Workshop: Novell E-Directory 8.7 für Linux

Zentralregister

Novells Meta-Verzeichnisdienst E-Directory bildet die Basis für die meisten Dienste der Nterprise Linux Services, aber auch für andere Novell-Produkte. Als LDAP-Verzeichnisdienst speichert es darüber hinaus die Informationen anderer Verzeichnisse. Martin Kuppinger

Wie andere Verzeichnisdienste will ein E-Directory auch administriert sein. Der Aufwand liegt zwischen überschaubar und ausgesprochen hoch – je nach Nutzungskomplexität und der vorhandenen Server- und Abteilungsstruktur. Größere Netzwerke können auch mit vielen verteilten replizierenden E-Directory-Servern arbeiten. Dann passieren die Zugriffe lokal und die Systeme laufen fehlertolerant, da ein Server die Aufgaben des anderen übernehmen kann. Wie auch immer: Die Verwaltung erfolgt zum überwiegenden Teil mit dem I-Manager. Dieser Artikel demonstriert die wichtigen administrativen Arbeiten.

Organisationseinheiten als Objektklasse

Wenn Sie die Nterprise Linux Services ([1], [2]) oder das E-Directory als Standalone-Anwendung ([3], 2 US-Dollar Einstandspreis pro Benutzer plus 0,42 Dollar pro Jahr für Updates) installieren, definieren Sie auch einen ersten Organisationscontainer im Baum und gegebenenfalls eine untergeordnete organisatorische Einheit (OU, Organizational Unit). Sie nimmt den administrativen Benutzer »admin« und das Objekt für den Server sowie einige andere interne Objekte auf. Je nach Struktur des Unternehmens benötigen Sie noch weitere Container, um Objekte geordnet abzulegen statt in unübersichtlichen Strukturen. Sie könnten beispielsweise unterhalb von »o = acme« die drei Container »ou = vertrieb«, »ou = verwaltung« und »ou = fertigung« anlegen und dort die Benutzer und andere Informationen verwalten.

Um eine OU zu erstellen, verwenden Sie im I-Manager den Befehl »eDirectory-Verwaltung | Objekt erstellen« und wählen dort »Organisatorische Einheit« als Objektklasse. Im nächsten Dialogfeld müssen Sie einen Namen für das Objekt eintragen und den Kontext angeben. Den Kontext rufen Sie über den Object Selector, dargestellt durch das Lupensymbol, auf. Sie können dort durch die Objektstrukturen des E-Directory navigieren und Objekte suchen – fertig!

Sie können in einem Baum auch weitere Organisationen anlegen, was aber nur Sinn hat, wenn mehrere Unternehmen innerhalb eines Konzerns ein Verzeichnis gemeinsam nutzen. Es gibt auch die Möglichkeit, E-Directory-Bäume zu verbinden, was in solchen Strukturen meist die sinnvollere Lösung ist.

Neue Benutzerkonten richten Sie mit dem Befehl »Benutzer« ein, den Sie sowohl bei Helpdesk als auch im I-Manager finden. Nach dem Aufruf des Befehls startet eine Maske, in der Sie den Benutzernamen, Kennwort und so weiter eintragen (siehe Abbildung 1). Sie können Benutzer auch aus Schablonen kopieren – das ist oft hilfreich.

Bei dem Punkt zum Basisverzeichnis müssen Sie keine Angaben machen, er bezieht sich auf Netware-Server. Basisverzeichnisse auf den Linux-Systemen werden unabhängig davon für LUM-Benutzer (Linux User Management) erzeugt. Ein »Einfaches Kennwort« ist nötig, wenn Sie mit den Native File Access Protocols (NFAP) von Netware arbeiten – auch das eine Option, die auf die Nterprise Linux Services nicht zutrifft.

Der untere Bereich nimmt Angaben zum Benutzer wie Titel, Standort, Telefonnummer und E-Mail-Adresse auf. Damit ist die Erstellung des Benutzers weitgehend abgeschlossen. Die mit den Nterprise Linux Services installierte I-Manager-Version fragt aber gleich, ob sie die neu angelegten Anwender auch als Benutzer für das LUM einrichten soll. Wenn Sie das bejahen, wird der Benutzereintrag in der beim LUM definierten Form gleich für Linux bereitgestellt. Dazu müssen Sie zuvor mindestens eine primäre Gruppe im E-Directory definiert haben, der der Benutzer zuzuordnen ist. Außerdem können Sie den User gleich als Samba-Benutzer konfigurieren.

