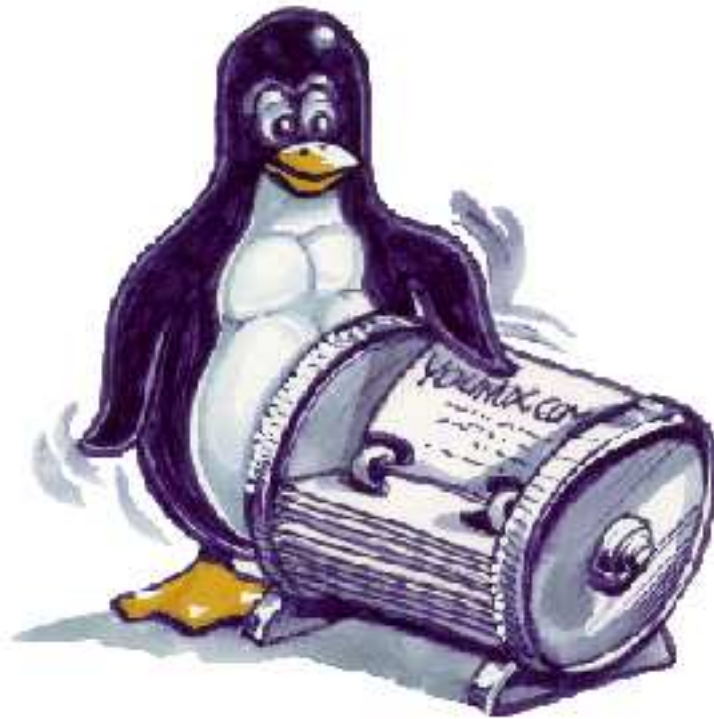


MAKING USERS HAPPY

Nikolai Domaev
Afdeling Netwerkassistent,
CLW Don Bosco,
Wilrijk
`nikolai.domaev@gmail.com`

25 mei 2009



Linux and Databases

Inhoudsopgave

I	Inleiding	1
1	LDAP	5
1.1	Lightweight Directory Access Protocol	5
1.2	LDAP en X.500	5
1.3	LDAP-implementaties	6
2	Hierarchische database	7
2.1	Opzet	7
3	AD	9
3.1	Active Directory	9
4	Sun	11
4.1	Sun Java System Directory Server	11
5	OpenLDAP	13
II	Theoretisch gedeelte	15
6	Terminologie	19
7	OpenLDAP	21
8	Overzicht van de configuratie	23
8.1	Installatie van de software	23
8.2	Configuratie van de server: slapd.conf	24
8.3	slapd starten	27
8.4	Gegevens aan de directory toevoegen	28
8.5	ldap.conf bewerken	29
8.6	Kijken of het werkt	29
9	LDAP-client	31
9.1	ldap.conf aanpassen	31
9.2	nsswitch.conf aanpassen	32

9.3	PAM aanpassen	33
9.4	Gebruikers met de juiste attributen maken	35
9.5	Werken met de migratiescripts	36
10	Uw container integreren in een andere tree	39
10.1	Replicatie	40
III	Praktisch gedeelte	43
11	Installatie	47
11.1	Installeer CentOS 5.1	47
11.2	Installeer OpenLdap	47
12	Configuratie	49
12.1	Configureer OpenLdap server	49
12.2	OpenLDAP vullen	50
12.3	Migration Tools	50
12.4	Aanmeldingscontrole	50
13	phpLdapAdmin	53
13.1	phpLdapAdmin installatie	53
14	SaMBa	57
14.1	SaMBa configureren	57
14.2	SMBLDAP-Tools installeren	59
15	Replica	61
15.1	Replica van LDAP maken	61

Goede dag beste lezer. Als u het al ziet, eerst en vooral wou ik de mensen bedanken. Die mij ondersteuning hebben gegeven in al mijn noden en vragen. Ten eerste wou ik Maarten Michiels bedanken. Door zijn advies had ik deze school binnen gewandeld. En het was leuke verrassing voor mij. Dat op het netwerk-assistent opleiding wordt hier vooral met free and open source software gewerkt. Dat is ook de opleiding die ik heb gevolgd. Door de advies van Robert Keersse. Wie dat ik ook van harte wil danken door zijn inzet in leerlingen. Onder andere mij. Ik dank Peter Peeters, met wie zijn hulp heb ik mijn kennis van websites bouwen en beheren nog meer uitgebreid. Luc Jennes wil ik ook bedanken dat hij de vershiel had laten zien. Tussen hoe verschillend dat ingenieur en nieuweling, in tegenstelling, de opdracht kunnen bekijken. Waarschijnlijk wil ik ook mijn manager Victor Martin bedanken voor zijn coordinatie. Het is heel leuke eerwaring om bij Xylos de stage te doen.

Het opleiding netwerk-assistent ziet als volgt uit.

Omschrijving:

Netwerken en toebehoren installeren
software installeren en gebruiken
werken met internet, e-mail, e.d.
websites bouwen en beheren
en bij de PAV les krijgen wij ook kans om VCA en ECDL atesten te haalen

Minimumvoorwaarden:

Minimum 17 jaar, liefst +18 jaar
Minstens geslaagd voor 4 TSO
Sterk geïnteresseerd in alles wat met computers te maken heeft.

Aanbod:

Werk- en opleidingskansen bij Agfa-Mortsel, Xylos, ITp, Coriotech, Gacs, Reynaers Alu, Pluma, Logstat, ...
Beroepsopleiding op school: kennis van hardware, netwerken en software

Deel I

Inleiding



Waar gaan wij dus naartoe?

Hoofdstuk 1

LDAP

1.1 Lightweight Directory Access Protocol

Lightweight Directory Access Protocol (LDAP) is een netwerkprotocol dat beschrijft hoe gegevens uit directoryservices benaderd moeten worden over bijvoorbeeld TCP/IP.

Een directory is in dit verband informatie die op een hiërarchische manier, gegroepeerd naar een bepaald attribuut, is opgeslagen. Denk aan een telefoonboekje, waarin telefoonnummers en adressen van personen of bedrijven alfabetisch worden opgeslagen. Een directorynaam komt overeen met de eerste letter van de naam (het attribuut) van de persoon of bedrijf. Iedere directory bevat dan alle personen en bedrijven, waarvan de naam begint met een bepaalde letter.

1.2 LDAP en X.500

Het bovenstaande voorbeeld schetst de oorsprong van het LDAP, namelijk de telecommunicatie. Vanuit deze wereld zijn de telefoondirectory's het domein van de computernetwerken binnengekomen. Om de nu elektronische telefoondirectory's beter te kunnen beheren is door International Telecommunication Union (ITU) de zogenaamde X.500-standaard ontwikkeld. Een onderdeel van deze standaard is het Directory Access Protocol (DAP). Via dit protocol werden achterliggende directory's op een gecontroleerde en gestructureerde manier toegankelijk.

De omschrijving van de X.500-standaarden waren precies en daarom ook erg omvangrijk. Vandaar dat er betrekkelijk weinig implementaties van de standaarden waren gemaakt. De implementaties die er wel waren, behoeften echter veel rekenkracht. Er ontstond dan ook een vraag om een lichtere implementatie van de X.500-standaarden: LDAP.

De huidige versie van LDAP is LDAPv3. Deze heeft minder overhead dan zijn zwaardere voorganger DAP. Zo kent de huidige versie slechts negen basisoperaties, en kende de oorspronkelijke versie van LDAP zelfs geen beveiligingsopties. LDAP is ontwikkeld aan de universiteit van Michigan. Het protocol is vastgelegd in volgende RFC's:

- * RFC 1777 LDAP
- * RFC 1778 String Representation of Standard Attribute Syntaxes
- * RFC 1959 URL Format
- * RFC 1960 String Representation of Search Filters
- * RFC 1823 C API
- * RFC 3377 LDAP v3

1.3 LDAP-implementaties

Er zijn meerdere instanties, die een implementatie, zowel open source als commercieel, hebben gemaakt van LDAP, waaronder de volgende:

- * Apache Directory Server
- * Red Hat Directory Server
- * OpenLDAP
- * Novell eDirectory
- * Sun Directory Server Enterprise Edition
- * Windows Server 2003 Active Directory

Hoofdstuk 2

Hierarchische database

De hierarchische database is de oudste vorm van de databases. Het is de opvolger van de flat file, het platte bestand, een manier van het opslaan van gegevens waarbij alles zonder ordening opgeslagen kan worden.

Van de hierarchische database is niet bekend hoe en wanneer die precies ontstaan is, of wie de grondleggers ervan geweest zijn. Het model is ontstaan in de jaren vijftig en zestig van de 20e eeuw, de systemen die het model in de praktijk brengen ontstaan in de jaren zestig. Het bekendste voorbeeld hiervan is IMS/360 van IBM dat in 1969 het licht zag.

Hierarchische databases worden tegenwoordig niet meer gemaakt, daar waar ze nog in gebruik zijn betreft het legacy-systemen, systemen die steeds vaker vervangen zullen worden omdat ze verouderd zijn en omdat de kennis nodig voor het onderhoud ervan steeds zeldzamer wordt. "Directorystructuren" (zoals LDAP of Active Directory) kunnen echter nog wel aanzien worden als moderne versies, geschikt voor hierarchische gegevensopslag, zoals adressen, personeelslijsten in organisaties, documentenbeheer, enzovoort.

2.1 Opzet

De hierarchische database gaat ervan uit dat elk record in een database weer kan verwijzen naar een n-aantal andere records. Het is zo een boomstructuur, die steeds verder kan vertakken. Kenmerkend is wel dat ieder recordtype een en niet meer dan een eigenaar (owner) kent.

