Antero Istolainen

Active Directoryn ja eDirectoryn yhteiskäyttö Mikkelin ammattikorkeakoulussa

Opinnäytetyö
Sähköisen asioinnin ja arkistoinnin koulutusohjelma

Joulukuu 2010

KUVAILULEHTI

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Opinnäytetyön päivämäärä** **27.11.2010**
Tekijä(t) Antero Istolainen	**Koulutusohjelma ja suuntautuminen** **Sähköisen asioinnin ja arkistoinnin ko.**

Nimeke
Active Directoryn ja eDirectoryn yhteiskäyttö Mikkelin ammattikorkeakoulussa

Tiivistelmä

Microsoft Active Directory on vakauttanut asemansa työasemaverkkojen autentikointilähteenä ja tämä asettaa myös Mikkelin ammattikorkeakoululle vaatimuksia toteutustapojen suhteen. Monet keskitetyn hallinnan työvälineet sekä virtualisointituotteet tukeutuvat Active Directoryyn. Ongelmana on vain se, kuinka tieto integroituu eri järjestelmien välillä. Tästä syystä käynnistin projektin, jossa oli tarkoitus tutkia mahdollisuuksia, joiden avulla Mikkelin ammattikorkeakoulu voisi hyödyntää niin eDirectoryn tehokkuutta hakemistopalveluna kuin Active Directoryn joustavuutta autentikointilähteenä.

Projektin ensimmäinen vaihe oli tutustua tarkemmin Mikkelin ammattikorkeakoululla oleviin järjestelmiin ja erityisesti ottaa huomioon migraatioon liittyvät näkökulmat. Tutkimuksessa selvisi, että suurin osa palveluista oli toteutettu Novell eDirectoryyn sidoksissa olevilla järjestelmillä. Tämä oli monessa suhteessa haaste ja on edelleen. Kartoituksessa kävin läpi myös jo olemassa olevat integraatiot Active Directoryn ja eDirectoryn välillä. Tämä helpotti testiympäristön rakentamista, koska ei tarvinnut miettiä mitä työkaluja käyttää.

Rakensin testiympäristöön toimivan eDirectoryn ja Active Directoryn. eDirectory-palvelimia oli kaksi, joilla kummallakin oli oma roolinsa. Toinen palvelimista hoiti identiteetinhallinnan (Novell IDM) eDirectoryn ja Active Directoryn välillä ja toinen palvelin emuloi Active Directorya Domain Services for Windows –palvelulla.

Testaukset antoivat erinomaista tietoa järjestelmien integroimisesta. Tutkimus oli kannattavaa siinä mielessä, että se antoi selkeän näkökulman siihen, miten Mikkelin ammattikorkeakoulun tietojärjestelmäpalveluita tulisi kehittää. Active Directory integroituu Windows-työasemiin parhaiten ja eDirectory on käyttäjätietojen metahakemistona paras vaihtoehto. Vielä tässä vaiheessa on vaikea sanoa, mihin ratkaisuun Mikkelin ammattikorkeakoululla päädytään, mutta uskoisin näistä tiedoista olevan hyötyä tulevaisuuden suunnitelmille.

Asiasanat (avainsanat)
Atk-järjestelmät, emulointi, järjestelmänhallinta, käyttäjätunnukset, Linux, Windows

Sivumäärä	**Kieli**	**URN**
58	Suomi	

Huomautus (huomautukset liitteistä)

Liite 1, NDS:n/eDirectoryn versiokehitys

Ohjaavan opettajan nimi	**Opinnäytetyön toimeksiantaja**
Jukka Selin	Mikkelin ammattikorkeakoulu

DESCRIPTION

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Date of the master's thesis** 27 November 2010
Author(s) Antero Istolainen	**Degree programme and option** eServices and Digital Archiving

Name of the master's thesis

Active Directory and eDirectory integration in Mikkeli University of Applied Sciences

Abstract

Active Directory has become a standard considering client authentication. Therefore Mikkeli University of Applied Sciences should consider how to develop their authentication methods on the client side. That is the reason why I started this study. My aim was to think about means for integrating Active Directory's possibilities on the client side authentication and eDirectory's strength in directory services.

I started the process by gathering a lot of information about the background systems in Mikkeli University of Applied Sciences by paying special attention to migration. Study revealed that most of the main systems rely on eDirectory presenting one big challenge in migration process. I also studied our present directory integration and sorted out what tools were used. That helped me in building up the test environment.

The test environment had an Active Directory network and eDirectory network based on two separate servers. One of the servers had basic eDirectory installation and Novell IDM identity management tools. The other had with eDirectory an Active Directory emulation system called Domain Services for Windows. The workstation that I used for the tests had a Windows XP installed and connections to both Active Directory and eDirectory.

This work gave excellent information about different directory services and explained how to integrate them. This study gave me a lot of information for developing IT services in Mikkeli University of Applied Sciences. What I observed was that Active Directory was the best way to integrate clients to a directory service. eDirectory, in turn, provided excellent directory service for users' metadirectory integrated for instance to a HR system. It is hard to say what are the decisions Mikkeli University of Applied Sciences is going to make, but this study gives good guidelines for choosing suitable products and services.

Subject headings, (keywords)

ADP systems, emulation, system management, user accounts, Linux, Windows

Pages	**Language**	**URN**
58	Finnish	

Remarks, notes on appendices

Appendice 1, NDS/eDirectory version history chart

Tutor	**Master´s thesis assigned by**
Jukka Selin	Mikkeli University of Applied Sciences

SISÄLTÖ

1 JOHDANTO 1

2 TAUSTATIETOJA JÄRJESTELMISTÄ 2

2.1 Microsoft Active Directory 2

2.2 Novell eDirectory 4

2.3 Novell IDM -identiteetinhallintajärjestelmä 6

2.4 LDAP-protokolla 7

2.5 Mikä hakemistopalvelu? 9

2.6 Taustatietoja MAMKin järjestelmistä 13

3 HAKEMISTOPALVELUIHIN KOHDISTUVAT VAATIMUKSET 15

4 TESTIYMPÄRISTÖN ESITTELY 20

4.1 Virtuaalijärjestelmän esittely 20

4.2 Virtuaalikoneiden esittely 21

4.2.1 eDirectory-palvelinympäristö 21

4.2.2 Active Directory -palvelinympäristö 23

4.2.3 Windows XP -testityöasema 24

5 EDIRECTORYN JA ACTIVE DIRECTORYN YHTEISKÄYTTÖ 25

5.1 eDirectoryn määritykset 25

5.2 Active Directoryn määritykset 34

5.3 Identiteetinhallinnan määritykset 35

5.4 Windows XP –työaseman toiminta 40

5.5 Arvio kokonaisuudesta 41

6 DEDIKOITU ACTIVE DIRECTORY -YMPÄRISTÖ 42

6.1 Novell-verkon palveluiden kartoitus 43

6.1.1 Hakemistopalvelu ja levypalvelut 43

6.1.2 Muut tarjottavat palvelut 44

6.2 Miten toteutin? 45

6.3 Yhteenveto puhtaan Active Directory -ympäristön käytöstä 46

7 EDIRECTORYN KÄYTTÖ ACTIVE DIRECTORYNA 46

7.1 Vaadittavat komponentit 47

7.2 DNS-nimipalvelun määritykset 48

7.3 Open Enterprise Serveriin tehtävät määritykset 49

7.4 Työaseman määritykset ja käyttäytyminen 51
7.5 Arvio kokonaisuudesta 52
8 LOPPUPÄÄTELMÄT 53
9 SANASTO 56
LÄHTEET 57
LIITTEET

1 JOHDANTO

Syksyllä 2010 Mikkelin ammattikorkeakoulu käynnisti prosessin, jonka tarkoituksena oli tuottaa opiskelukäyttöön erilaisia virtualisointiratkaisuja. Vahvimpana vaihtoehtona tuolloin oli VMware View -työpöytävirtualisointijärjestelmä. Tämä vaihtoehto osoittautui kuitenkin ongelmalliseksi, koska VMware View oli voimakkaasti Microsoft Active Directory -sidonnainen. Tämä johti siihen, että virtualisointituote piti vaihtaa sellaiseksi, joka tukisi paremmin standardeja eikä niinkään tiettyä tuotetta. Lopputuloksena oli Oracle Sunin VDI (Virtual Desktop Infrastructure) -järjestelmä, jonka käyttö soveltui myös Mikkelin ammattikorkeakoulun eDirectory-ympäristöön. Mikä merkitys edellä mainitulla huomiolla sitten oli hakemistopalveluintegraatiota silmällä pitäen? Yksinkertaisesti se, että pitäisi löytää konsti erilaisten hakemistopalveluiden yhteiskäytölle.

Microsoft on tunnetusti hallinnut Windows-ympäristöjen hakemistopalveluita Active Directoryllaan. Active Directory ja sen olemassaolo on kuitenkin vain pieni osa niistä mahdollisuuksista, joita taustajärjestelmissä voidaan erilaisilla hakemistopalveluratkaisuilla tehdä. Jokaisella korkeakoululla on käytössä jonkinlainen hakemistoratkaisu ja monet käyttävät Novell eDirectorya käyttäjätietojen säilytykseen. eDirectory on suorituskykyinen hakemistopalvelu, joka pystyy hoitamaan suurenkin käyttäjätietokannan ilman ongelmia. Suurimpana ongelmana eDirectoryssa pidänkin sen huonoa integroitumista Windows-ympäristöön. Tässä suhteessa Active Directory on vetänyt pidemmän korren. Tämä tosin johtuu siitä, että Windows on käyttöjärjestelmänä koodattu siten, että sen Professional ja Enterprise -tuotteet tukevat suoraan Active Directorya.

Novell on tajunnut tilanteen ja alkanut kehitellä tuotteita, joilla voidaan jäljitellä Active Directorya. Tässä opinnäytetyössä tutkin sitä, miten tätä toiminnallisuutta voitaisiin hyödyntää myös Mikkelin ammattikorkeakoulussa (MAMK). Faktaa on, että Active Directory on jo oleellinen osa MAMKin verkkoa ja sen palveluita vaaditaan entistä useammassa verkon palvelussa. Tutkimuksen kohteena on se, miten käyttäjätieto liikkuu eri hakemistopalveluiden välillä ja miten hyvin Novellin Domain Services for Windows soveltuu Active Directoryn korvaajaksi.

2 TAUSTATIETOJA JÄRJESTELMISTÄ

Tässä luvussa kerron hiukan tarkemmin työssä esille tulevista järjestelmistä. Hakemistopalveluita löytyy monelta eri valmistajalta, kuten myös identiteetinhallintatyökaluja. Olen valinnut tutkimuksen kohteeksi Microsoft Active Directoryn sekä Novellin tuotteet eDirectory ja IDM.

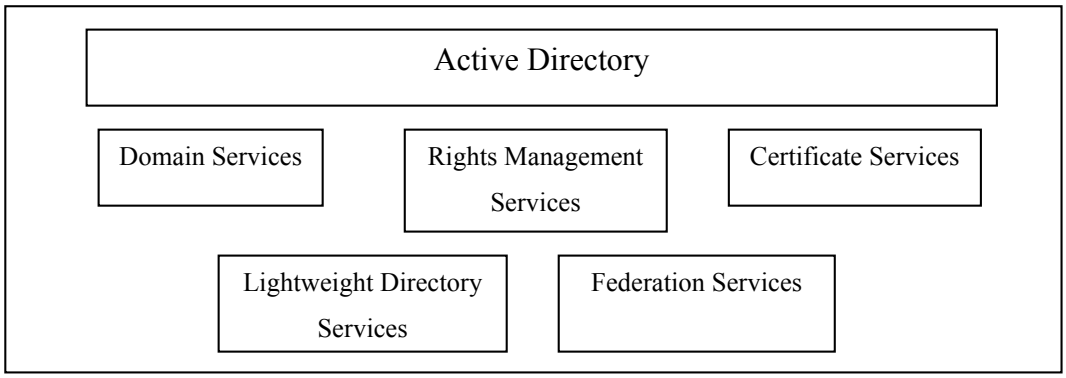
2.1 Microsoft Active Directory

Active Directory on Microsoftin luoma hakemistopalvelu, joka julkaistiin ensimmäisen kerran Windows 2000 Serverissä. Tätä ennen on puhuttu Windows NT -toimialueesta, joka pohjautuu alun perin IBM OS/2 -järjestelmästä tuttuun LAN Manager -verkkojärjestelmään (Kivimäki 2003, 6). Microsoftin mukaan Active Directory on ”aikaisempien Windows-hakemistopalvelujen parannettu versio”.

Active Directory on nimensä mukaisesti palvelu, joka tallettaa kaikki tarvittavat tiedot yhteen hakemistoon. Tieto tallentuu hakemistopalveluun strukturoituna ja muodostaa loogisen kokonaisuuden, mikä mahdollistaa helpon tavan hallita järjestelmää (Honeycutt 2003, 37 – 38.) Active Directory on siinä mielessä kätevä hakemistopalvelu, että se on jo valmiiksi kiinteä osa Windows XP Professional, Windows 7 Business, Windows 7 Professional- ja Windows 7 Enterprise -käyttöjärjestelmiä. Tämä mahdollistaa sen, että erillisiä kolmannen osapuolen sovelluksia ei tarvita hakemistopalveluun liityttäessä.