Weniger zentral: Gruppen

Über Gruppen können Sie Benutzer zusammenfassen und gemeinsam administrieren. Im Gegensatz zu den vielen anderen Plattformen haben die Gruppen beim E-Directory allerdings etwas weniger Bedeutung, da der Admin Zugriffsberechtigungen auch für Container vergeben kann, die damit implizit eine Gruppe darstellen. Wer mit recht fein differenzierten OUs arbeitet, wird wenige Gruppen benötigen.

Eine neue Gruppe definieren Sie mit »Gruppen | Gruppe«. Dort sind nur der Name und der Kontext für die Gruppe anzugeben. Im Anschluss können Sie die Gruppe gleich zu einer LUM-Gruppe

machen. Dafür geben Sie das Linux-Config- oder Linux-Workstation-Objekt an, in dem weitere Informationen abgelegt sind. Von den Objektklassen wird jeweils eine Instanz bei der ersten Installation der Nterprise Linux Services angelegt, die Sie hier verwenden können. Anschließend sollten Sie das Gruppenobjekt mit »Gruppen | Gruppe bearbeiten« öffnen und dort im Register »Allgemein | Mitglieder« die Benutzer auswählen, die die Gruppe zusammenfassen sollen.

Zugriffsberechtigungen im E-Directory

Zu den Benutzern, die Sie erstellen, werden auch weitere Administratoren und Operatoren gehören, die dem Standardbenutzer »admin« gleichgestellt sein sollen oder zumindest Teile der Systemfunktionen verwalten dürfen. Jedes Objekt besitzt das Register »Sicherheit«, bei Benutzerobjekten dient es zum Konfigurieren der Sicherheitsäquivalenzen –

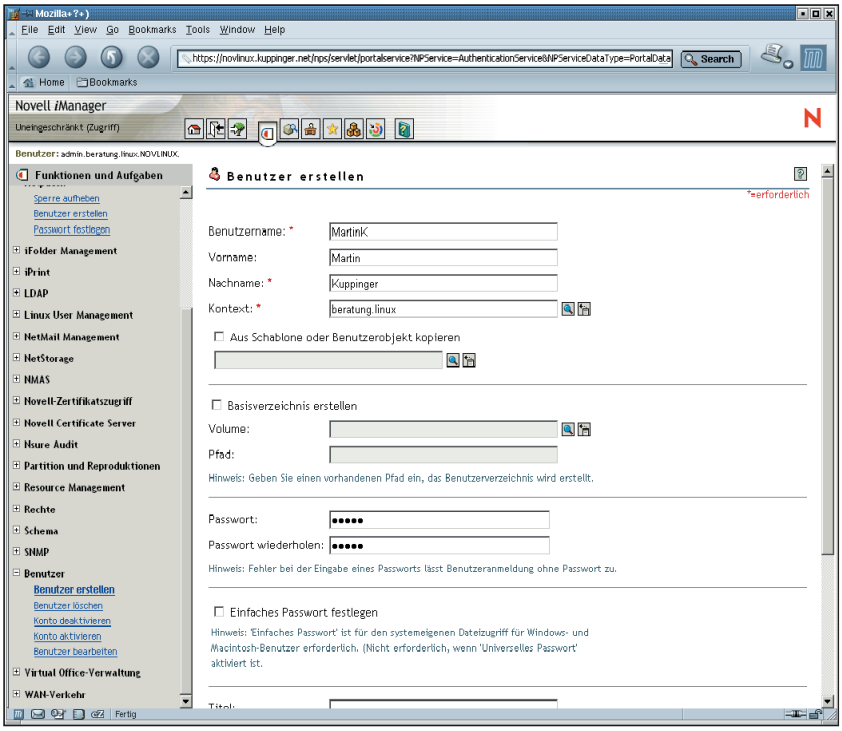

Abbildung 1: Der Administrator legt die Benutzer für das E-Directory über den I-Manager an und bestimmt dabei außerdem die wichtigsten Attribute.

also welche Benutzer unter Sicherheitsaspekten gleich zu behandeln sind. Um aber einen Benutzer dem Standardadministrator gleichzustellen, ist dies Verfahren gut geeignet. In der Regel ist es sinnvoll, hierzu Gruppen oder auch Container zu verwenden, denen in den entsprechenden Bereichen explizit Zugriffsberechtigungen gegeben werden.