Het hierarchische model kent maar een boom per database, de takken hebben onderling geen samenhang en de enige ingang van de boomstructuur is van bovenaf. Om een voorbeeld te nemen, de database "bedrijf" heeft als hoofdtakken "vestigingen", "producten", "klanten". In dat geval is er geen relatie tussen vestiging en product, product A kan in elke vestiging gemaakt

worden. Wanneer product A alleen in vestiging X gemaakt wordt, kan dat in dit hierarchische model niet vastgelegd worden.

Wanneer nu in het bovenstaande model onder "klanten" een recordtype "orders" wordt toegevoegd, dan houdt dat in dat elke order bij een klant hoort, maar dat een klant meer dan een order kan hebben. De op de order voorkomende producten kunnen echter niet automatisch gekoppeld worden, omdat de gegevens van de order in een andere tak staan.

Dit schetst de zwakte van het hierarchische model, de opvolger van dit model is het netwerkmodel

Hoofdstuk 3

AD

3.1 Active Directory

Active Directory is een eigen implementatie door Microsoft van de directoryservice LDAP in combinatie met DNS en Kerberos voor het gebruik in Windows-omgevingen vanaf Windows 2000.

Active Directory staat beheerders toe om het beleid (rechten en instellingen) in het netwerk van een volledig bedrijf te beheren. Ook het automatisch installeren van software en patches behoort tot de mogelijkheden. Active Directory slaat instellingen in relatie tot een object centraal op in een database. Een AD-netwerk kan variëren van een netwerk van een paar honderd tot miljoenen objecten.

Een Active Directory bestaat uit:

- * Forests
- * Domein(en)
- * Sites
- * Organizational Units (OU)

Active Directory werd geïntroduceerd met Windows 2000 Server. De komst van Windows 2003 Server markeerde een nieuwe versie van Active Directory.

Hoofdstuk 4

Sun

4.1 Sun Java System Directory Server

The Sun Java System Directory Server is Sun Microsystems' schaalbaar LDAP directory server en een component van Java Enterprise System. Sun Java System Directory Server was voorheen Sun ONE Directory Server en iPlanet Directory Server.

Sun Java System Directory Server (hierna "Directory Server") wordt geleverd als onderdeel van de Directory Server Enterprise Edition.

De software is gratis beschikbaar voor gebruik in eeuwigdurende Individuele, Commercieel, Service Provider of Research and Instructional omgevingen. Software-ondersteuning is beschikbaar van Sun Microsystems voor een vergoeding.

Hoofdstuk 5

OpenLDAP

OpenLDAP is het Open Source project voor het netwerkprotocol Lightweight Directory Access Protocol (LDAP) een 'directory service'. De software is gelicentieerd onder de OpenLDAP Public License. De software draait zowel op linuxdistributies als op diverse andere besturingssystemen zoals Windows, MacOS X en Solaris.

Het project is in 1998 begonnen door Kurt Zeilenga, welke momenteel nog steeds adviesfuncties vervult en directeur is van de OpenLDAP Foundation.

Deel II

Theoretisch gedeelte



Theorie != praktijk.

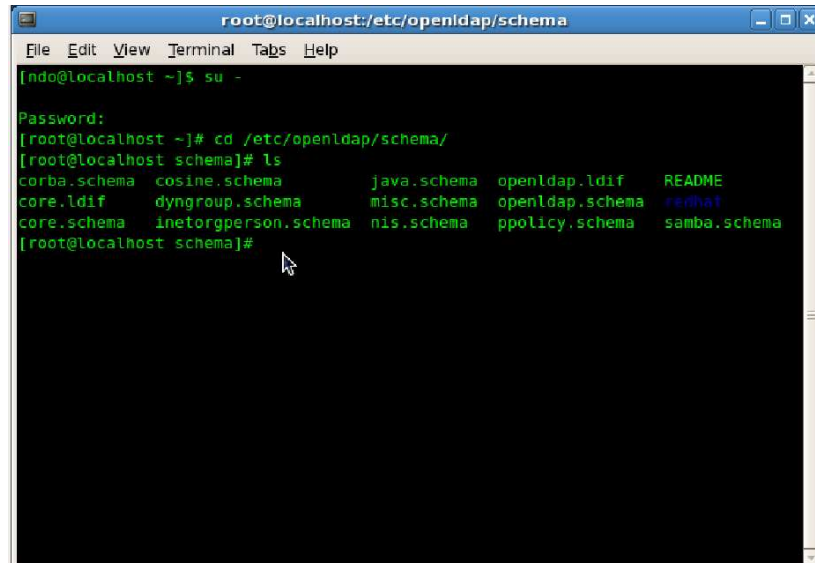
Hoofdstuk 6

Terminologie

LDAP is Lightweight Directory Access Protocol dat toegang biedt tot de Directory. Deze Directory is een hiërarchisch opgebouwde database waarin gegevens van zeer verschillende aard bijgehouden kunnen worden. De meeste gebruikte gegevens zijn waarschijnlijk de combinaties van gebruikersnamen en e-mailadressen, maar er kan ook heel andere informatie in voorkomen, zoals bijvoorbeeld gegevens over de printers die op het netwerk voorkomen. De hiërarchie; denk daarbij aan namen zoals `www.ndomain1.local`. Ook zijn deze directory's qua functionaliteit te vergelijken met directory's die op een bestandssysteem gebruikt worden om bestanden op een logische wijze op te slaan.

In de Directory komen entry's voor. Deze entry's worden ook wel objecten of classes genoemd. Zo bestaat er bijvoorbeeld voor elke gebruiker waarvan de gegevens in de Directory zijn opgenomen een gebruikersobject. Deze objecten zijn de bouwstenen waaruit de Directory bestaat. Elk van deze classes heeft zijn eigen unieke naam, die Distinguished Name (DN) genoemd wordt. Deze Distinguished Name bestaat uit de objectnaam (Common Name = CN) van het object met daaraan toegevoegd de namen van de containers waarin dit object voorkomt. Zo is bijvoorbeeld de DN van gebruiker NikolaiD die bij Xylos werkt `cn=NikolaiD,dc=Xylos,dc=be`. Alle objecten hebben attributen. De attributen zijn de stukjes informatie die met het object verbonden zijn. Denk daarbij aan een gebruikersnaam, een e-mailadres en een wachtwoord. Om te kunnen valideren in de LDAP-database, is het belangrijk dat juiste attributen een waarde hebben; zo kan bijvoorbeeld niet ingelogt worden op een Linux-systeem als het attribuut `uidnummer` geen waarde heeft. Welke attributen precies door welk object gebruikt kunnen en moeten worden, wordt gedefinieerd in het LDAP-schema. Dit gebeurt door middel van een definitie van zogeheten objectclasses. Op Linux wordt het schema gedefinieerd in verschillende bestanden. U vindt deze bestanden in de directory `/etc/openldap/schema`. Let op: een standaard-LDAP-installatie

maakt slechts van een eenvoudig schema gebruik. Wilt u ondersteuning voor meer dan alleen de basis? Dan moet u ervoor zorgen dat het standaardschema uitgebreid wordt door de hiervoor noodzakelijke modules te laden.



```
root@localhost:/etc/openldap/schema
File Edit View Terminal Tabs Help
[indo@localhost ~]$ su -
Password:
[root@localhost ~]# cd /etc/openldap/schema/
[root@localhost schema]# ls
corba.schema  cosine.schema      java.schema  openldap.ldif  README
core.ldif     dyngroup.schema    misc.schema  openldap.schema  README
core.schema   inetorgperson.schema  nis.schema  ppolicy.schema  samba.schema
[root@localhost schema]#
```

Het LDAP-schema bestaat uit verschillende bestanden die alle aangeroepen moeten worden vanuit het configuratiebestand `/etc/openldap/slapd.conf`.

Het algemene formaat dat door LDAP gebruikt wordt om te werken met gegevens, is het LDAP Data Interchange Format (LDIF). Dit ASCII-formaat wordt bijvoorbeeld gebruikt om gegevens toe te voegen aan de Directory. Daarbij is het belangrijk dat voor elke class in elk geval de verplichte attributen gespecificeerd worden. Als dat niet gebeurt, kunnen er vervellende foutmeldingen volgen en wordt het object niet gemaakt.

Hoofdstuk 7

OpenLDAP

De LDAP-implementatie die vooral op het Linux-platform gebruikt wordt, is OpenLDAP (<http://www.openldap.org>). Na installatie van dit product, dat op de meeste Linux-systemen deel uitmaakt van een custom-installatie, wordt op uw systeem een aantal configuratiebestanden, hulpprogramma's en programmabestanden weggezet. Voordat we ingaan op de precieze configuratie, zullen we hier eerst een overzicht geven van de verschillende componenten die met OpenLDAP geïnstalleerd worden.

Het belangrijkste programmabestand dat deel uitmaakt van de OpenLDAP-software is de daemon `slapd`. Dit is de stand-alone LDAP-daemon. Dit process moet geactiveerd worden om over LDAP-functionaliteit te kunnen beschikken; `slapd` is dus gewoon de LDAP-server. Als u meer dan een LDAP-server binnen een netwerk gebruikt, kunt u daarnaast ook gebruik maken van `slurpd`. Als er meerdere server zijn die eenzelfde database bedienen, moeten de gegevens immers up-to-date gehouden worden tussen de verschillende kopieën van de Directory die op deze servers voorkomen. `Slurpd` is het process dat ervoor zorgt dat replicatie van gegevens plaatsvindt. Hier toe verstuurt `slurpd` de gegevens van de master-server naar alle aanwezige slave-servers.

