten diese Dateien nur dann auf einen früheren Stand wiederherstellt werden, wenn sie durch einen Systemabsturz oder einen menschlichen Fehler beschädigt wurden. Es ist wichtig zu verstehen, dass durch Überschreiben eines vorhandenen Satzes an NICI-Benutzerverzeichnissen und -dateien eine vorhandene Anwendung zerstört werden könnte.

Der erforderliche Datenbankschlüssel zum Öffnen der DIB ist im Paket mit den NICI-Schlüsseln enthalten. Aus diesem Grund ist eine eDirectory-Sicherung unbrauchbar, wenn sie unabhängig von einer NICI-Sicherung durchgeführt wird.

Änderungen im Vergleich zur früheren NICI-Sicherungs- und Wiederherstellungsmethode

Früher musste die NICI-Sicherung und -Wiederherstellung manuell durchgeführt werden. In dieser Version wurde eine neue NICI-Sicherungs- und -Wiederherstellungslösung hinzugefügt. Ein Schalter (`-e`) wurde zur eDirectory-Sicherungslösung (eMBox-Sicherung und DSBK) hinzugefügt und dieser Schalter aktiviert Folgendes:

1. Sichern der NICI-Schlüssel während der Ausführung einer eDirectory-Sicherung
2. Wiederherstellen der NICI-Schlüssel während der Ausführung einer eDirectory-Sicherung

Informationen hierzu finden Sie im Abschnitt „Sichern und Wiederherstellen von NICI“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

5 Dienstprogramm "ndspassstore"

"ndspassstore" ist ein neues Dienstprogramm zum Speichern verschlüsselter Passwörter für den sadmin-Benutzer oder den eDirectory-Benutzer. Dieses Dienstprogramm ist auf der Linux- und Windows-Plattform verfügbar. Dieses Dienstprogramm nimmt Benutzernamen und Passwörter als Eingabe und speichert sie als verschlüsselte Schlüsselwertpaare.

In dieser Version wird diese Version zum Festlegen des sadmin-Passworts verwendet.

Dieses Dienstprogramm ist standardmäßig unter Windows unter `C:\Novell\NDS` und unter Linux unter `/opt/novell/eDirectory/bin` verfügbar.

Befehlssynopse

Sie könnten das Dienstprogramm "ndspassstore" durch Eingabe des folgenden Befehls an der Serverkonsole verwenden:

```
ndspassstore -a <Admin-Kontext> -w <Passwort>
```

Option	Verwendung
-a Admin-Kontext	Diese Option wird verwendet, um den Admin-Kontext zu akzeptieren, der den eindeutigen Namen eines Benutzers mit Verwaltungsrechten darstellt.
-w Passwort	Diese Option wird verwendet, um das Passwort (Benutzerpasswort) für die Authentifizierung zu akzeptieren.

6 Mehrere Instanzen

Früher konnten Sie nur eine Instanz von NetIQ eDirectory auf einem einzelnen Host konfigurieren. Durch die Unterstützung der Funktion für mehrere Instanzen in eDirectory 8.8 können Sie Folgendes konfigurieren:

- Mehrere Instanzen von eDirectory auf einem einzelnen Host
- Mehrere Bäume auf einem einzelnen Host
- Mehrere Reproduktion desselben Baums oder derselben Partion auf einem einzelnen Host

eDirectory 8.8 bietet Ihnen auch das Dienstprogramm (ndsmanage) zur einfachen Überwachung der Instanzen.

In der folgenden Tabelle sind die Plattformen aufgeführt, die mehrere Instanzen unterstützen:

Funktion	Linux	Windows
Unterstützung für mehrere Instanzen	✓	✗

Dieses Kapitel enthält die folgenden Informationen:

6.1 Notwendigkeit mehrerer Instanzen

Mehrere Instanzen sind aus der Notwendigkeit der folgenden Vorgänge entstanden:

- Nutzung von High-End-Hardware durch Konfigurieren von mehr als einer Instanz von eDirectory.
- Testen Ihrer Pilot-Einrichtung auf einem einzelnen Host, bevor Sie in die erforderliche Hardware investieren.

6.2 Beispielszenarien für die Bereitstellung mehrerer Instanzen

Mehrere Instanzen desselben Baums oder mehrere Bäume können in den folgenden Szenarien effektiv verwendet werden.

eDirectory in einem großen Unternehmen

- In großen Unternehmen können Sie für Lastausgleich und hohe Verfügbarkeit von eDirectory-Diensten sorgen.

  Wenn beispielsweise auf drei Reproduktionsservern LDAP-Dienste auf den Ports 1524, 2524 und 3524 ausgeführt werden, können Sie eine neue Instanz von eDirectory konfigurieren und einen hochverfügbaren LDAP-Dienst auf einem neuen Port 636 bereitstellen.
- Sie können High-End-Hardware abteilungsübergreifend in einer Organisation nutzen, indem Sie mehrere Instanzen auf einem einzelnen Host konfigurieren.

eDirectory in einer Evaluierungseinrichtung

- **Universitäten:** Viele begeisterte Studenten können eDirectory durch mehrere Instanzen am selben Host evaluieren.
- **Schulung für die eDirectory-Verwaltung:**
  - Schulungsteilnehmer können die Verwaltung an mehreren Instanzen testen.
  - Schulungsleiter können einen einzelnen Host zum Unterrichten einer Gruppe von Studenten verwenden. Jeder Student kann über einen jeweils eigenen Baum verfügen.

6.3 Verwenden von mehreren Instanzen

Mit eDirectory 8.8 fällt Ihnen die Konfiguration von mehreren Instanzen ganz leicht. Um mehrere Instanzen effektiv verwenden zu können, müssen Sie die Einrichtung planen und anschließend mehrere Instanzen konfigurieren.

- Abschnitt 6.3.1, „Planen der Einrichtung“, auf Seite 36
- Abschnitt 6.3.2, „Konfigurieren mehrerer Instanzen“, auf Seite 36

6.3.1 Planen der Einrichtung

Um diese Funktion effektiv nutzen zu können, empfehlen wir Ihnen, die eDirectory-Instanzen zu planen und sicherzustellen, dass jede Instanz eindeutige Instanzkennungen wie Hostname, Portnummer, Servername oder Konfigurationsdatei aufweist.

Bei der Konfiguration von mehreren Instanzen müssen Sie sicherstellen, dass Sie Folgendes geplant haben:

- Speicherort der Konfigurationsdatei
- Speicherort der Variablendaten (wie Protokolldateien)
- Speicherort der DIB
- NCP™-Schnittstelle, eindeutiger Identifizierungsport für jede Instanz und Ports anderer Dienste (wie LDAP-, LDAPS-, HTTP- und HTTPS-Port)
- Eindeutiger Servername für jede Instanz

6.3.2 Konfigurieren mehrerer Instanzen

Sie können mehrere Instanzen von eDirectory mit dem Dienstprogramm "ndsconfig" konfigurieren. In der folgenden Tabelle sind die ndsconfig-Optionen aufgeführt, die Sie einbeziehen müssen, wenn Sie mehrere Instanzen konfigurieren.

HINWEIS: Alle Instanzen verwenden denselben Serverschlüssel (NICI).

Option	Beschreibung
--config-file	Gibt den absoluten Pfad und Dateinamen zum Speichern der Konfigurationsdatei `nds.conf` an. Verwenden Sie beispielsweise zum Speichern der Konfigurationsdatei im Verzeichnis `/etc/opt/novell/eDirectory/` den Pfad `--config-file /etc/opt/novell/eDirectory/nds.conf`.
-b	Gibt die Portnummer an, auf der die neue Instanz überwachen sollte. **HINWEIS:** `-b` und `-B` werden exklusiv verwendet.

-B	Gibt die Portnummer zusammen mit der IP-Adresse oder der Schnittstelle an. Beispiel:
	
	`-B eth0@524`
	
	Alternativ:
	
	`-B 100.1.1.2@524`
	
	HINWEIS: `-b` und `-B` werden exklusiv verwendet.

-D	Erstellt die Verzeichnisse `data`, `dib` und `log` im Pfad, der für die neue Instanz angegeben wurde.
S	Gibt den Servernamen an.

Durch die Verwendung der oben genannten Optionen können Sie eine neue Instanz von eDirectory konfigurieren.

Sie können auch eine neue Instanz mithilfe des Dienstprogramms "ndsmanage" konfigurieren. Weitere Informationen hierzu finden Sie in „Erstellen einer Instanz über "ndsmanage"“, auf Seite 38.

6.4 Verwalten mehrere Instanzen

Dieser Abschnitt enthält folgende Informationen:

6.4.1 Dienstprogramm "ndsmanage"

Das Dienstprogramm "ndsmanage" ermöglicht Ihnen Folgendes:

- Auflisten der konfigurierten Instanzen
- Erstellen einer neuen Instanz
- Ausführen der folgenden Aktionen für eine ausgewählte Instanz:
  - Auflisten der Reproduktionen am Server
  - Starten der Instanz

- Stoppen der Instanz
- Ausführen von DSTrace (ndstrace) für die Instanz
- Dekonfigurieren der Instanz

- Starten und Stoppen aller Instanzen

Auflisten der Instanzen

In der folgenden Tabelle wird beschrieben, wie die eDirectory-Instanzen aufgeführt werden.

Tabelle 6-1 *Verwendung von "ndsmanage" zum Auflisten der Instanzen*

Syntax	Beschreibung
ndsmanage	Führt alle von Ihnen konfigurierten Instanzen auf.
ndsmanage -a|--all	Führt alle Instanzen der Benutzer auf, die eine bestimmte Installation von eDirectory verwenden.
ndsmanage *Benutzername*	Führt die von einem bestimmten Benutzer konfigurierten Instanzen auf

Die folgenden Felder werden für jede Instanz angezeigt:

- Pfad der Konfigurationsdatei
- Server-FDN und Port
- Status (gibt an, ob die Instanz aktiv oder inaktiv ist)

HINWEIS: Dieses Dienstprogramm führt alle für eine einzelne Binärdatei konfigurierten Instanzen auf.

Weitere Informationen finden Sie unter Abbildung 6-1 auf Seite 38.

Erstellen einer Instanz über "ndsmanage"

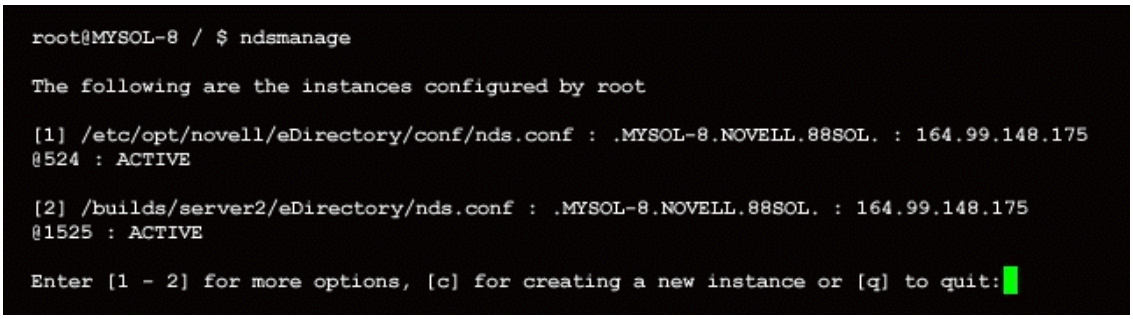
So erstellen Sie eine neue Instanz über "ndsmanage":

1 Geben Sie den folgenden Befehl ein:

```
ndsmanage
```

Wenn Sie zwei Instanzen konfiguriert haben, wird der folgende Bildschirm angezeigt:

Abbildung 6-1 *Ausgabebildschirm des Dienstprogramms "ndsmanage"*



2 Geben Sie "c" ein, um eine neue Instanz zu erstellen.

Sie können entweder einen neuen Baum erstellen oder einem vorhandenen Baum einen Server hinzufügen. Befolgen Sie die Anweisungen am Bildschirm, um eine neue Instanz zu erstellen.

Durchführen von Vorgängen für eine spezifische Instanz

Sie können für jede Instanz die folgenden Vorgänge durchführen:

- „Starten einer spezifischen Instanz“, auf Seite 39
- „Stoppen einer spezifischen Instanz“, auf Seite 40
- „Dekonfigurieren einer Instanz“, auf Seite 40

Zusätzlich zu den oben aufgeführten Befehlen können sie für eine ausgewählte Instanz auch "DSTrace" ausführen.

Starten einer spezifischen Instanz

Gehen Sie folgendermaßen vor, um eine von Ihnen konfigurierte Instanz zu starten:

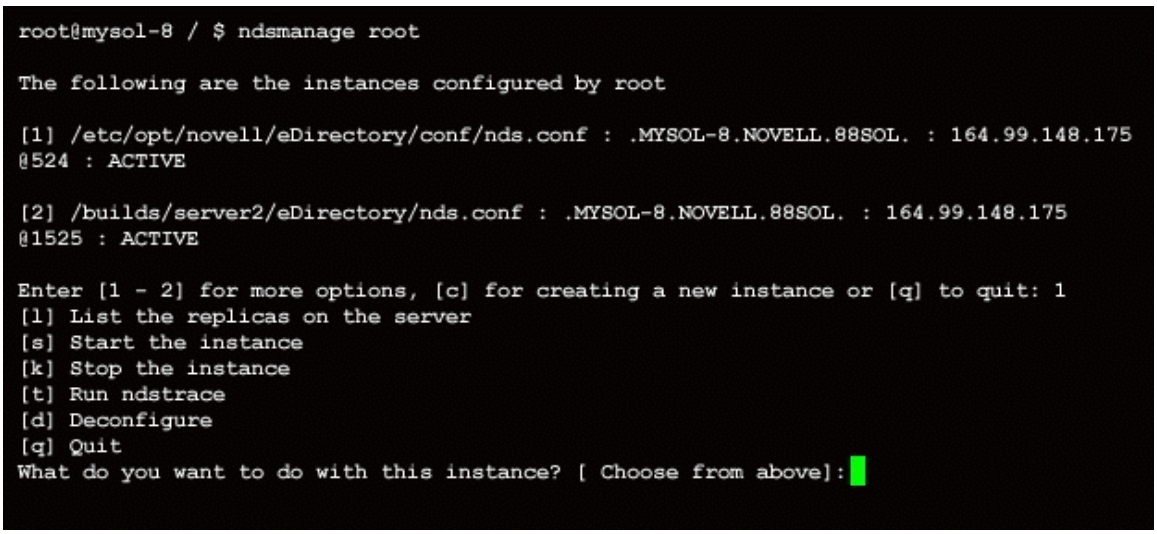
1 Geben Sie Folgendes ein:

```
ndsmanage
```

2 Wählen Sie die zu startende Instanz aus.

Das Menü wird erweitert, um die Optionen einzubeziehen, die Sie für eine spezifische Instanz durchführen können.