Monet sovelluskehittäjät ja itsenäiset sovellustoimittajat ovat mieltyneet Active Directoryyn autentikointilähteenä ja tästä syystä mielellään ohjelmoivat nimenomaan Active Directory –yhteensopivia sovelluksia (Honeycutt 2003, 37). Tätä voi ajatella myös tuottavuuden kannalta parhaana ratkaisuna, koska Microsoftin tuotteet ovat laajalle levinneet ja valtaosa organisaatioista hyödyntää nimenomaan Active Directorya hakemistopalveluna. Active Directory toimii monen sovelluksen ja järjestelmän autentikointilähteenä. Näitä järjestelmiä ovat monet virtualisointijärjestelmät (muun muassa VMware View ja Citrix Xen Desktop).

Mielestäni Steve Clines ja Marcia Loughry kuvaavat kirjassaan (2008, 8) hyvin Active Directorya. Yksinkertaisuudessaan Active Directory on kuin sateenvarjo, joka suojaa alleen joitakin oleellisia komponentteja.

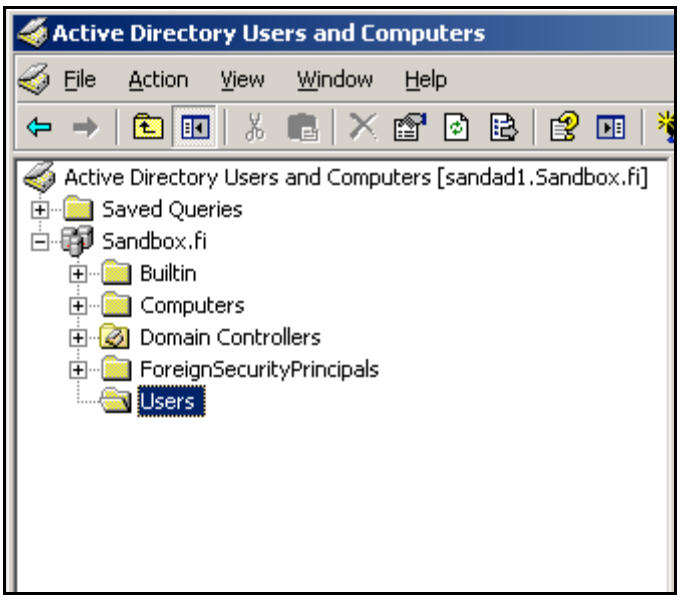


KUVA 1. Active Directoryn palvelut

Kuten kuva 1 kertookin, Active Directory pitää sisällään erilaisia palveluita ja ne on helpoin kuvata nimenomaan ”sateenvarjomaisesti” yhden kokonaisuuden alle.

- Domain Services, eli itse toimialueen palvelut. Yleisimmin käytetty komponentti Active Directoryssa.
- Lightweight Directory Services on uusi komponentti, joka on tullut Windows 2008 Serverin mukana. Aiemmin vastaava komponentti oli Active Directory Application Mode (ADAM), joka mahdollisti kevennetyn version hakemistopalvelusta. ADAM on mahdollista asentaa Windows 2003 Serverille ja Windows XP Professional –työasemille.
- Federation Services mahdollistaa erilaisia kertakirjautumistoimintoja (Single Sign-On). Tämä oli Windows Server 2003 R2:ssa lisäosa, mutta Windows 2008 Serverissä se on jo kiinteä osa kokonaisuutta.
- Certificate Services tuo Active Directoryyn varmenteet, joita voidaan hyödyntää muun muassa toimikorttikirjautumisessa. Kuten edelläkin, Certificate Services kuuluu osana Windows 2008 Serveriä.
- Rights Management Services nimensä mukaisesti hallinnoi käyttäjien tietoja siten, että dataa ei voida välittää sellaisille tahoille joilla ei ole siihen oikeutta.

Palvelut ovat siis jonkin verran muuttuneet Active Directoryn versioiden myötä, mutta perustoiminnallisuus on pysynyt samana. Yleisimmin käytetty osio on ehdottomasti Domain Services, koska se nimenomaan määrittelee sen, miten käyttäjätietoja käsitellään loppukäyttäjän työasemalla. Active Directory on tietovarasto, jossa on mahdollista säilöä erinäisiä määriä erilaisiin käyttötarkoituksiin soveltuvia objekteja.



KUVA 2. Näkymä Active Directoryn hallintaliittymästä

Kuvassa 2 on esitetty tyypillinen Active Directory –kokoonpano. Perusasettelussa ei paljoa muuta tarvita kuin oletusasetukset. Edellisestä kuvasta voimme todeta, että Active Directory on rakenteeltaan varsin yksinkertainen.

Active Directory –toimialueiden suunnittelusta ja toteuttamisesta on tehty paljon oppaita. Syy tähän lienee se, että Active Directoryn suosio hakemistopalveluna on säilynyt vakaana, mahdollisesti jonkin verran kasvanutkin. Active Directoryn käyttöönotto on yksinkertaista, kuten myöhemmin tässä opinnäytetyössä asiasta kerronkin.

2.2 Novell eDirectory

Novell toi ensimmäisen verkkokäyttöön suunnitellun käyttöjärjestelmän jo vuonna 1983. Novell NetWaresta tuli tuolloin hyvin suosittu verkkokäyttöjärjestelmä (Dean 2005, 452). Myöhemmin Novell toi NetWarelle myös TCP/IP-tuen, NetWaren käyttämän IPX/SPX-protokollan lisäksi. NetWaren rooli verkkokäyttöjärjestelmänä oli nimenomaan tiedosto- ja kirjoitinpalvelimena, myöhemmin mukaan tulivat erilaiset Web-palvelut kuten FTP-palvelin ja itse Web-palvelin. eDirectory tuli NetWareen versiossa 6.5 korvaten entisen Novell Directory Services:n (NDS.)

Novellin hakemistopalvelu on aikaisemmin tunnettu nimellä NDS ja ensimmäiset versiot siitä ovat olleet käytössä jo 90-luvun alussa. Novell NDS on ollut kiinteä osa Novell NetWare -verkkokäyttöjärjestelmää, joka on edelleenkin erittäin suorituskykyinen

palvelinratkaisu hakemistopalveluita tarjottaessa. Liitteenä 1 on kaaviokuva eDirectoryn eri versioiden kehitysvaiheista. Liitteestä käy ilmi se, että vuosien myötä NetWaren rinnalle on tullut useita palvelinkäyttöjärjestelmäratkaisuja, jopa hiukan harvinaisempiakin, kuten HP-UX tai IBM AIX.

KUVA 3. eDirectoryn perusnäkymä iManagerissa

Kuten voimme huomata, Novell eDirectoryssa on paljon samankaltaisuutta verrattuna Active Directoryn hakemistopalvelun hallintanäkymään. Kumpikin, niin Active Directory kuin eDirectorykin, noudattaa samankaltaista hierarkiaa, jossa hakemistopuu koostuu organisaatioista, organisaatioyksiköistä ja niiden alla olevista lehtiobjekteista.

eDirectoryn asennusvaiheessa on mahdollista vaikuttaa siihen, mitä edellä olevassa kuvassa näkyy. Esimerkiksi pääkäyttäjätunnuksen nimi on mahdollista määrittää sellaiseksi kuin haluaa ja sen sijainti on valittavissa. Lisäksi itse palvelinobjektin sijainti on määriteltävissä sellaiseksi kuin haluaa.

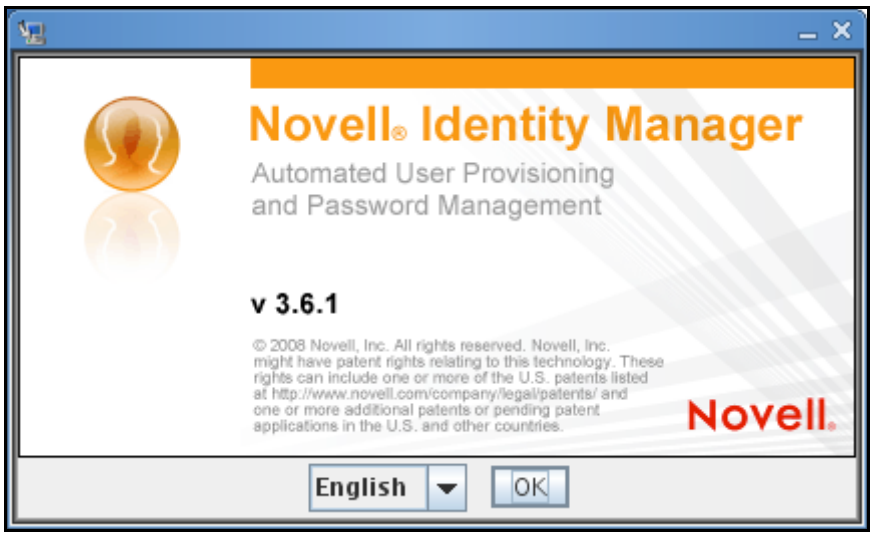
Kuvassa 3 on näkymä iManagerista, joka on keskeisin työkalu eDirectoryn hallinnassa. iManager ei vaadi mitään lisäosia selaimeen, mutta sillä pystyy hoitamaan kaikki eDirectoryyn kohdistuvat muutokset. iManagerin lisäksi on olemassa Java-pohjainen työasemasovellus nimeltään ConsoleOne. Tämä työkalu on myös laajassa käytössä eDirectoryn hallinnassa ja erityisesti vanhan Novell ZENworks Desktop Management –järjestelmän ja GroupWise-järjestelmän hallinnassa. Tulen testiympäristössä käyttämään pääsääntöisesti nimenomaan iManageria, koska siihen on keskitetty kaikki tarvittavat hallintatyökalut.

Jotta työasemat voisivat hyödyntää eDirectorya, täytyy niissä olla asennettuna Novell Client. Tämä asiakassovellus mahdollistaa työasemien ja eDirectoryn välisen kommunikaation. Ongelmana tässä on se, että työasemiin täytyy erikseen määritellä hakemistopalvelun nimi sekä erinäinen määrä palvelinmäärityksiä.

eDirectory toimii monissa organisaatiossa (erityisesti oppilaitoksissa) käyttäjäidentiteettien välitysjärjestelmänä. Tämä johtuu siitä, että Novell on onnistunut luomaan hyvän ja toimivan tavan synkronoida identiteettejä järjestelmistä toiseen. Tästä hiukan tarkemmin seuraavassa luvussa.

2.3 Novell IDM -identiteetinhallintajärjestelmä

Novell on luonut tuotteen, jolla voidaan yhdistää erilaisia palveluita keskenään hyödyntämällä standardeja attribuutteja. Tietoa voidaan siirtää esimerkiksi ActiveDirectoryn ja eDirectoryn välillä. Novell IDM, joka on kehitetty Novell DirXML -tuotteesta, on monipuolinen tuote, jota myös MAMK käyttää identiteetinhallintaan.



KUVA 4. Novell Identity Manager

Kuten kuva 4 kertookin, kyseessä on tuote, joka ylläpitää käyttäjätietoja ja hallinnoi salasanoja. Testiympäristössä käyttämäni versio on 3.6.1, mutta markkinoilla on jo versio 4.

Novellin IDM on luonnollinen valinta identiteetinhallintajärjestelmäksi, koska se istuu varsin mutkattomasti osaksi Novell eDirectorya. Muitakin mahdollisia vaihtoehtoja

(Sun/Oracle) on olemassa, mutta Novell IDM:ään ollaan MAMKissa niin tyytyväisiä, ettei sen vaihtamiseen ole nähty tarvetta.

Puhuttaessa identiteetinhallintajärjestelmien käyttöönotosta, tulee väistämättä esille myös kustannustehokkuus. Monessa dokumentissa on maininta siitä, miten järjestelmän käyttöönotto vaikuttaa organisaation kulurakenteisiin, kun ei ylläpitohenkilöstön tarvitse panostaa enää niin paljoa käyttäjätunnusten kanssa työskentelyyn. Näin ollen käytettävissä oleva aika kohdentuu muihin, tärkeämpiin toimiin.

International Data Corporation:n (IDC) tekemässä tutkimuksessa oli haastateltu Pohjois-Amerikkalaisia ja Eurooppalaisia organisaatioita joilla on Novellin Identity and Access Management (IAM) –tuotteita käytössä. Tarkoituksena oli selvittää IAM-järjestelmien vaikutusta ylläpitohenkilöstön toimintaan. Dokumentin mukaan taloudelliset syyt eivät ole ainoa asia mihin halutaan muutosta. Myös tietoturvaan ja yhteensopivuustekijöihin halutaan panostaa. Lopputulos oli se, että identiteetinhallintajärjestelmä toi vuosittaisia säästöjä yli 18 000 dollaria sataa käyttäjää kohden (Hudson & Hatcher 2010, 1 – 3.)

Identiteetinhallinnan hyödyntäminen MAMKissa laajenee jatkuvasti ja seuraavana on tarkoitus siirtää hallinnon tunnusten käsittely identiteetinhallinnan piiriin. Tällä hetkellä haasteena on se, että käyttäjätunnuksien voimassaoloajat vaihtelevat melkoisesti ja niiden hallinta on vaikeata. Tästä syystä informaation olisi hyvä tulla jostain sellaisesta järjestelmästä, jossa tieto on autenttinen. Tällainen järjestelmä pääsääntöisesti on jonkinlainen henkilöstönhallintajärjestelmä. Opiskelijoiden käyttäjätunnukset siirtyvät automaattisesti opiskelijahallintajärjestelmästä ja se on helpottanut ylläpitohenkilöstön manuaalista työskentelyä huomattavasti.