De configuratie van LDAP vindt plaats doordat een aantal configuratiebestanden wordt bewerkt. Deze configuratiebestanden komen doorgans voor in de directory `/etc/openldap`, maar let op: sommige distributies plaatsen ook een exemplaar van de betreffende configuratiebestanden in een andere directory, zoals bijvoorbeeld direct onder `/etc`. Zorg er altijd voor dat u zeker weet dat u het juiste bestanden bewerkt voordat u er mee aan het werk gaat.

Het belangrijkste configuratiebestand is `slapd.conf`. Hierin vindt vrijwel de gehele configuratie van de LDAP-daemon `slapd` plaats. Dit bestand moet

in elk geval aangepast worden voordat u het proces slapd opstart. Naast slapd.conf bestaat er een aantal bestanden waarin het schema van de LDAP-Directory gedefinieerd is. Dit schema bepaalt welke classes verbonden zijn. Het schema bestaat uit een aantal bestanden dat voorkomt in de directory /etc/openldap/schema.

Als laatste is er een aantal opdrachten waarmee gegevens aan de database toegevoegd, eruit verwijderd en erin bewerkt kunnen worden. Het betreft hier ldapadd waarmee gegevens toegevoegd worden, ldapmodify om gegevens te wijzigen, ldapdelete om gegevens te verwijderen en ldapsearch om te zoeken naar gegevens vanuit het algemene LDIF-formaat vertaald kunnen worden in het door LDAP vereiste LDBM-format.

Daarnaast komen er meestal nog twee modules voor die door de client software gebruikt kunnen worden. U mag er echter niet vanuitgaan dat deze modules daadwerkelijk voorkomen; ze maken namelijk deel uit van andere software-packages. Als eerste is er de LDAP-module die door de nameservice switch gebruikt kan worden; deze heeft de naam nss_ldap. U gebruikt hem in de algemene procedure waarmee ingesteld wordt welke configuratiebestanden gebruikt moeten worden om informatie over bijvoorbeeld gebruikers, groepen, servers enzovoort te achterhalen. U regelt de configuratie hiervan met behulp van het instellingenbestand /etc/nsswitch.conf.

Een andere belangrijke module die door de clients gebruikt kan worden is pam_ldap. Dit is de module die ervoor zorgt dat het standaardmechanisme van Pluggable Authentication Modules (PAM) dat op Linux gebruikt wordt, ook kan gebruikmaken van LDAP om gebruikers te laten inloggen op basis van gegevens in de LDAP-database.

Hoofdstuk 8

Overzicht van de configuratie

Om een LDAP-server te configureren moeten in elk geval de volgende stappen doorlopen worden:

1. Zorg ervoor dat de OpenLDAP-software geïnstalleerd is. Haal deze eventueel op van <http://www.openldap.org>.
2. Configureer het bestand `slapd.conf`.
3. Start `slapd`.
4. Voeg gegevens aan de database toe door met `ldapadd` gegevens uit een LDIF-bestand te importeren.
5. Kijk met `ldapsearch` of dit goed gelukt is.

Door deze vijf stappen uit te voeren, zorgt u voor een basisinstallatie van LDAP. U kunt nu met een LDAP-client gegevens uit uw LDAP-directory halen. Als u echter in staat wilt zijn meer geavanceerde zaken te doen, zoals bijvoorbeeld inloggen op de LDAP-database, dan moeten er nog enkele extra taken uitgevoerd worden.

8.1 Installatie van de software

In veel gevallen kan de LDAP-server tijdens de installatie van de distributie gekopieerd worden; op de meeste moderne distributies zijn hier niet eens extra opies voor nodig. Als dit niet het geval is, kunt u de meest recente software zelf ophalen en uitpakken. U gaat als volgt te werk om deze te installeren:

Standaardbestandslocaties

In deze beschrijving gaan we ervan uit dat u zelf de LDAP-software downloadt en installeert. Soms echter is de LDAP-server al op uw systeem geïnstalleerd. In het laatste geval het voorkomen dat andere directory's gebruikt worden dan de directory's die in dit vermeld worden. Gebruik bij twijfel locate om te achterhalen waar de bestanden zich bevinden.

1. Haal de software op en pak de bestanden uit. Gebruik hiervoor de opdracht `tar -zxvf openldap-2.4.9.tgz`. (De exacte naam van het uit te pakken bestand is per release verschillend.)
2. Selecteer met de opdracht `cd` de directory die na het uitpakken is gemaakt.
3. Activeer het script `configure` in deze directory. Gebruik hiervoor de opdracht `./configure`. Voor informatie over de parameters die u aan dit script kunt meegeven, gebruikt u de opdracht `./configure --help`. Dit script controleert of uw systeem aan alle voorwaarden voldoet om OpenLDAP succesvol te kunnen gebruiken en maakt vervolgens een aantal bestanden.
4. Vervolgens kunnen de LDAP-librarybestanden en -toepassingen gebouwd worden met de opdracht `make`. Maak eerst de dependencies (afhankelijkheden) met `make depend` en compileer vervolgens het programma met de opdracht `make`.
5. Nu kunt u testen of alles goed gegaan is. Geef hiervoor in de subdirectory `tests` de opdracht `make`.
6. Dan is het moment daar dat de software op uw systeem geïnstalleerd wordt. Geef hiervoor in de LDAP-installatiedirectory de opdracht `make install`.

8.2 Configuratie van de server: `slapd.conf`

Na installatie van de software wordt een standaardvoorbeeldbestand `/etc/openldap/slapd.conf` gemaakt. Dit moet bewerkt worden, zodat het aan de behoeften van uw organisatie voldoet. We bespreken nu een voorbeeld van dit bestand. In een eenvoudige vorm kan dit bestand er als volgt uitzien:

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/rfc2307bis.schema
```

```
include /etc/openldap/schema/yast.schema
pidfile /usr/local/var/slapd.pid
argsfile /usr/local/var/slapd.args
# load dynamic backend modules:
modulepath /usr/lib/openldap/modules
access to dn.base=
by * read
access to dn.base="cn=Subschema"
by * read
access to attr=userPassword,userPKCS12
by self write
by * auth
access to attr=shadowLastChange
by self write
by * read
access to *
by * read
loglevel 0
TLSCertificateFile /etc/ssl/servercerts/servercert.pem
TLSCACertificatePath /etc/ssl/certs/
TLSCertificateKeyFile /etc/ssl/servercerts/serverkey.pem
database bdb
suffix "dc=ndomain1, dc=local"
rootdn "cn=Administrator,dc=ndomain1 dc=nl"
rootpw "sshasBnNOCZ1MWsg0720IKLzPOB9SmVaTFZCVg=="
directory /var/lib/ldap
checkpoint 1024 5
checksize 10000
index objectClass,uidNumber,gidNumber eq
index member,mail eq,pres
index cn,displayname,uid,sn,givenname sub,eq,pres
```

We zullen nu bespreken wat er in dit bestand gebeurt

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/rfc2307bis.schema
include /etc/openldap/schema/yast.schema
```

In de eerste regels van dit bestand wordt een aantal extra configuratiebestanden aangeroepen. Deze bestanden vormen met elkaar het LDAP-schema. Hierin wordt aangegeven welke objecten in de LDAP-Directory kunnen worden gemaakt, waar in de tree (structuur) deze objecten mo-

gen voorkomen en welke attributen met deze objecten verbonden kunnen worden. LDAP maakt gebruik van een schema dat uitbreidbaar is. Elke LDAP-server heeft om te beginnen een basisschema. In dit geval wordt het basisschema gedefinieerd in het bestand `core.schema`. In dit basisschema bestaan alle objecten die altijd sowieso moeten voorkomen. Dit basisschema wordt in deze configuratie uitgebreid met een aantal extra schemamodules.

Vervolgens zijn er twee regels waarin het beheer van de LDAP-server wordt bijgehouden. Om te beginnen gebeurt dat in het bestand `slapd.pid`, waarin bijgehouden. Om te beginnen gebeurt dat in het bestand `slapd.pid`, waarin het procesidentificatienummer van de server bewaard wordt. Daarnaast is er `slapd.args`, waarin de argumenten bewaard worden waarmee de LDAP-server gestart is.

In het volgende deel van het configuratiebestand kan een aantal LDAP-modules geladen worden. U ziet hier alleen de definitie van het pad waarin deze modules horen voor te komen; seze regel wordt doorgaans gevolgt door een aantal regels waarop de namen staan van de modules die geladen moeten worden. Dit kan er bijvoorbeeld als volgt uitzien:

```
modulepath /usr/lib/openldap/modules
modulepath back_ldap.la
modulepath back_meta.la
modulepath back_monitor.la
modulepath back_perl.la
```

Nadat de werking van additionele LDAP-modules ingesteld is, wordt aangegeven wie rechten heeft voor welke delen van de LDAP-Directory. U ziet dat op de grootste delen van de LDAP-server leesmachtigingen gegeven worden aan iedereen. Voor sommige belangrijke attributen zoals het wachtwoord van gebruikers hebben gebruikers zelf rechten om te schrijven. Dit is handig; zo is namelijk een gebruiker in staat zijn eigen wachtwoord te wijzigen. Houdt er rekening mee dat een LDAP-server in principe een open karakter heeft: iedereen heeft rechten overal te schrijven.

Als laatste gedeelte van het algemene configuratiebestand volgt een aantal algemene parameters dat bepaalt hoe de LDAP-server zich moet gedragen. Om te beginnen moet ervoor gezorgd worden dat een bewijligde verbinding mogelijk is. Hiervoor zijn de drie regels waarin wordt aangegeven waar de TLS-certificaten teruggevonden kunnen worden. Vervolgens wordt aangegeven van welk type database gebruikgemaakt wordt. Hiervoor zijn verschillende mogelijkheden; in dit geval is gekozen voor het type `bdb`.