Abbildung 6-2 *Ausgabebildschirm des Dienstprogramms "ndsmanage" mit Instanzoptionen*



3 Geben Sie s ein, um die Instanz zu starten.

Alternativ können Sie an der Eingabeaufforderung für den Befehl Folgendes eingeben:

```
ndsmanage start --config-file
Konfigurationsdatei_der_von_Ihnen_konfigurierten_Instanz
```

Stoppen einer spezifischen Instanz

Gehen Sie folgendermaßen vor, um eine von Ihnen konfigurierte Instanz zu stoppen:

1. Geben Sie Folgendes ein:

   ```
   ndsmanage
   ```

2. Wählen Sie die zu stoppende Instanz aus.

   Das Menü wird erweitert, um die Optionen einzubeziehen, die Sie für eine spezifische Instanz durchführen können. Weitere Informationen hierzu finden Sie in Ausgabebildschirm des Dienstprogramms "ndsmanage" mit Instanzoptionen (Seite 39).

3. Geben Sie `k` ein, um die Instanz zu stoppen.

Alternativ können Sie an der Eingabeaufforderung für den Befehl Folgendes eingeben:

```
ndsmanage stop --config-file
Konfigurationsdatei_der_von_Ihnen_konfigurierten_Instanz
```

Dekonfigurieren einer Instanz

Gehen Sie folgendermaßen vor, um eine Instanz zu dekonfigurieren:

1. Geben Sie Folgendes ein:

   ```
   ndsmanage
   ```

2. Wählen Sie die Instanz aus, die dekonfiguriert werden soll.

   Das Menü wird erweitert, um die Optionen einzubeziehen, die Sie für eine spezifische Instanz durchführen können. Weitere Informationen hierzu finden Sie in Ausgabebildschirm des Dienstprogramms "ndsmanage" mit Instanzoptionen (Seite 39).

3. Geben Sie `d` ein, um die Instanz zu dekonfigurieren.

Starten und Stoppen aller Instanzen

Sie können alle von Ihnen konfigurierten Instanzen starten und stoppen.

Starten aller Instanzen

Geben Sie Folgendes an der Eingabeaufforderung für den Befehl ein, um alle von Ihnen konfigurierten Instanzen zu starten:

```
ndsmanage startall
```

Informationen zum Starten einer spezifischen Instanz finden Sie unter „Starten einer spezifischen Instanz“, auf Seite 39.

Stoppen aller Instanzen

Geben Sie Folgendes an der Eingabeaufforderung für den Befehl ein, um alle von Ihnen konfigurierten Instanzen zu stoppen:

```
ndsmanage stopall
```

Informationen zum Stoppen einer spezifischen Instanz finden Sie unter „Stoppen einer spezifischen Instanz“, auf Seite 40.

6.4.2 Identifizieren einer spezifischen Instanz

Bei der Konfiguration mehrere Instanzen weisen Sie jeder Instanz einen Hostnamen, eine Portnummer und einen eindeutigen Pfad für die Konfigurationsdatei zu. Dieser Hostname und diese Portnummer sind die Instanz-IDs.

Die meisten Dienstprogramme verfügen über die Option `-h`*`Hostname`*`:`*`Port`* oder `--config-file`*`Speicherort_der_Konfigurationsdatei`*, mit der Sie eine bestimmte Instanz angeben können. Weitere Informationen finden Sie auf den man-Seiten der Dienstprogramme.

6.4.3 Aufrufen eines Dienstprogramms für eine spezifische Instanz

Wenn Sie ein Dienstprogramm für eine spezifische Instanz ausführen möchten, müssen Sie die Instanz-ID in den Dienstprogrammbefehl einbeziehen. Die Instanz-IDs sind der Pfad der Konfigurationsdatei sowie der Hostname und die Portnummer. Sie können dazu `--config-file` *`Speicherort_der_Konfigurationsdatei`* oder `-h`*`Hostname`*`:`*`Port`* verwenden.

Wenn Sie die Instanz-IDs nicht in den Befehl einbeziehen, zeigt das Dienstprogramm verschiedene Instanzen an, die Sie besitzen, und fordert Sie auf, die Instanz auszuwählen, für die das Dienstprogramm ausgeführt werden soll.

Um beispielsweise DSTrace für ein spezfisches Dienstprogramm mit der Option `--config-file` auszuführen, sollten Sie Folgendes eingeben:

```
ndstrace --config-file configuration_filename_with_location
```

6.5 Beispielszenario für mehrere Instanzen

Mary ist eine Nicht-Root-Benutzerin, die zwei Bäume an einem einzelnen Host-Computer für eine einzelne Binärdatei konfigurieren möchte.

6.5.1 Planen der Einrichtung

Mary gibt die folgenden Instanz-IDs an.

- **Instanz 1:**

Portnummer, an der die Instanz überwachen sollte	1524
Pfad der Konfigurationsdatei	`/home/maryinst1/nds.conf`
DIB-Verzeichnis	`/home/mary/inst1/var`

- **Instanz 2:**

Portnummer, an der die Instanz überwachen sollte	2524
Pfad der Konfigurationsdatei	`/home/mary/inst2/nds.conf`
DIB-Verzeichnis	`/home/mary/inst2/var`

6.5.2 Konfigurieren der Instanzen

Mary muss die folgenden Befehle eingeben, um die Instanzen auf Basis der oben genannten Instanz-IDs zu konfigurieren:

- **Instanz 1:**

  ```
  ndsconfig new -t mytree -n o=novell -a cn=admin.o=company -b 1524 -D
  /home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
  ```

- **Instanz 2:**

  ```
  ndsconfig new -t corptree -n o=novell -a cn=admin.o=company -b 2524 -D
  /home/mary/inst2/var --config-file /home/mary/inst2/nds.conf
  ```

6.5.3 Aufrufen eines Dienstprogramms für eine Instanz

Wenn Mary das DSTrace-Dienstprogramm für Instanz 1 ausführen möchte, die an Port 1524 überwacht, deren Konfigurationsdatei sich unter `/home/mary/inst1/nds.conf` befindet und deren DIB-Datei unter `/home/mary/inst1/var`, dann kann sie das Dienstprogramm wie folgt ausführen:

```
ndstrace --config-file /home/mary/inst1/nds.conf
```

Alternativ:

```
ndstrace -h 164.99.146.109:1524
```

Wenn Mary die Instanz-IDs nicht angibt, zeigt das Dienstprogramm alle Instanzen an, die Mary besitzt, und fordert sie auf, eine Instanz auszuwählen.

6.5.4 Auflisten der Instanzen

Wenn Mary Details zu den Instanzen im Host erfahren möchte, kann sie das Dienstprogramm "ndsmanage" ausführen.

- So werden alle Instanzen von Mary angezeigt:

  ```
  ndsmanage
  ```

- So werden alle Instanzen von John (Benutzername ist "john") angezeigt:

  ```
  ndsmanage john
  ```

- So werden alle Instanzen von allen Benutzern angezeigt, die eine bestimmte Installation von eDirectory verwenden:

  ```
  ndsmanage -a
  ```

6.6 Weiterführende Informationen

Weitere Informationen über die Unterstützung für mehrere Instanzen finden Sie in den folgenden Dokumentationen:

- *NetIQ eDirectory 8.8 SP8-Installationshandbuch*
- Für Linux: man-Seiten für "ndsconfig" und "ndsmanage"

7 Authentifizierung bei eDirectory über SASL-GSSAPI

Anhand der SASL-GSSAPI-Methode für NetIQ eDirectory 8.8 können Sie sich bei eDirectory über LDAP anhand eines Kerberos-Tickets authentifizieren ohne das eDirectory-Benutzerpasswort verwenden zu müssen. Das Kerberos-Ticket sollte durch Authentifizieren bei einem Kerberos-Server abgerufen werden.

Diese Funktion ist hauptsächlich nützlich für Benutzer der LDAP-Anwendung in Umgebungen, in denen bereits eine Kerberos-Infrastruktur installiert ist. Daher sollten diese Benutzer in der Lage sein, sich am LDAP-Server zu authentifizieren, ohne ein separates LDAP-Benutzerpasswort angeben zu müssen.

Um dies zu erleichtern, führt eDirectory die SASL-GSSAPI-Methode ein.

Die aktuelle Implementierung von SASL-GSSAPI ist kompatibel mit RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222) und unterstützt nur Kerberos v5 als Authentifizierungsmethode.

Dieses Kapitel enthält die folgenden Informationen:

7.1 Konzepte

7.1.1 Was ist Kerberos?

Kerberos ist ein eigenständiges Protokoll, das eine Methode zur Authentifizierung von Entitäten in einem Netzwerk bereitstellt. Es basiert auf einem verbürgten Drittanbietermodell. Es verwendet gemeinsame geheime Schlüssel und eine symmetrische Schlüsselkryptografie.

Weitere Informationen finden Sie unter RFC 1510 (http://www.ietf.org/rfc/rfc1510.txt?number=1510).

7.1.2 Was ist SASL?

Simple Authentication and Security Layer (SASL) stellt eine Authentifizierungsabstraktionsschicht für Anwendungen bereit. Es ist ein Framework, in das Authentifizierungsmodule integriert werden können.

Weitere Informationen finden Sie unter RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222).

7.1.3 Was ist GSSAPI?

Generic Security Services Application Program Interface (GSSAPI) bietet Authentifizierungsdienste und andere Sicherheitsdienste über einen Standardsatz von APIs. Es unterstützt verschiedene Authentifizierungsmethoden. Kerberos v5 ist die geläufigste Methode.

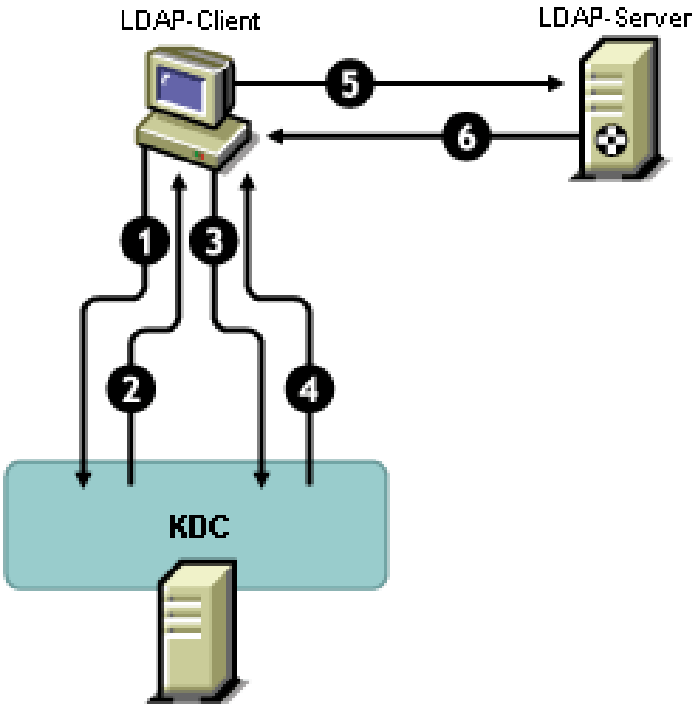
Weitere Informationen zu den GSS-APIs finden Sie unter RFC 1964 (http://www.ietf.org/rfc/rfc1964.txt?number=1964).

Diese SASL-GSSAPI-Implementierung stammt aus Abschnitt 7.2 von RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222).

7.2 Wie arbeiten GSSAPI und eDirectory zusammen?

In der folgenden Grafik ist dargestellt, wie GSSAPI mit einem LDAP-Server zusammenarbeitet.

Abbildung 7-1 *Wie funktioniert GSSAPI?*



In der Abbildung oben bezeichnen die Zahlen Folgendes:

1. Ein eDirectory-Benutzer sendet eine Anforderung über einen LDAP-Client an den Kerberos-KDC (Key Distribution Center)-Server für ein erstes Ticket, genannt Ticket Granting Ticket (TGT).

Ein Kerberos-KDC kann von MIT oder Microsoft* stammen.

2. KDC antwortet dem LDAP-Client mit einem TGT.
3. Der LDAP-Client sendet das TGT zurück an das KDC und fordert ein LDAP-Serviceticket an.
4. KDC antwortet dem LDAP-Client mit dem LDAP-Serviceticket.
5. Der LDAP-Client führt den Befehl "ldap_sasl_bind" an den LDAP-Server aus und sendet das LDAP-Serviceticket.
6. Der LDAP-Server validiert das LDAP-Serviceticket mithilfe der GSSAPI-Methode und sendet dem LDAP-Client je nach Ergebnis eine Meldung über die erfolgreiche Ausführung von "ldap_sasl_bind" oder einen Fehler zurück.

7.3 Konfigurieren von GSSAPI

1. Das iManager-Plugin für SASL-GSSAPI funktioniert nicht, wenn iManager nicht zur Verwendung der SSL/TLS-Verbindung mit eDirectory konfiguriert ist. Eine sichere Verbindung ist obligatorisch, um den Masterschlüssel und die Prinzipalschlüssel des Bereichs zu schützen.

   Standardmäßig wird iManager für die SSL/TLS-Verbindung mit eDirectory konfiguriert. Wenn die Kerberos-Anmeldemethode für GSSAPI an einem anderen Baum als den, in dem die iManager-Konfiguration gehostet wird, konfiguriert werden soll, müssen Sie iManager für die SSL/TLS-Verbindung mit eDirectory konfigurieren.

   Informationen zur Konfiguration von iManager mit der SSL/TLS-Verbindung mit eDirectory finden Sie im *NetIQ iManager 2.7-Verwaltungshandbuch* (https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html).

   Das iManager-Plugin für SASL-GSSAPI (`kerberosPlugin.npm`) ist als Teil der Dateien `eDir_88_iMan26_Plugins.npm` und `eDir_88_iMan27_Plugins.npm` verfügbar. Laden sie die NPMs von der Novell-Download-Website (http://download.novell.com) herunter.
2. So verwenden Sie ein Kerberos-Ticket zur Authentifizierung an einem eDirectory-Server:
   - **2a** Erweitern Sie das Kerberos-Schema.
   - **2b** Erstellen Sie einen Bereichscontainer.
   - **2c** Extrahieren Sie einen Service-Prinzipalschlüssel oder gemeinsamen Schlüssel vom KDC.
   - **2d** Erstellen Sie das Prinzipalobjekt des LDAP-Diensts.
   - **2e** Verknüpfen Sie einen Kerberos-Prinzipalnamen mit dem Benutzerobjekt.