Alle anderen Berechtigungen konfigurieren Sie im Bereich »Rechte«. Dort taucht der Novell-typische Begriff Trustee auf. Trustees sind, salopp gesagt, dazu berechtigt, mit irgendwelchen Objekten irgendetwas zu tun. Die Zuordnungen von Trustees – die ja auch Objekte wie Benutzer, Gruppen oder Container sind – zu Objekten bezeichnet man als Trustee Assignments. Mit »Rechte | Trustees« passen Sie die Rechtezuordnungen an. Nach der Auswahl des zu bearbeitenden Objekts wird eine Liste der derzeit definierten Trustees angezeigt.

Leider kann der I-Manager in dieser Liste nicht zugleich die Berechtigungen zeigen. Dazu müssen Sie auf »Zugewiesene Rechte« klicken und die einzelnen Berechtigungen anpassen: »Supervisor« gibt volle Zugriffsberechtigungen und »Inherit« bewirkt, dass sich diese Berechtigungen nach unten vererben und damit beispielsweise für Objekte in einem Container und untergeordnete Container gelten. Die Liste zeigt entweder einzelne Eigenschaften, für die Sie Berechtigungen vergeben können, oder die speziellen Einträge »All Attribute Rights« und »Entry Rights«, mit denen Sie die Berechtigung für alle Attribute setzen (Abbildung 2).

Die Vererbung ist nicht nur über das Optionsfeld »Inherited« steuerbar, sondern auch über IRFs (Inherited Rights Filter). Die konfigurieren Sie bei »Rechte | Filter für vererbte Rechte«, um die Vererbung der angegebenen Berechtigungen auszufiltern. IRFs sollten Sie nur selten und gezielt einsetzen, da sie die Sicherheitsadministration im E-Directory schnell sehr unübersichtlich machen.

LDAP-Konfiguration

Das E-Directory unterstützt mehrere eigene, proprietäre Protokolle. Es ist aber auch und vor allem ein LDAP-v3-Verzeichnis (siehe Kasten „Linux-Clients am E-Directory“). Für die Konfiguration gibt es zwei verschiedene Objekttypen. »LDAP Group«-Objekte speichern Festlegungen, die für mehrere Server gelten, »LDAP Server«-Objekte jene für einen individuellen. Beim Einrichten des ersten E-Directory-Servers in einem Verzeichnisbaum wird jeweils eine Instanz der beiden Objektklassen angelegt, folgende Server erzeugen zusätzliche LDAP-Server-Objekte.

Am einfachsten greifen Sie auf diese Objekte über »LDAP | LDAP-Überblick« zu. Damit werden die LDAP-Group- und -User-Objekte angezeigt. Beim LDAP-Group-Objekt bearbeiten Sie im Register »Allgemein | Informationen« die Liste der dem Objekt zugeordneten LDAP-Server. Bei »Allgemein | Verweise« konfigurieren Sie, auf welche LDAP-Server referenziert wird, wenn der lokalen Server die Abfrage nicht bearbeiten kann.