Dan komt er een aantal instellingen waarmee meer geregeld wordt voor

de database zelf. Als eerste is dat de standaardsuffix, die hier staat ingesteld als `ndomain1`, `local`. Deze suffix bepaald in welke plaats in de database nieuwe objecten standaard worden neergezet. Vervolgens wordt gedefinieerd wie de beheerder is van de database/ Houd er rekening mee dat deze beheerder oppermachtig is en toegang krijgt tot werkelijk alle aspecten van de database.

Wachtwoord van de beheerder

Er zijn verschillende manieren om het wachtwoord van de beheerder in te voeren. De meest eenvoudige manier is om het in ASCII-tekst in het configuratiebestand `slapd.conf` plaatsen. Dit heeft echter nadelen voor de bewijling van uw server. Om ervoor te zorgen dat het wachtwoord in een onleesbaar formaat wordt opgeslagen, maakt u gebruik van de opdracht `slappasswd`. Deze opdracht wordt speciaal gebruikt voor het invoeren van het wachtwoord van de beheerder.

Vervolgens wordt met directory `/var/lib/ldap` bepaald in welke directory op het lokale bestandssysteem de LDAP-database moet worden weggeschreven. Tot slot is er aantal regels dat de prestaties van de LDAP-database beïnvloedt. De parameter `cache_size` bepaalt hoeveel objecten in de database cache bewaard kunnen worden en de drie indexregels tot slot zorgen ervoor dat een aantal indexen automatisch wordt aangemaakt. Het gebruik van deze indexen zorgt ervoor dat in de database sneller gezocht kan worden naar objecten en attributen die vaak opgevraagd worden.

8.3 slapd starten

Als `slapd.conf` eenmaal op de juiste wijze is gemaakt, moet de server gestart worden. Hiervoor kunt u natuurlijk handmatig het programmabestand `/usr/sbin/slapd` activeren. Als u het op deze manier doet, kan het vooral in de testfase interessant zijn de optie `-dx` mee te geven bij het starten van deze server. Wanneer u in plaats van de `x` in deze optie een getal opgeeft, bepaald u hiermee het debug-level waarmee de server gestart wordt. Hoe hoger dit getal is, hoe meer details u terugvindt in de logboek bestanden van server. Naast de mogelijkheid de LDAP-server handmatig te starten, kunt u als alternatief gebruikmaken van het script dat meegeleverd wordt om de server automatisch te starten in de SystemV-opstartroutine van uw server. Zo start u bijvoorbeeld op CentOS Linux de LDAP-server met de opdracht `/etc/init.d/ldap start`.

8.4 Gegevens aan de directory toevoegen

U bent nu klaar om gegevens toe te voegen aan de directory. De meest gebruikelijke manier om dit te doen, is door middel van LDIF. U maakt een bestand waarin gegevens in het LDIF-formaat voorkomen en de inhoud van dit bestand voegt u vervolgens met een opdracht als `ldapadd` toe aan de Directory. Dit bestand kan bijvoorbeeld de volgende eenvoudige inhoud hebben:

```
dn: dc=ndomain1, dc=local
dc: ndomain1
o: ndomain1
objectclass: organisation
objectclass: dcObject
dn: cn=Manager, dc=ndomain1, dc=local
cn: Manager
sn: Manager
objectclass: person
dn: cn=Robert, dc=ndomain1, dc=local
objectClass: person
cn: Robert
sn: Keersse
userPassword: geheim
dn: cn=VictorM, dc=ndomain1, dc=local
objectClass: person
cn: Victor
sn: Martin
userPassword: geheim
dn: cn=Maarten, dc=ndomain1, dc=local
objectClass: person
cn: Maarten
sn: Michielsen
userPassword: geheim
```

Containers eerst!

Als u met behulp van een LDIF-bestand gegevens wilt toevoegen aan een LDAP-directory, is het belangrijk erop te letten dat u dit in de goede volgorde doet. Als u bijvoorbeeld een gebruiker `cn=VictorM, dc=ndomain1, dc=local` toe wilt voegen, lukt dat alleen als u er eerst voor gezordt hebt dat de container `dc=ndomain1, dc=local` bestaat. In het voorgaande voorbeeld ziet u dat aan deze voorwaarde wordt voldaan.

Als dit bestand de naam `users.ldif` heeft, kunt u het toevoegen aan de Directory met de opdracht `ldapadd -x -D "cn=Manager, dc=ndomain1, dc=local-W ; users.ldif`. Als het goed is, krijgt u als antwoord op deze opdracht `Enter LDAP Password:` te zien. Geef hier het wachtwoord van de account op die u de manager gespecificeerd hebt. De naam en het wachtwoord van deze manager komen overigens overeen met de naam en de wachtwoord van die u in `slapd.conf` hebt opgenomen voor de account `rootdn`. Controleer trouwens goed of er niet per ongeluk aan het begin van een regel ergens een spatie te veel staat. Dit kan er toe leiden dat u met een foutmelding geconfronteerd wordt, waardoor het onmogelijk is de gegevens aan de database toe te voegen.

8.5 ldap.conf bewerken

Als alles goed gegaan is, hebt u nu de LDAP-database gevuld met gebruikersgegevens. Voordat u echter ook de LDAP-database kunt gebruiken, moet u ervoor zorgen dat uw workstation deze database ook terug kan vinden. Op een Linux-computer doet u dit door het configuratiebestand `/etc/openldap/ldap.conf` te bewerken. In dit bestand moeten in elk geval twee parameters voorkomen: de parameter `HOST`, waarmee u verwijst naar het IP-adres van de LDAP-server, en de parameter `BASE`, waarmee u verwijst naar de container waarin gezocht moet worden. De inhoud van dit bestand zou er bijvoorbeeld als volgt uit kunnen zien:

```
HOST 192.168.123.10
BASE dc=ndomain1, dc=local
```

8.6 Kijken of het werkt

Voordat u nu ook maar iets kunt doen, moet u eerst kijken of het allemaal werkt. Gebruik hiervoor de opdracht `ldapsearch`, bijvoorbeeld `ldapsearch -x -L -b "dc=ndomain1, dc=local-W "(objectclass=*)"`. Hierna kunt u overgaan naar fase 2, het configureren van een clienttoepassing.

Hoofdstuk 9

LDAP-client

Als de server eenmaal draait, wat meestal het grootste probleem niet is, kunt u uw Linux-werkstation configureren om gebruikersnaam en wachtwoord te valideren in de LDAP-database. Zorg er om te beginnen voor op elke client-machine de volgende RPM-packages geïnstalleerd zijn: `openldap`, `auth_ldap` en `nss_ldap`. U kunt met de opdracht `rpm -q packagenaam` verifiëren of het betreffende package geïnstalleerd is; kijk gelijk ook even met `rpm -V packagenaam` of alle bestanden uit het package nog intact zijn. Wanneer de juiste packages op de LDAP-client aanwezig zijn, moet u ervoor zorgen dat de gebruikers voortaan het lokale wachtwoordmechanisme kunnen omzetten en kunnen inloggen op de LDAP-server. Voer hiervoor de volgende stappen uit.

1. Pas `ldap.conf` aan.
2. Pas `/etc/nssswitch.conf` aan.
3. Zorg ervoor dat PAM gaat gebruikmaken van LDAP.
4. Zorg ervoor dat de gebruikers met de juiste attributen in de database geplaatst worden.

9.1 `ldap.conf` aanpassen

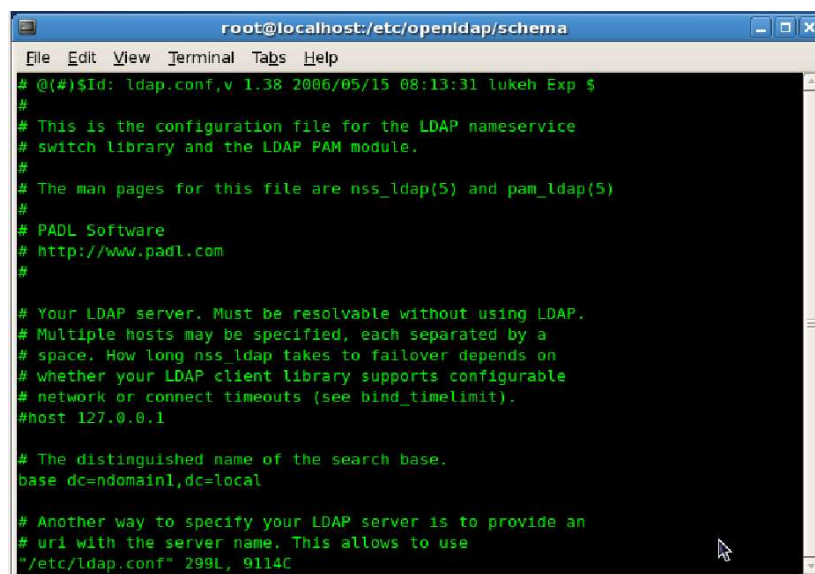
Op uw systeem bestaan soms twee bestanden met de naam `ldap.conf`. Het bestand `/etc/ldap.conf` wordt gebruikt door de modules `nss_ldap` en `pam_ldap` om te bepalen waar de informatie vandaan gehaald moet worden; het bestand `/etc/openldap/ldap.conf` wordt gebruikt door clienttoepassingen zoals `ldapsearch` en `ldapadd`, maar ook om ervoor te zorgen dat uw computer de LDAP-server waarop aangemeld moet worden terug kan vinden. Beide bestanden moeten aangepast worden om gebruikt te kunnen worden. Om verwarring te voorkomen, doet u er verstandig aan een van deze bestanden

te vervangen door een symbolic link naar het andere bestand. In dit bestand moet in elk geval aangegeven worden vanaf welke host de informatie gehaald moet worden en in welke container standaard naar informatie gezocht moet worden. Er kan meer geconfigureerd worden; dit is echter in eerste installatie niet noodzakelijk.