Informationen zu den oben genannten Schritten finden Sie im Abschnitt „Konfigurieren von GSSAPI mit eDirectory“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

7.4 Wie wird GSSAPI von LDAP verwendet?

Nach der Konfiguration wird GSSAPI zusammen mit den anderen SASL-Methoden dem Attribut `supportedSASLMechanisms` unter `rootDSE` hinzugefügt. `rootDSE (DSA [Directory System Agent]-spezifischer Eintrag)` ist ein Eintrag, der sich im Stamm des Directory Information Tree (DIT) befindet. Weitere Informationen finden Sie im Abschnitt „Verstehen, wie LDAP mit eDirectory zusammenarbeitet“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

Der LDAP-Server fragt SASL nach den installierten Methoden, wenn er seine Konfiguration erhält, und unterstützt automatisch alles, was installiert ist. Der LDAP-Server meldet außerdem die aktuell unterstützten SASL-Methoden in seinem `rootDSE` durch Verwendung des Attributs `supportedSASLMechanisms`.

Wenn Sie GSSAPI konfigurieren, wird es daher zur Standardmethode. Um speziell einen LDAP-Vorgang über die SASL GSSAPI-Methode auszuführen, können Sie GSSAPI an der Befehlszeile angeben.

Um beispielsweise eine Suche in OpenLDAP anhand der GSSAPI-Methode durchzuführen, würden Sie Folgendes eingeben:

```
ldapsearch -Y GSSAPI -h 164.99.146.48 -b "" -s base
```

7.5 Allgemein verwendete Begriffe

In der folgenden Tabelle sind die Termini definiert, die üblicherweise mit Kerberos und GSSAPI verwendet werden.

Tabelle 7-1 *Kerberos/GSSAPI-Terminologie*

Begriff	Definition
Key Distribution Center (KDC)	Kerberos-Server, der Benutzer- und Problemtickets authentifiziert.
Prinzipal	Eine Entität (Benutzer oder Dienstinstanz), die am KDC registriert ist.
Bereich	Eine Domäne oder Gruppe von Prinzipalen, die von einem Satz von KDCs bedient werden.
Serviceticket (ST)	Ein Datensatz mit Client-Informationen, Dienstinformationen und einem Sitzungsschlüssel, der mit dem speziellen gemeinsamen Schlüssel des Dienstprinzipals verschlüsselt wurde.
Ticket Granting Ticket (TGT)	Ein Tickettyp, mit dem der Client zusätzliche Kerberos-Tickets abrufen kann.

8 Erzwingen von universellen Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird

In NetIQ eDirectory 8.8 können Sie "Universelles Passwort" deaktivieren und die Unterscheidung von Groß- und Kleinschreibung für Ihr Passwort verwenden, wenn Sie auf den eDirectory 8.8-Server über die folgenden Clients und Dienstprogramme zugreifen:

- Novell Client 4.9 und höher
- Verwaltungsdienstprogramme, die auf eDirectory 8.8 aufgerüstet wurden
- NetIQ iManager 2.7 und höher, außer wenn es unter Windows ausgeführt wird

Sie können jede beliebige Version von LDAP SDK verwenden, um Passwörter zu nutzen, bei denen zwischen Groß- und Kleinschreibung unterschieden wird.

In der folgenden Tabelle sind die Plattformen aufgeführt, auf denen die Funktion für Passwörter unterstützt wird, bei denen zwischen Groß- und Kleinschreibung unterschieden wird:

Funktion	Linux	Windows
Erzwingen von universellem Passwort, bei dem zwischen Groß- und Kleinschreibung unterschieden wird	✓	✓

Dieses Kapitel enthält die folgenden Informationen:

8.1 Notwendigkeit von Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird

Die Verwendung von Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, macht die Anmeldung im Verzeichnis sicherer. Wenn Sie beispielsweise über ein Passwort "aBc" verfügen, bei dem zwischen Groß- und Kleinschreibung unterschieden wird, dann würden alle Anmeldeversuche wie "abc", "Abc" oder "ABC" fehlschlagen.

In eDirectory 8.8 und höher können Sie Passwörter, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, für alle Clients verwenden, die auf eDirectory 8.8 aufgerüstet werden.

Durch die Erzwingung von Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, können Sie verhindern, dass alte Novell-Clients auf den eDirectory 8.8-Server zugreifen. Weitere Informationen finden Sie unter Abschnitt 8.4, „Verhindern des Zugriffs auf den eDirectory 8.8-Server durch alte Novell-Clients“, auf Seite 51.

8.2 Methode zum Erstellen von Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird

In eDirectory 8.8. und höher können Sie Passwörter, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, für alle Clients erstellen, indem Sie "Universelles Passwort" aktivieren. "Universelles Passwort" ist standardmäßig deaktiviert.

8.2.1 Voraussetzungen

Standardmäßig führen LDAP und andere Dienstprogramme auf Serverseite zuerst die NDS-Anmeldung durch. Wenn diese fehlschlägt, wird die Anmeldung vom Typ "Einfaches Passwort" verwendet. Damit die Funktion für Passwörter, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, funktioniert, muss die Anmeldung über den Novell Modular Authentication Service (NMAS) erfolgen. Daher müssen Sie die Umgebungsvariable `NDSD_TRY_NMASLOGIN_FIRST` auf "Wahr" festlegen, damit die Funktion für Passwörter, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, verfügbar ist.

Führen Sie den folgenden Vorgang aus, um die Funktion für Passwörter, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, verfügbar zu machen:

1. Legen Sie die Umgebungsvariable fest
   - Linux:

     Fügen Sie Folgendes am Ende des Pfads `/opt/novell/eDirectory/sbin/pre_ndsd_start` hinzu.

     ```
     NDSD_TRY_NMASLOGIN_FIRST=true
     export NDSD_TRY_NMASLOGIN_FIRST
     ```

   - Windows:

     Klicken Sie mit der rechten Maustaste auf Eigener Computer und wählen Sie Eigenschaften aus. Klicken Sie auf der Registerkarte "Erweitert" auf "Umgebungsvariablen". Fügen Sie unter "Systemvariablen" die Variable hinzu und legen Sie den Wert auf "Wahr" fest.
2. Starten Sie den eDirectory-Server neu.

HINWEIS: Durch die Verwendung von NMAS für die Authentifizierung dauert der Anmeldvorgang länger.

8.2.2 Erstellen von Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird

1. Melden Sie sich bei eDirectory mit dem vorhandenen Passwort an.

   Im Fall einer neuen Installation ist das vorhandene Passwort dasjenige, das Sie bei der Konfiguration von eDirectory 8.8 festgelegt haben.

   Ihr Passwort lautet beispielsweise "novell".

   HINWEIS: Bei diesem Passwort wird nicht zwischen Groß- und Kleinschreibung unterschieden.

   ---

2. Universelles Passwort aktivieren.

   Weitere Informationen finden Sie im Abschnitt „Bereitstellen eines universellen Passworts“ im *Novell-Passwortverwaltung 3.3 - Verwaltungshandbuch* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html).

3. Melden Sie sich bei eDirectory ab.

4. Melden Sie sich bei eDirectory mit dem vorhandenen Passwort an und verwenden Sie die Groß- und Kleinschreibung.

   Bei dem nun vergebenen Passwort wird zwischen Groß- und Kleinschreibung unterschieden.

   Sie geben beispielsweise "NoVELL" ein.

   Ihr Passwort lautet nun "NoVELL". Daher wäre nun "novell" oder eine andere Kombination von Groß- und Kleinschreibung als "NoVELL" ungültig.

Informationen zur Migration zu Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, finden Sie unter Abschnitt 8.3.1, „Migrieren zu Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird“, auf Seite 50.

Bei jedem neu festgelegten Passwort wird nun zwischen Groß- und Kleinschreibung unterschieden, abhängig davon, auf welcher Ebene (Objekt oder Partition) Sie das universelle Passwort aktiviert haben.

8.2.3 Verwalten von Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird

Sie können die Unterscheidung zwischen Groß- und Kleinschreibung für Ihre Passwörter verwalten, indem Sie die Option "Universelles Passwort" über iManager aktivieren oder deaktivieren. Weitere Informationen finden Sie im Abschnitt „Bereitstellen eines universellen Passworts“ im *NetIQ-Passwortverwaltung 3.3 - Verwaltungshandbuch* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html).

8.3 Aufrüsten der alten Novell-Clients und -Dienstprogramme

Nachfolgend sehen Sie die neuesten Versionen der Novell-Clients und NetIQ-Dienstprogramme:

- Novell Client 4.9
- Verwaltungsdienstprogramme mit eDirectory 8.8
- NetIQ iManager 2.7 und höher

Die Clients und Dienstprogramme, die älter als die oben genannten Versionen sind, werden als alte Novell-Clients betrachtet.

Sie können für die alten Novell-Clients nach deren Aufrüstung auf die neuesten Versionen Passwörter festlegen, bei denen zwischen Groß- und Kleinschreibung unterschieden wird. Mit eDirectory 8.8 ist die Migration von Ihren vorhandenen Passwörtern zu Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, ganz leicht und flexibel durchführbar. Weitere Informationen finden Sie unter Abschnitt 8.3.1, „Migrieren zu Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird“, auf Seite 50.

Falls Sie die alten Clients nicht auf die neuesten Versionen aufrüsten, können diese Clients für die Verwendung von eDirectory 8.8 auf Serverebene blockiert werden. Weitere Informationen finden Sie unter Abschnitt 8.4, „Verhindern des Zugriffs auf den eDirectory 8.8-Server durch alte Novell-Clients“, auf Seite 51.

8.3.1 Migrieren zu Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird

Die Option "Universelles Passwort" ist standardmäßig deaktiviert und daher sind Ihre vorhandenen Passwörter erst dann davon betroffen, wenn Sie "Universelles Passwort" in iManager aktivieren. Eine schrittweise Anleitung finden Sie unter Abschnitt 8.2, „Methode zum Erstellen von Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird“, auf Seite 48.

Im folgenden Beispiel wird die Migration zu Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, erklärt:

Anmeldesitzung 1: Die Option "Universelles Passwort" ist standardmäßig deaktiviert.

- Sie melden sich mit Ihrem vorhandenen Passwort an. Nehmen Sie beispielsweise an, dass Ihr Passwort "netiq" lautet.
- Bei diesem Passwort wird nicht zwischen Groß- und Kleinschreibung unterschieden. Daher sind sowohl "netiq" als auch "NetIQ" gültige Passwörter.
- Nach der Anmeldung aktivieren Sie "Universelles Passwort". Weitere Informationen finden Sie im Abschnitt „Bereitstellen eines universellen Passworts“ im *NetIQ-Passwortverwaltung 3.3 - Verwaltungshandbuch* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html).

Anmeldesitzung 2: Universelles Passwort wurde in der vorigen Sitzung aktiviert.

- Sie melden sich mit Ihrem vorhandene Passwort an. Beispiel: Angenommen, Sie tippen das Passwort "noVell" ein.
- Wenn die Option "Universelles Passwort" aktiviert ist, wird bei diesem Passwort zwischen Groß- und Kleinschreibung unterschieden. Daher müssen Sie sich merken, wie Sie das Passwort eingetippt haben.

Anmeldesitzung 3 und folgende Anmeldungen.

- Wenn Sie sich mit dem Passwort "netIQ" anmelden, ist es gültig.
- Wenn Sie sich mit dem Passwort "NetIQ" (oder einer anderen Version außer "noVell") anmelden, ist es ungültig.

8.4 Verhindern des Zugriffs auf den eDirectory 8.8-Server durch alte Novell-Clients

In eDirectory 8.7.1 und 8.7.3 konnten Sie verhindern, dass alte Novell-Clients das NDS-Passwort festlegen oder ändern. Mit eDirectory 8.8 können Sie außerdem auch verhindern, dass diese sich bei eDirectory 8.8 anmelden und die Passwörter überprüfen.

Um die Verwendung von eDirectory 8.8 durch alte Novell-Clients zuzulassen oder zu verhindern, müssen Sie die NDS-Anmeldung entweder über iManager oder über LDAP konfigurieren.

Dieser Abschnitt enthält folgende Informationen:

8.4.1 Notwendigkeit der Verhinderung des Zugriffs auf den eDirectory 8.8-Server durch alte Novell-Clients

Bei den Passwörtern der alten Novell-Clients wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn Sie daher in eDirectory 8.8 und höher die Verwendung von Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, erzwingen möchten, müssen Sie möglicherweise den Zugriff auf das Verzeichnis für alte Clients sperren.

In älteren Versionen als Novell Client 4.9 wurde die Option "Universelles Passwort" nicht unterstützt. Der Grund dafür bestand darin, dass Anmeldungs- und Passwortänderungen direkte Auswirkung auf das NDS-Passwort anstatt auf NMAS hatten. Wenn Sie nun die Option "Universelles Passwort" verwenden, kann die Änderung von Passwörtern durch alte Clients ein Problem verursachen, das als "Passwortabweichung (password drift)" bekannt ist. Dies bedeutet, dass das NDS-Passwort und das universelle Passwort nicht synchronisiert werden. Um dieses Problem zu verhindern, können Sie Passwortänderungen durch Clients älter als Version 4.9 blockieren.

Im nächsten Abschnitt, Verwalten von NDS-Anmeldekonfigurationen, finden Sie weitere Informationen darüber, wie der Zugriff auf den eDirectory 8.8-Server durch alte Clients blockiert wird.

8.4.2 Verwalten von NDS-Anmeldekonfigurationen

Durch Konfigurieren der NDS-Anmeldung können Sie den Zugriff auf den eDirectory 8.8-Server durch alte Novell-Clients zulassen oder verhindern. Sie können die NDS-Anmeldungsverwaltung über iManager 2.6 und über LDAP verwalten.

In eDirectory 8.8 und höher können Sie das Festlegen und Ändern über LDAP und iManager konfigurieren.

Dieser Abschnitt enthält Informationen zu Folgendem:

- „Verwalten von NDS-Konfigurationen über LDAP“, auf Seite 54
- Abschnitt 8.4.4, „Erzwingen von Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, in einem gemischten Baum“, auf Seite 55

NDS-Konfigurationen auf unterschiedlichen Ebenen

Sie können NDS-Anmeldungen auf einer oder allen der folgenden Ebenen konfigurieren:

- Partitionsebene
- Objektebene

Wenn Sie die Konfiguration auf keiner dieser Ebenen ausdrücklich angeben, wird die NDS-Anmeldekonfiguration auf allen Ebenen aktiviert.