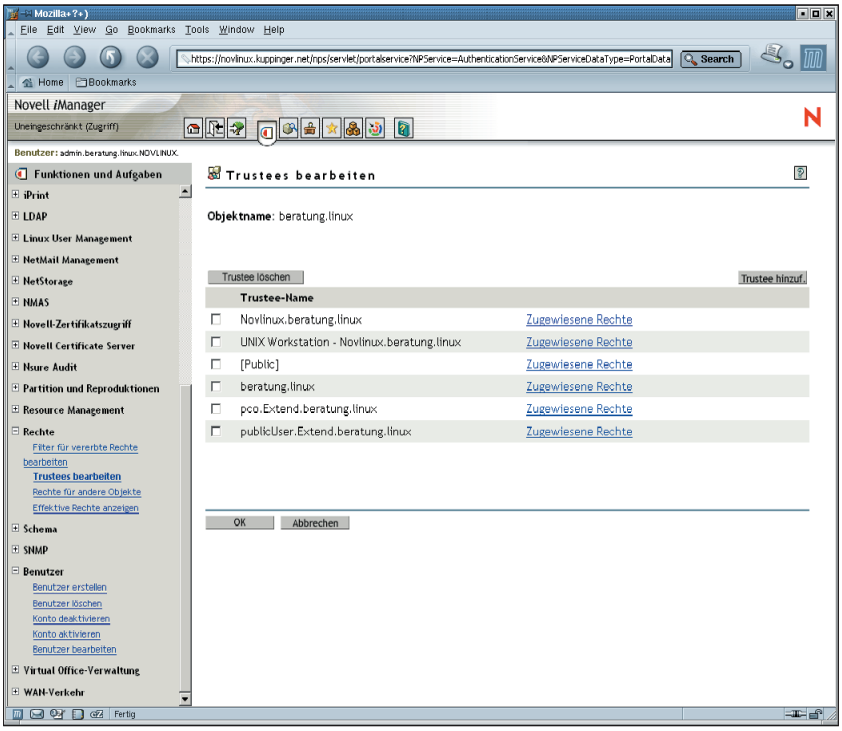

Abbildung 2: Berechtigungen auf Objekte – sie sind selbst auch als Objekte des E-Directory aufzufassen – heißen in der Novell-Sprache Trustee Assignments. Sie sind flexibel und granular konfigurierbar.

Struktur-Mappings

»Allgemein | Attributzuordnung« respektive »Allgemein | Klassenzuordnung« liefert das jeweilige Mapping zwischen den Schemata von E-Directory und LDAP-Baum. Im Standardfall ist hier alles vollständig definiert (Abbildung 3). Das Modifizieren dieser Abbildungen setzt sehr fundierte Kenntnisse beider Schemata voraus. Anpassungen sind zum

Linux-Clients am E-Directory

Um Linux-Clients von den Diensten eines oder mehrerer E-Directory-Server profitieren zu lassen, gibt es mehrere Ansätze. Zum einen kann das E-Directory als Anwendungsverzeichnis für LDAP-Anwendungen dienen sowie für Anwendungen, die spezifisch für das E-Directory entwickelt wurden und auch proprietäre Schnittstellen nutzen. Zur zweiten Gruppen gehören die verschiedenen Novell-Anwendungen. Mit Hilfe des LUM (Linux User Management) sowie des NAM (Novell Account Management) erreicht man eine engere Integration. Mit diesen Produkten werden die Module Pam_nam und Nss_nam geliefert. Sie bilden die Schnittstelle zwischen PAM auf der einen und dem E-Directory auf der anderen Seite.

Prinzipiell kann sich der Admin aber auch für Pam_ldap entscheiden. Dazu muss er allerdings die Benutzerobjekte im E-Directory manuell um die Zusatzklasse »posixAccount« erweitern, damit es Informationen wie GID und UID zu speichern vermag. Da das E-Directory generell als LDAP-Server arbeitet, ist es in gleicher Weise wie andere LDAP-Server einsetzbar.

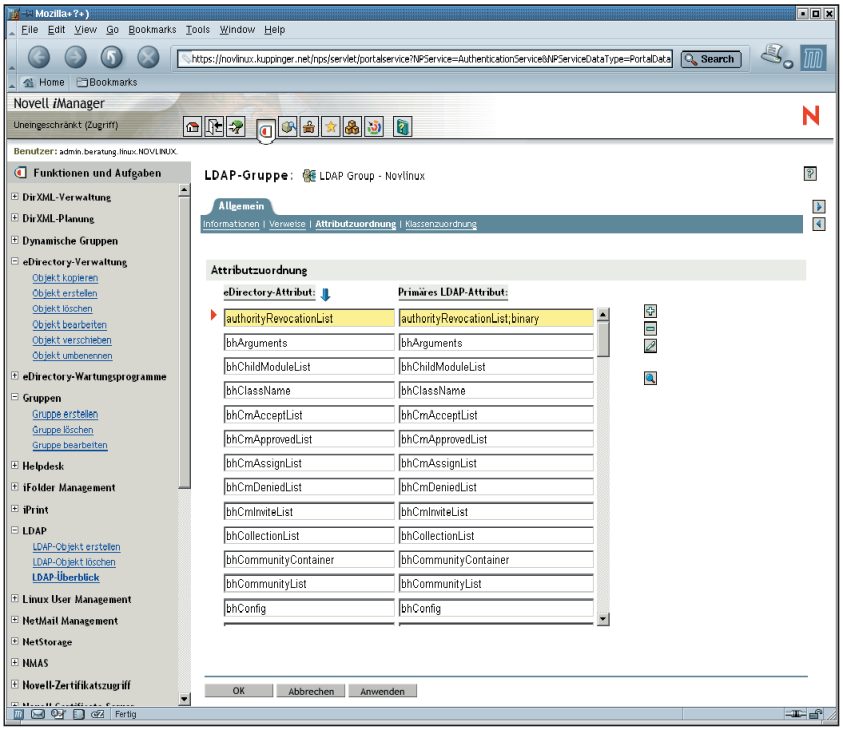

Abbildung 3: »Allgemein | Attributzuordnung« respektive »Allgemein | Klassenzuordnung« liefert das jeweilige Mapping zwischen den Schemata von E-Directory und LDAP-Baum.