2.4 LDAP-protokolla

Tekstissä mainitaan useasti LDAP. LDAPissa kyse on standardista, jonka avulla mahdollistetaan hakemistopalvelun monipuolinen hyödyntäminen (IBM Redbooks 2004, 3). Microsoft käyttää vastaavaa tuotetta, joka on ADSI (Active Directory Service Interface). Loppujen lopuksi kyseessä on rajapinta, jolla mahdollistetaan esimerkiksi web-sovelluksen käyttäjäautentikointi hakemistopalveluun, oli toteutusrajapintana sitten ADSI tai LDAP. LDAP on kuitenkin varsin laajasti käytössä oleva protokolla ja

sen käyttötarkoitukset vaihtelevat identiteetinhallinnan työkaluista yksinkertaisiin hakemistopalvelua hyödyntäviin web-sovelluksiin. MAMK hyödyntää varsin laajasti LDAPia. MAMKilla on käytössä muutamia järjestelmiä, jotka tukeutuvat LDAP-standardin mahdollisuuksiin.

LDAP on eräänlainen kieli, jota palvelimet ja asiakasohjelmat käyttävät keskinäiseen kommunikointiinsa. LDAPissa on monia merkittäviä etuja, kuten esimerkiksi keveys ja varmuus siitä, että LDAPia hyödyntävät sovellukset ovat aina yhteensopivia LDAP-standardin mukaisissa palvelimissa. LDAP on huomattavasti kevyempi verrattuna edeltäjäänsä, X.500 DAP protokollaan. DAPin ongelma oli siinä, että se oli koodattu melko monimutkaisesti. Toisekseen, DAP hyödynsi suoraan OSI-mallin verkkokerrosta, joka monissa tapauksissa tarkoitti lisäkustannuksia organisaation hakemistopalveluratkaisuissa. Edellä mainitut syyt vaikuttivat siihen, miksi DAPista ei koskaan tullut yhtä suosittua kuin mitä LDAP on. (Howes ym. 1999, 67.)

```
<?xml version="1.0" encoding="UTF-8"?><policy>
        <rule>
                <description>Break if not a User</description>
                <conditions>
                        <or>
                                <if-class-name mode="nocase" op="not-equal">User</if-class-name>
                                <if-class-name op="not-equal">Group</if-class-name>
                        </or>
                </conditions>
                <actions>
                        <do-break/>
                </actions>
        </rule>
        <rule>
                <description>Veto if nspmDistributionPassword is not available</description>
                <conditions>
                        <and/>
                </conditions>
                <actions>
                        <do-veto-if-op-attr-not-available name="nspmDistributionPassword"/>
                </actions>
        </rule>
```

KUVA 5. XML-koodia LDAP-tunnuksen käsittelyyn

Kuvassa 5 on esimerkki XML-koodista, jolla voidaan ohjata LDAP-yhteensopivaa hakemistopalvelua. Koodiesimerkki on Novell IDM –järjestelmän ajurista, joka siirtää käyttäjätietoja eDirectoryn ja Active Directoryn välillä.

LDAPin hyödyntäminen ei ole pelkästään kaupallisten tuotteiden varassa. Moniin Linux-versioihin on saatavissa OpenLDAP-tuotetta, joka mahdollistaa LDAP-hakemistopalvelun rakentamisen ilmaisilla tuotteilla. Tämä saattaa olla monelle yritykselle erinomainen vaihtoehto, mikäli käytössä on useampi autentikointia vaativa web-sovellus.

2.5 Mikä hakemistopalvelu?

Kun mietitään vaihtoehtoja hakemistopalveluille, nousevat useimmin vaihtoehdoiksi juuri nämä edellä mainitut. Mutta kumpi näistä sitten on parempi? Sitä on vaikea sanoa, mutta paremmuuden määrää useimmiten käyttötarkoitus. Hakemistopalveluista on tehty vertailuja ja useimmiten niitä ovat tehneet sellaiset tahot, jotka itse toimittavat hakemistopalvelua. Tällaisiin tutkimuksiin ja vertailuihin on suhtauduttava tietyllä varauksella, koska tulos ei välttämättä ole objektiivinen.

Mitä vaatimuksia hakemistopalvelulle on sitten asetettava? Novellin tekemän dokumentin (2004) mukaan huomioon otettavia seikkoja ovat skaalautuvuus, yhteensopivuus, luotettavuus, hallittavuus ja turvallisuus.

- skaalautuvuus
  Tämä tarkoittaa sitä, miten hyvin hakemistopalvelu täyttää sille asetetut vaatimukset koon suhteen ja kuinka hyvin se skaalautuu tulevaisuuden vaatimuksiin, kuten siihen, että palvelu voisi kasvaa merkittävästi.
- yhteensopivuus
  Kuinka hyvin hakemistopalvelu sopii yhteen muiden organisaation käyttämien sovellusten kanssa. Ei kannata hankkia sellaista hakemistopalvelua, joka ei järkevästi integroidu muiden järjestelmien kanssa.
- luotettavuus
  Miten hyvin voidaan taata järjestelmän toimivuus ja kuinka hyvin hakemistopalvelu elpyy virhetilanteista.
- hallittavuus
  Hakemistopalvelun hallinta on yksi haasteellisin osa-alue, jota voidaan joko helpottaa tai vaikeuttaa hallintatyökaluilla. Hallittavuus osa-alueena tarkoittaa lähinnä sitä, miten eri työkalut soveltuvat ja integroituvat muiden järjestelmien hallintatyökaluihin.
- turvallisuus
  Määrittää sen, kuinka voidaan turvallisesti luoda käyttäjille identiteetti, mutta samalla ehkäistä erilaisten palvelunestohyökkäysten yms. muiden haittaohjelmien hyökkäykset hakemistopalveluun.

Käytännön tasolla tämä tarkoittaa sitä, että täytyy tarkkaan miettiä, mihin hakemistopalvelua käyttää ja pyrkiä integroimaan se olemassa oleviin järjestelmiin. On myös syytä miettiä jonkin verran tulevaisuutta ja arvioida liiketoiminnan kehityksen suuntaa. Edellä listatut seikat on hyvä pitää mielessä, jotta kokonaisuus olisi mahdollisimman toimiva. Isoissa organisaatioissa ei ole mitenkään epätavallista, että käytössä on kaksikin eri hakemistopalvelua, jotka integroituvat keskenään erilaisilla identiteetinhallintavälineillä. Kyse on siitä, miten tietoa halutaan säilöä ja kuinka informaatio siirtyy järjestelmistä toiseen. Otetaan käsittelyyn nämä yleisimmin käytössä olevat hakemistopalvelut, Novell eDirectory ja Microsoft Active Directory.

TAULUKKO 1. Active Directoryn ja eDirectoryn vertailu

	Active Directory (2003)	**eDirectory**
Skaalautuvuus	- pienet ympäristöt (alle 10 miljoonaa objektia) - suurissa ympäristöissä tietokanta paisuu → vie enemmän laitteistoresursseja	- myös suuret ympäristöt (vuonna 1999 testattu miljardin objektin tietokanta) - kohtuullinen tietokannan koko → vaatimattomammat laitevaatimukset
Yhteensopivuus	- ei LDAP-sertifioitu - DSML-tuki (Directory Services Markup Language) websovelluksille - Aito Active Directory ainoastaan Windows 2003 –alustalle - Domain Services for Windows (Novell-tuote, Active Directory –emulointi) SuSE Linux Enterprise Server ja Open Enterprise Server 2 - Ei tue vanhempaa Active Directorya	- LDAP-sertifioitu (http://www.opengroup.org) - DSML-tuki (Directory Services Markup Language) websovelluksille - Useat palvelinkäyttöjärjestelmät tuettu: Linux, NetWare, Windows, HP-UX, IBM AIX ja Solaris
Luotettavuus / Toimintavarmuus	- Skeeman laajennuksen poisto ei mahdollinen - Ei voida klusteroida - toimintojen replikointi muille toimialueen palvelimille mahdollista. PDC emulator (salasanojen replikointi) voi olla vain yhdellä toimialueen ohjauskoneella - korjaustoimenpiteet vain *offline*-tilassa olevaan hakemistoon - varmistus/palautus mahdolli-	- skeeman laajennuksen poisto mahdollinen - automaattinen virheiden paikallistaminen ja korjaus - klusteroitavissa - replikoitavissa, kaikille hakemistopalvelun palvelimille periaatteessa samat roolit - käytössä olevan hakemiston korjausajot mahdollisia - varmistus/palautus mahdollinen - *Hot Continuous Backup*, eli

Luotettavuus / Toimintavarmuus	- Skeeman laajennuksen poisto ei mahdollinen - Ei voida klusteroida - toimintojen replikointi muille toimialueen palvelimille mahdollista. PDC emulator (salasanojen replikointi) voi olla vain yhdellä toimialueen ohjauskoneella - korjaustoimenpiteet vain *offline*-tilassa olevaan hakemistoon - varmistus/palautus mahdollinen	- skeeman laajennuksen poisto mahdollinen - automaattinen virheiden paikallistaminen ja korjaus - klusteroitavissa - replikoitavissa, kaikille hakemistopalvelun palvelimille periaatteessa samat roolit - käytössä olevan hakemiston korjausajot mahdollisia - varmistus/palautus mahdollinen - *Hot Continuous Backup*, eli jatkuva varmistus joka mahdollistaa palautuksen mihin tahansa hakemistopalvelun tilaan.
Hallittavuus	- luottosuhteiden hallinta hankalaa - palveluiden uudelleennimeäminen työlästä - koko toimialue replikoitava	- ei luottosuhteita, kahden puun yhdistäminen yksinkertaista - palveluiden uudelleennimeäminen ”oletusarvo” - ei välttämättä koko hakemis-

Taulukossa 1 on kerrottu hiukan Active Directoryn ja eDirectoryn eroavaisuuksista. Vertailevia dokumentteja on aika vähän ja vertailut keskittyvät pääsääntöisesti itse hakemistopalvelun toimintaan, eivätkä niinkään siihen, miten toiminta näkyy loppukäyttäjälle. Tärkeätä on kuitenkin ottaa huomioon myös se, miten järjestelmä toimii loppukäyttäjällä. Active Directory integroituu Windows XP/Vista/7 – käyttöjärjestelmiin suoraan ilman mitään kolmannen osapuolen sovelluksia. Jotta voidaan kirjautua Novell eDirectoryyn, täytyy työasemaan asentaa Novell Client ja määritellä LDAP-asetukset sekä muut tarvittavat eDirectoryn vaatimat palvelinasetukset. Active Directoryn tapauksessa riittää, että nimipalvelu on tietoinen toimialueen nimestä ja Active Directory –palvelimen osoitteista. Nämä tiedot luonnollisesti tulee olla myös työasemien käytettävissä. Työasema liitetään toimialueelle sen nimen perusteella, muita määrityksiä ei tarvita.

Edellinen taulukko määritteli joukon asioita, jotka ovat ylläpidon kannalta oleellisia. Myös loppukäyttäjän rooli on otettava huomioon. Ylläpidon haasteet näkyvät työasemien käyttäjille, mutta loppujen lopuksi itse käytettävyys merkitsee eniten. Loppukäyttäjän kannalta käytettävyyteen kuuluvat yksinkertaisuus ja nopeus.

Haastattelin opinnäytetyötäni varten kahta hakemistopalveluiden asiantuntijaa. Harri Karjalainen ja Pekka Sapman ovat työskennelleet erilaisten hakemistopalveluiden ja tiedonhallintajärjestelmien parissa jo useiden vuosien ajan. Harri Karjalaisen (2010) näkemys hakemistopalveluiden tulevaisuudesta on se, että Active Directory tulee edelleen olemaan voimakas nimenomaan työasemien autentikointilähteenä ja Novell eDirectory vahvistaa asemaansa identiteetinhallinnan keskuksena. Pekka Sapman (2010) näkee asian siten, että tulevaisuudessa on tärkeätä keskittyä myös avoimen lähdekoodin ratkaisuihin. Hänen mukaan hakemistopalvelu olisi täysin rakennettavissa myös ilmaisilla ratkaisuilla. Sapman kertoi haastattelussa erilaisten kolmannen osapuolen sovellusten tuomista autentikointiin liittyvistä haasteista. Hänen mukaan verkkoon on tuotu erilaisia järjestelmiä, jotka käyttävät omaa käyttäjätietokantaa. Monissa näissä on olemassa mahdollisuus LDAP-autentikointiin, mutta sitä ei ole otettu käyttöön. Sapman on sitä mieltä, ettei eDirectorysta ole kannattavaa luopua, koska on hyvä olla olemassa järjestelmä joka on avoimempi erilaisille ratkaisuille.

Harri Karjalaisen (2010) mukaan pienissä ympäristöissä yksi hakemistopalvelu riittää ja mikäli kyseessä on Windows-työasemien verkko, on tällöin Active Directory yleisimmin käytetty ratkaisu. Suuremmissa ympäristöissä on hyvin tavallista, että metahakemistona on eDirectory ja työasemat käyttävät autentikoitumiseen Active Directorya. Karjalainen mainitsi myös siitä, että Active Directoryn rooli tulee entisestään korostumaan kun todennäköistä on, että Windows-työasemat säilyttävät asemansa yritysten keskeisimpinä käyttöjärjestelminä. eDirectoryn rooli tulee olemaan nimenomaan identiteetin hallinnassa, johon Novell on kehittänyt erinomaisen tuotteen, joka tukee useita erilaisia identiteetin hallintaan liittyviä komponentteja.

