Novell E-Directory als LDAP-Verzeichnis für Linux

Tuxnovelle

Um ein Novell E-Directory von Linux aus zu nutzen, genügen die LDAP-Schnittstellen für NSS sowie eine Schema-Erweiterung im E-Directory. Eine der Novell-Komponenten LUM (Linux User Management) oder NAM (Novell Account Management) braucht der Client nicht. Martin Kuppinger

Mit den NNLS (Novell Nterprise Linux Services, [1]) liefert Novell eine ganze Palette von Komponenten für Linux aus. Dazu gehören auch das Novell E-Directory [2] und das Linux User Management (LUM). Das E-Directory als Verzeichnisdienst besitzt zwar proprietäre Schnittstellen, spricht aber auch LDAP. Seit der Version 8 ist die LDAP-Unterstützung der NNLS komplett und auch ernsthaft in Produktivumgebungen einsetzbar. Im Gegensatz zu früheren Versionen ist sie auch standardmäßig installiert, sodass sich der Konfigurationsaufwand in Grenzen hält.

Wer LDAP für die Authentifizierung und die Auflösung von Identitäten im Linux-Umfeld bereits einsetzt, wird nach der Lektüre dieses Artikels feststellen, dass sich aus Sicht von Linux ein E-Directory nicht von anderen LDAP-Verzeichnisdiensten wie OpenLDAP unterscheidet. Allerdings muss der Admin das E-Directory stellenweise modifizieren, wie schon in [2] angedeutet.

Der Grundansatz

Die Basis dafür bilden die flexiblen Möglichkeiten von NSS (Name Service Switch, »man nsswitch.conf«) – bei Bedarf auch PAM (siehe Artikel in diesem Heft) – auf Linux-Systemen sowie die entsprechenden Module, die aktuelle Distributionen wie Suse und Red Hat Linux mitliefern.

Sie werden so konfiguriert, dass die Authentifizierung zunächst lokal per »/etc/passwd« erfolgt und danach auf das LDAP zugreift. Der Admin muss dann das E-Directory so anpassen, dass es die im RFC 2307 [3] definierte LDAP-Schema-Erweiterung für die Authentifizierung von Linux- und Unix-Benutzern unterstützt. Dazu nimmt er insbesondere GIDs und UIDs ins Schema auf. Das E-Directory unterstützt diese Erweiterungen standardmäßig nicht, lässt sich entsprechend aber flexibel erweitern.

Schemata im E-Directory anpassen

Novell stellt dafür die LDIF-Datei »/usr/lib/nds-schema/rfc2307-usergroup.ldif« bereit. Der Hersteller liefert sie nur mit den E-Directory-Implementierung für Linux- und Unix-Plattformen, nicht aber mit den E-Directory-Versionen für Windows- und Netware-Server. Besitzer dieser schmählich vernachlässigten Betriebssysteme können hilfsweise die fehlende LDIF-Datei von einem Testsystem unter Linux abzweigen.

Zu beachten ist zudem eine Eigenschaft des E-Directory: Jede Schema-Anpassung, die auf einer beliebigen Maschine im Verzeichnisbaum passiert, wirkt sich auf alle anderen E-Directory-Server im Baum aus – unabhängig von der Betriebssystem-Plattform. Auf dem lokalen System erweitert

```
ndssch -t /usr/lib/nds-modules/schema
/rfc2307-usergroup.sch
```

das Schema. Für eine Schema-Erweiterung auf einem entfernten System eignet sich ein Befehl in dieser Form:

```
ndssch -h Server -t Admin /usr/lib
/nds-modules/schema/rfc2307-usergroup.sch
```

»*Server*« ist die IP-Adresse oder der Hostnamen des E-Directory-Servers und »*Admin*« der FDN des Administrators. Nach der Eingabe des Kennworts erfolgt die Schema-Erweiterung.

Benutzer für anonyme Zugriffe anlegen

Im nächsten Schritt legt man im I-Manager einen Benutzer an, in dessen Kontext die Zugriffe von anonymen Benutzern über LDAP auf das E-Directory erfolgen werden. Dazu erstellt der Admin ein neues Benutzerkonto und vergibt kein (!) Kennwort. Außerdem lässt er beim Anlegen auch das Schlüsselpaar mit dem privaten und dem öffentlichen Schlüssel erzeugen. Bei den Eigenschaf-

ten des Benutzers deaktiviert er unter »Beschränkungen | Passwortbeschränkungen« die Option »Passwortänderung durch Benutzer zulassen«.

Damit über dieses Objekt nur die unbedingt erforderlichen Informationen lesbar sind, ist bei »Rechte | Trustees bearbeiten« das Objekt für die Wurzel des E-Directory-Baums auszuwählen: Der eben angelegte Benutzer wird Trustee und erhält die Berechtigungen zum Durchsuchen, Lesen und Vergleichen – aber ausschließlich für bestimmte Attribute (siehe **Kasten „Attribute des anonymen Benutzers“**).