Die Konfiguration auf Objektebene hat immer Vorrang vor der Konfiguration auf Partitionsebene. Dies wird in der folgenden Tabelle beschrieben:

Tabelle 8-1 *NDS-Konfiguration*

Konfiguration auf Objektebene	Konfiguration auf Partitionsebene	Konfiguration
Nicht angegeben	Aktiviert	Aktiviert
Aktiviert	Nicht angegeben	Aktiviert
Nicht angegeben	Deaktiviert	Deaktiviert
Deaktiviert	Nicht angegeben	Deaktiviert
Aktiviert	Aktiviert	Aktiviert
Aktiviert	Deaktiviert	Aktiviert
Deaktiviert	Aktiviert	Deaktiviert
Deaktiviert	Deaktiviert	Deaktiviert

Auf allen Ebenen (Objekt und Partition) können Sie die NDS-Anmeldung für Folgendes konfigurieren:

- Anmelden im Verzeichnis mit einem NDS-Passwort oder Überprüfen des NDS-Passworts
- Festlegen eines neuen Passworts und Ändern des vorhandenen Passworts

Anmelden im Verzeichnis oder Überprüfen des NDS-Passworts

Anmeldung/Überprüfung des NDS-Passworts bedeutet:

- Anmelden im Verzeichnis mit einem NDS-Passwort.
- Überprüfen des vorhandenen Passworts im Verzeichnis.

Anmeldung/Überprüfung des NDS-Passworts ist standardmäßig aktiviert. Wenn Sie den Schlüssel für Anmeldung/Überprüfung deaktivieren, können Sie sich nicht bei der neuesten Version von eDirectory anmelden oder die Passwörter überprüfen. Sie können die Anmeldung/Überprüfung des NDS-Passworts auf Partitions- und Objektebene aktivieren oder deaktivieren. Wenn Anmeldung/Überprüfung deaktiviert ist, können Sie nicht NDS-Passwörter festlegen oder ändern.

Sie können das NDS-Passwort für die Anmeldung/Überprüfung über iManager und LDAP konfigurieren. Weitere Informationen finden Sie in „Verwalten von NDS-Konfigurationen über iManager“, auf Seite 53 und „Verwalten von NDS-Konfigurationen über LDAP“, auf Seite 54.

Festlegen eines neuen Passworts oder Ändern des NDS-Passworts

NDS-Passwortfestlegung/-änderung bedeutet

- Festlegen eines neuen Passworts für ein Objekt.
- Ändern des vorhandenen Passworts für ein Objekt.

Die NDS-Passwortfestlegung/-änderung ist standardmäßig aktiviert. Wenn Sie den Schlüssel für die Festlegung/Änderung deaktivieren, können Sie in eDirectory kein neues Passwort festlegen oder das vorhandene Passwort ändern. Sie können die NDS-Passwortfestlegung/-änderung auf Partitions- und Objektebene aktivieren oder deaktivieren. Wenn Anmeldung/Überprüfung deaktiviert ist, können Sie keine Passwörter festlegen/ändern.

Früher konnten Sie NDS-Passwörter nur über LDAP festlegen/ändern. Nun können Sie dies auch über iManager erledigen. Weitere Informationen finden Sie in „Verwalten von NDS-Konfigurationen über iManager“, auf Seite 53 und „Verwalten von NDS-Konfigurationen über LDAP“, auf Seite 54.

Verwalten von NDS-Konfigurationen über iManager

Dieser Abschnitt enthält folgende Informationen:

Sie können den Schlüssel für die Anmeldung/Überprüfung oder den Schlüssel für die Festlegung/Änderung bei der NDS-Anmeldungskonfiguration aktivieren.

Aktivieren/Deaktivieren der NDS-Konfiguration für eine Partition

So aktivieren Sie die NDS-Anmeldung für eDirectory-Clients vor Version 8.8:

1. Klicken Sie in iManager auf die Schaltfläche *Rollen und Aufgaben*  .
2. Wählen Sie *NMAS > Erzwingung des universellen Passworts* aus.
3. Wählen Sie im Plugin "Erzwingung des universellen Passworts" die Option *NDS-Konfiguration für eine Partition* aus.
4. Befolgen Sie die Anweisungen im Assistenten für die NDS-Konfiguration für eine Partition, um die Anmeldungs- und Passwortsverwaltung auf Partitionsebene zu konfigurieren.

   Die Hilfe steht Ihnen im Assistenten jederzeit zur Verfügung.

Aktivieren/Deaktivieren der NDS-Konfiguration für ein Objekt

So aktivieren Sie die NDS-Anmeldung für eDirectory-Clients vor Version 8.8:

1. Klicken Sie in iManager auf die Schaltfläche *Rollen und Aufgaben*  .
2. Wählen Sie *NMAS > Erzwingung des universellen Passworts* aus.
3. Wählen Sie im Assistenten die Option *NDS-Konfiguration für ein Objekt* aus.

4 Befolgen Sie die Anweisungen im Assistenten für die NDS-Konfiguration für eine Partition, um die Anmeldungs- und Passwortverwaltung auf Objektebene zu konfigurieren.

Die Hilfe steht Ihnen im Assistenten jederzeit zur Verfügung.

Verwalten von NDS-Konfigurationen über LDAP

WICHTIG: Wir empfehlen Ihnen dringend, iManager für die Verwaltung von NDS-Konfigurationen zu verwenden und nicht LDAP.

Sie können NDS-Konfigurationen über LDAP anhand eines eDirectory-Attributs am Stammcontainer einer Partition oder an einem Objekt verwalten. Die Attribute sind Teil des Schemas in eDirectory 8.7.1 oder höher; sie werden nicht unter eDirectory 8.7 oder einer älteren Version unterstützt.

Die von alten Clients verwendete Methode zum Konfigurieren der NDS-Anmeldungskonfigurationen wird NDAP-Anmeldungsverwaltung genannt und die Methode für NDS-Passwortkonfigurationen wird NDAP-Passwortverwaltung genannt.

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:

- „Aktivieren/Deaktivieren der NDS-Konfiguration für eine Partition“, auf Seite 54
- „Aktivieren/Deaktivieren der NDS-Konfigurationen für ein Objekt“, auf Seite 54

Aktivieren/Deaktivieren der NDS-Konfiguration für eine Partition

Verwaltung der Passwort-Anmeldung/Überprüfung

Verwenden Sie das Attribut `ndapPartitionLoginMgmt`, um die Verwaltung der NDS-Passwort-Anmeldung/Überprüfung für eine Partition zu aktivieren oder zu deaktivieren.

Attributwert `ndapPartitionLoginMgmt`	Beschreibung
Nicht vorhanden oder nicht angegeben	NDAP-Anmeldungsverwaltung ist aktiviert.
0	Die NDAP-Anmeldungsverwaltung ist deaktiviert.
1	NDAP-Anmeldungsverwaltung ist aktiviert.

NDS-Passwort festlegen und ändern

Verwenden Sie das Attribut `ndapPartitionPasswordMgmt`, um die Festlegung/Änderung eines NDS-Passworts für eine Partition zu aktivieren oder zu deaktivieren.

Attributwert `ndapPartitionPasswordMgmt`	Beschreibung
Nicht vorhanden oder nicht angegeben	NDAP-Anmeldungsverwaltung ist deaktiviert.
0	Die NDAP-Passwortverwaltung ist deaktiviert.
1	NDAP-Anmeldungsverwaltung ist deaktiviert.

Aktivieren/Deaktivieren der NDS-Konfigurationen für ein Objekt

NDS-Passwort-Anmeldung/-Überprüfung

Verwenden Sie das Attribut `ndapLoginMgmt`, um die Verwaltung der NDS-Anmeldung/-Überprüfung für ein Objekt zu aktivieren oder zu deaktivieren.

Attributwert `ndapLoginMgmt`	Beschreibung
Nicht vorhanden oder nicht angegeben	Die NDAP-Anmeldungsverwaltung hängt von der Konfiguration auf Partitionsebene ab.
0	Die NDAP-Anmeldungsverwaltung ist deaktiviert, wenn Sie auf Partitionsebene deaktiviert wurde.
1	Die NDAP-Anmeldungsverwaltung ist aktiviert, unabhängig von der Konfigurationseinstellung auf Partitionsebene.

NDS-Passwort festlegen und ändern

Verwenden Sie das Attribut `ndapPasswordMgmt`, um die Festlegung und Änderung eines NDS-Passworts für ein Objekt zu aktivieren oder zu deaktivieren.

Attributwert `ndapPasswordMgmt`	Beschreibung
Nicht vorhanden oder nicht angegeben	Die NDAP-Passwortverwaltung hängt von der Konfiguration auf Partitionsebene ab.
0	Die NDAP-Passwortverwaltung ist deaktiviert, wenn Sie auf Partitionsebene deaktiviert wurde.
1	Die NDAP-Passwortverwaltung ist aktiviert, unabhängig von der Konfigurationseinstellung auf Partitionsebene.

HINWEIS: Weitere Informationen zur Erstellung und Verwaltung von Prioritätssynchronisierungsrichtlinien finden Sie in den Abschnitten „Verwenden von LDAP-Tools unter Linux“ und „NetIQ-Import/Export-Konversionsprogramm“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

8.4.3 Partitionsoperationen

Wenn Sie eine Partition teilen, werden die NDS-Konfigurationen von der untergeordneten Partition nicht übernommen. Wenn Sie Partitionen zusammenführen, werden die NDS-Konfigurationen der übergeordneten Partition von der resultierenden Partition beibehalten.

8.4.4 Erzwingen von Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, in einem gemischten Baum

Wenn ein Baum auf einem eDirectory 8.8-Server oder höher und einem eDirectory 8.7-Server oder früher vorhanden ist, und wenn sich die beiden Server eine Partition teilen, dann führt die Deaktivierung der NDS-Anmeldungskonfiguration zu unzuverlässigen Ergebnissen. Der 8.8-Server erzwingt die Einstellung und verhindert, dass alte Clients Zugriff auf das Verzeichnis haben. Der 8.7-Server erzwingt die Einstellungen jedoch nicht, sodass Sie über den 8.7-Server auf das Verzeichnis zugreifen können.

8.5 Weiterführende Informationen

Weitere Informationen zu Passwörtern, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, finden Sie in den folgenden Dokumentationen:

- iManager-Online-Hilfe
- Abschnitt „Bereitstellung eines universellen Passworts“ im *NetIQ-Passwortverwaltung 3.3-Verwaltungshandbuch* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html)

9 Unterstützung für die Microsoft Windows Server 2008-Passwortrichtlinie

In früheren Versionen von eDirectory konnten Benutzer entweder die standardmäßige Microsoft-Komplexitätsrichtlinie oder die alte Novell-Syntax verwenden. NetIQ eDirectory 8.8 SP8 unterstützt jedoch die Verwendung von Passwortrichtlinien, die mit den Komplexitätsanforderungen der Microsoft Windows Server 2008-Passwortrichtlinie konform sind, die sich von den Anforderungen in der früheren Microsoft-Komplexitätsrichtlinie unterscheiden. Sie können iManager zur Erstellung einer Richtlinie verwenden, die die neue Syntaxoption der Microsoft Server 2008-Passwortrichtlinie verwendet, und diese Richtlinie wie für Ihre Umgebung erforderlich konfigurieren.

Dieses Kapitel enthält die folgenden Informationen:

9.1 Erstellen von Windows Server 2008-Passwortrichtlinien

Sie können iManager zur Erstellung von Passwortrichtlinien verwenden, die die Komplexitätsanforderungen von Microsoft Windows Server 2008 verwenden und Benutzer in Ihrer eDirectory-Umgebung den neuen Richtlinien zuweisen. Detaillierte Anweisungen zur Erstellung von Passwortrichtlinien finden Sie im *NetIQ-Passwortverwaltung 3.3.2-Verwaltungshandbuch* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html).

HINWEIS

- Bevor Sie eine neue Passwortrichtlinie mit der Syntax der Microsoft Server 2008-Passwortrichtlinie erstellen, müssen Sie sich vergewissern, dass die neueste Version des Plugins für die Novell iManager-Passwortverwaltung installiert ist. Weitere Informationen zu den iManager-Plugin-Modulen finden Sie im *NetIQ iManager 2.7-Verwaltungshandbuch* (https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html).
- Sie müssen außerdem sicherstellen, dass die Optionen "Universelles Passwort" und "Erweiterte Passwortregeln" für die zu erstellende oder zu konfigurierende Richtlinie aktiviert sind.

9.2 Verwalten der Windows Server 2008-Passwortrichtlinien

Sie können mit iManager Ihre Richtlinien verwalten, die die Komplexitätsanforderungen der Windows Server 2008-Passwortrichtlinie verwenden. Weitere Informationen finden Sie im Abschnitt „Verwalten von Passwörtern anhand von Passwortrichtlinien“ im *Novell-Passwortverwaltung 3.3.2-Verwaltungshandbuch* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/ampxjj0.html).

9.3 Weiterführende Informationen

Weitere Informationen zu den Passwortrichtlinien in eDirectory finden Sie in den folgenden Dokumentationen:

- iManager-Online-Hilfe
- *Novell Password Management 3.3.2-Verwaltungshandbuch* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html)
- *Novell Modular Authentication Services 3.3.4-Verwaltungshandbuch* (http://www.netiq.com/documentation/nmas33/admin/data/a20gkue.html)

10 Prioritätssynchronisierung

Prioritätssynchronisierung ist eine neue Funktion in NetIQ Directory 8.8, die den aktuellen Synchronisierungsvorgang in eDirectory ergänzt. Durch die Prioritätssynchronisierung können Sie bearbeitete kritische Daten wie Passwörter umgehend synchronisieren.

Sie können Ihre kritischen Daten über die Prioritätssynchronisierung synchronisieren, wenn Sie nicht auf die normale Synchronisierung warten können. Der Vorgang der Prioritätssynchronisierung ist schneller als der normale Synchronisierungsvorgang. Die Prioritätssynchronisierung wird nur zwischen zwei oder mehreren eDirectory-Servern der Version 8.8 oder höher unterstützt, die dieselbe Partition hosten.