Yhteenvetona sanottakoon se, että hakemistopalvelun valinta riippuu hyvin pitkälle siitä, kuinka isoa järjestelmää ollaan rakentamassa. Ammattikorkeakoulut ympäri Suomea ovat siirtymässä erilaisista Novell-ratkaisuista Active Directory –ympäristöön, säilyttämällä kuitenkin vaihtoehtoisen hakemistopalveluratkaisun identiteetinhallintaa varten. Tämä on mielestäni selkeä suuntaus ja tällaisella ratkaisulla pyritään kuitenkin loppujen lopuksi luomaan eräänlaista keskitettyä ratkaisua. Keskitetyllä tarkoitan sitä, että eri amkit pyrkivät yhteisiin ja yhtenäisiin ratkaisuihin, jotka mahdollistavat tulevaisuudessa paremmin erilaisten keskitettyjen ratkaisuiden hyödyntämisen. Mielestäni tilanne tällä hetkellä suosii sitä, että työasemien autentikointi toteutettaisiin Microsoftin ratkaisuilla ja identiteetinhallinta Novellin työkaluilla. Tällai-

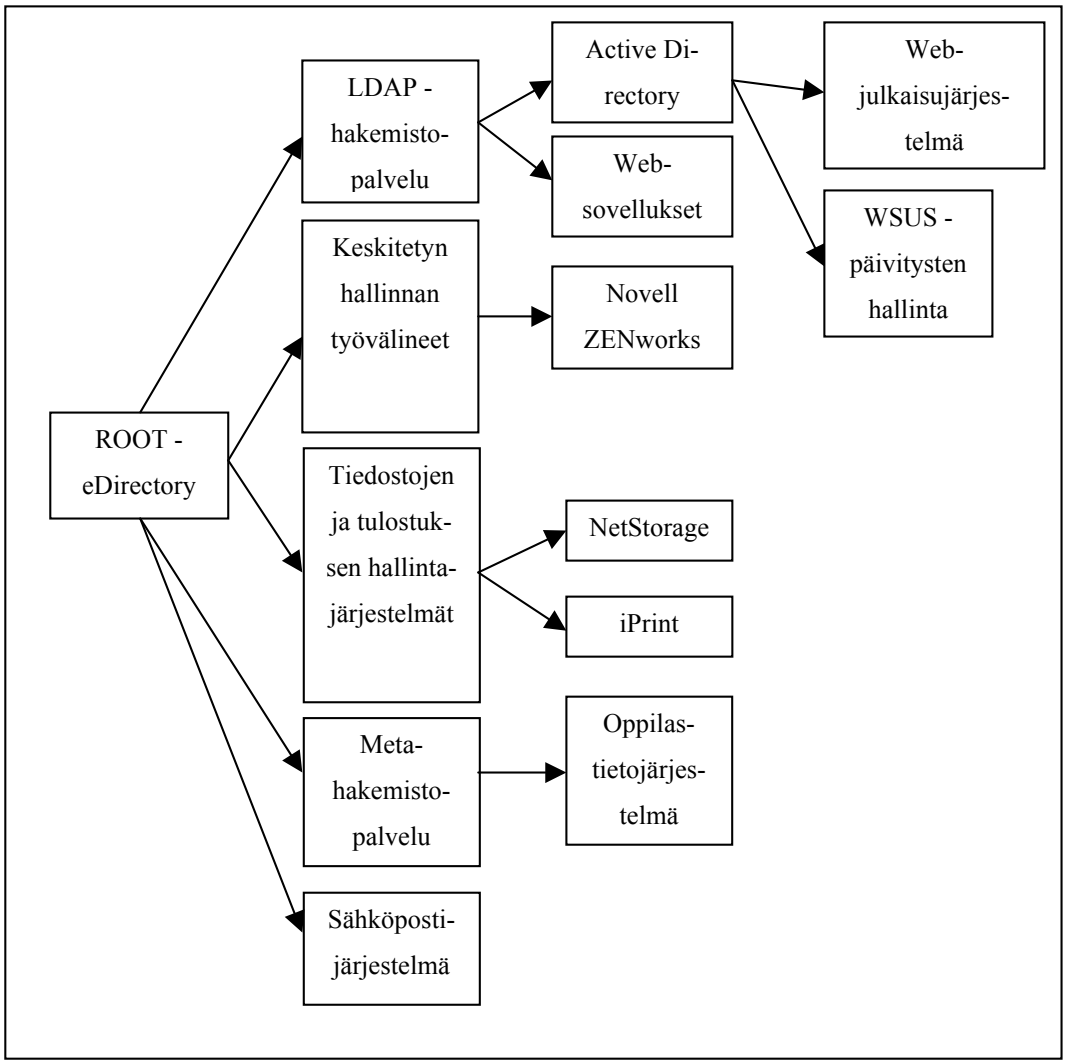
nen kokoonpano mahdollistaa dynaamisen ympäristön ja helpottaa kolmannen osapuolen liittämisen järjestelmään.

2.6 Taustatietoja MAMKin järjestelmistä

MAMKilla on tällä hetkellä käytössä päähakemistopalveluna Novell eDirectory, eikä siitä olla tässä vaiheessa luopumassa. Edellä mainittuun hakemistopalveluun on liitettynä erilaisilla identiteetinhallintajärjestelmillä myös muita hakemistopalveluita, kuten LDAP ja Active Directory. Muut hakemistopalvelut ovat tiedon välitystä varten, eikä niillä ole käytännössä kirjautumisen kannalta merkitystä. Kansalliset identiteetinhallintajärjestelmät (kuten Shibboleth) ovat tuoneet perinteisiin hakemistopalveluihin omat mielenkiintoiset piirteensä, eli myös näitä palveluita on alettu tarjota opiskelijoille ja tullaan aikanaan tarjoamaan myös henkilökunnalle.

eDirectory koostuu pääsääntöisesti NetWare 6.5 -palvelimista, joilla jokaisella on hiukan erilainen rooli. Käytössä on yksi hakemistopuu, jonka palvelimet on jaettu kahteen eri verkkoon. Palvelimilla on täysi näkyvyys toisiinsa, mutta verkoissa opetusverkosta ei ole hallinnon verkkoon näkyvyyttä. Suurin osa palvelimista on järjestelmän toiminnan kannalta oleellisessa roolissa, koska ne jakavat verkkoon joko sijaintitietoa (SLP, Service Location Protocol) tai sitten toimivat LDAP-palvelimina kirjautuville käyttäjille. Osa palvelimista tarjoaa pelkästään levypalveluita tai muita Web-Access -tyyppisiä palveluita.

Aikaisemmin mainitsemani identiteetinhallintaympäristö toimii siten, että opiskelijahallintojärjestelmä ASIO luo siirtotaulun tietyin väliajoin ja Novellin identiteetinhallintatyökalut lukevat siirtotaulusta tarvittavat tiedot ja kirjoittavat ne hakemistopalveluun määriteltyjen ajuritietojen perusteella.



KUVA 6. Kaaviokuva MAMKin järjestelmistä

Kuvassa 6 on kuvattu MAMKin järjestelmät karkealla tasolla. Kukin lohko pitää sisällään useamman eri palvelimen tai palvelun, jotka yhdessä muodostavat yhdestä toiminnosta kokonaisuuden. Pääsääntöisesti järjestelmät voidaan jakaa kolmeen eri osa-alueeseen, hakemistopalveluihin, gateway-tyyppisiin palveluihin ja tiedosto- sekä tulostuspalveluihin. Gateway-tyyppiset palvelut ovat järjestelmiä, jotka vain välittävät tietoja järjestelmältä toiselle. Tällaisia palveluita ovat muun muassa sähköpostipalveluiden web-sähköpostipalvelimet sekä internet-sähköpostien välitysjärjestelmät.

Järjestelmän ytimenä toimii Novell eDirectory –hakemistopalvelu, johon jokainen järjestelmä on yhteydessä tavalla tai toisella. Osa järjestelmistä on yhteydessä suoraan ja osa on joko LDAP-hakemistopuun kautta tai sitten Meta-hakemistopalvelun kautta. Meta-hakemistopalvelu toimii säilönä kaikille opiskelijatunnuksille, josta niitä sitten hyödynnetään niin ROOT-hakemistopalvelun kuin esimerkiksi GroupWise –

sähköpostijärjestelmän käyttöön. Käyttäjät autentikoivat Novell Clientien avulla eDirectoryyn ja Novell ZENworks tuo identiteetin Windows-työasemille.

Mainitsin aikaisemmin, että Novell eDirectorysta ei olla luopumassa. Tämä pitää osittain paikkaansa. Tosiasia on kuitenkin se, että erilaiset Active Directory -sidonnaiset järjestelmät yleistyvät ja se asettaa tiettyjä haasteita myös loppukäyttäjien työasemien käytölle. Uskoisin, että työasemat tulevat lähivuosina hyödyntämään Active Directorya autentikointiin. Muutoksen syynä on osittain se, että monet muutkin ammattikorkeakoulut siirtyvät Active Directoryn hyödyntämiseen ja osittain se, että olemassa oleva Microsoftin kampussopimus mahdollistaa nopean siirtymisen Active Directoryyn. On tässä osittain kyse myös lisenssipoliittisesta näkökulmasta. Active Directoryn käytöstä maksetaan joka tapauksessa, joten sen kannalta ylimääräisiä kustannuksiakaan ei tule.

eDirectory tulee edelleen olemaan se käyttäjähakemisto, joka sisältää suuren määrän käyttäjätietoja. Hakemistopalveluna se toimii erinomaisena pohjana niille järjestelmille, jotka sitä kykenevät hyödyntämään joko suoraan tai erilaisten identiteetinhallintasovellusten avulla. Kuvassa 6 on mainittu myös oppilastietojärjestelmä, joka MAMKilla on ASIO. ASIOsta tiedot siirtyvät Meta-hakemistopalvelun hyödynnettäviksi Novell Identity Management –työkalujen avulla. Novell –identiteetinhallinta perustaa oman toimintansa eDirectoryyn. Tästä syystä eDirectory tulee säilyttämään asemansa MAMKin palvelininfrastruktuurissa.

3 HAKEMISTOPALVELUIHIN KOHDISTUVAT VAATIMUKSET

Nykyisellään ei voi tukeutua pelkästään yhden hakemistopalvelun varaan, vaan on tehtävä erilaisia integraatioita erilaisten hakemistopalveluiden välille. Novell eDirectory pystyy mainiosti hallitsemaan suurenkin käyttäjätietokannan, mutta sen integroituvuus Windows-ympäristöön on hiukan kankea. Monet kolmannen osapuolen järjestelmät vaativat käyttäjäautentikointiin Active Directoryn. Tästä syystä myös MAMKilla on jouduttu pohtimaan erilaisia ratkaisuja tämän toiminnallisuuden käyttöönotolle.

Tieto siirtyy järjestelmistä toiseen ongelmattomasti identiteetinhallintajärjestelmien kautta. MAMKilla on varsin laajassa käytössä Novell Identity Manager, joka synkronoi käyttäjätunnustietoja eDirectory-hakemistopalvelun, meta-hakemistopalvelun, LDAP-hakemistopalvelun ja Active Directoryn välillä. Tämä järjestelmä laajenee jatkuvasti ja sen ylläpito vaatii jo melkoisesti panosta. Tästä syystä tiettyjen asioiden yksinkertaistaminen ei olisi pahitteeksi.

Miten sitten toimia, kun vaatimukset Active Directoryn tulevat myös tuotantoon? Vaihtoehtoja on käytännössä kolme:

1. ”Puhdas” Active Directory -ratkaisu Microsoft Windows 2003/2008 Serverin avulla, jossa työasemat ovat liitettynä toimialueelle ja saavat tarvittavat palvelut Microsoft-verkon kautta.
2. Yhdistetty Novell eDirectory- ja Active Directory -ratkaisu, jossa työasemat ovat toimialueessa, mutta esimerkiksi levypalvelut jaetaan Novell-ympäristöstä
3. Novell Open Enterprise Server Domain Services for Windows, eli Novellin emuloima Active Directory -palvelu, joka saa Linux Open Enterprise Serverin näyttämään toimialueen ohjauskoneelta. Tällöin työasemat voidaan liittää Novellin luomaan toimialueeseen ja kaikki verkon palvelut voidaan tuottaa Novellin työkaluilla.

Jokaisessa edellä mainitussa mekanismissa on omat heikkoutensa. Ensimmäinen vaihtoehto on Microsoft Windows -ympäristössä kaikkein paras, mutta kun MAMKilla on käytössä eDirectory ja sitä kautta Novellin levypalvelut, on erittäin haasteellista ja ennen kaikkea työlästä siirtää levypalvelut Microsoftin levypalveluille. Toisessa vaihtoehdossa on se hankaluus, että käyttäjätiedon on oltava identtinen kummassakin hakemistopalvelussa ja työasemissa pitää olla autentikointimenetelmät kumpaankin hakemistopalveluun. Kolmannessa vaihtoehdossa käytössä olisi emulointi, mikä ei luonnollisestikaan vastaa autenttista Active Directory -ympäristöä. Domain Services for Windowsista ei ole vielä ole paljoa näkyviä käytännön kokemuksia, jolloin sen toimivuudesta ei ole täyttä varmuutta. Olisi oikeastaan testattava, kuinka suurta ympäristöä tällaisella järjestelmällä voisi ylläpitää.