9.2 nsswitch.conf aanpassen

In `/etc/nsswitch.conf` wordt bepaald voor welke functionaliteit gebruikge maakt moet worden van welke configuratiebestanden en/of databases. Zorg ervoor dat in elk geval de volgende regels in dit bestand komen te staan:

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



In het configuratiebestand `ldap.conf` wordt gespecificeerd met welke LDAP-server contact gemaakt moet worden.

Hierdoor kan behalve naar gegevens in de normale bestanden, zoals `/etc/passwd`, `/etc/shadow` en `/etc/group`, ook in de LDAP-database gekeken worden naar informatie om gebruikers te valideren. U neemt deze maatregel om er zeker van te zijn dat elke toepassing in staat is contact te maken met de LDAP-server. De meeste toepassingen echter zullen deze regels niet nodig hebben en door middel van PAM contact maken met de LDAP-server.

9.3 PAM aanpassen

De laatste en wellicht ook meest complexe stap in de configuratie is dat u PAM moet aanpassen, zodat gebruikgemaakt wordt van LDAP. De belangrijke informatie over PAM wordt hier nog even voor u samengevat.

Sinds gebruikgemaakt wordt van PAM is het niet langer noodzakelijk dat elke toepassing zijn eigen programmacode bevat om de validatie van gebruikers af te kunnen handelen. In plaats daarvan kan elke toepassing verwijzen naar het PAM-mechanisme. PAM is daarbij de algemene methode die uit verschillende modules bestaat. Deze modules bepalen hoe er uiteindelijk gevalideerd moet worden. Zo is er standaardmodule die gebruikt wordt om gebruikers te valideren op basis van informatie in `/etc/passwd`, zo kunt u een module toevoegen zodat gebruikers kunnen worden geverifieerd op basis van informatie in de LDAP-Directory, zo is het ook mogelijk PAM-modules toe te voegen op basis waarvan ter validatie gegevens van een smartcard gecontroleerd worden. PAM biedt zo dus een hele flexibele wijze om te kunnen valideren. Om dit te doen, wordt gebruikgemaakt van verschillende configuratiebestanden. In principe is er voor elke service waarbij gebruikers zichzelf bekend moeten maken een configuratiebestand waar staat aangegeven wat er precies moet gebeuren. Deze configuratiebestanden komen voor in de directory `/etc/pam.d`.

In deze configuratiebestanden wordt gebruikgemaakt van vier soorten modules:

- Auth-modules zorgen voor de daadwerkelijke afhandeling van de validatie van gebruikers (authentication). Onder andere het vragen naar en controleren van wachtwoorden wordt door deze module afgehandeld. Ook zorgen ze ervoor dat credentials zoals groepslidmaatschap en Kerberos-tickets worden ingesteld.
- Account-modules zorgen ervoor dat gecontroleerd wordt bij de accountinformatie of de gebruiker ook daadwerkelijk toestemming heeft gebruik te maaken van resources. Denk hierbij aan een controle of de account niet verlopen is, of de gebruiker wel ingelogt mag zijn op dit tijdstip enzovoort.
- Password-modules worden gebruikt om wachtwoorden in te stellen.
- Session-modules worden gebruikt om na het inloggen gebruik te maken van resources die met de gebruiker verbonden zijn. Denk daarbij bijvoorbeeld aan het benaderen van de homedirectory van de gebruiker.

Nu worden er per soort functionaliteit, zoals hierboven genoemd, meestal meerdere modules gebruikt. U ziet hiervan een voorbeeld in het volgende bestand, dat waarschijnlijk veel lijkt op `/etc/pam.d/login` op uw systeem:

```
auth required /lib/security/pam_securetty.so
auth required /lib/security/pam_unix.so shadow nullok
auth required /lib/security/pam_nologin.so
account required /lib/security/pam_unix.so
password required /lib/security/pam_cracklib.so
password required /lib/security/pam_unix.so shadow nullok
use_authok
session required /lib/security/pam_unix.so
```

U ziet in dit bestand dat er een module is die met name vaak naar voren komt, namelijk de module `pam_unix.so`. Deze zorgt ervoor dat de validatie van gebruikers en wachtwoorden wordt afgehandeld door het standaard UNIX-mechanisme waarin gebruikgemaakt wordt van `/etc/passwd` en `/etc/shadow`. Daarnaast is er de module `pam_securetty.so`, die ervoor zorgt dat in het bestand `/etc/securetty` gecontroleerd wordt of de gebruiker root wel vanaf een veilige terminal inlogt; `pam_nologin.so`, die controleert of er misschien een bestand `/etc/nologin` bestaat dat ervoor zorgt dat geen gebruiker nog mag inloggen en `pam_cracklib.so`, waarmee gecontroleerd wordt of de wachtwoorden die ingevoerd worden wel veilig zijn. Voor elk van deze modules staat de aanduiding `required`; dit betekent dat aan de voorwaarden die door de module gesteld worden voldaan moet worden.

Nu willen wij nog instellen dat het ook goed is als de gebruiker zich bij de LDAP-Directoryserver aanmeldt. Dit kan door in het PAM-mechanisme, voordat de normale verificatie bij `pam_unix` gedaan wordt, een regel op te nemen die verwijst naar de module `pam_ldap`. Gebruik van deze module is niet verplicht; het is echter voldoende als de gebruiker zich kan aanmelden op basis van deze module. Hiermee bouwt u een achterdeurtje in: als niet via LDAP ingelogd kan worden, kan het normale mechanisme nog gebruikt worden. Waar het op neerkomt, is dat in plaats van de aanduiding `required` nu een aanduiding `sufficient` gebruikt kan worden. Het uiteindelijke configuratiebestand komt er dan als volgt uit te zien:

```
auth required /lib/security/pam_securetty.so
auth sufficient /lib/security/pam_ldap.so
auth required /lib/security/pam_unix.so shadow nullok
auth required /lib/security/pam_nologin.so
account sufficient /lib/security/pam_ldap.so
account required /lib/security/pam_unix.so
password required /lib/security/pam_cracklib.so
```



```
password sufficient /lib/security/pam_ldap.so
password required /lib/security/pam_unix.so shadow nullok
use_authok
session sufficient /lib/security/pam_ldap.so
session required /lib/security/pam_unix.so
```

9.4 Gebruikers met de juiste attributen maken

Als dit allemaal gebeurd is, bent u er bijna. U moet er nu alleen nog voor zorgen dat gebruikers met de benodigde attributen worden gemaakt. Dit betekent dat alle gebruikersinformatie die normaal in `/etc/passwd` en `/etc/shadow` voorkomt, nu in de LDAP-database geplaatst moet worden. U kunt er op twee manieren voor zorgen dat dit gebeurt. De eerste is dat u door middel van een aantal perl-scripts de gegevens uit gebruikersdatabases in de LDAP-database importeert. Maak hiervoor gebruik van de migratie-scripts die geïnstalleerd zijn in `/usr/share/openldap/migration`. Met deze scripts kunt u alle netwerkinformatie die waar dan ook gebruikt moet worden, importeren; het gaat dus niet alleen om gebruikers, maar bijvoorbeeld ook om computernamen.

U kunt er zelf voor zorgen dat de gebruikers met de juiste attributen worden gemaakt; hiervoor moet u gebruikmaken van een LDIF-bestand waarvan dan later de inhoud met `ldapadd` in de database wordt toegevoegd. Zorg er in dat geval wel voor dat de container waarin u de gebruikers wilt toevoegen bestaat voordat u begint met importeren van gebruikers! Hieronder ziet u een voorbeeld van zo'n bestand:

```
dn: cn=ndo,dc=dnomain1,dc=com
uid: ndo
cn: ndo
objectclass: account
objectclass: posixAccount
objectclass: top
objectclass: shadowAccount
userpassword: cryptS1SpW0yoDDYSyPGD1cJfqB28exnrVyNcy
shadowlastchange: 11354
shadowmax: 99999
shadowwarning: 7
shadowinactive: -1
shadowexpire: -1
shadowflag: -1073744532
loginshell: /bin/bash
```

uidnumber: 511
gidnumber: 100
homedirectory: /home/ndo

Houd wel rekening met twee tekortkomingen die nog aan deze werkwijze verbonden zijn. Als eerste is dat de homedirectory; die wordt niet automatisch gemaakt als dit bestand geïmporteerd wordt. Dit probleem kunt u echter oplossen door gebruik te maken van PAM-configuratiebestand `pam_mkhomedir`. Vervolgens is dit wachtwoord. U wilt natuurlijk wachtwoorden in een versleutelde vorm in de database hebben. De eenvoudigste wijze om dit correct te doen, is door eerst de gebruiker zonder wachtwoord met behulp van een LDIF-bestand in de directory te importeren. Vervolgens kunt u de gebruiker met behulp van een opdracht `ldappasswd` achteraf een wachtwoord geven.