In der folgenden Tabelle sind die Plattformen aufgeführt, die die Funktion der Prioritätssynchronisierung unterstützen:

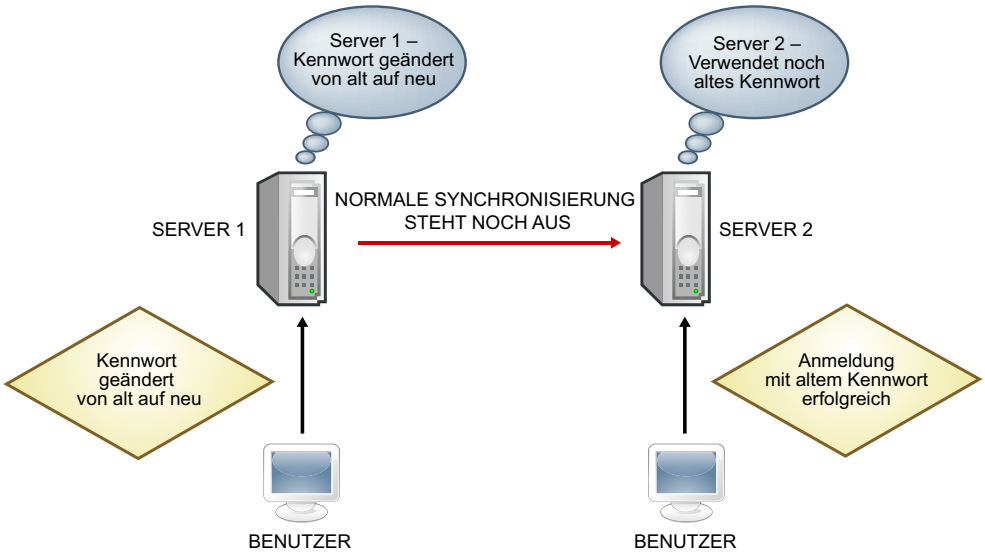
Liste der Funktionen	Linux	Windows
Prioritätssynchronisierung	✓	✓

Dieses Kapitel enthält die folgenden Informationen:

10.1 Notwendigkeit der Prioritätssynchronisierung

Die normale Synchronisierung kann einige Zeit in Anspruch nehmen, während der die geänderten Daten nicht auf anderen Servern verfügbar sind. Nehmen Sie beispielsweise an, dass sich in Ihrer Einrichtung verschiedene Anwendungen befinden, die mit dem Verzeichnis kommunizieren. Sie ändern Ihr Passwort am Server1. Bei der normalen Synchronisierung dauert es einige Zeit, bis die Änderung mit Server2 synchronisiert wurde. Daher könnte ein Benutzer sich weiterhin über eine Anwendung, die mit Server2 kommuniziert, mit dem alten Passwort beim Verzeichnis authentifizieren.

Abbildung 10-1 *Notwendigkeit der Prioritätssynchronisierung*



In großen Bereitstellungen müssen Änderungen sofort synchronisiert werden, wenn kritische Daten eines Objekts bearbeitet wurden. Durch den Vorgang der Prioritätssynchronisierung wird dieses Problem behoben.

10.2 Verwenden der Prioritätssynchronisierung

Sie müssen folgendermaßen vorgehen, um Datumsänderungen über die Prioritätssynchronisierung zu synchronisieren:

1. Aktivieren Sie die Prioritätssynchronisierung, konfigurieren Sie die Anzahl der Threads und wenden Sie die Prioritätssynchronisierung für die Größe der Warteschlange über iMonitor an.
2. Definieren Sie die Prioritätssynchronisierungsrichtlinien, indem Sie die Attribute, die kritisch sind, über iManager identifizieren.
3. Wenden Sie die Prioritätssynchronisierungsrichtlinien über iManager auf die Partitionen an.

10.3 Weiterführende Informationen

Weitere Informationen zur Prioritätssynchronisierung finden Sie in der folgenden Dokumentation:

- *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*
- Online-Hilfe für iManager und iMonitor

11 Datenverschlüsselung

In NetIQ eDirectory 8.8 und höher können Sie spezifische Daten verschlüsseln, wenn sie auf Festplatte gespeichert und zwischen zwei oder mehr eDirectory 8.8-Servern übermittelt werden. Dadurch sind vertrauliche Daten besser geschützt.

In der folgenden Tabelle sind die Plattformen aufgeführt, die die Funktion zur Datenverschlüsselung unterstützen:

Funktion	Linux	Windows
Verschlüsselte Attribute	✓	✓
Verschlüsselte Reproduktion	✓	✓

Dieses Kapitel enthält die folgenden Informationen:

11.1 Verschlüsseln von Attributen

eDirectory 8.8 ermöglicht es Ihnen, auf der Festplatte gespeicherte sensible Daten zu verschlüsseln. Das Verschlüsseln von Attributen ist eine serverspezifische Funktion.

Sie können nur über sichere Kanäle auf verschlüsselte Attribute zugreifen, es sei denn, Sie lassen den Zugriff auch über Klartextkanäle zu. Weitere Informationen finden Sie unter Abschnitt 11.1.3, „Zugreifen auf die verschlüsselten Attribute“, auf Seite 62.

Dieser Abschnitt enthält folgende Informationen:

Die Funktion für verschlüsselte Attribute wird nur von eDirectory 8.8-Servern und höher unterstützt.

11.1.1 Notwendigkeit verschlüsselter Attribute

Vor eDirectory 8.8 wurden Daten in Klartext auf der Festplatte gespeichert. Es bestand die Notwendigkeit, die Daten zu schützen und Zugriff auf die Daten nur über sichere Kanäle zuzulassen.

Sie können diese Funktion in Szenarien verwenden, in denen Sie vertrauliche Daten wie Kreditkartennummern von Bankkunden schützen müssen.

11.1.2 Methode zur Verschlüsselung von Attributen

Sie können Attribute verschlüsseln, indem Sie Richtlinien für verschlüsselte Attribute erstellen und definieren und diese Richtlinien auf die Server anwenden. Sie können Richtlinien für verschlüsselte Attribute über iManager und LDAP erstellen, definieren, anwenden und verwalten.

1. Erstellen und Definieren einer Richtlinie für verschlüsselte Attribute:
   - **1a** Legen Sie die zu verschlüsselnden Attribute fest.
   - **1b** Legen Sie das Verschlüsselungsschema für die Attribute fest.
2. Wenden Sie die Richtlinie für verschlüsselte Attribute auf einen Server an.

11.1.3 Zugreifen auf die verschlüsselten Attribute

Sie können nur über sichere Kanäle wie den LDAP-SSL-Port oder den HTTPS-Port auf die verschlüsselten Attribute zugreifen. Sie können wählen, den Zugriff auf die verschlüsselten Attribute mit dem iManager-Plugin über Klartextkanäle zuzulassen. Weitere Informationen finden Sie im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

11.2 Verschlüsseln der Reproduktion

Die verschlüsselte Reproduktion verweist auf Verschlüsselungsdaten, die zwischen zwei oder mehr eDirectory 8.8-Servern übertragen wird.

Die verschlüsselte Reproduktion ergänzt die normale Synchronisierung in eDirectory.

Dieser Abschnitt enthält folgende Informationen:

- Abschnitt 11.2.1, „Notwendigkeit der verschlüsselten Reproduktion“, auf Seite 62
- Abschnitt 11.2.2, „Aktivieren der verschlüsselten Reproduktion“, auf Seite 63

11.2.1 Notwendigkeit der verschlüsselten Reproduktion

Vor eDirectory 8.8 wurden Daten drahtgebunden während der Reproduktion in Klartext übertragen. Es bestand die Notwendigkeit, vertrauliche Daten, die drahtgebunden übertragen wurden, zu verschlüsseln, insbesondere wenn die Reproduktionen geografisch getrennt und über Internet verbunden waren.

Diese Funktion kann in den folgenden Szenarien verwendet werden:

- Wenn die Verzeichnisserver über WAN und das Internet auf verschiedene geografische Standorte verteilt sind und die Notwendigkeit besteht, sensible Daten im Netz zu verschlüsseln.
- Wenn nur einige Partitionen Ihres Baums geschützt werden sollen, können Sie die für die Reproduktion zu verschlüsselnden Partitionen selektiv angeben.

- Wenn Sie eine verschlüsselte Reproduktion zwischen spezifischen Reproduktionen einer Partition mit sensiblen Daten benötigen.
- Wenn Sie das Gefühl haben, dass das Netzwerk in Ihrer Einrichtung unsicher ist, möchten Sie möglicherweise die sensiblen Daten während der Reproduktion schützen.

11.2.2 Aktivieren der verschlüsselten Reproduktion

Sie können die verschlüsselte Reproduktion über iManager aktivieren. Sie können die verschlüsselte Reproduktion auf Partitionsebene und auf Reproduktionsebene aktivieren.

WICHTIG: Vergewissern Sie sich vor der Aktivierung der verschlüsselten Reproduktion, dass sowohl der Ursprungs- als auch der Zielserver über die Standardzertifikate verfügt. Wenn Sie Änderungen wie Umbenennen an den Zertifikaten vorgenommen haben, tritt bei der verschlüsselten Reproduktion ein Fehler auf.

11.3 Weiterführende Informationen

Weitere Informationen zum Verschlüsseln von Daten in eDirectory finden Sie in der folgenden Dokumentation:

- *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*
- Online-Hilfe für iManager und iMonitor

12 Bulkload-Leistung

NetIQ eDirectory 8.8 bietet Ihnen Verbesserungen, die die Bulkload-Leistung erhöhen.

Informationen zur Erhöhung der Bulkload-Leistung finden Sie in den folgenden Abschnitten im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*:

- „eDirectory-Cache-Einstellungen“
- „Einstellung für die Größe der LBURP-Transaktion“
- „Erhöhen der Anzahl der asynchronen Anforderungen in ICE“
- „Erhöhte Anzahl der LDAP-Writer-Threads“
- „Deaktivieren der Schemavalidierung in ICE“
- „Deaktivieren der ACL-Schablonen“
- „Backlinker“
- „Aktivieren/Deaktivieren des Inline-Cache“
- „Verlängern des Zeitraums für die LBURP-Zeitüberschreitung“
- „Offline-Bulkload-Dienstprogramm“

13 iManager-ICE-Plugins

Vor NetIQ eDirectory 8.8 gab es zu einigen der Befehlszeilenoptionen des Novell Import Conversion Export (ICE)-Dienstprogramms keine entsprechenden Optionen im iManager-Plugin.

In der folgenden Tabelle sind die Plattformen aufgeführt, die diese Funktion unterstützen:

Funktion	Linux	Windows
ICE-iManager-Verbesserungen	✓	✓

Der ICE-Assistent in iManager 2.7 mit eDirectory 8.8 bietet die folgenden Funktionen:

- Fehlendes Schema hinzufügen
- Schema vergleichen
- Reihenfolgedatei generieren

13.1 Hinzufügen eines fehlenden Schemas

In eDirectory 8.8 bietet Ihnen iManager einige Optionen zum Hinzufügen eines fehlenden Schemas zum Schema eines Servers. Dieser Vorgang umfasst auch den Vergleich zwischen Ursprung und Ziel. Wenn ein zusätzliches Schema im Ursprungsschema vorhanden ist, wird dieses dem Zielschema hinzugefügt. Der Ursprung kann entweder eine Datei oder ein LDAP-Server sein. Das Ziel sollte ein LDAP-Server sein.

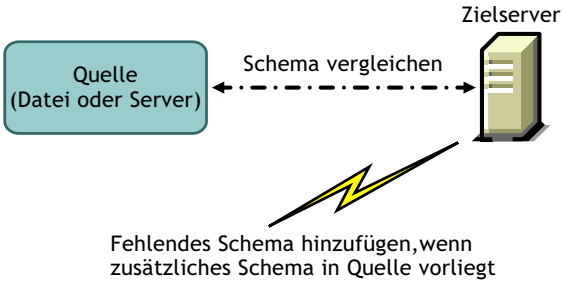
Über den ICE-Assistenten in iManager können Sie das fehlende Schema anhand der folgenden Optionen hinzufügen:

- Schema aus Datei hinzufügen
- Schema von einem Server hinzufügen

13.1.1 Schema aus Datei hinzufügen

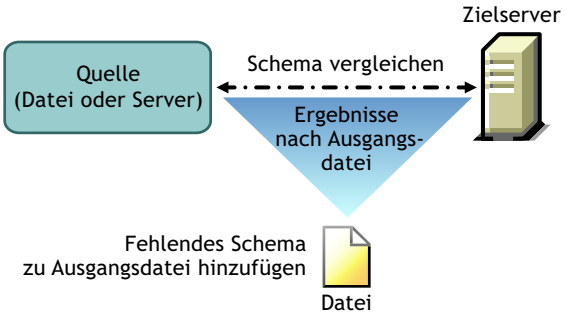
ICE kann das Schema im Ursprung und Ziel vergleichen. Der Ursprung ist eine Datei oder ein LDAP-Server, das Ziel ist ein LDAP-Server. Die Datei mit dem Ursprungsschema kann entweder das LDIF-Format oder das SCH-Format aufweisen.

Abbildung 13-1 *Schema aus Datei vergleichen und hinzufügen*



Wenn Sie das Schema nur vergleichen und das zusätzliche Schema dem Zielserver nicht hinzufügen möchten, wählen Sie die Option *Schema nicht hinzufügen, sondern vergleichen* aus. In diesem Fall wird das zusätzliche Schema nicht dem Zielserver hinzugefügt, doch die Unterschiede zwischen den Schemas stehen Ihnen als Link am Ende des Vorgangs zur Verfügung.

Abbildung 13-2 *Schema vergleichen und Ergebnisse einer Ausgabedatei hinzufügen*



Weitere Informationen finden Sie im Abschnitt „NetIQ eDirectory-Verwaltungsdienstprogramme“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

13.1.2 Schema von einem Server hinzufügen

Der Ursprung und das Ziel sind LDAP-Server.

Wenn Sie das Schema nur vergleichen und das zusätzliche Schema dem Zielserver nicht hinzufügen möchten, wählen Sie die Option *Schema nicht hinzufügen, sondern vergleichen* aus. In diesem Fall wird das zusätzliche Schema nicht dem Zielserver hinzugefügt, doch die Unterschiede zwischen den Schemas stehen Ihnen als Link am Ende des Vorgangs zur Verfügung.

Weitere Informationen finden Sie im Abschnitt „NetIQ eDirectory-Verwaltungsdienstprogramme“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

13.2 Vergleichen des Schemas

Mit iManager können Sie das Schema zwischen einem Ursprung und einem Ziel vergleichen. Der Ursprung kann entweder eine Datei oder ein Server sein, das Ziel sollte eine LDIF-Datei sein.

iManager vergleicht das Schema zwischen einem Ursprung und einem Ziel und speichert die Ergebnisse dann in einer Ausgabedatei.