Man lässt sich dazu in der Liste der Attribute alle Schema-Attribute anzeigen und wählt die gewünschten aus (**Abbildung 1**). Abschließend wird der Benutzer durch Anpassen des LDAP-Group-Objekts noch zum Proxy-Benutzer gemacht. Damit der LDAP-Server die Einstellungen sofort mitbekommt, ist das entsprechende LDAP-Server-Objekt im E-Directory zu aktualisieren.

Benutzerkonten anpassen

Die Schema-Erweiterung allein führt – im Gegensatz zum LUM – nicht dazu, dass man die zusätzlichen Attribute beim Anlegen oder Modifizieren eines Benutzerkontos direkt nutzen kann. Es fehlen NPM-Plugins für Novells I-Manager. Stattdessen muss der Admin die Zusatzklasse »posixAccount« manuell den Benutzerkonten zuweisen, bei denen er die Attribute setzen möchte. Der Befehl dazu ist »Schema | Objekterweiterungen«. Nach der Wahl des Objekts lässt sich die Zusatzklassenerweiterung »posixAccount« hinzufügen (**Abbildung 2**). In direktem Anschluss erscheint ein Dialogfeld zum Eintragen der Attributwerte (**Abbildung 3**).

Je nach Konfiguration kann es erforderlich werden, als weiteres Attribut »loginShell« zu konfigurieren – ohne klappt beispielsweise bei Suse Linux die X11-Anmeldung nicht. Zum Bearbeiten wählt man bei »eDirectory Verwaltung | Objekt« das Benutzerobjekt im Register »Allgemein | Sonstiges« und passt es an: Der Klick auf einen Pfeil verfrachtet es von der Liste »Ungewertete Attribute« in die Liste »Gewertete Attribute«. Hier lässt sich auch gleich ein Wert für das Attribut eingeben.

Attribute des anonymen Benutzers

```
CN
Description
O
OU
Object Class
Dc
Gecos
gidNumber
homeDirectory
loginShell
memberUid
uidNumber
uniqueID
```

Konfiguration der Linux-Systeme

Das E-Directory ist durchkonfiguriert. Jetzt muss der Linux-Host zum LDAP-Client werden, wofür sich beispielsweise bei Red Hat Linux »authconfig« eignet. Da sich der E-Directory-Server nun verhält wie jeder andere LDAP-Server mit RFC-2307-Unterstützung, darf der Admin den Linux-Host so konfigurieren, als ob die Maschine auf einen OpenLDAP-Server zugriffe.

Vor dem Starten von »authconfig« ist gegebenenfalls noch das Root-Certificate der Zertifizierungsstelle (CA) zu importieren. Wer für seine Netware-Server mit einer CA auf Basis der Novell Certificate Services ar-

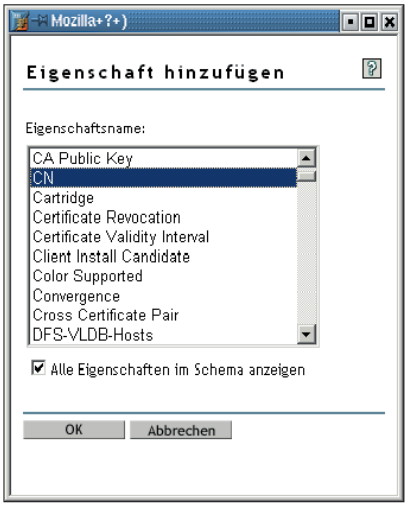

Abbildung 1: Bei den Berechtigungen für den anonymen Proxy-Benutzer muss der Admin eine Reihe von Attributen wie »CN« explizit auswählen.

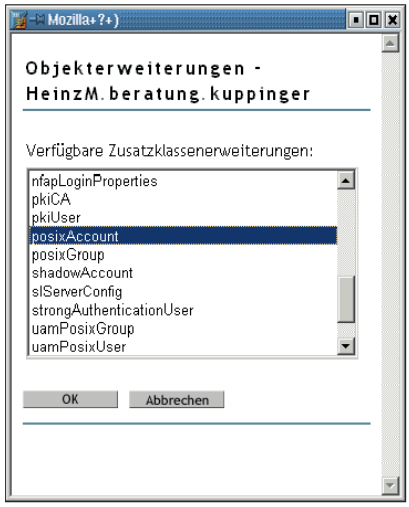

Abbildung 2: Die Benutzerkonten im E-Directory werden um die Zusatzklasse »posixAccount« erweitert, um die RFC-2307-Attribute zu speichern.

beitet, wählt zwischen DER- und Base-64-Zertifikaten. OpenSSL kann das DER-Format importieren und konvertieren. Danach lassen sich mit »stunnel« sichere Verbindungen aufbauen.