Beispiel beim Hinzufügen von Attributen im Verzeichnis zur Integration eigener Anwendungen erforderlich.

Bei den einzelnen LDAP-Servern können Sie Parameter wie die Verbindungseinstellungen konfigurieren, zu finden unter »Allgemein | Verbindungen«. Dort steht die Entscheidung an, ob mit SSL gearbeitet wird – was unbedingt zu empfehlen ist – und wie viele parallele Anforderungen zulässig sind. Hinzu kommen die Zeitlimits für die Suche und Weiterleitungen zu anderen Servern.

Partitionierung und Replikation

Einige der interessantesten Funktionen enthält der Bereich »Partition und Reproduktionen«. Er beeinflusst die physische Speicherstruktur des E-Directory und die Replikation. So lassen sich auf der Ebene aller Container-Objekte – das können auch Objekte innerhalb von OUs sein – eigene Partitionen konfigurieren. Eine Partition ist unabhängig von anderen Partitionen replizierbar. Sie können somit Informationen, die eine Anwendung in einem LDAP-Verzeichnis speichert, in eine eigene Partition legen und diese auf genau jene Server replizieren, auf denen auch die entsprechende Anwendung läuft. So reduziert sich die Netzlast für die Replikation der Verzeichnisinformationen zwischen mehreren E-Directory-Servern signifikant.

Das hat aber seinen Preis: Wenn eine Information nicht lokal auf dem Server liegt, muss sie auf anderen Servern im Netzwerk gesucht werden. Das wiederum kann zu mehr Netzlast als die Replikation führen! Die Partitionierung des E-Directory will allein deshalb sehr gut geplant sein. Partitionen lassen sich auch wieder zusammenführen und sogar gefilterte Reproduktionen oder Repliken erstellen, in denen nur Teilinformationen des E-Directory liegen – was vor allem für Anwendungen, die beispielsweise nur einige Attribute von Benutzerobjekten benötigen, oft sehr effizient ist.

Dank der Flexibilität seiner Verzeichnisstrukturen vermag ein E-Directory die Daten von sehr unterschiedlichen Anwendungen aufzunehmen. Mit den Daten anderer (Open-)LDAP-Server synchronisiert sich ein E-Directory-Server über den Meta-Directory-Dienst DirXML. Alternativ dazu kann der Admin per LDIF die Daten des LDAP-Servers in eine Datei exportieren und diese wieder über LDIF ins E-Directory importieren.

Beide Formen der Migration sind aber in der Praxis nicht trivial, da sie oft Schema-Anpassungen erforderlich machen. Und bei der Speicherung im E-Directory will genau geplant sein, welche Daten eigene Partitionen erfordern, was wiederum die hierarchische Verzeichnisstruktur widerspiegeln muss.

Ausgereifte Vielfalt

Die vorgestellten Verwaltungsfunktionen decken die wichtigen administrativen Aufgaben beim I-Manager ab, streifen aber die Möglichkeiten nur. Ein E-Directory bietet seinem Administrator Optionenvielfalt – schon wenn er ein Benutzerobjekt zur Bearbeitung öffnet. Dann bekommt er nämlich deutlich mehr Attribute zu sehen als beim Anlegen des Accounts (siehe oben).

Auch die Verwaltungsfunktionen gehen wesentlich weiter ins Detail, etwa mit Konfigurationsparametern für das E-Directory. Auch lässt sich das Verhalten des Dienstes über die Directory Service Trace (DStrace, [4]) detailliert analysieren. Diese Möglichkeiten machen deutlich, dass sich das E-Directory über lange Jahre zu einem mächtigen Verzeichnisdienst entwickelt hat. *(jk)*

Infos

[1] Novell Nterprise Linux Services: [http://www.novell.com/de-de/products/linux/]

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

[3] Novell E-Directory: [http://www.novell.com/de-de/products/edirectory/]

[4] Directory Service Trace: [http://developer.novell.com/research/sections/netmanage/dirprimer/2001/august/p010801.htm] und [http://developer.novell.com/research/sections/netmanage/dirprimer/2001/septembe/p010901.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.