Über den ICE-Assistenten in iManager können Sie das Schema anhand der folgenden Optionen vergleichen:

- Schemadateien vergleichen
- Schema zwischen einem Server und einer Datei vergleichen

13.2.1 Schemadateien vergleichen

Die Option *Schemadateien vergleichen* vergleicht das Schema zwischen einer Ursprungsdatei und einer Zieldatei und speichert das Ergebnis in einer Ausgabedatei. Um das fehlende Schema der Zieldatei hinzuzufügen, müssen Sie die Datensätze der Ausgabedatei auf die Zieldatei anwenden.

Weitere Informationen finden Sie im Abschnitt „NetIQ eDirectory-Verwaltungsdienstprogramme“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

13.2.2 Schema zwischen einem Server und einer Datei vergleichen

Die Option *Schema zwischen einem Server und einer Datei vergleichen* vergleicht das Schema zwischen einem Ursprungsserver und einer Zieldatei und speichert das Ergebnis anschließend in einer Ausgabedatei. Um das fehlende Schema der Zieldatei hinzuzufügen, müssen Sie die Datensätze der Ausgabedatei auf die Zieldatei anwenden.

Weitere Informationen finden Sie im Abschnitt „NetIQ eDirectory-Verwaltungsdienstprogramme“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

13.3 Generieren einer Reihenfolgedatei

Diese Option erstellt eine Reihenfolgedatei, die zusammen mit der Behandlungsroutine für Begrenzungszeichen verwendet wird, um Daten aus einer Datendatei mit Begrenzungszeichen zu importieren. Der Assistent unterstützt Sie beim Erstellen dieser Reihenfolgedatei, die eine Liste von Attributen für eine bestimmte Objektklasse enthält.

Weitere Informationen finden Sie im Abschnitt „NetIQ eDirectory-Verwaltungsdienstprogramme“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

13.4 Weiterführende Informationen

Weitere Informationen zu dieser Funktion finden Sie in den folgenden Dokumentationen:

- *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*
- iMonitor-Online-Hilfe

14 LDAP-basierte Sicherung

Die LDAP-basierte Sicherungsfunktion wird mit NetIQ eDirectory 8.8 eingeführt. Diese Funktion wird zur Sicherung der Attribute und Attributwerte für jeweils ein Objekt verwendet.

In der folgenden Tabelle sind die Plattformen aufgeführt, die diese Funktion unterstützen:

Funktion	Linux	Windows
LDAP-basierte Sicherung	✓	✓

Mit dieser Funktion können Sie eine inkrementale Sicherung durchführen, bei der das Objekt nur gesichert wird, wenn es geändert wurde.

Die LDAP-basierte Sicherung bietet eine Reihe von Schnittstellen für die Sicherung und Wiederherstellung von eDirectory-Objekten, die über die LDAP-Bibliotheken für C durch erweiterte LDAP-Vorgänge dargestellt werden.

Weitere Informationen zu LDAP-Bibliotheken für C SDK finden Sie in der Dokumentation zu LDAP-Bibliotheken für C (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html).

Ein Beispiel der Sicherung und Wiederherstellung von eDirectory-Objekten über LDAP finden Sie im Beispielcode backup.c (http://developer.novell.com/ndk/doc/samplecode/cldap_sample/extensions/backup.c.html).

14.1 Notwendigkeit der LDAP-basierten Sicherung

Die LDAP-basierte Sicherung versucht Probleme der aktuellen Sicherung und Wiederherstellung zu beheben.

Probleme, die durch diese Funktion behoben werden:

- Bietet eine konsistente Schnittstelle, die alle Drittanbieteranwendungen oder Entwickler zur Sicherung von eDirectory auf allen unterstützten Plattformen verwenden können.
- Bietet eine Sicherungslösung zum inkrementalen Sichern von Objekten.

14.2 Weiterführende Informationen

Weitere Informationen zu dieser Funktion finden SIe in den folgenden Dokumentationen:

- LDAP-Bibliotheken für C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html)
- Beispielcode: backup.c (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/backup.c.html)

15 LDAP-Liste "Effektive Berechtigungen erlangen"

Die API für die LDAP-Liste "Effektive Berechtigungen erlangen" wurde mit NetIQ eDirectory 8.8 SP6 eingeführt.

In der folgenden Tabelle sind die Plattformen aufgeführt, die diese Funktion unterstützen:

Funktion	Linux	Windows
LDAP-Liste "Effektive Berechtigungen erlangen"	✓	✓

Diese Funktion kann zum Abrufen der effektiven Berechtigungen für eine vorliegende Subjekt-DN oder eine vorliegende Ziel-DN für einen vorliegenden Satz von Attributen verwendet werden. Sie bietet eine Schnittstelle zum Abrufen der Liste von Berechtigungen über die LDAP-Bibliotheken für C über erweiterte LDAP-Vorgänge.

Weitere Informationen zu LDAP-Bibliotheken für C SDK finden Sie in der Dokumentation zu LDAP-Bibliotheken für C (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html).

15.1 Notwendigkeit der Schnittstelle für die LDAP-Liste "Effektive Berechtigungen abrufen"

Die Schnittstelle für die LDAP-Liste "Effektive Berechtigungen abrufen" versucht, die Probleme mit der API "Effektive Berechtigungen abrufen" zu beheben.

Probleme, die durch diese Funktion behoben werden:

- Erfordert nur eine einzige Anforderung an das Verzeichnis, um die effektiven Rechte für mehrere Attribute abzurufen.
- Reduziert die Zeit für das Verzeichnis zum Abrufen der effektiven Rechte für mehrere Attribute.
- Erkennt alle Fehler in den Eingaben in der Anforderung oder im Verzeichnis.

15.2 Weiterführende Informationen

Weitere Informationen zu dieser Funktion finden Sie in den folgenden Dokumentationen:

- LDAP-Bibliotheken für C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html).
- Beispielcode: getpriv.c (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/getpriv.c.html).

16 Verwalten der Fehlerprotokollierung in eDirectory 8.8

Viele Kunden haben berichtet, dass die Fehlerprotokollierung in NetIQ eDirectory nicht sehr hilfreich ist für die Erkennung und Behebung der üblichen Probleme. Die Fehlerprotokollierung wird während der eDirectory-Installation automatisch gestartet.

Dieses Kapitel enthält die folgenden Abschnitte:

16.1 Schweregrade bei Meldungen

Alle Meldungen weisen einen Schweregrad auf, damit Sie erkennen, wie kritisch die Meldung ist. Die Schweregrade in abnehmender Reihenfolge lauten wie folgt:

16.1.1 Fatal (Schwerwiegend)

Eine schwerwiegende Meldung zeigt ein größeres Problem wie zum Beispiel Datenverlust oder Funktionsverlust auf.

Beispiele:

- Wenn der eDirectory-Server beim Laden von Modulen Systemmodule wie NCPEngine und DSLoader nicht lädt, wird ein schwerwiegender Fehler gemeldet und protokolliert.
- Wenn der eDirectory-Server keine Verbindung auf dem sicheren Port 636 herstellt, wird ein schwerwiegender Fehler gemeldet und protokolliert.

16.1.2 Warnhinweis

Eine Meldung, die nicht notwendigerweise schwerwiegend sein muss, doch eine mögliche Ursache für ein künftiges Problem darstellt.

Beispiele:

- Verbindungsfehler zwischen zwei Servern in einem Baum, die dazu führen, dass der Server zum Cache der ungültigen Adressen hinzugefügt wird. Der Server kann diesen speziellen Zustand beheben, indem er den Cache der ungültigen Adressen zurücksetzt.
- Wenn die LDAP-Clientanwendung eine Bindung ausführt und die Verbindung schließt, ohne die Bindung aufzuheben, dann sollte der LDAP-Server eine Warnung mit der entsprechenden Warnmeldung protokollieren.
- Wenn der eDirectory-Server alle Dateibeschreibungen aufgebraucht und die Schwellwertgrenze erreicht hat, dann kann der Server aufgrunddessen keine Eingangsanforderungen verarbeiten und darauf antworten, was dazu führt, dass die Anwendung nicht ausgeführt wird.

16.1.3 Fehler

Eine Meldung, die durch einen ungültigen Vorgang verursacht wurde, die jedoch kein Problem verursacht.

Beispiele:

- Wenn eine Client-Anwendung versucht, ein Objekt hinzuzufügen, für das im Schema keine Attributdefinitionen definiert wurden, dann meldet der eDirectory-Server den Fehler "ERR_NO_SUCH_ATTRIBUTE".
- Wenn ein Benutzer versucht, sich mit einem ungültigen Passwort anzumelden, dann meldet der eDirectory-Server den Fehler "ERR_FAILED_AUTHENTICATION".

16.1.4 Informationen

Eine Meldung, die die erfolgreiche Durchführung eines Vorgangs oder Ereignisses am eDirectory-Server beschreibt.

Beispiele:

- Wenn ein Modul erfolgreich geladen/entladen wird, kann es sinnvoll sein, eine Informationsmeldung zum Vorgang zu protokollieren.
- Wenn die Datenbank-Cache-Konfiguration geändert wird, sollte eine Informationsmeldung zum erfolgreichen Speichern der Konfiguration protokolliert werden.

16.1.5 Debug

Eine Meldung, die Informationen enthält, die Entwicklern bei der Fehlersuche in einem Programm helfen.

Beispiele:

Während der Durchführung einer dynamischen Gruppensuche werden alle dynamischen Gruppenmitglieder mit Informationen zur Eintrags-ID, Partitions-ID und DN der Mitglieder angezeigt. Diese Informationen unterrichten Sie darüber, dass alle Mitglieder auf eDirectory-Ebene zurückgegeben wurden.

16.2 Konfigurieren der Fehlerprotokollierung

16.2.1 Linux

Zur Konfiguration der Einstellungen für die Fehlerprotokollierung für die Meldungen auf Serverseite können Sie die Parameter `n4u.server.log-levels` und `n4u.server.log-file` in der Konfigurationsdatei `/etc/opt/novell/eDirectory/conf/nds.conf` verwenden.

Festlegen des Schweregrads

Die verfügbaren Schweregrade lauten `LogFatal`, `LogWarn`, `LogErr`, `LogInfo` und `LogDbg` (in abnehmender Reihenfolge des Schweregrads). Weitere Informationen zu den Schweregraden finden Sie unter Abschnitt 16.1, „Schweregrade bei Meldungen“, auf Seite 75.

Standardmäßig ist der Schweregrad auf `LogFatal` festgelegt. Daher werden nur die Meldungen mit dem Schweregrad "Schwerwiegend" protokolliert.

Verwenden Sie zum Festlegen des Schweregrads den Parameter `n4u.server.log-levels` in der Datei `nds.conf` wie folgt:

`n4u.server.log-levels=`*`Schweregrad`*

Beispiel:

- Um den Schweregrad auf `LogInfo` und höher festzulegen, tippen Sie Folgendes ein:

  `n4u.server.log-levels=LogInfo`

  Bei dieser Konfiguration werden Meldungen mit dem Schweregrad `LogInfo` und höher (also `LogFatal`, `LogWarn` und `LogErr`) in der Protokolldatei protokolliert.
- Um den Schweregrad auf `LogWarn` und höher festzulegen, tippen Sie Folgendes ein:

  `n4u.server.log-levels=LogWarn`

  Bei dieser Konfiguration werden Meldungen mit dem Schweregrad `LogWarn` und höher (`LogFatal`) in der Protokolldatei protokolliert.

Angeben des Protokolldateinamens

Verwenden Sie zur Angabe des Speicherorts der Protokolldatei, in der die Meldungen protokolliert werden, den Parameter `n4u.server.log-file` in der Datei `nds.conf`. Standardmäßig werden die Meldungen in der Datei `ndsd.log` protokolliert.

Tippen Sie beispielsweise zur Protokollierung der Meldung in Datei `/tmp/edir.log` Folgendes ein:

`n4u.server.log-file=/tmp/edir.log`

Verwenden Sie zur Protokollierung der Meldungen im Systemprotokoll den Parameter `n4u.server.log-file` wie folgt:

`n4u.server.log-file=syslog`

16.2.2 Windows

Festlegen des Schweregrads

Die verfügbaren Schweregrade lauten `LogFatal`, `LogWarn`, `LogErr`, `LogInfo` und `LogDbg` (in abnehmender Reihenfolge des Schweregrads). Weitere Informationen zu den Schweregraden finden Sie unter Abschnitt 16.1, „Schweregrade bei Meldungen“, auf Seite 75.

Gehen Sie folgendermaßen vor, um den Schweregrad festzulegen:

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung* > *NetIQ eDirectory Services*.
2. Wählen Sie auf der Registerkarte *Dienste* die Option *dhlog.dlm* aus.
3. Geben Sie die Protokollstufe im Feld *Startparameter* ein.

   Geben Sie beispielsweise zur Festlegung der Protokollstufe `LogErr` und höher Folgendes ein:

   ```
   LogLevels=LogErr
   ```
4. Klicken Sie auf *Konfigurieren*.
5. Klicken Sie auf der Registerkarte *ACS-Konfiguration* auf das Pluszeichen neben *DHostLogger*.

   Der Parameter `LogLevel` wird mit dem konfigurierten Wert aktualisiert.

Angabe des Protokolldateinamens und -pfads

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung*> *NetIQ eDirectory Services*.
2. Wählen Sie auf der Registerkarte *Dienste* die Option *dhlog.dlm* aus.
3. Geben Sie den Pfad zur Protokolldatei unter *Startparameter* wie folgt ein:

   `LogFile=`*`file_path`*

   Geben Sie beispielsweise zur Festlegung des Pfads für die Protokolldatei auf `/tmp/Err.log` in den Startparametern Folgendes ein:

   ```
   LogFile=/tmp/Err.log
   ```
4. Klicken Sie auf *Konfigurieren*.
5. Klicken Sie auf der Registerkarte *ACS-Konfiguration* auf das Pluszeichen neben *DHostLogger*.

   Der Parameter `LogFile` wird mit dem konfigurierten Wert aktualisiert.

Angabe der Größe der Protokolldatei

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung*> *NetIQ eDirectory Services*.
2. Wählen Sie auf der Registerkarte *Dienste* die Option *dhlog.dlm* aus.
3. Geben Sie den Pfad zur Protokolldatei unter *Startparameter* wie folgt ein:

   `LogSize=`*`size`*

   Die Standard-Dateigröße ist 1 MB.
4. Klicken Sie auf *Konfigurieren*.

5 Klicken Sie auf der Registerkarte *ACS-Konfiguration* auf das Pluszeichen neben *DHostLogger*.

Der Parameter `LogSize` wird mit dem konfigurierten Wert aktualisiert.