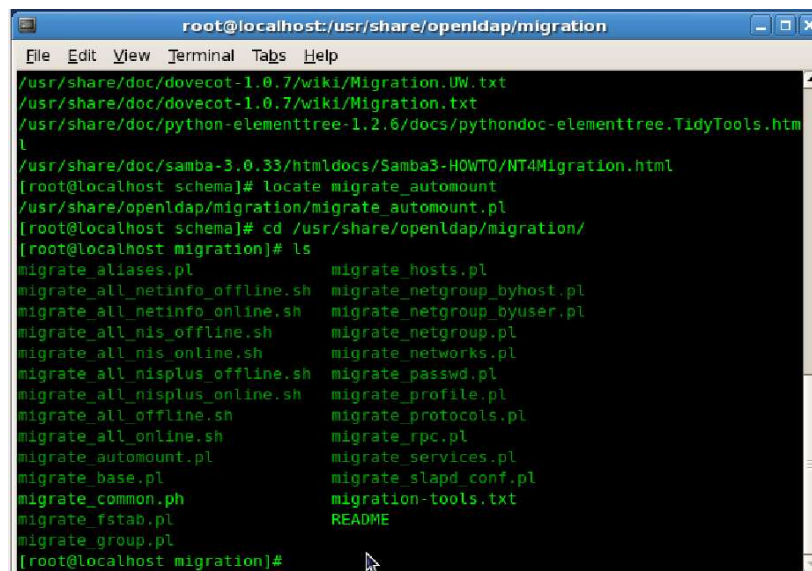
9.5 Werken met de migratiescripts

Het overzetten van gegevens van uw locale computer naar de LDAP-server, is een zeer bewerkelijke taak. U moet er immers voor zorgen dat alle gegevens die u wilt migreren in het juiste format in een LDIF-bestand gezet worden. Het is aangeraden om dit niet zelf te doen, maar gebruik te maken van de Migration Tools. U kunt deze downloaden van www.padl.com/OSS/LigrationTools.html. In de volgende procedure wordt besproken hoe u deze handige Perl-scripts downloaden en installeren en hoe u ze vervolgens gebruikt om gegevens uit lokale bestanden op uw computer te migreren naar de LDAP-database.

1. Download vanaf www.padl.com/OSS/LigrationTools.html het bestand `MigrationTools.tgz` en sla dit bestand op in uw homedirectory.
2. Installeer de MigrationTools door in de directory waar u het bestand hebt opgeslagen de opdracht `tar -zxvf MigrationTools.tgz` te geven. Het resultaat van deze opdracht is dat er een directory wordt aangemaakt waaronder u alle migration tools terugvindt. Er zijn er meerdere, voor elk belangrijk configuratiebestand op het netwerk is er een afzonderlijk bestand. Zo is er bijvoorbeeld het bestand `migrate_passws.pl` waarmee u informatie uit uw lokale `passwd`-bestand kunt migreren.
3. Open het bestand `migrate_common.ph` met een editor. In dit bestand worden verschillende variabelen met de naam `NAMINGCONTEXT` gedefinieerd. Verzeker u ervan dat de containernamen waarnaar deze variabelen verwijzen, ook daadwerkelijk in de LDAP-Directory bestaan voordat u de Migration Tools gaat gebruiken om informatie in de LDAP-Directory te importeren. Hebt u geen zin om voor elke afzonderlijke informatiecategorie een aparte container aan te maken? Zorg

er dan voor dat de waarde van al deze variabelen leeg wordt. Dit doet u bijvoorbeeld door een regel als `$NAMINGCONTEXT{'passwd'} - ou=People` te wijzigen in `$NAMINGCONTEXT{'passwd'}`.

4. Zoek ook in het bestand `migrate_common.ph` de regel `$DEFAULT_BASE = "dc=padl,dc=com"`. Op deze regel wordt aangegeven in welke container de LDAP-objecten aangemaakt moeten worden. Wijzig deze regel zodat verwezen wordt naar de container die u wilt gebruiken, bijvoorbeeld `$DEFAULT_BASE = "dc=ndomain1,dc=local"`.
5. Gebruik nu de opdracht `./migrate_passwd.pl /etc/passwd ; newusers.ldif`. Met deze opdracht zorgt u ervoor dat alle gebruikers die nu voorkomen in `/etc/passwd`, in een LDIF-bestand gezet worden.
6. Gebruik tot slot de opdracht `ldapadd -x -D "cn=Manager, dc=ndomain1, dc=local-W ; newusers.ldif` (let op de namen van de LDAP-manager en het LDIF-bestand dat u wilt gebruiken), om de gebruikers die u zojuist uit `/etc/passwd` geëxporteerd hebt in uw LDAP-database te importeren.
7. U bent nu klaar met importeren van gegevens uit `/etc/passwd` en `/etc/shadow`. Om te bewijzen dat het ook inderdaad werkt, verwijdert u nu een willekeurige gebruikersnaam uit deze twee bestanden. U zult zien dat u toch nog als deze gebruiker in kunt loggen.



```

root@localhost:usr/share/openldap/migration
File Edit View Terminal Tabs Help
/usr/share/doc/dovecot-1.0.7/wiki/Migration.UW.txt
/usr/share/doc/dovecot-1.0.7/wiki/Migration.txt
/usr/share/doc/python-elementtree-1.2.6/docs/pythondoc-elementtree.TidyTools.htm
l
/usr/share/doc/samba-3.0.33/html/docs/Samba3-HOWTO/NT4Migration.html
[root@localhost schema]# locate migrate_automount
/usr/share/openldap/migration/migrate_automount.pl
[root@localhost schema]# cd /usr/share/openldap/migration/
[root@localhost migration]# ls
migrate_aliases.pl          migrate_hosts.pl
migrate_all_netinfo_offline.sh migrate_netgroup_byhost.pl
migrate_all_netinfo_online.sh migrate_netgroup_byuser.pl
migrate_all_nis_offline.sh  migrate_netgroup.pl
migrate_all_nis_online.sh   migrate_networks.pl
migrate_all_nisplus_offline.sh migrate_passwd.pl
migrate_all_nisplus_online.sh migrate_profile.pl
migrate_all_offline.sh      migrate_protocols.pl
migrate_all_online.sh       migrate_rpc.pl
migrate_automount.pl        migrate_services.pl
migrate_base.pl             migrate_slapd_conf.pl
migrate_common.ph           migration-tools.txt
migrate_fstab.pl            README
migrate_group.pl
[root@localhost migration]#

```

Met behulp van de migration tools u alle belangrijke informatie van uw computer omzetten naar een geldig LDIF-formaat.

```

root@localhost:/usr/share/openldap/migration
File Edit View Terminal Tabs Help

if ($NETINFOBRIDGE) {
    $NAMINGCONTEXT{'aliases'}      = "cn=aliases";
    $NAMINGCONTEXT{'fstab'}        = "cn=mounts";
    $NAMINGCONTEXT{'passwd'}       = "cn=users";
    $NAMINGCONTEXT{'netgroup_byuser'} = "cn=netgroup.byuser";
    $NAMINGCONTEXT{'netgroup_byhost'} = "cn=netgroup.byhost";
    $NAMINGCONTEXT{'group'}        = "cn=groups";
    $NAMINGCONTEXT{'netgroup'}      = "cn=netgroup";
    $NAMINGCONTEXT{'hosts'}         = "cn=machines";
    $NAMINGCONTEXT{'networks'}      = "cn=networks";
    $NAMINGCONTEXT{'protocols'}     = "cn=protocols";
    $NAMINGCONTEXT{'rpc'}           = "cn=rpcs";
    $NAMINGCONTEXT{'services'}      = "cn=services";
} else {
    $NAMINGCONTEXT{'aliases'}      = "ou=Aliases";
    $NAMINGCONTEXT{'fstab'}        = "ou=Mounts";
    $NAMINGCONTEXT{'passwd'}       = "ou=People";
    $NAMINGCONTEXT{'netgroup_byuser'} = "nisMapName=netgroup.byuser";
    $NAMINGCONTEXT{'netgroup_byhost'} = "nisMapName=netgroup.byhost";
    $NAMINGCONTEXT{'group'}        = "ou=Group";
    $NAMINGCONTEXT{'netgroup'}      = "ou=Netgroup";
    $NAMINGCONTEXT{'hosts'}         = "ou=Hosts";
    $NAMINGCONTEXT{'networks'}      = "ou=Networks";
}

```

In het bestand `migrate_common.ph` geeft u aan naar welke containers informatie van uw lokale computer gemigreerd moet worden.

```

Terminal - root@localhost:/home/ndo/Documents/Eindwerk Net-Ast/Eindwerk NA - juni 2009
File Edit View Terminal Go Help

version: 1

# LDIF Export for: ou=Xylos Applied ICT,ou=tewerkstelling,dc=donboscowilrijk,dc=be
# Generated by phpLDAPadmin ( http://phpldapadmin.sourceforge.net/ ) on May 25, 2009 9:08 am
# Server: DonBoscoWilrijk LDAP-Server (127.0.0.1)
# Search Scope: sub
# Search Filter: (objectClass=*)
# Total Entries: 6

dn: ou=Xylos Applied ICT,ou=tewerkstelling,dc=donboscowilrijk,dc=be
objectClass: organizationalUnit
objectClass: top
ou: Xylos Applied ICT
postalCode: 2030
telephoneNumber: 03 543 75 00
facsimileTelephoneNumber: 03 542 69 56
street: Noorderlaan 139
l: Antwerpen
businessCategory: IT
st: Antwerpen

Xylos\ Applied\ ICT.ldif

```

Met het `migrate-passwd.pl`-script exporteert u alle gegevens uit `/etc/passwd` naar een geldig LDIF-formaat.