Active Directorya vaaditaan jo monessa eri käytössä. Tästä syystä sen käyttöä ei voida välttää mitenkään. Siksi onkin ennemmin mietittävä keinoja, joilla sen käyttöönottoa

voitaisiin helpottaa. Tutkailen tällä opinnäytetyöllä näitä mahdollisuuksia ja painotan niiden toimivuutta nimenomaan MAMKin tietoverkossa. Hakemistopalvelun vaihdos on aina iso prosessi, joten se olisikin hyvä suunnitella tarkoin ja mietittävä vaihtoehdot mahdollisimman monelta eri kantilta.

Hakemistopalveluita pitää pystyä yhdistelemään. Monilla organisaatioilla on käytössä useita erilaisia hakemistopalveluita, jotka palvelevat hiukan erilaisia käyttötarkoituksia. Pääsääntöisesti tilanne on se, että on päähakemistopalvelu, johon käyttäjät kirjautuvat. Tämän lisäksi on olemassa esimerkiksi LDAP-hakemistopalvelu, jota käytetään integroimaan vaikkapa identiteetinhallinta päähakemistopalveluun. Yleensä eri hakemistopalveluiden yhdistämisen tarve tulee esille siinä, kun halutaan kuljettaa esimerkiksi henkilötietoja henkilöstöhallinnasta päähakemistopalvelun käytettäväksi. Toki voi olla mahdollista, että henkilöstöhallinto integroidaan suoraan päähakemistopalveluun ja se toimii siinä sellaisenaan. Todennäköistä kuitenkin on, että organisaatiolla on tarve käyttää LDAP-autentikointia jonkin sovelluksen autentikointiin. Tällaisessa tapauksessa on kätevä olla erillinen LDAP-palvelu, joka hoitaa kolmannen osapuolen sovellusten LDAP-autentikoinnin. Käytännössä tilanne olisi siis se, että identiteetinhallintajärjestelmä välittää henkilöstöhallinnosta tarvittavat tiedot LDAP-palveluun, josta sitten halutut järjestelmät hakevat autentikointitiedot. Esimerkkejä tällaisista kolmannen osapuolen sovelluksista on erilaiset web-sovellukset (Moodle, SoleTM).

Organisaatiolle voi tulla sovellus, joka haluaa käyttää autentikointiin Active Directorya. Tämä ei ole mikään ongelma mikäli käytössä on jo aktiivinen Active Directory -palvelu. Mutta mikäli käytössä on esimerkiksi eDirectory-hakemistopalvelu ja työasemat autentikoituvat eDirectoryyn, ei Active Directory -sidonnaisia sovelluksia tai palveluita voi työasemilla käyttää. Tällaisissa tilanteissa vaihtoehtoja on joitakin. Vaihtoehdot ovat:

1. Migraatio Novell eDirectorysta Microsoft Active Directoryyn
2. eDirectoryn ja Active Directoryn yhdistäminen identiteetinhallinnan keinoin
3. Active Directoryn emulointi eDirectoryssa

Ensimmäisessä vaihtoehdossa ongelma on siinä, että pitkään Novell-palveluita käyttänyt organisaatio on vähitellen rakentanut palveluitaan eDirectoryn ympärille ja käytännössä kaikki data, kirjoitinpalvelut ja työasemien hallinta on sidoksissa eDirecto-

ryyn. Tiedon siirtäminen Active Directoryn ymmärtämään muotoon vaatii isoja muutoksia niin palvelininfrastruktuurissa kuin työasemissa. Etuna olisi se, että tällöin käytössä olisi puhdas Active Directory -palvelu, joka integroituu erinomaisesti Windows -työasemiin.

Toisessa vaihtoehdossa ongelmaksi muodostuu se, että joudutaan autentikoitumaan kahteen erilliseen hakemistopalveluun. Lisäksi informaation täytyy olla täsmälleen samaa molemmissa hakemistopalveluissa, muutoin autentikointi ei onnistu kuten pitäisi. Tällainen ratkaisu kuitenkin mahdollistaisi sen, että käyttäjien data ja esimerkiksi kirjoittimet ovat edelleen eDirectoryssa, mutta tiettyjen sovellusten Active Directory -sidonnaisuus poistettaisiin liittämällä työasemat Active Directoryyn. Kaksi rinnakkaista hakemistopalvelua on aina hiukan hankala kuvio, joskin identiteetinhallinnan keinoin tiedon yhtenäistäminen ei ole ongelma. Työasemien suorituskyky kärsii jonkin verran, kun tehdään autentikointi molempiin hakemistoihin.

Kolmas vaihtoehto on Novellin oma järjestelmä, joka käytännössä toimii siten, että SuSE Linux Enterprise Serveriin asennetaan Open Enterprise Server -lisäosat. Lisäosien mukana tulee Domain Services for Windows -palvelukokonaisuus, joka saa Linux-palvelimen näyttämään Active Directory -palvelimelta. Testauksissa tämän kaltainen palvelu on toiminut moitteetta, mutta ison käyttäjähakemiston (noin 6000 tunnusta) muuntaminen Active Directorya emuloivaksi voi olla ongelmallista ja jossain mielessä jopa riskialtista. Joissakin tapauksissa tällaisen palvelun käyttöönotto voisi olla helpoin ja nopein tapa päästä Active Directory -palveluihin käsiksi.

Kun mietitään tietojen synkronointia eri järjestelmien välillä, tulee mieleen, kuinka voidaan taata tiedon integroituminen järjestelmästä toiseen aukottomasti sekä varmistaa attribuuttien standardinmukaisuus. Onneksi suuremmat hakemistopalveluiden rakentajat ovat yhtenäistäneet attribuutit ja LDAP-attribuuteista on olemassa omat standardinsa, joita LDAP-yhteensopivan hakemistopalvelun on noudatettava. Aina kuitenkin on tilanteita, joissa LDAP-standardista huolimatta jonkin attribuutin muoto poikkeaa hiukan ja joutuu miettimään tarkasti sen, miten tällaisissa tapauksissa tieto siirtyy oikein. Toinen tilanne on se, että LDAP-attribuuttien määrä voi vaihdella eri hakemistopalveluissa. Tämä ei sinänsä ole ongelma, koska LDAP-attribuutteja voi jonkin verran muokata ja tarpeen mukaan lisäillä. Esittelin aikaisemmin ensimmäisessä vaihtoehdossa migraation eDirectorysta Active Directoryyn. Tällaisessa tapaukses-

sa tiedon synkronointi ei ole tarpeen kuin kerran, koska kohdehakemistopalvelu ottaa tämän jälkeen roolin päähakemistopalveluna ja attribuutit menevät kohdehakemistopalvelun ehdoilla. Erilaisissa identiteetinhallintajärjestelmissä on olemassa valmiita malleja siitä, kuinka eri hakemistopalvelut voidaan yhdistää. Useimmissa tapauksissa ne toimivat, mutta mikäli organisaatiolla on käytössä joitain eksoottisempia attribuutteja, vaatii niiden kanssa toimiminen hiukan muutoksia tiedonsiirtoajureihin.

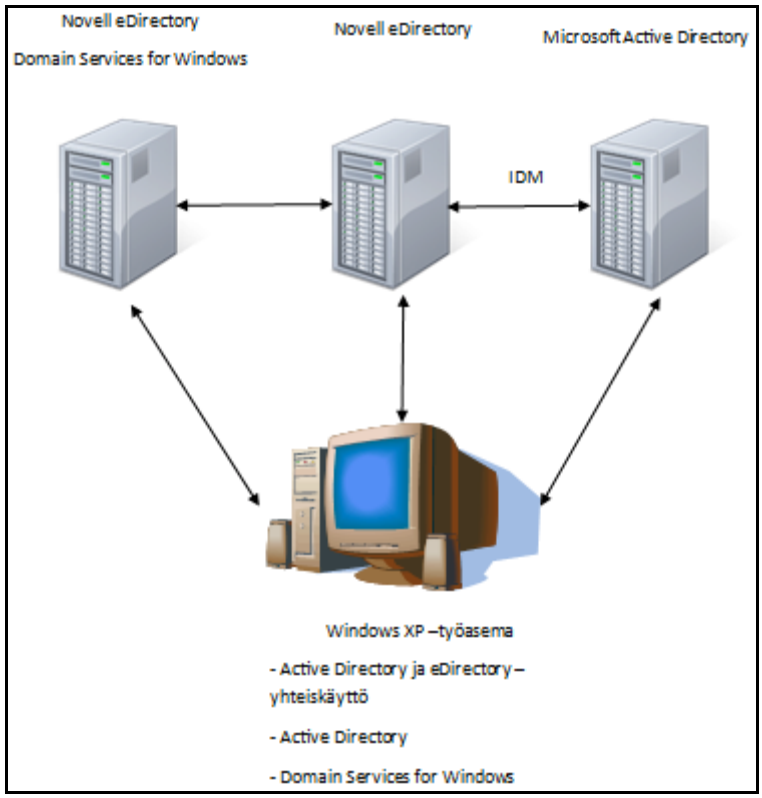
Miten järjestelmä toimii MAMKilla? MAMK on varsin tyypillinen kahden hakemistopalvelun kokonaisuus, jonka päähakemistopalveluna on eDirectory. eDirectoryn kupeessa on myös sähköpostipalvelu (Novell GroupWise). Yksinkertaisuudessaan kokonaisuus on sellainen, että kaiken keskellä on Novell eDirectory –hakemistopalvelu, johon on liitetty LDAP-hakemistopalvelu, joka integroi Active Directoryn eDirectoryyn. Tämän lisäksi varsinaiseen päähakemistopalveluun on liitetty metahakemistopalvelu, joka toimittaa opiskelijoiden tiedot päähakemistopalveluun opiskelijahallintojärjestelmästä (ASIO). Lisäksi päähakemistopalveluun on liitetty Novell ZENworks -työasemahallinta, Novell iPrint -tulostuspalvelu, Novell NetStorage -webpalvelu verkkolevyille ja Novell iChain -proxypalvelu.

MAMKissa kaikki tieto on eDirectoryssa. Henkilökunnan tunnukset luodaan suoraan päähakemistopalveluun, josta tieto siirtyy Novell Identity Management -palveluiden avulla LDAP -hakemistopalveluun, joka välittää tiedon eteenpäin Active Directoryyn ja sitä kautta myös intranet-palveluun. Työasemat ovat yhteydessä eDirectoryyn Novell Client -työasemaohjelmiston avulla. Novell ZENworks -työasemahallintajärjestelmä hoitaa työasemaan kohdistuvan autentikoinnin ja luo tarvittavat tunnukset Windows-työasemilla eDirectory-tunnistautumisen mukaisesti. Järjestelmä on toiminut kohtalaisen hyvin, toisinaan on ollut erilaisia kirjautumista hidastavia ongelmia, mutta pääsääntöisesti nekin ovat ratkenneet eDirectory-hakemistopalveluun kohdistuvilla huolto- ja korjausajoilla.

Novell toimii kuten pitääkin, joskaan sen integroitavuus tiettyihin palveluihin ei ole yhtä joustava kuin Active Directoryssa. Esimerkiksi erilaiset virtualisointipalvelut ovat suorastaan Active Directory -sidonnaisia.

4 TESTIYMPÄRISTÖN ESITTELY

Helpoin tapa tämän projektin läpiviennille oli se, että rakensin asianmukaisen testiympäristön. Kerron tässä luvussa hiukan tästä testiympäristöstä ja jokaisesta erilaisesta konfiguraatiosta, mitä käytin.



KUVA 7. Testiympäristö.

Kuvassa 7 on esitelty käyttämäni testiympäristö. Kaikki testiympäristössä olevat järjestelmät ovat virtuaalijärjestelmässä. Kerron tässä luvussa tarkemmin tuosta kokonaisuudesta ja jokaisesta komponentista erikseen.

4.1 Virtuaalijärjestelmän esittely

Testausvaiheessa ei ole järkevää tehdä testauksia tuotantoympäristöön, koska ei ole täyttä varmuutta siitä, miten hakemistopalvelut reagoivat erilaisiin muutoksiin. Jotta testaaminen olisi helppoa ja voisi tarvittaessa nopeasti siirtyä alkutilaan, päätin hyödyntää VMwaren ilmaisia virtualisointituotteita. Asensin kohtalaisen tehokkaaseen HP Compaq dc7700 -työasemaan VMware ESXi 4:n, joka on viimeisin versio VMwaren Datacenter -tuotteesta. Muistia työasemassa oli 7 Gt, mikä riittää hyvin muutaman

virtuaalipalvelimen ja -työaseman käyttämiseen. Virtuaaliympäristö on testauskäytössä erinomainen. Ei tarvita kuin yksi tehokas palvelinlaite, joka hoitaa kaikki tarvittavat virtuaalikoneet. Toinen selkeä syy virtuaalijärjestelmän käyttöön oli se, että paluu alkutilaan oli helppoa ja nopeaa. Tämä tarkoittaa sitä, että kun olin suorittanut virtuaalikoneen käyttöjärjestelmän asennuksen, otin siitä levykuvan (snapshot). Erilaisia konfiguraatioita tehdessä minun oli aina mahdollista palata alkutilaan ja testata vaihtoehtoinen tapa. Tämä säästää aikaa ja vaivaa käyttöjärjestelmän asennuksen suhteen.