16.3 DSTrace-Meldungen

Sie können die Trace-Meldungen auf Basis der Thread-ID, Verbindungs-ID und des Schweregrads der Meldungen filtern.

Sobald Sie einen Filter für die Meldungen angegeben haben, werden nur die Meldungen am Bildschirm angezeigt, die mit dem Filter übereinstimmen. Alle anderen Meldungen für die aktivierten Tags werden in der Datei `ndstrace.log` protokolliert, wenn die Datei auf EIN festgelegt wurde.

Es gilt jeweils nur ein Filter. Der Filter muss für jede Sitzung von DSTrace angegeben werden.

Standardmäßig ist der Schweregrad auf "INFO" festgelegt, was bedeutet, dass alle Meldungen mit Schweregrad höher als "INFO" angezeigt werden würden. Sie können den Schweregrad sehen, wenn Sie das Tag `svty` aktivieren.

Sie können auch iMonitor zum Filtern der Trace-Meldungen verwenden. Weitere Informationen hierzu finden Sie in Abschnitt 16.4, „Filterfunktion für iMonitor-Meldungen“, auf Seite 82.

16.3.1 Linux

Führen Sie den folgenden Vorgang aus, um die Trace-Meldungen zu filtern:

1 Aktivieren Sie die Filterfunktion mit dem folgenden Befehl:

```
ndstrace tag filter_value
```

Geben Sie den folgenden Befehl ein, um die Filterfunktion zu deaktivieren:

```
ndstrace tag
```

Beispiele für die Aktivierung der Filterfunktion:

- Geben Sie Folgendes ein, um die Filterfunktion für Thread-ID 35 zu aktivieren:

  ```
  ndstrace thrd 35
  ```

- Geben Sie Folgendes ein, um die Filterfunktion für den Schweregrad "Schwerwiegend" zu aktivieren:

  ```
  ndstrace svty fatal
  ```

  Die Schweregrade können `FATAL`, `WARN`, `ERR`, `INFO` und `DEBUG` lauten.

- Geben Sie Folgendes ein, um die Filterfunktion für Verbindungs-ID 21 zu aktivieren:

  ```
  ndstrace conn 21
  ```

Beispiele für die Deaktivierung der Filterfunktion:

- Geben Sie Folgendes ein, um die Filterfunktion auf Basis der Thread-ID zu deaktivieren:

  ```
  ndstrace thrd
  ```

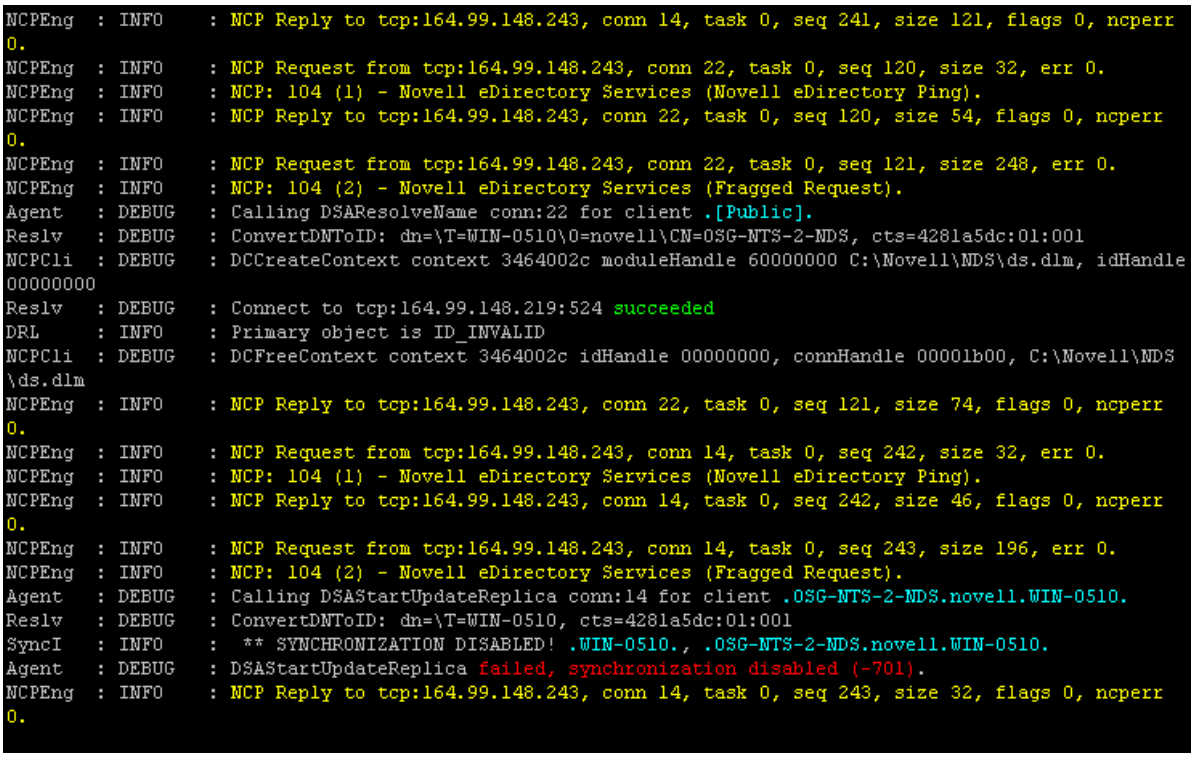
- Geben Sie Folgendes ein, um die Filterfunktion auf Basis der Verbindungs-ID zu deaktivieren:

  ```
  ndstrace conn
  ```

- Geben Sie Folgendes ein, um die Filterfunktion auf Basis des Schweregrads zu deaktivieren:

  ```
  ndstrace svty
  ```

Abbildung 16-1 *Beispiel eines Bildschirms mit Trace-Meldungen und Filtern*



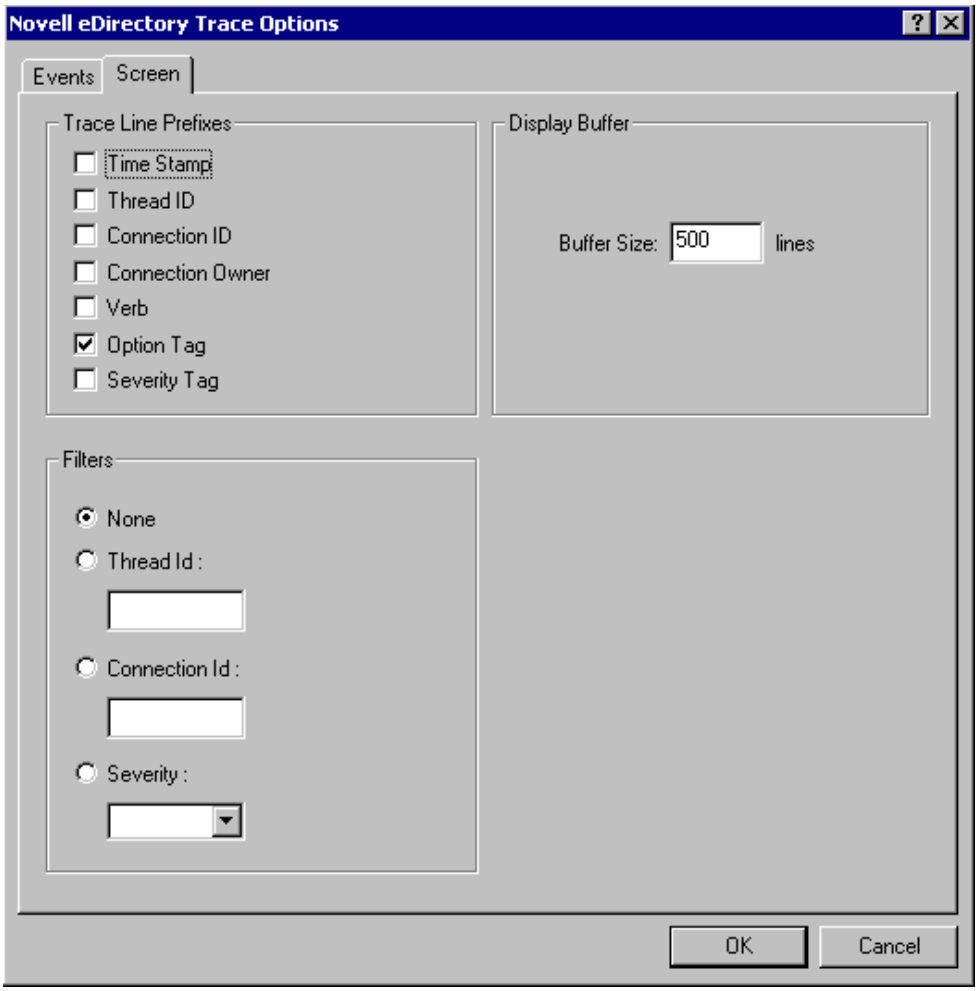
16.3.2 Windows

Führen Sie den folgenden Vorgang aus, um die Trace-Meldungen zu filtern:

1. Wählen Sie *Start* > *Systemsteuerung* > *NetIQ eDirectory Services* aus.
2. Wählen Sie in der Registerkarte *Services* die Datei *dstrace.dlm* aus.
3. Klicken Sie im Trace-Fenster auf *Bearbeiten* > *Optionen*.

   Das Dialogfeld "NetIQ eDirectory-Trace-Optionen" wird angezeigt.

Abbildung 16-2 *Bildschirm mit den Trace-Optionen unter Windows*



4 Klicken Sie auf die Registerkarte *Bildschirm*.

5 Wählen Sie die Filteroption aus der Gruppe der *Filter* aus und geben Sie den Filterwert ein.

Sie können die Meldungen nach Folgendem filtern:

- Thread-ID
- Verbindungs-ID
- Schweregrad

Bevor Sie einen der Filter auswählen, müssen Sie sicherstellen, dass er unter *Trace-Zeilenpräfixe* aktiviert ist.

Sie können die Filterfunktion auch deaktivieren, indem Sie *Keine* auswählen oder die Auswahl der Filteroption aufheben.

HINWEIS: Wenn Sie die *Thread-ID* oder *Verbindungs-ID* als Filteroption ausgewählt haben und einen Wert eingeben, der nicht vorhanden ist, dann werden die Meldungen nicht am Bildschirm angezeigt. Alle anderen Meldungen werden jedoch weiterhin in der Datei `ndstrace.log` protokolliert.

16.4 Filterfunktion für iMonitor-Meldungen

Sie können die iMonitor-Trace-Meldungen auf Basis der Verbindungs-ID, Thread-ID oder Fehlernummer filtern.

Um nach der Verbindungs-ID und Thread-ID filtern zu können, müssen Sie diese auf der Registerkarte "Trace-Konfiguration" aktiviert haben.

Weitere Informationen dazu entnehmen Sie bitte der Online-Hilfe zu iMonitor.

16.5 Filterfunktion für SAL-Meldungen

SAL wurde verbessert, um nach Bedarf umfassende Informationen zu Fehlern zu protokollieren. Funktionsaufrufe können mit Argumenten in den Debug-Builds überwacht werden.

16.5.1 Konfigurieren der Schweregrade

Sie können den Parameter `SAL_LogLevels` verwenden, um die Schweregrade für die SAL-Meldungen zu konfigurieren. `SAL_LogLevels` ist eine durch Komma getrennte Liste der gewünschten Protokollstufen.

Die Protokollstufen sind in der folgenden Tabelle erklärt:

Tabelle 16-1 *Filterparameter für SAL-Meldungen*

Parametername	Beschreibung
`LogCrit`	Kritische Meldungen. Diese Stufe ist standardmäßig aktiviert. Nach der Protokollierung eines kritischen Fehlers wird das System heruntergefahren.
`LogErr`	Alle Fehlermeldungen. Das System funktioniert weiterhin, doch die Ergebnisse sind unvorhersehbar.
`LogWarn`	Warnmeldungen. Dies ist nur eine Warnung, die Sie darauf aufmerksam macht, dass ein Fehler bevorsteht.
`LogInfo`	Informative Fehlermeldungen.
`LogDbg`	Debug-Meldungen, die zur Fehlersuche zum Zeitpunkt der Entwicklung verwendet werden. Diese Meldungen werden aus einem Versions-Build zusammengesetzt, um die Größe der Binärdatei zu verringern.
`LogCall`	Überwacht die Funktionsaufrufe. Diese sind Teil der Debug-Meldungen.
`LogAll`	Aktiviert alle Meldung mit Ausnahme von `LogCall`.

Das Minuszeichen ("-") am Anfang einer spezifischen Protokollstufe deaktiviert diese Stufe.

Beispiele

Führen Sie die folgenden Schritte aus, um auf Basis aller Protokollstufen mit Ausnahme von `LogInfo` und `LogDbg` zu filtern:

Linux

1. Halten Sie `ndsd` an.
2. Tippen Sie folgenden Befehl ein:

   ```
   export SAL_LogLevels=LogAll,-LogInfo,-LogDbg
   ```

3. Starten Sie `ndsd`.

Windows

1. Fahren Sie den `DHost` herunter.
2. Tippen Sie folgenden Befehl an der Eingabeaufforderung für den Befehl ein:

   ```
   set SAL_LogLevels=LogAll,-LogInfo,-LogDbg
   ```

   ```
   c:\novell\nds>dhost.exe /datadir=c:\novell\nds\DIBFiles\
   ```

3. Starten Sie `DHost` neu.

16.5.2 Festlegen des Protokolldateipfads

Sie können die Umgebungsvariable `SAL_LogFile` verwenden, um den Speicherort der Protokolldatei anzugeben. Dies kann ein gültiger Dateiname mit einem gültigen Pfad sein oder auch Folgendes:

- Konsole: Alle Meldungen werden an der Konsole protokolliert.
- Syslog: Unter Linux werden alle Meldungen im Syslog protokolliert. Unter Windows werden die Meldungen in einer Datei mit dem Namen "syslog" protokolliert. Dies ist das Standardverhalten für die Protokollierung.

  Alle kritischen Fehler werden immer im Syslog protokolliert, es sei denn, er wurde ausdrücklich deaktiviert.

17 Offline-Bulkload-Dienstprogramm: ldif2dib

"ldif2dib" ist ein neues Dienstprogramm, das mit NetIQ eDirectory 8.8 für das Hinzufügen von Daten-Bulkloads von LDIF-Dateien in der eDirectory-Datenbank eingeführt wurde. Hierbei handelt es sich um ein Offline-Dienstprogramm, das im Vergleich zu anderen Online-Tools schnellere Bulkloads erzielt.