Hoofdstuk 10

Uw container integreren in een andere tree

Vaak is het voor een server meer dan voldoende als de hele Directory-tree op een enkele server voorkomt. In dat geval beheerst slapd alles wat er is. Het is echter ook mogelijk slapd naar een andere server te laten verwijzen, waarop een ander deel van de Directory-tree voorkomt. Op die andere server kan dan gebruikgemaakt worden van slapd, maar eventueel ook van een hele andere met LDAP compatibele directory-service. Het voordeel van een dergelijke configuratie is dat de Directory in zijn geheel dan verspreid over meerdere servers in het netwerk voorkomt. Hierdoor wint de gebruiker die op een andere locatie informatie uit de Directory moet halen aan snelheid. Als u slapd laat verwijzen naar een onderliggende container, wordt dat "subordinate knowledge information" genoemd; als verwezen wordt naar een bovenliggende container wordt dat "superior knowledge information" genoemd.

Verwijzen naar een onderliggende container is niet al te moeilijk. Als server `ndo1.ndomain1.local` de partitie `dc=ndomain1, dc=local` bevat en server `ndo2.ndomain1.local` bevat `dc=main, dc=ndomain1, dc=local`, wordt de verwijzing naar de onderliggende container als volgt aangebracht:

```
dn: dc=main, dc=ndomain1, dc=local
objectClass: referral
objectClass: extensibleObject
dc: subtree
ref: ldap://main.ndomain1.local/dc=main, dc=ndomain1, dc=local
```

Alle informatie over de onderliggende container zal in dat geval opgehaald worden van `main.ndomain1.local`. Over het extra objectClass `extensibleObject` dat in het voorbeeld is opgenomen, doen wij niet moeilijk; zorg er gewoon voor dat er bij staat om problemen te voorkomen. Verwijzen naar

een bovenliggende container gebeurt op een soortgelijke wijze, namelijk ook door middel van een referral object.

Om de wijzigingen door te voeren in uw directory, maakt u een LDIF-bestand en voegt u de inhoud van dat bestand met behulp van de opdracht `ldapmodify -M -f referral.ldif -x -D "cn=Manager, dc=ndomain1, dc=lcoal-W geheim`.

10.1 Replicatie

In sommige omgevingen is het niet voldoende als er slechts een slapd actief is. Als deze namelijk om een of andere reden niet meer beschikbaar is, zijn alle gegevens uit de database ook niet langer te benaderen. Dat zou een reden kunnen zijn slapd op meerdere servers te activeren, waarbij al deze slapd's wel dezelfde database beheren. Een van deze servers is dan de master die ervoor zorgt dat wijzigingen doorgevoerd worden op de slave-servers. Om dit met OpenLDAP te regelen, moet u ervoor zorgen dat slurpd (de Standalone LDAP Update Replication Daemon) op de master-slapd-server geactiveerd wordt.

In dit scenario kunnen wijzigingen alleen worden aangebracht op de master-server. Op deze server wordt vervolgens de wijziging weggeschreven in een replicatielogboek, replication log, waardoor de wijziging door slurpd overgebracht kan worden naar de slave-databases. Dit replication log-bestand wordt gemaakt in LDIF-formaat. Het object en de betreffende wijziging worden er in weggeschreven, waarbij een tijdstempel wordt toegevoegd, zodat herkend kan worden of een slave-database up-to-date is.

Om replicatie te activeren, gaat u als volgt te werk: voeg in `slapd.conf` op de server die u als master wilt gebruiken een parameter `replica` toe voor elke slave-replica die u wilt gebruiken. U verwijst naar een replica op `ndo3.ndomain1.local`, waar u op kunt inloggen met de naam `cn=Manager, dc=ndomain1, dc=local` door de regel `replica host ndo3.ndomain1.local bind cn=Manager, dc=ndomain1, dc=local` op te nemen. Eventueel kunt u hier nog bij opgeven op welke manier op de remote host ingelogt moet worden. Als gebruikgemaakt wordt van ASCII-wachtwoorden, doet u dat door de regel `bindmethod=simple` achter de definitie van de replica te plaatsen. Zo zou een volledige regel waarmee replicatie geregeld wordt, er uit kunnen zien als:

```
replica host=ndo3.ndomain1.local binddn=cn=Manager, dc=ndomain1, dc=local  
bindmethod=simple
```

Voeg vervolgens de parameter `repllogfile` toe aan slapd op de master-server. Het argument van deze parameter specificeert waar het replica log-

bestand gemaakt kan worden.

De slave-server moet vervolgens precies zo worden opgezet als de master-server, met uitzondering van de parameters replica en replogfile. Daarnaast moet in slapd.conf op de slave-server een parameter updatedn worden opgenomen. Deze parameter heeft als argument dezelfde naam als de naam die op de master-server achter de parameter replica met binddn is opgegeven. U specificeert hier dus de naam van de beheerder van de LDAP-servers.

Zorg ervoor dat de naam die als updatedn gespecificeerd is op de slave-server ook rechten heeft om in de database te schrijven. U kunt dit instellen door dezelfde naam als rootdn op te geven.

Neem de parameter updateref op, waarin als argument de url staat die de slave moet opgeven als deze een updateverzoek binnenkrijgt.

Vervolgens moet u slapd op de master-server downloaden. Kopieer nu de database van de master- naar de slave-server. De database bevindt zich in de directory die u met de parameter directory in slapd.conf op de master-server gekopieerd hebt. Start vervolgens de master-server weer op. Breng een wijziging aan, zodat u kunt controleren of inderdaad gegevens weggeschreven worden naar het replication log-bestand. Start vervolgens slapd ook op de slave-servers. U kunt nu slurpd starten. Dit proces zorgt ervoor dat wijzigingen vanaf de master automatisch worden doorgegeven naar de slave-servers.

Deel III

Praktisch gedeelte



Work in progress.

Hoofdstuk 11

Installatie

11.1 Installeer CentOS 5.1

Installeer CentOS 5.1

```
server-gui  
extras repository
```

```
update met yum  
yum update
```

```
maak zoekdatabase aan  
updatedb
```

11.2 Installeer OpenLdap

Installeer OpenLdap

```
install packages  
yum install openldap-servers openldap-clients perl-LDAP
```


Hoofdstuk 12

Configuratie

12.1 Configureer OpenLdap server

Configureer OpenLdap server

```
copy samba.schema -> /etc/openldap/schema/
```

```
localiseer samba.schema
```

```
locate samba.schema
```

```
cp /usr/share/doc/samba-3.0.25b/LDAP/samba.schema /etc/openldap/schema/
```

bijwerken /etc/openldap/slapd.conf

```
include          /etc/openldap/schema/samba.schema
```

```
database         bdb (of ldbm)
```

```
suffix           "dc=belbob,dc=thuis"
```

```
rootdn           "cn=Manager,dc=belbob,dc=thuis"
```

```
rootpw           {SSHA}5QW+VXt171S0cL17xjzX4zEYtzHCtmhB    (slappasswd - copy en paste)
```

bijwerken /etc/openldap/ldap.conf

```
URI ldap://127.0.0.1/
```

```
BASE dc=belbob,dc=thuis
```

Opstarten OpenLdap

```
service ldap start
```

na start zonder foutmeldingen, mag deze ldap opstarten

```
chkconfig --level 35 ldap on
```

12.2 OpenLDAP vullen

Ldap vullen

aanmaken base.ldif

```
base.ldif
dn: dc=belbob,dc=thuis
dc: belbob
objectclass: top
objectclass: domain
```

toevoegen base.ldif

```
ldapadd -a -W -x -D "cn=Manager,dc=belbob,dc=thuis" -f base.ldif
```

12.3 Migration Tools

(andere manier - RedHat Migration tools)

LDAP Migration tools (RedHat includes these tools since RH9)

bijwerken /usr/share/openldap/migration/migrate_common.ph

```
# Default DNS domain\\
$DEFAULT_MAIL_DOMAIN = "belbob.thuis";
```

```
# Default base
$DEFAULT_BASE = "dc=belbob,dc=thuis"
```

aanmaken base.ldif

```
/usr/share/openldap/migration/migrate\_base.pl > base.ldif
```

toevoegen base.ldif

```
ldapadd -a -W -x -D "cn=Manager,dc=belbob,dc=thuis" -f base.ldif
```

12.4 Aanmeldingscontrole

maak gebruik van authconfig om aanmeldingscontrole te configureren:

```
authconfig-tui
```


- [*] LDAP gebruiken
- [*] LDAP-aanmelding gebruiken

Aanmelding PAM Controleren

pas /etc/nsswitch.conf aan:

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


Hoofdstuk 13

phpLdapAdmin

13.1 phpLdapAdmin installatie

install phpldapadmin

download phpldapadmin (<http://phpldapadmin.sourceforge.net/download.php>)

plaats alle bestanden in /usr/share/phpldapadmin

kopieer config.php.example naar /etc/phpldapadmin en noem deze config.php

```
cp /usr/share/phpldapadmin/config/config.example.php /etc/phpldapadmin/config.php
```

maak een link config.php -> /etc/phpldapadmin

```
ln -s /etc/phpldapadmin/config.php /usr/share/phpldapadmin/config
```

pas config.php aan en werk bij (copy config.php.example)

```
$ldapservers->SetValue($i,'server','name','BELBOB Ldap-Server');  
$ldapservers->SetValue($i,'server','base',array('dc=belbob,dc=thuis'));  
$ldapservers->SetValue($i,'server','auth_type','config');  
$ldapservers->SetValue($i,'login','dn','cn=Manager,dc=belbob,dc=thuis');  
$ldapservers->SetValue($i,'login','pass','xxxxxxx'); (geef je paswoord in platte tekst !)  
$ldapservers->SetValue($i,'server','tls',false);
```