Authconfig modifiziert die Datei »/etc/ldap.conf« und fügt in der NSS-Steuerdatei »/etc/nsswitch.conf« den Eintrag »ldap« in die damit befassten Zeilen ein:

```
passwd: files nisplus ldap
shadow: files nisplus ldap
group:  files nisplus ldap
```

Welche Werte hier auftauchen, hängt vom gewählten Authentifizierungsmechanismus ab. Die Reihenfolge der Einträge bestimmt den Ablauf der Authentifizierung. Oft ist es sinnvoll, »ldap« sofort nach »files« aufzuführen. Der Verweis »files« auf die lokale Anmeldung steht in der Regel an erster Stelle, zum Beispiel um Root auch dann eine Authentifizierung zu erlauben, wenn das E-Directory beziehungsweise der LDAP-Server mal abgeschmiert sein sollten.

Spezialitäten einfach per Hand eintragen

Authconfig nimmt neben den erwähnten auch andere wichtige Eintragungen in der Datei »/etc/ldap.conf« vor. Wer mit ganz speziellen NCs (Naming Contexts) oder ähnlichen Exotika jonglieren will, setzt in derselben Datei die entsprechenden Parameter auf geeignete Werte – sie sind gut dokumentiert.

Ein umfassendes Beispiel für die »/etc/ldap.conf« beschreibt ein Artikel in den Novell App-Notes [4]. Die dort für Sun Solaris gelieferten Informationen lassen sich leicht auf die gängigen Linux-Distributionen übertragen. Derselbe Artikel liefert auch ein umfassendes Beispiel für eine PAM-Konfiguration.

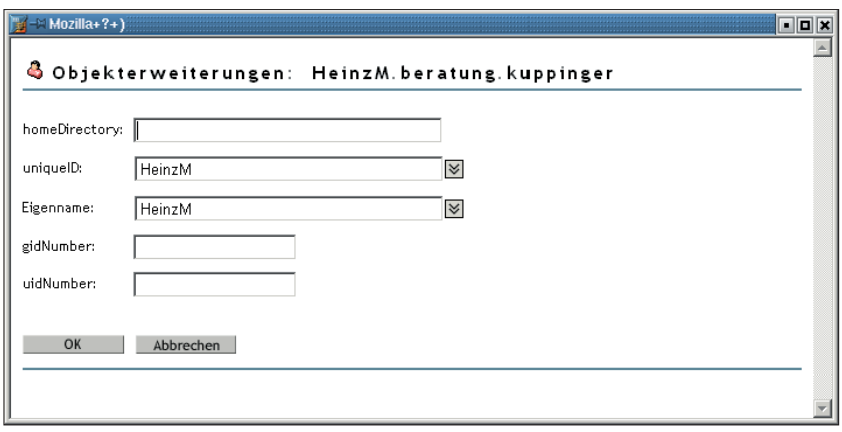

Abbildung 3: Der Admin kann die Werte für die laut RFC 2307 benötigten Attribute nach dem Hinzufügen der Zusatzklasse an dieser Stelle eingeben.

Schwächen der Basislösung und die Alternativen

Eine offensichtliche Schwäche bei diesem Ansatz liegt im mangelnden Administrationskomfort der Benutzerobjekte. Insbesondere das wichtige Erweitern einzelner Benutzerobjekte um die Zusatzklasse »posixAccount« ist etwas umständlich. Das LUM wäre hier die elegantere Lösung. Das Problem relativiert sich, wenn der Administrator keine vorhandenen Benutzerkonten modifizieren muss, sondern neue Benutzer anlegt, da er diese von bestehenden Benutzerkonten kopieren kann.

Zuletzt bleibt immer die Frage: Auf LUM und damit die NNLS verzichten oder sie lizenzieren? Als Ausweg aus dem Dilemma kommen LDIF-Dateien für die Anpassungsvorgänge im E-Directory nach der Schema-Erweiterung in Frage oder Skripte für den E-Directory-Zugriff per LDAP-Schnittstelle. Es ist aber auch möglich, das Novell E-Directory ohne zusätzliche Software als LDAP-Server für die Authentifizierung von Linux-Benutzern zu verwenden. *(jk)* ■

Infos

[1] M. Kuppinger, „Überblick über Novell Nterprise Linux Services 1.0“: Linux-Magazin 02/04, S. 59

[2] M. Kuppinger, „Novell E-Directory 8.7 für Linux“: Linux-Magazin 03/04, S. 68

[3] RFC 2307: [ftp://ftp.isi.edu/in-notes/rfc2307.txt]

[4] Novell-App-Notes-Artikel „Authenticating Users to UNIX Systems with Novell eDirectory and LDAP“, Novell App-Notes: [http://developer.novell.com/research/appnotes/2002/june/02/a020602.htm]

Der Autor

Martin Kuppinger hat sich auf das Thema Identity Management spezialisiert. Er hat im Laufe der vergangenen Jahre viele Artikel insbesondere zu diesem Thema sowie zu Novell- und Windows-Themen verfasst und zudem gut 40 IT-Fachbücher geschrieben.