Virtuaalijärjestelmän verkkoympäristö oli toteutettu siten, että virtuaalikoneet olivat samassa virtuaaliverkossa, joka oli yhteydessä fyysiseen verkkorajapintaan. Tällöin virtuaalikoneet eivät olleet eristyksissä, vaan niitä pystyi hallinnoimaan virtuaalipalvelimen ulkopuoleltakin. Todellisuudessa virtuaaliympäristön hallinta ja virtuaalikoneiden verkko olisi erotettu toisistaan, eli kokonaan omille fyysisille verkkoliitännöille.

4.2 Virtuaalikoneiden esittely

Järjestelmässä oli kolme palvelinta ja yksi testityöasema. Seuraavassa esittelen hiukan tarkemmin palvelimia ja niiden rooleja. Myöhemmässä vaiheessa (luvuissa 5, 6 ja 7) esittelen järjestelmän osien toimintaa hiukan yksityiskohtaisemmalla tasolla. Tuotantokäytössä kannattaa kiinnittää tarkempaa huomiota muistin käyttöön ja sitä luonnollisesti suuremmissa ympäristöissä tarvitaankin enemmän. Muuten tässä esitellyt virtuaalikoneet ovat käyttökelpoisia jopa tuotantokäyttöön.

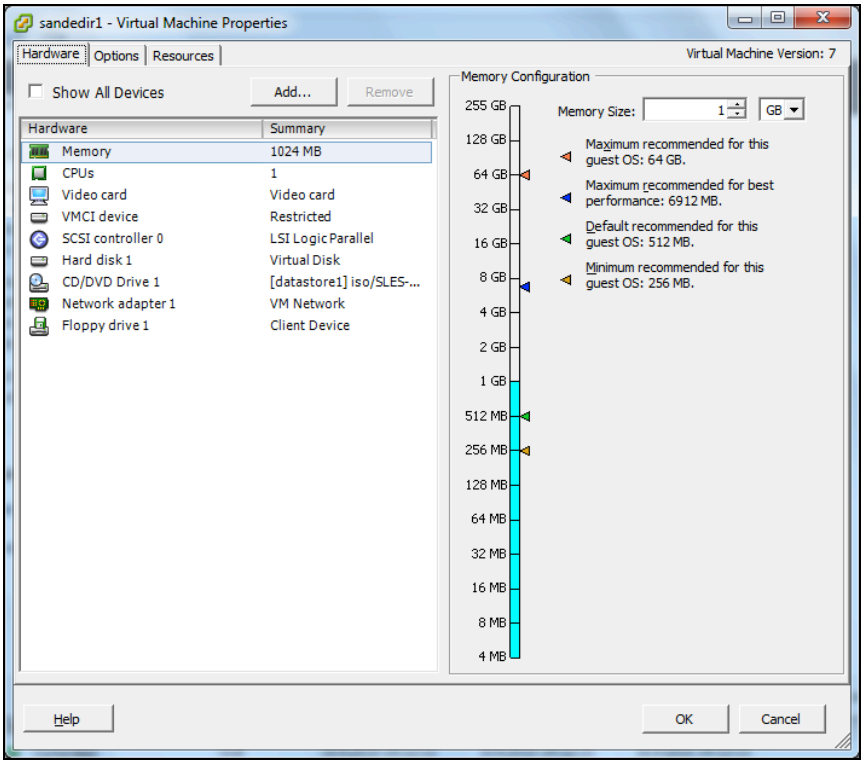
4.2.1 eDirectory-palvelinympäristö

Käytin testissäni kahta SuSE Linux Enterprise Server 10 SP3 -palvelinta, joihin asensin Novell Open Enterprise Server 2 SP2:n. Open Enterprise Server 2 SP2 mahdollistaa muun muassa eDirectoryn ja Directory Services for Windows -toiminnallisuuden SuSE Linux Enterprise Server -käyttöjärjestelmälle. Tästä kerron tarkemmin luvussa 7. Vaihtoehtona eDirectoryn alustaksi olisi ollut Novell NetWare 6.5 SP8, joka olisikin ollut hyvä ja tehokas verkkokäyttöjärjestelmä, mutta kuitenkin tiensä päässä oleva järjestelmä. Tästä syystä päädyin Linux-käyttöjärjestelmään.

eDirectoryn olisi voinut asentaa erikseenkin, ilman Open Enterprise Server 2 -lisäosia. Open Enterprise 2 -lisäosien tarkoituksena on helpottaa ja nopeuttaa Novell-

palveluiden käyttöönottoa SuSE Linux Enterprise Server 10:ssä. Lisäksi Open Enterprise Server 2 -paketissa on juuri sopivat versiot eri komponenteista ja hallintatyökaluista. Tämä on hyvä asia silloin, kun pyritään yhdistämään monta eri osa-aluetta, kuten esimerkiksi Linux-palvelin, eDirectory ja JavaEE-ympäristö.

Toisessa palvelimessa oli asennettuna myös Novell Identity Management – identiteetin-hallintaympäristö. Tarkoituksena oli siis synkronoida tietoa Active Directoryn ja eDirectoryn välillä.



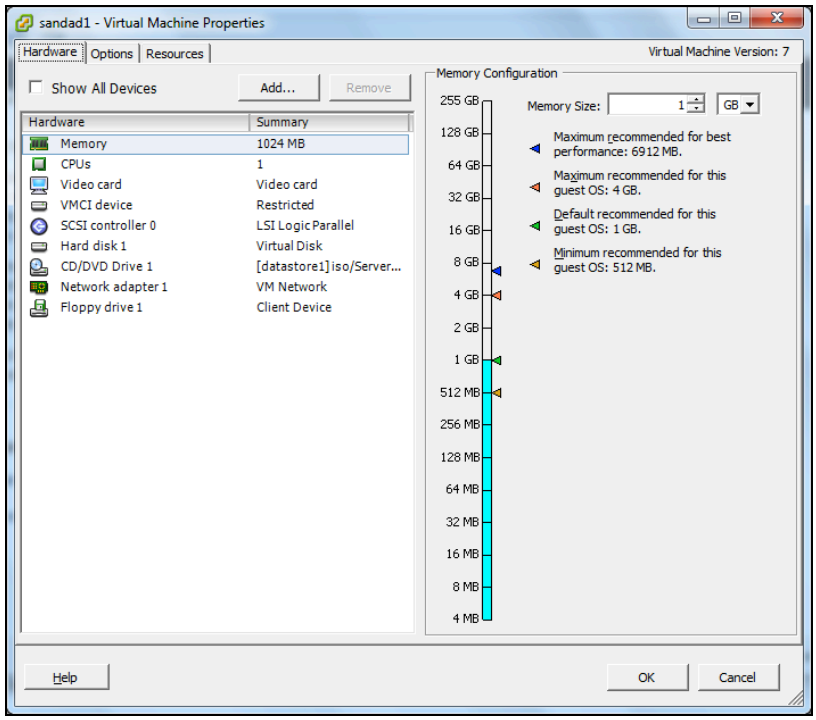
KUVA 8. eDirectory-palvelimen laitteistokokoonpano

Kuvassa 8 on esitelty eDirectory palvelimen laitteisto. Virtuaalilaitteisto on sellainen, että virtuaalikoneeseen asennettu käyttöjärjestelmä luulee kyseessä olevan fyysisen koneen. Virtuaalikoneen etu on se, että fyysisiä asennusmedioita ei tarvitse käyttää, vaan käyttöjärjestelmä on asennettavissa suoraan internetistä ladattavasta ISO-levykuvasta. Osa näistä ominaisuuksista on muutettavissa koneen ollessa käynnissä. Ideana joka tapauksessa on se, että laitteistokokoonpanon muuttaminen on helppoa ja nopeata.

4.2.2 Active Directory -palvelinympäristö

Toinen palvelin on Microsoft Windows 2003 Server R2 Standard ja hoitaa järjestelmän DNS, DHCP ja Active Directory -palveluita. DHCP-palvelu ei ole välttämätön, mutta helpottaa verkkokonfiguraatioita. DNS-palvelu oli testiympäristössä loogisinta asentaa Active Directoryn yhteyteen, mutta olisi ollut mahdollista asentaa myös SuSE Linux Enterprise Server 10:een.

Active Directory on siinä mielessä kiitollinen asennettava, että se on käytännössä jo valmiina Windows 2003 Serverissä. Tällöin ei tarvita muuta kuin itse konfiguraatio ja sekin menee ohjatun toiminnon kautta varsin yksinkertaisesti läpi. Windows 2003 Server ei pienessä ympäristössä vaadi kovin paljon resursseja, joten käyttämässäni testiympäristössä tällä palvelimella ei ole kovin kummoisia laitevaatimuksia. Kuvasta 9 näkyy hyvin se, millaisen laitekokoonpanon VMware on määrittänyt Windows Server 2003:lle.



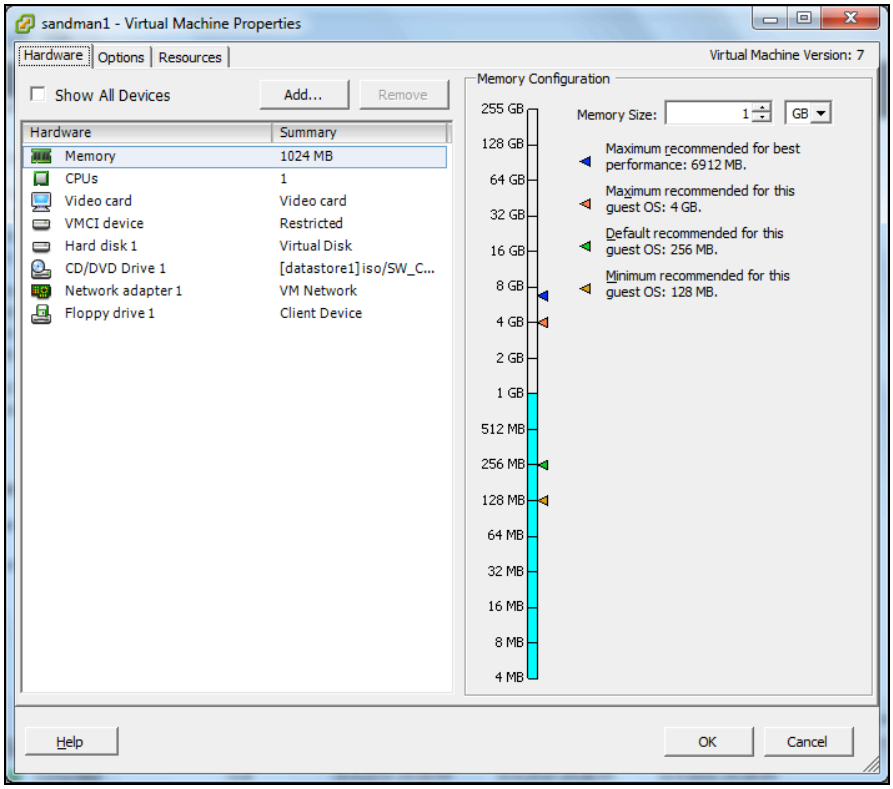
KUVA 9. Windows 2003 Serverin laitteistokokoonpano

Kuvassa 8 esittelin eDirectory-palvelimen laitteiston ja kuvasta 9 voimme huomata, että kyseessä on identtinen kokoonpano, lukuun ottamatta käytettävää asennusmediaa (ISO-levykuvaa).

4.2.3 Windows XP -testityöasema

Testityöasemaan päätin asentaa Windows XP Professional SP3:n, koska en halua käyttää aikaa Novell-tuotteiden virittelyyn Windows 7 Enterprisessä. Periaatteessa kaikki tarvittava toimii myös Windows 7 Enterprisessä, mutta siinä on joitakin kummallisuuksia, joiden tutkimus vaatii oman aikansa. Windows XP Professional on edelleen varsin laajalti käytössä, eikä mikään ihme, koska se on kohtuullisen kevyt ja toimiva käyttöjärjestelmä pyörittämään tarvittavia sovelluksia. Monet sovellukset ovat yhä edelleen riippuvaisia Windows XP:stä.

Testityöasemaan asennetaan ainoastaan Novell Client eDirectoryn testaukseen ja se liitetään Active Directory -testejä varten toimialueelle. Nämä ovat kaksi erillistä prosessia, joista lisää tuonnempana.

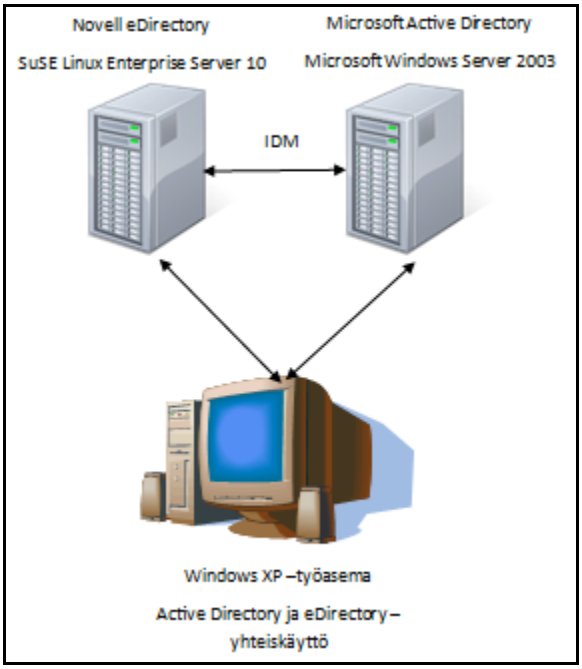


KUVA 10. Tyypillinen Windows XP –virtuaalityöasema

Kuvasta 10 on nähtävissä, että virtuaalityöasema on hyvin samankaltainen verrattuna edellä esiteltyihin palvelinlaitteistoihin.