Rechten bijwerken:

```
chown apache.apache /etc/phpldapadmin/config.php  
chmod 600 /etc/phpldapadmin/config.php  
restorecon -R -v /usr/share/phpldapadmin
```

maak verwijzing naar webserver

```
/etc/httpd/conf.d/phpldapadmin.conf
```

```
Alias /phpldapadmin /usr/share/phpldapadmin/htdocs
Alias /ldapadmin /usr/share/phpldapadmin/htdocs
<Directory /usr/share/phpldapadmin/htdocs>
    Order Deny,Allow
    Deny from All
    Allow from 127.0.0.1
    Allow from 192.168.1.
</Directory>
```

bijwerken /etc/php.ini

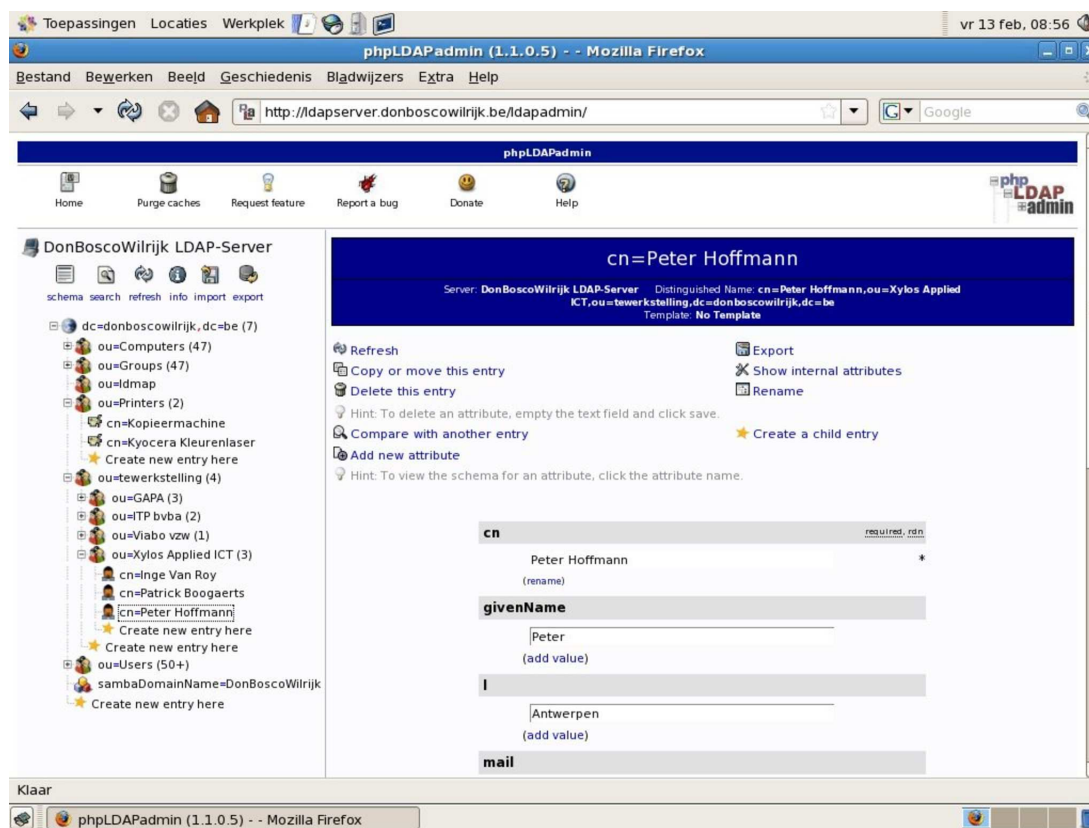
```
memory_limit = 32M      ; Maximum amount of memory a script may consume
```

herstart webserver

```
service httpd restart
```

na start zonder foutmeldingen, mag deze httpd opstarten

```
chkconfig --level 35 httpd on
```



That's how IT looks. ;)

Hoofdstuk 14

SaMBa

14.1 SaMBa configureren

SaMBa configureren:

opm SELINUX

gebruik van useradd/groupadd scripts

setsebool -P samba_domain_controller on

gebruik van home directories

setsebool -P samba_enable_home_dirs on

(andere opties -> lees smb.conf)

aanpassen /etc/samba/smb.conf:

```
workgroup = BELBOB
```

```
server string = Samba Server Version %v
```

```
netbios name = MainServer    (-> inschakelen)
```

```
security = user
```

```
; passdb backend = tdbsam    (-> uitschakelen)
```

```
#-----LDAP_Conf-----
```

```
passdb backend = ldapsam:ldap://127.0.0.1/
```

```
ldap suffix = dc=belbob,dc=thuis
```

```
ldap user suffix = ou=Users
```

```
ldap group suffix = ou=Groups
```

```

ldap machine suffix = ou=Computers
ldap admin dn = "cn=Manager,dc=belbob,dc=thuis"

ldap delete dn = Yes
add user script = /usr/sbin/smbldap-useradd -m "%u"
add machine script = /usr/sbin/smbldap-useradd -w "%u"
add group script = /usr/sbin/smbldap-groupadd -p "%g"
add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
enable privileges = yes

delete user script = /usr/local/sbin/smbldap-userdel "%u"
delete group script = /usr/local/sbin/smbldap-groupdel "%g"

domain master = yes
domain logons = yes
preferred master = yes
wins support = yes

#-----

##### mogelijk is het niet nodig onderstaande bij te werken #####
# Un-comment the following and create the netlogon directory for Domain Logons
[netlogon]
    comment = Network Logon Service
    path = /home/%U
    guest ok = yes
    writable = no
    share modes = no
    valid users = %U

# Un-comment the following to provide a specific roving profile share
# the default is to use the user's home directory
[Profiles]
    path = /home/%U
    browseable = no
    guest ok = yes

Controleer smb.conf
testparm

Opstarten SaMBa:
    service smb start

```


na start zonder foutmeldingen, mag deze smb opstarten

```
chkconfig --level 35 smb on
```

14.2 SMLDAP-Tools installeren

SMLDAP-Tools installeren: (meer info [/smbldap-tools-versie/doc/html](http://smbldap-tools-versie/doc/html))

install RPMforge repository:

zie <http://dag.wieers.com/rpm/FAQ.php#B> voor de juiste rpm

```
wget wget http://apt.sw.be/packages/rpmforge-release/rpmforge-release-versie.rf.i386.rpm
```

```
rpm -ihv rpmforge-release-versie.rf.i386.rpm
```

```
yum install smbldap-tools
```

indien nodig - net getlocalsid

SID for domain LOCALHOST is: S-1-5-21-3661944173-1270763961-3613858768

bijwerken /etc/smbldap-tools/smbldap.conf:

```
SID="S-1-5-21-3661944173-1270763961-3613858768" (copy & paste)
sambaDomain="BELBOB"
masterLDAP="127.0.0.1"
ldapTLS="0"
suffix="dc=belbob,dc=thuis"
userSmbHome="//mainserver/%U"
userProfile="//mainserver/profiles%U"
mailDomain="belbob.thuis"
```

bijwerken /etc/smb-tools/smbldap_bind.conf:

```
masterDN="cn=Manager,dc=belbob,dc=thuis"
masterPw="secret" (-> wachtwoord in platte tekst)
```

Rechten bijwerken:

```
chmod 644 /etc/smbldap-tools/smbldap.conf
chmod 600 /etc/smbldap-tools/smbldap_bind.conf
```

Initialiseren OpenLdap directory

```
smbldap-populate
```

Ldap Admin password aanmaken:

```
smbpasswd -W
```

Root smbpasswd aanpassen
smbpasswd -a root

Herstarten SaMBa:
service smb restart

User management

add user: smbldap-useradd -a -G 512,544,1001 -m -d /home/robert -F "" -P robert
remove user: smbldap-userdel -r robert

opm:

initiele groep is 513 -> Domain Users (-g)
-a maken windows account (smb)
-G andere groepen (544 -> Administrators, 1001 -> vb. Docenten)
-m Aanmaken van Posix map
-d home dir
-F initiele profile dir
-P vragen naar wachtwoord

Hoofdstuk 15

Replica

15.1 Replica van LDAP maken

Replica van LDAP maken

Pas je DNS server aan zodat zowel master als slave opgezocht kunnen worden

zorg ervoor dat je /etc/resolv juist is ingesteld

Installeer een identieke ldapserver op de slave (zie boven)

maak op de master een volledige backup

```
slapcat -b "dc=belbob,dc=thuis" -l contents.ldif
```

kopieer contents.ldif van master naar slave

voeg deze backup toe aan de slave ldap

```
ldapadd -a -W -x -D "cn=Manager,dc=belbob,dc=thuis" -f contents.ldif
```

Toevoegen in master slapd.conf file:

```
vi /etc/openldap/slapd.conf
```

```
repllogfile /var/lib/ldap/slapd.repllog
```

```
access to *
```

```
by * read
```

```
replica      host=replica.belbob.thuis:389
             suffix="dc=belbob,dc=thuis"
             binddn="cn=Manager,dc=belbob,dc=thuis"
             credentials=jtl141
             bindmethod=simple
             tls=yes
```

Toevoegen in slave slapd.conf file

```
vi /etc/openldap/slapd.conf
```

```
access to *
by * read
```

```
updatedn "cn=manager,dc=belbob,dc=thuis"
updateref ldap://mainserver.belbob.thuis
```



That's it. We're done. :)

Bibliografie

- [1] <http://nl.wikipedia.org/wiki/Processor>
- [2] Stephen J. Bigelow: Bigelow's PC Hardware Desk Reference (2003), McGraw-Hill/Osborne, 2600 Tenth Street, Californie 94710 (USA). 1552p.