

Netware-Directory Services (Überblick)

Wozu ?

Damit das Anmelden an einzelner Server entfällt, d.h. das Netzwerk als ein homogenes Ganzes für den Anwender erscheint.

Objekte in den NDS

Ähnlich der Version 3.11 existieren Objekte innerhalb der NDS (z.B.: User), die mit bestimmten Eigenschaften (Properties) ausgestattet sind. Diese Objekte können Werte annehmen. Objekte im Sinne der NDS sind nur Informationsstrukturen aber nicht die physikalischen Objekte selbst (obwohl es in den NDS physische und logische Objekte gibt). Zum Unterschied zur Version 3.11 gibt es aber zu allen Objekten und deren Eigenschaften Rechte ähnlich den bekannten Rechten auf Dateien und Verzeichnissen.

Begriffe dazu:

- Object Rights**
- Property Rights**
- Access Control List (ACL)**
- Inherited Rights Filter (IRF)**
- Effective Rights**

Verzeichnisbaum

Die Objekte sind in den NDS hierarchisch wie ein DOS-Verzeichnisbaum abgespeichert (analog X.500), dabei werden drei Arten von Objekten unterschieden:

Root Object

Das Root-Objekt wird während der Installation angelegt und kann weder verändert noch gelöscht werden, allerdings wird auch ein User-Objekt (ADMIN) mit Supervisor-Rechten auf das Root-Objekt angelegt. (Root-Objekt ¹ Root-Verzeichnis)

Container Object

Ein Container-Objekt kann seinerseits wieder Objekte beinhalten. Dabei werden folgende Container-Objekte unterschieden:

Country (C)	muß nicht existieren
Organization (O)	mindestens 1
Organizational Unit (OU)	beliebig

Leaf Object

Leaf-Objekte sind Endpunkte der NDS; folgende Arten von Leaf-Objekten existieren:

AFP Server	Apple Filing Protocol Server
Alias	Verbindung zu anderem Objekt
Bindery	Zur Abwärts=
Bindery Queue	kompatibilität
Computer	Workstation, Router, ...
Directory Map	Verzeichnis im Dateisystem
Group	Benutzergruppe
Netware Server	Server
Organizational Role	Manager für Teilaufgaben wird bei Bedarf einem Benutzer zugeordnet (Wenn die Aufgabe zu einem anderen wechselt, ist die Umstellung vereinfacht).
Print Server	Druckserver

Printer	Drucker
Profile	Profile script (zwischen System- und Userloginscript)
Print Queue	Druckerwarteschlange
User	Benutzer
Unknown	Beschädigtes Objekt
Volume	Logische Platte

Context

Unter dem Context versteht man den Ort innerhalb der NDS d.h. den vollständigen Namen eines Objektes.

Aufbau:

**common name.Organizational Unit name.
Organizational name.Country name**

z.B.:

COUFAL.LEHRER.SCHULE.HBLVA.AT

oder auch

**CN=COUFAL.OU=LEHRER.OU=SCHULE.
O=HBLVA.C=AT**

NDS-Partitionen

Gespeichert werden die NDS als Partitionen auf mehrere Server verteilt. Dabei sollte man darauf achten, daß Kopien der einzelnen Partitionen existieren, damit der Ausfall eines Server die NDS nicht beeinträchtigen bzw. damit der Zugriff insbesondere im WAN-Bereich beschleunigt wird.

Diese Kopien werden Replicas genannt und existieren auf drei Arten:

**Master
Read/Write
Read Only**

Planung eines NDS-Baumes

Wozu ?

- Zugriff vereinfachen
- Verwaltung vereinfachen
- Netzbelastung verringern
- Fehlermöglichkeiten reduzieren

NDS-Standards festlegen

Standards für Benutzerobjekte

Loginnamen	z.B.: Familienname_Vorname
Voller Name	Familienname Vorname Titel
Ort	Gebäudekürzel Zimmernr.
Abteilung	Abteilungskürzel
Telefonnummer	inklusive internat. Vorwahl
E-Mail Adresse	Internetspezifikationen
Sprache	Benutzerspezifisch
Default Server	Abteilungsserver
Heimatverzeichnis	Volumename:Pfad
Restriktionen	Passwortlänge=6, ...

Standards für Druckerwarteschlangen

Standards für Druckernamen

Standards für Servernamen

...

NDS-Baum aufbauen

Countryobject nur wenn unbedingt notwendig, da dadurch immer die längere Schreibweise (CN=.OU=...) verwendet werden muß und die Komplexität steigt. Man kann mehrere Länder auch über die Organisation lösen (siehe Novell). Novell gibt als Definition eines kleinen Netzes ca. 5 Server und 100 Benutzer innerhalb eines

LAN's vor, bei dem sogar nur ein Objekt Organization notwendig ist. Prinzipiell sollte der Baum die Organisation der Firma wiedergeben, allerdings ist das sicher kein Mußkriterium für alle Firmen. Bei einem Upgrade von V3.x oder V2.x würden alle Objekte des Binderies innerhalb eines OU-Objektes kreiert werden. Für Neuinstallationen sollte man dabei aber bedenken, daß in keinem Containerobjekt mehr als 1000 Objekte angelegt werden sollten.

Verteilung der NDS auf die einzelnen Server festlegen

Wie schon erwähnt wird der NDS-Baum in mehrere Partitionen zerlegt und auf die Server verteilt. Dabei sollte immer die Minimierung des Datenaustausches und die Sicherheit beachtet werden. Die Masterreplika wird immer am ersten Server des entsprechenden Objektes angelegt, standardmäßig wird auch eine "Secondary Replica" am Server, der die übergeordnete Masterreplika hat, angelegt.

Zeitsynchronisation festlegen

Damit in einem Netware 4.x-Netz die Zeiten aufeinander abgestimmt sind, hat jeder Server neben seiner Zeitzone und dem Wissen über seine Sommerzeitregelung auch noch eine der folgenden Eigenschaften:

**Single Reference Time Server (Default)
Daneben nur mehr Secondary Time Server möglich, besonders für kleine Netze interessant, allerdings um den Preis der Fehleranfälligkeit.**

Primary Time Server

Mindestens noch ein zweiter Primary oder Reference Time Server notwendig, die untereinander die Uhrzeit ausmachen (Mehrheitsbeschluß oder Diktat).

Reference Time Server

Meist nur einer, da ein Reference Time Server seine Uhrzeit bei einem Abstimmungsvorgang nicht ändern würde, mehrere nur mit externer Zeitbasis möglich (z.B.: Funkuhr).

Secondary Time Server

Bekommt die Uhrzeit von einem anderen Timeserver vorgeschrieben und stellt sie selbst nur Clients zur Verfügung. Der andere Timeserver könnte zwar selbst auch ein Secondary Time Server, sollte aber mindestens ein Primary Time Server sein.

Die Zeitserver können den Synchronisationsvorgang auf zwei Arten durchführen:

SAP (Server Advertising Protocol)

**Automatisch ohne Administrationsaufwand,
Mehr Netzbelastung**

Benutzerkonfiguriert

**Weniger Netzbelastung, aber
Administrationsaufwand und fehleranfälliger.**

Art des Aufbaus der Sicherheit festlegen

Benutzerorientiert	analog
Gruppenorientiert	Verzeichnissen und
Sicherheitsgleichheit	Dateien