LDAP

D. Leeuw

15 januari 2024
v.0.4.0

Over dit Document

0.1 Leerdoelen

In dit document wordt de basis van LDAP uitgelegd en wordt beschreven waarom LDAP handig is.

0.2 Voorkennis

Voor een goed begrip van dit document dient de lezer de volgende voorkennis te hebben:

- Kennis van hoe een besturingssysteem omgaat met gebruikers en groepen
- Kennis van de manier waarop een bestandssystemen bestanden opslaat en hoe en welke meta-data wordt opgeslagen
- Kennis van TCP/IP

Inhoudsopgave

Over dit Document **i**
0.1 Leerdoelen i
0.2 Voorkennis i

1 Inleiding **1**

2 Directory Information Tree **3**

3 LDIF **5**

Index **7**

Hoofdstuk 1

Inleiding

Bestandssystemen gebruiken nummers om bestanden te koppelen aan gebruikers. Bij een bestand wordt de User-ID en de Group-ID opgeslagen om te bepalen welke gebruikers en groepen toegang hebben tot een bestand. Als we een bestandssysteem willen delen over het netwerk om data met elkaar te kunnen delen dan moeten alle systemen die bij de gedeelde data kunnen weten welke UID of GID bij welke gebruikers en groepen horen. We kunnen natuurlijk proberen om dat op elk systeem handmatig op orde te maken, maar het zou makkelijker zijn als we een centrale database hebben waar elke machine aan kan vragen wat er bij een UID of GID hoort.

Een mogelijke centrale netwerk oplossing die heel veel gebruikt wordt is LDAP. De afkorting LDAP staat voor Lightweight Directory Access Protocol. Het Lightweight deel staat voor het feit dat het een uitgeklede versie is van het ITU X.500 protocol. X.500, afkomstig uit de telefoniewereld, kent het DAP (Directory Access Protocol) om data uit het systeem te halen. DAP is heel uitgebreid en dus arbeidsintensief, vandaar dat er voor gebruik over TCP/IP netwerken een lichter alternatief werd bedacht: LDAP.

LDAP is een netwerk protocol dat beschrijft hoe data aangeboden moet worden aan het LDAP systeem. De data die uit het systeem verkregen worden of erin gestopt worden zijn in het LDIF formaat.

Hoofdstuk 2

Directory Information Tree

LDAP is een database met informatie over een gebruiker, zoals de gebruikersnaam, de groepen waarvan de gebruiker lid is en de User ID, maar ook gegevens als telefoonnummers, e-mail adressen en andere gegevens van een gebruiker kunnen worden opgenomen in LDAP. We kunnen LDAP dan ook vergelijken met een adresboek (telefoonboek). In LDAP kan ook data worden opgeslagen over computers en groepen. Kortom LDAP is eigenlijk een manier om data gestructureerd op te slaan. De structuur is vergelijkbaar met een bestandssysteem, een hiërarchische manier, met mappen en submappen waarin data staat. Vandaar de naam Directory in LDAP.

Een "map" in LDAP zou een gebruiker kunnen zijn waaronder de gegevens van de gebruiker worden opgeslagen. Een map kan ook een bedrijf zijn met daarin de bedrijfsgegevens, zoals adressen, met daaronder mappen voor werknemers met daarin de gebruikersgegevens en contactgevens van deze medewerkers. Een LDAP-tree kan dus op verschillende manieren gestructureerd zijn. Via zoekopdrachten kan er in deze databoom gezocht worden. Binnen LDAP heten de mappen objecten. Een object kan andere objecten bevatten.

LDAP is een hiërarchische tree van opgeslagen data. Via zogenaamde schema bestanden wordt bepaald wat er in een object in de boom opgeslagen kan, mag of moet worden. Een schema bestand zegt dus wat bij bijvoorbeeld een user object er aan data aanwezig moet zijn en welke data er ook aanwezig mag zijn. De gebruikersnaam is verplicht, net als een UID, een telefoonnummer is niet verplicht. Dit geldt voor een LDAP systeem dat is ingericht met schema bestanden voor gebruik als gebruikersdatabase.

Omdat elke organisatie zijn eigen LDAP-tree kan hebben met zijn eigen gebruikers (zijn eigen interne adresboek) en LDAP systemen theoretisch wereldwijd te koppelen zijn is het handig om de basis van de tree (de root) aan te laten sluiten bij wereldwijd unieke naam van de organisatie. De keuze binnen de meeste organisaties is gevallen op het aansluiten bij het DNS systeem,

daar dit het enige systeem is dat een unieke naam heeft voor een organisatie namelijk zijn domeinnaam. Er kan wereldwijd maar één microsoft.com zijn.

LDAP werk niet met domeinnamen, maar met objecten. Waarbij het eerst genoemde object de root. Zo zou de basis van de LDAP tree voor Microsoft DC=microsoft,DC=com kunnen zijn. DC staat voor Domain Component en verwijst naar het feit dat deze LDAP tree is opgebouwd volgens het DNS systeem. In de notatie valt op dat het aansluit op de DNS structuur met een beschrijving van elk object in de tree. Zo zouden we onze gebruikers kunnen stoppen in een organisatorische eenheid ofwel een Organizational Unit. Laten we daarvoor de LDAP eenheid nemen: OU=users, DC=microsoft,DC=com. Daaronder kunnen we onze gebruikers stoppen CN=bgates,OU=users,DC=microsoft,DC=com. CN staat hierbij voor Common Name. Sommige organisaties gebruiken voor de Common Name de loginnaam, andere gebruiken de volledige naam van de gebruiker of het nummer van werknemer. Het is belangrijk dat de naam van elk object binnen een tak (branch) van de boom uniek is. Er kan dus niet nog een CN=bgates voorkomen binnen OU=users,DC=microsoft,DC=com. Een object in de boom die andere objecten kan bevatten worden ook wel Containers genoemd, in de Windows wereld wordt met Container vaak een Common Name object bedoeld.

Het "pad" CN=bgates,OU=users,DC=microsoft,DC=com is een unieke entry van een object in LDAP. Dit noemen we de Distinguished Name. De Distinguished Name is het volledige pad naar een object in de tree.

De volledige LDAP data boom van een organisatie noemen we een DIT (Directory Information Tree). Een DIT bevat zoals gezegt objecten en objecten hebben Attributes. Een attribute kan bijvoorbeeld het telefoonnummer zijn.

Hoofdstuk 3

LDIF

Index

Attribute, 4

CN, 4
Common Name, 4
Container, 4

DC, 4
Directory, 3
Directory Information Tree, 4
Distinguished Name, 4
DIT, 4

Domain Component, 4

LDAP, 1, 3
    Directory, 3
Lightweight Directory Access
        Protocol, 1

Object, 3, 4
Organizational Unit, 4
OU, 4