In der folgenden Tabelle sind die Plattformen aufgeführt, für die "ldif2dib" aktiviert ist.

Funktion	Linux	Windows
ldif2dib	✓	✓

17.1 Notwendigkeit von "ldif2dib"

Das Dienstprogramm "ldif2dib" wird benötigt, wenn eine große Benutzerdatenbank mit Einträgen aus einer LDIF-Datei befüllt werden muss. Online-Tools wie "ice" oder "ldapmodify" sind in dieser Hinsicht aufgrund des Mehraufwands durch Bulkloads wie die Schemaüberprüfung, Protokollübersetzung und Zugriffssteuerungsprüfungen langsamer als "ldif2dib". "ldif2dib" ermöglicht eine schnelle Aktivzeit, wenn eine große Benutzerdatenbank befüllt werden muss und wenn die anfängliche Ausfallzeit kein Problem darstellt.

17.2 Weiterführende Informationen

Weitere Informationen zu diesem Dienstprogramm finden Sie im Abschnitt „Offline-Bulkload-Dienstprogramm“ im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

18 eDirectory-Sicherung mit SMS

Speicher-Management-Services (SMS) von Novell ist ein API-Framework, das durch Sicherungsanwendungen belegt ist, um eine vollständige Sicherungslösung bereitzustellen. Das SMS-Framework wird durch zwei Hauptkomponenten implementiert:

- Daten-Requester des Speicher-Managements (SMDR)
- Ziel-Service-Agent (TSA)

Der TSA für eDirectory (`tsands`) bedient eDirectory-Ziele und bietet eine Implementierung der Novell-Speicher-Management-Services-API für die Verzeichnisbäume. Anwendungen können oben auf `SMS API` geschrieben werden, um eine vollständige Sicherungslösung bereitzustellen.

Der TSA für NDS wird unter Linux unterstützt.

19 LDAP-Revision

Die Revision ist eine der primären Funktionen, an denen ein Administrator interessiert ist, wenn er ein Verzeichnis evaluiert. Die eDirectory-Ereignismethode erleichtert die eDirectory-Revision. Da die Anwendungen weitgehend das LDAP-Protokoll für den Zugriff auf Verzeichnisse verwenden, wird die Anforderung für die Revision von LDAP-Vorgängen immer wichtiger.

Dieses Kapitel enthält die folgenden Abschnitte:

19.1 Notwendigkeit der LDAP-Revision

Diese Ereignismethode fehlte auf dem vorhandenen LDAP-Server, der nicht genügend LDAP-Informationen bieten konnte. Obwohl das NDS-Ereignissystem Ereignisse für alle eDirectory-Vorgänge produzierte, reichten die meisten dieser Informationen nicht aus oder waren irrelevant für die Revision des LDAP-Servers durch eine Anwendung. Informationen, die das Protokoll abdecken und Details, Netzwerkadresse, Authentifizierungsmethoden, Authentifizierungstypen, LDAP-Suche und Transaktionsdetails etc. umfassen, die für die Revision eines LDAP-Servers entscheidend sind, waren nicht mit den NDS-Ereignissen verfügbar. Für Anwendungsentwickler war es schwierig, basierend auf diesen Ereignissen in LDAP-Revisionsanwendungen zu schreiben.

Da LDAP eine wichtige Schnittstelle von eDirectory ist, wird zur Bereitstellung einer Methode für die Revision eines eDirectory LDAP-Servers durch Anwendungen ein neues LDAP-Ereignisteilsystem in NetIQ eDirectory 8.8 SP3 eingeführt. Dieses Teilsystem generiert LDAP-spezifische Ereignisse mit allen relevanten Informationen für die Revision eines LDAP-Servers durch eine Anwendung. Dies ist als LDAP-Revision bekannt.

19.2 Verwenden der LDAP-Revision

Durch die LDAP-Revision können die Anwendungen LDAP-Vorgänge wie Hinzufügen, Bearbeiten, Suchen etc. überwachen. Durch diese Funktion werden nützliche Informationen vom LDAP-Server abgerufen wie Verbindungsinformationen, die IP des Clients, mit dem der Server zum Zeitpunkt des LDAP-Vorgangs verbunden war, die Meldungs-ID, der Ergebniscode des Vorgangs und so weiter.

Die LDAP-Revision kann über NDK-LDAP-Bibliotheken für C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html) ausgeführt werden, wodurch die Schnittstelle auf Client-Seite für diese Funktion über neue LDAP-Strukturen und Ereignisse bereitgestellt wird.

19.3 Weiterführende Informationen

Weitere Informationen zu LDAP-Revisionsereignissen finden Sie in der folgenden Dokumentation:

- „Konfigurieren von LDAP-Services für NetIQ eDirectory“im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.
- NDK: LDAP-Tools (http://developer.novell.com/documentation/cldap/ltoolenu/data/hevgtl7k.html) in der Dokumentation zu den LDAP-Bibliotheken für C.

Informationen zu den LDAP-Tools finden Sie unter LDAP-Bibliotheken für C (http://developer.novell.com/ndk/doc/cldap/index.html?ldaplibc/data/a6eup29.html).

20 Revision mit XDASv2

In der Spezifikation XDASv2 wird eine standardisierte Klassifizierung für Prüfereignisse bereitgestellt. Hier wird eine Reihe von generischen Ereignissen auf der Ebene eines globalen, verteilten Systems definiert. Mit XDASv2 wird ein allgemeines übertragbares Prüfdatensatzformat bereitgestellt, um die Zusammenführung und Analyse von Prüfinformationen mehrerer Komponenten auf der verteilten Systemebene zu erleichtern. Die XDASv2-Ereignisse sind in ein hierarchisches Notationssystem eingeschlossen, das dabei hilft, den standardmäßigen oder vorhandenen Ereignis-ID-Satz zu erweitern.

Wenn bei eDirectory 8.8 SP8 der XDASv2-Agent nicht mit dem Syslog-Server kommunizieren kann, dann kann der Agent so konfiguriert werden, dass er protokollierte Revisionsereignisse lokal im Cache speichert, wodurch sichergestellt wird, dass die Revisionsdaten nicht verloren gehen. Der Agent versucht dann, die gespeicherten Revisionsereignisse erneut zu senden, und fährt damit so lange fort, bis die Kommunikation wiederhergestellt ist. Das XDAS-Ereignis-Caching ist standardmäßig deaktiviert.

Weitere Informationen finden Sie im *NetIQ XDASv2-Verwaltungshandbuch*.

21 Sonstige

Dieses Kapitel behandelt verschiedene neue Funktionen in NetIQ eDirectory 8.8.

21.1 Cache-Dump-Berichte in iMonitor

Auf der Seite "Änderungscache" in iMonitor wird nur jeweils ein Objekt angezeigt, wodurch es schwierig ist, den gesamten Änderungscache zu durchsuchen. eDirectory 8.8 SP8 fügt den in iMonitor vorhandenen Standardberichten den Änderungscache-Dump-Bericht hinzu. Mit diesem Bericht können Sie den gesamten Änderungscache auf einen Blick sehen. Anhand dieses Berichts kann ein Administrator die Änderungen, die an einem bestimmten Server vorgenommen werden, besser verstehen.

Wenn Sie einen Änderungscache-Dump-Bericht ausführen, generiert iMonitor auch einen vollständigen XML-Dump aller Objekte im Cache, einschließlich der Attribute und Werte, die zwischen den Servern synchronisiert werden müssen.

Weitere Informationen zu den iMonitor-Berichten finden Sie im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.

21.2 Unterstützung der Microsoft Syntax mit großen Ganzzahlen in iManager

eDirectory 8.8 SP8 bietet eine neue Syntax zur Unterstützung der Microsoft-Syntax mit großen Ganzzahlen. Diese Syntax erlaubt das Speichern großer Ganzzahlen und Daten vor 1970 bzw. nach 2038. Sie können entweder LDAP oder iManager zur Erstellung oder Verwaltung von Attributen mit dieser Syntax verwenden.

HINWEIS: eDirectory verwendet weiterhin die vorhandene Syntax und 32-Bit-Werte für interne Zeitstempel.

21.3 Sicherheitsobjekt-Caching

Der Sicherheitscontainer wird aus der Stammpartition erstellt, wenn der erste Server im Baum installiert wird und Informationen wie globale Daten, Sicherheitsrichtlinien und Schlüssel enthält.

Nach der Einführung des universellen Passworts griff NMAS bei jeder Anmeldung eines Benutzers in eDirectory über NMAS auf die Informationen im Sicherheitscontainer zu, um die Anmeldung zu authentifizieren. Wenn die Partition mit dem Sicherheitscontainer lokal nicht vorhanden war, griff NMAS auf den Server zu, auf dem sich die Partition befand. Dies hatte negative Auswirkungen auf die Leistung der NMAS-Authentifizierung. Die Situation war noch schlimmer in Szenarien, in denen auf den Server mit der Partition, in der sich der Sicherheitscontainer befand, über WAN-Links zugegriffen werden musste.

Um dieses Problem zu beheben, werden bei eDirectory 8.8 die Sicherheitscontainerdaten im Cache des lokalen Servers gespeichert. Daher muss NMAS nicht bei jeder Anmeldung eines Benutzers auf den Sicherheitscontainer zugreifen, der sich auf einem anderen Computer befindet, sondern hat lokal Zugriff darauf. Dadurch wird die Leistung verbessert. Durch Hinzufügen der Partition mit dem Sicherheitscontainer zum lokalen Server wird die Leistung verbessert, doch dies ist möglicherweise nicht praktikabel in Szenarien mit zu vielen Servern.

Wenn die eigentlichen Daten im Sicherheitscontainer auf dem Server mit der Sicherheitscontainer-Partition geändert werden, wird der lokale Cache aktualisiert durch einen Hintergrundprozess names Backlinker. Standardmäßig wird Backlinker alle 13 Stunden ausgeführt und ruft die bearbeiteten Daten vom Remote-Server ab. Falls die Daten sofort synchronisiert werden müssen, können Sie Backlinker auf dem lokalen Server entweder über iMonitor, ndstrace unter Linux oder ndscons unter Windows zeitlich einplanen. Weitere Informationen finden Sie in der Online-Hilfe von iMonitor oder auf der man-Seite von "ndstrace".

Die Funktion des Sicherheitsobjekt-Cachings ist standardmäßig aktiviert. Wenn Backlinker keine Daten im Cache speichern soll, können Sie `CachedAttrsOnExtRef` aus dem NCP-Serverobjekt löschen.

21.4 Leistungsverbesserung für die Teilbaumsuche

Die Leistung der eDirectory-Teilbaumsuche für einen großen Baum mit einer besonders verschachtelten Struktur bleibt flach, unabhängig von der Basis-DN der Suche. Dieses Problem wurde durch die Verwendung des Attributs `AncestorID` behoben. Das Attribut `AncestorID` ist eine Liste von Eintrags-IDs aller übergeordneter Knoten, die mit jedem Eintrag verknüpft sind. Dieses Attribut `AncestorID` wird intern während der Teilbaumsuche verwendet und schränkt daher den Umfang der Suche ein.

Dieses Attribut wird eingetragen, wenn ein Eintrag hinzugefügt wird, und nach der Aufrüstung für alle Einträge in der DIB. Es wird erneut für alle Einträge im Teilbaum eingetragen, nachdem ein Teilbaum verschoben wurde. Die Teilbaumsuche verwendet jedoch das Attribut `AncestorID` nicht, wenn das Attribut nach der Aufrüstung und Verschiebung des Teilbaums eingetragen wird. Daher ist die Leistung des Teilbaums weiterhin so ähnlich wie die bei der Teilbaumsuche vor eDirectory 8.8.

So überprüfen Sie, ob die `IDs der übergeordneten Knoten` nach der Aufrüstung aktualisiert werden:

Sobald die `IDs der übergeordneten Knoten` eingetragen sind, ändert sich die Version der NDS-Objektaufrüstung zu Version 6 oder höher. Sie können dies sehen, wenn Sie iMonitor im Abschnitt *DIB-Verlauf* der Agenteninfo verwenden.

So überprüfen Sie, ob die `IDs der übergeordneten Knoten` nach dem Verschieben des Teilbaums aktualisiert wurden:

Während die `IDs der übergeordneten Knoten` eingetragen werden, enthält das Attribut `UpdateInProgress` im `Pseudo-Server`-Objekt die Liste der Eintrags-IDs des Partitionsstamms des Teilbaums. Sobald die `IDs der übergeordneten Knoten` eingetragen sind, ist das Attribut am `Pseudo-Server` nicht mehr vorhanden.

DSRepair aktualisiert das Attribut `AncestorID`, falls es ungültig ist.

21.5 Localhost-Änderungen

eDirectory 8.8-Server überwachen nicht an der Loopbackadresse. Dienstprogramme, die "localhost" verwenden, müssen geändert werden, um die Auflösung des Hostnamens oder der IP-Adresse zu verwenden.

Wenn ein Tool oder Dienstprogramm eines Drittanbieters die Auflösung über "localhost" durchführt, muss dies dahingehend geändert werden, dass die Auflösung über einen Hostnamen oder eine IP-Adresse und nicht über die localhost-Adresse erfolgt.

21.6 256 Dateihandler unter Solaris

Früher konnte die Solaris 2.*x* stdio-Streams Implementierung nur maximal 256 Dateibeschreibungen verwenden. Dies reichte nicht aus, damit eDirectory korrekt funktioniert. eDirectory 8.8 bietet eine Stub-Bibliothek, die diesen Grenzwert erhöht.

21.7 Arbeitsspeicher-Manager unter Solaris

Die früheren Versionen von eDirectory unter Solaris verwendeten Geodesic*, ein Drittanbieterprodukt, als Arbeitsspeicher-Manager. In dieser Version enthält eDirectory 8.8 keine Drittanbieter-Arbeitsspeicherzuweisungen, sondern nutzt den nativen Arbeitsspeicher-Manager.

Dies hat keinen Einfluss auf die Leistung von eDirectory. In den meisten Fällen ist die Leistung entweder besser oder genauso gut wie bei den Drittanbieter-Zuweisungen.

21.8 Verschachtelte Gruppen

eDirectory 8.8 SP2 unterstützt die Gruppierung von Gruppen und bietet somit eine strukturiertere Form der Gruppierung. Diese Funktion wird "Verschachtelte Gruppen" genannt. Aktuell ist die Verschachtelung für statische Gruppen zulässig.

Die Verschachtelung kann mehrere Ebenen haben, bis zu 200.

Weitere Informationen zu verschachtelten Gruppen finden Sie im *NetIQ eDirectory 8.8 SP8-Verwaltungshandbuch*.