5 EDIRECTORYN JA ACTIVE DIRECTORYN YHTEISKÄYTTÖ

Tämä kokonaisuus vaati eniten konfiguroitavia palveluita. Palvelimia ei järjestelmässä ollut kuin kaksi, mutta niihin oli asennettu useita erilaisia rooleja. Näistä rooleista kerron hiukan tarkemmin tässä luvussa.



KUVA 11. eDirectoryn ja Active Directoryn yhteiskäyttö

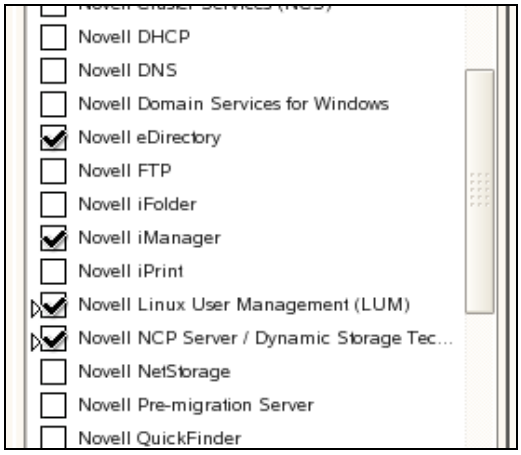
eDirectoryn ja Active Directoryn yhteiskäyttöä puoltaisi esimerkiksi se, että levypalvelut ovat Novell-verkossa. Novellin oma tiedostojärjestelmä NSS vaatii sellaisenaan eDirectoryyn autentikoitumisen, mutta sitä on mahdollista käyttää Windows-ympäristöissä ilman Novell Clientiä mikäli NSS:ään otettaan käyttöön CIFS-toiminnallisuus. CIFS on lyhenne sanoista Common Internet File System. CIFS on vastaava kuin Samba, joka taas on Linuxin tapa mahdollistaa sen omien tiedostojärjestelmien käyttö Windows-verkoissa. Tässä luvussa lähtökohtana on se, että levypalvelut ovat Novell-verkossa. Tutkin eri mahdollisuuksia siitä, miten näitä teknologioita voidaan hyödyntää yhdessä. Kuvassa 11 on esitelty kokoonpano, jossa on tässä kokonaisuudessa tarvittavat komponentit.

5.1 eDirectoryn määritykset

Olin asentanut virtuaalikoneeseen luvussa 4.2.1 esitellyn SuSE Linux Enterprise –ympäristön. Seuraava vaihe oli se, että määrittelin eDirectoryn hakemistopalveluksi.

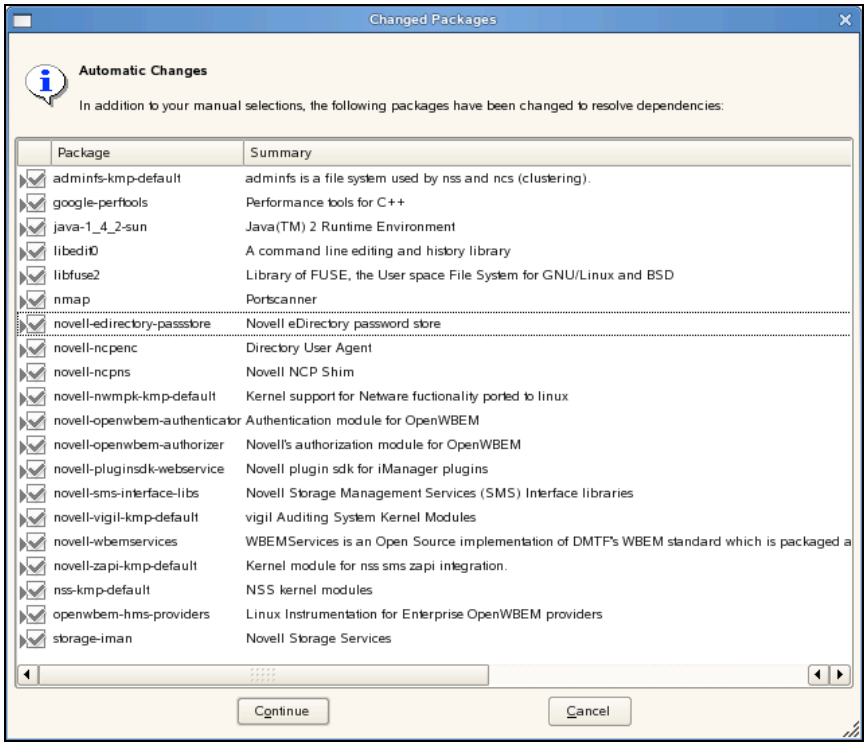
SuSE Linux Enterprise Serverissä on yksi keskeinen hallintatyökalu, YaST. Tällä työkalulla pystyin tekemään eDirectoryn konfiguroinnin täysin graafisesti. Tämä on erinomainen ominaisuus, mikäli graafisen käyttöliittymän käyttö on mahdollista. Muutoin konfiguraatio täytyy tehdä merkkipohjaisilla työkaluilla. Merkkipohjaisten työkalujen käyttöön on ohjeita Novellin dokumentaatiosivustoilla. YaSTista löytyy osio Open Enterprise Server, jossa on pikakuvake OES Install and Configuration.

Ennen palveluiden asentamista olin kartoittanut tarpeita ja luonut dokumentaatioon listan hallittavista osa-alueista. Tärkeätä on tietää, mitä tarvitsee ja millä työkaluilla niitä hallinnoi. Seuraavassa kuvassa on listaus asennettavissa olevista komponenteista. Jokainen näistä komponenteista on hallittavissa Novell iManager –hallintasivuston kautta, joten itse iManagerin asennus on ehdottoman oleellinen koko hakemistopalvelun kannalta. Aikaisemmin iManagerin hallintatyökalujen liitännäisten asennus tuotti päänvaivaa, mutta nyt nämä automatisoidut asennukset tekevät paljon asioita asentajan puolesta.



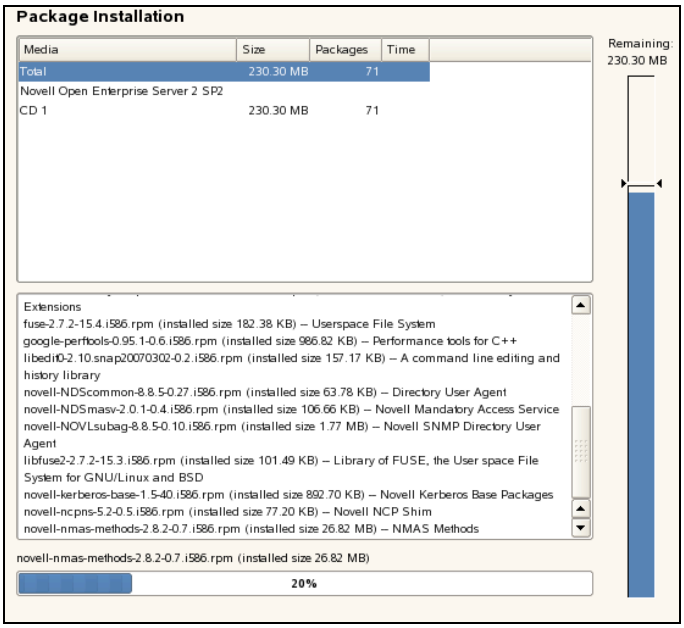
KUVA 12. OES Install and Configuration, asennettavissa olevia komponentteja

Kuva 12 näyttää osan niistä komponenteista, mitä Open Enterprise Serveriin on asennettavissa. Valitsen Novell eDirectoryn, Novell iManagerin ja Novell Storage Services (NSS) –ominaisuudet. Valintoja tehdessä voi huomata sen, että jotkin komponentit tulevat mukaan vaikkei niitä valitsisikaan. Tämä johtuu siitä, että näillä palveluilla on riippuvuussuhteita muiden sovellusten kanssa. Esimerkiksi Novell eDirectory –komponentti on riippuvainen Novell Linux User Management –komponentista ja eDirectoryn mukana asentuu erinomainen hallintatyökalu Novell Remote Manager. Riippuvuussuhteisiin on monia eri syitä, mutta tavallisesti riippuvuussuhteet muodostuvat jaettujen sovelluskomponenttien kautta.



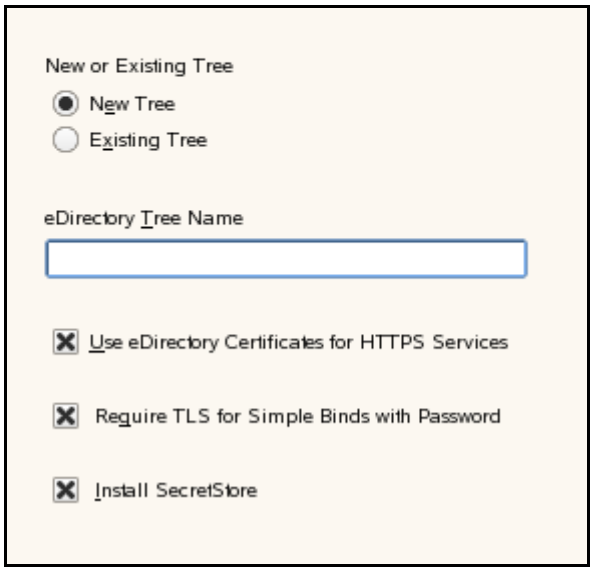
KUVA 13. Lista asennettavista komponenteista

Edellisessä kuvassa on listattu eDirectoryn vaatimat komponentit. Lista osoittaa sen että tarvittavia komponentteja on useita. Toisaalta tässä vaiheessa on vielä mahdollista vaikuttaa asennettaviin osa-alueisiin. Listassa huomio kiinnittyy Java 2 Runtime Environmentin versioon, joka asennusvaiheessa on 1.4.2. Versio on melkoisen vanha, joten myös järjestelmän päivittymiseen on syytä kiinnittää huomiota.



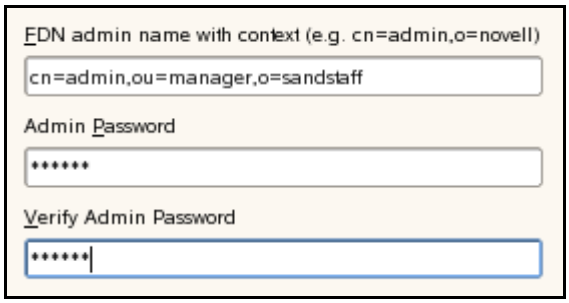
KUVA 14. Asennus käynnissä

Kuva 14 on hyvä esimerkki siitä, miten monipuolista tietoa asennettavista komponenteista saa asennusvaiheessa. Järjestelmä kertoo mitä asennuspaketteja se hakee ja kuinka paljon ne vievät tilaa järjestelmästä. Asennus loppuu automaattisesti ilman eri ilmoituksia ja tämän jälkeen alkaa itse eDirectoryn konfigurointi.



KUVA 15. Uuden hakemistopuun nimeäminen ja sertifikaattimääritykset

Tässä vaiheessa palvelin on mahdollista liittää osaksi olemassa olevaa hakemistopuuta tai luoda kokonaan uusi hakemistopuu. Hakemistopuun nimi on se juuritason käsite, jonka alle tarvittavat organisaatiot ja organisaatioyksiköt luodaan. Tulen käyttämään esimerkissä hakemistopuun nimenä SANDTREE:a. Järjestelmä tutkii verkosta löytyykö samalla nimellä olevia muita hakemistopuita ja varoittaa mikäli näin on. Mikäli hakemistopuun nimi on käytettävissä, seuraava vaihe on hakemistopalvelun pääkäyttäjän sijainnin määrittely ja autentikointimääritykset.

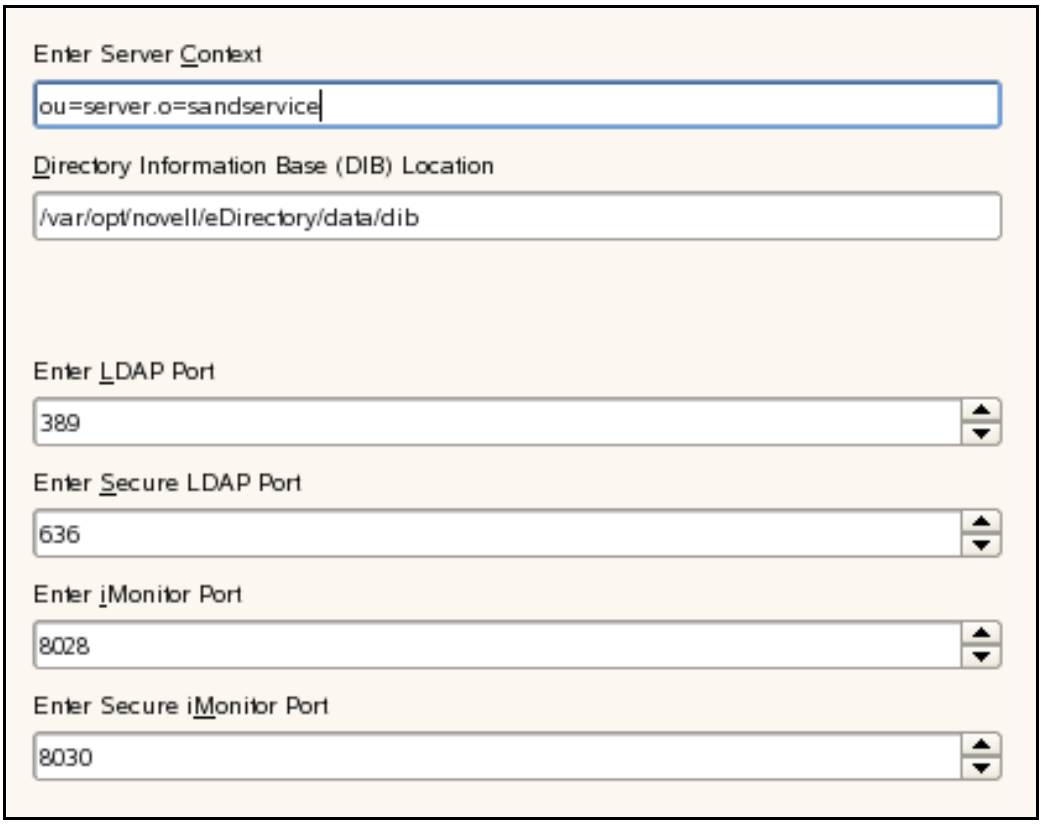


KUVA 16. Pääkäyttäjän nimeäminen ja sijaintitiedot

Olen luomassa pääkäyttäjää, jonka sijainti puussa on ou=manager,o=sandstaff. Joissakin tapauksissa käyttäjätunnustieto annetaan muodossa admin.manager.sandstaff. Ky-

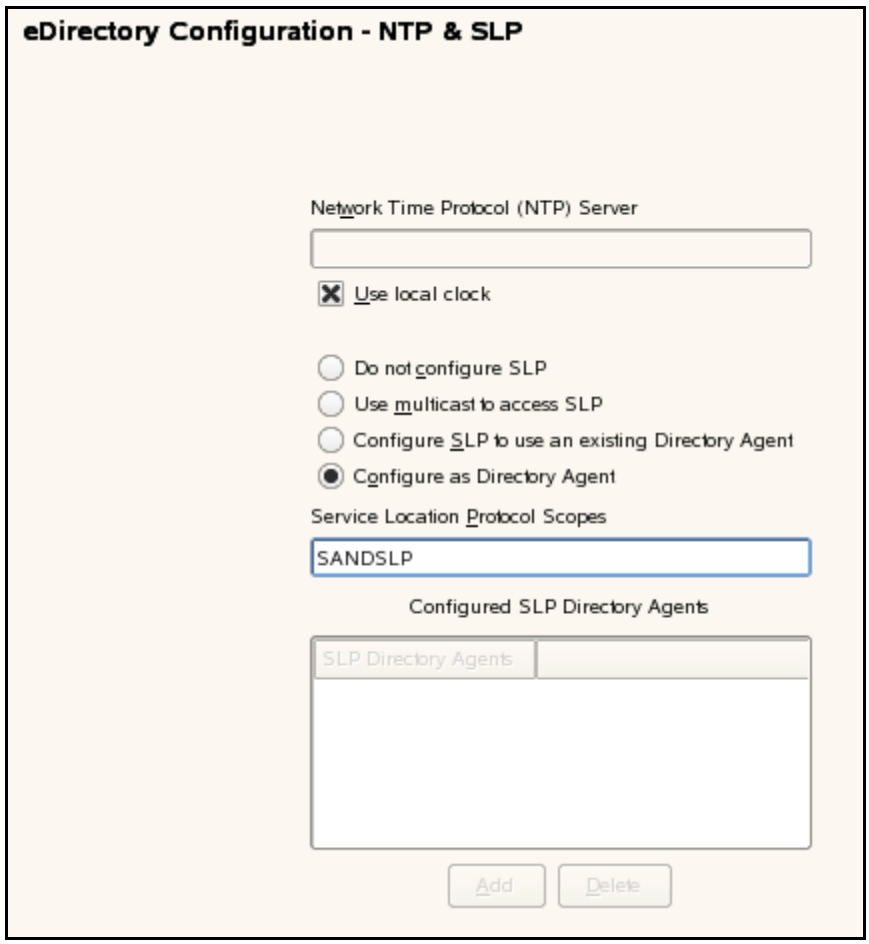
se on samasta asiasta, mutta eri osa-alueet tulkitsevat määrityksiä hiukan eri tavalla ja näin ollen vaativat tarkempaa kuvausta tunnuksista.

cn = common name, käyttäjätunnus
ou = organizational unit, käyttäjän sijainti puussa
o = organization, kontaineri johon kaikki kyseiseen organisaation kuuluvat objektit kuuluvat.



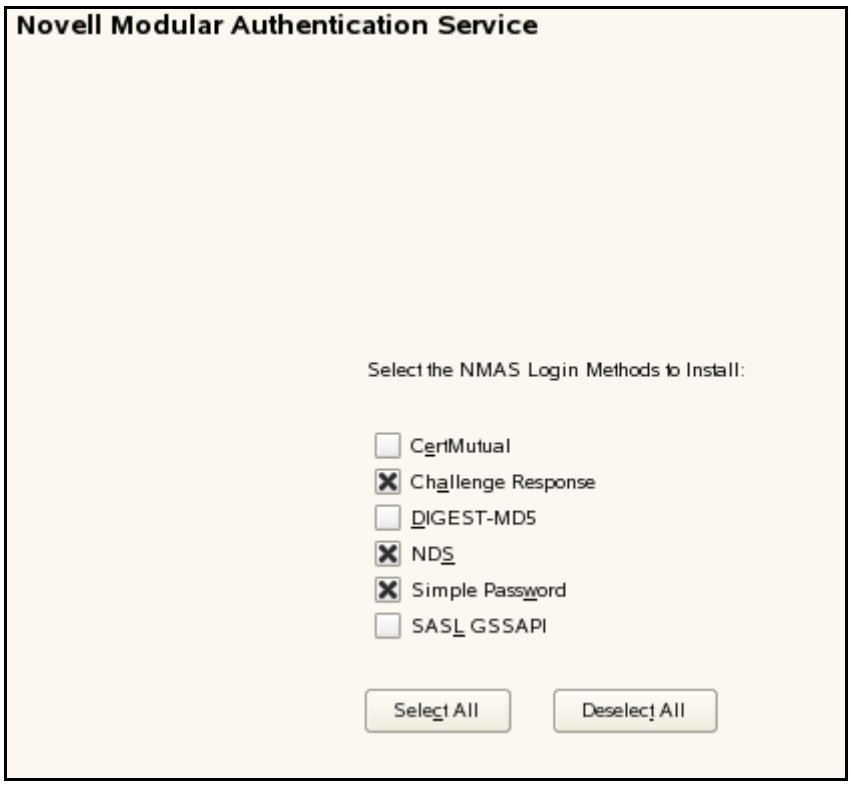
KUVA 17. Palvelinobjektin sijainti hakemistopalvelussa

Määritys mihin kontekstiin palvelinobjekti sijoitetaan. Pyrin konfiguraatioissa siihen että kokonaisuus olisi looginen ja että jokaiselle toiminnolle olisi oma ”organisaation-sa”. Tässä tapauksessa palvelinobjekti sijoitetaan organisaatioyksikköön server, joka kuuluu organisaatioon sandservice. Tässä on myös mahdollista määritellä LDAP-portit, sekä iMonitor-portit. LDAP-porteissa on kuitenkin hyvä käyttää oletusportteja (389 ja 636), koska ne ovat yleisesti käytössä monien kolmannen osapuolen sovellusten yhteyksissä. DIB-tiedoston sijaintiinkin voi vaikuttaa, joskin se on hyvä sitten dokumentoida. Novellin dokumentaatio viittaa oletuksiin, joten sitä kautta DIB-tiedoston sijainnin saa kätevästi selville.



KUVA 18. NTP ja SLP –asetukset

Normaalisti organisaation verkossa on käytössä NTP-palvelin, josta aikasynkronointi saadaan säännöllisin väliajoin. Pääsääntöisesti NTP-palvelin on eDirectory hakemistopuussa master-palvelin. Tämä siksi, että kaikilla replikoilla sekä muilla puuhun liittyneillä palvelimilla olisi sama aika. Käytän testissä paikallista aikaa. SLP-asetuksissa päätin luoda tästä palvelimesta uuden SLP Directory Agentin. SLP Directory Agent pitää tietoa hakemistopuun palvelimista ja toimii eräänlaisena DNS:nä hakemistopuuhun liittyneille työasemille ja muille palvelimille. DNS:stä ei suoranaisesti ole kyse, koska SLP (Service Location Protocol) on nimensä mukaisesti palvelujen sijaintipalvelu. SLP-palvelu kertoo objekteille, mistä palvelimesta löytyy haluttu palvelu ja yhdistää esimerkiksi vaikka työaseman autentikointiprosessin nopeimmin vastaavalle palvelimelle. SLP Scope on eräänlainen ryhmä, joka pitää sisällään listan hakemistopuussa olevista Directory Agenteista. Kun työasema tuntee SLP Scopen, on sen SLP-määrityksissä eräänlainen kahdennus.

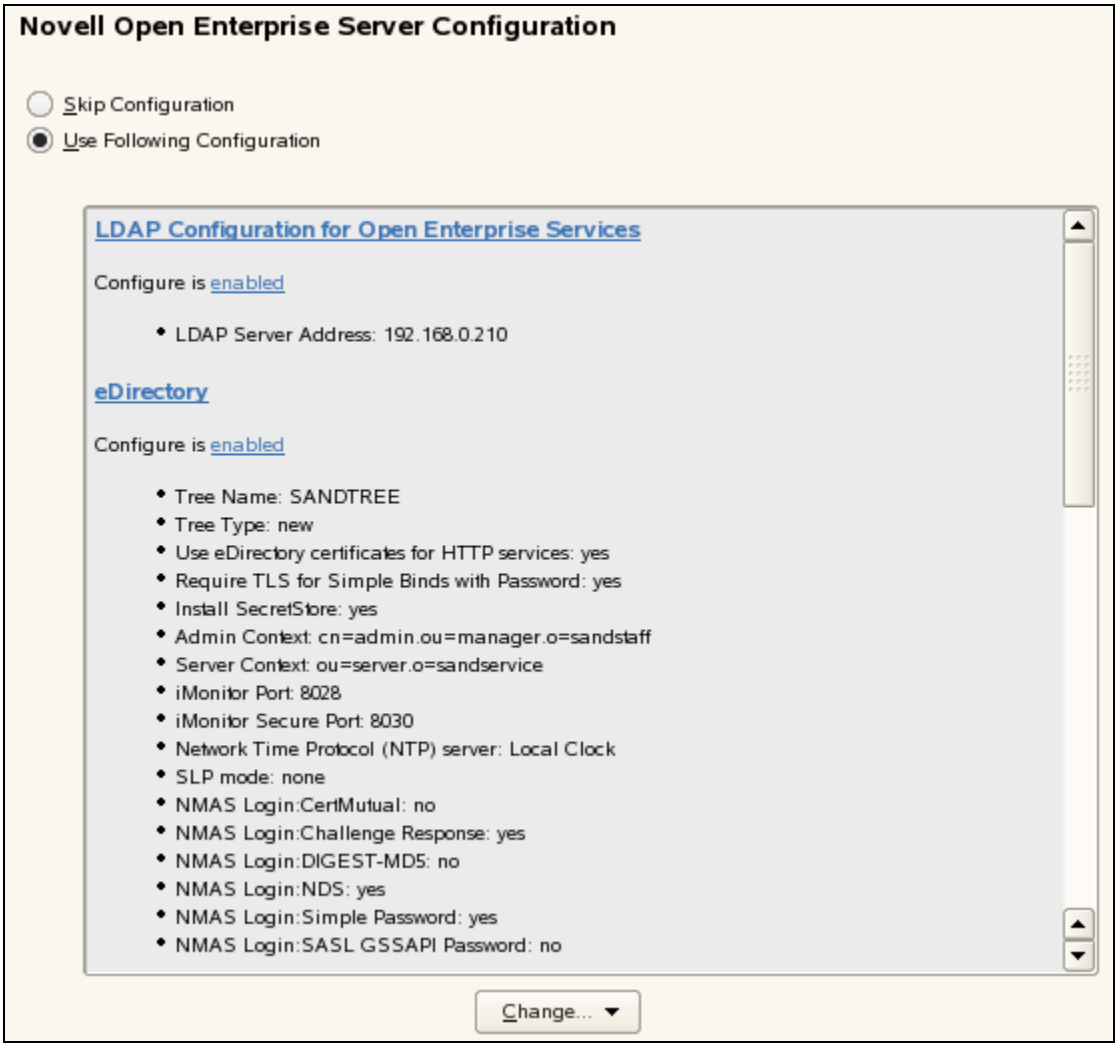


KUVA 19. NMAS-autentikointimeneltemät

CertMutual – hyödyntää yksinkertaista autentikointia ja SSL sertifikaatteja LDAP-autentikointiin.
Challenge Response – hyödynnetään muun muassa identiteetinhallinnan salasanakäytännöissä, missä joko pääkäyttäjä tai itse käyttäjä voi määrittää omalle salasanalle kysymyksen ja sille vastauksen helpottamaan unohtuneen salasanan vaihtoa.
DIGEST-MD5 – hyödyntää Simple Authentication and Security Layer (SASL) DIGEST-MD5 mekanismia LDAP-autentikointiin.
NDS – suojattu salasana yhdessä challenge-response –toiminnallisuuden kanssa. Autentikointi suoraan eDirectoryyn.
Simple Password – kuten NDS, mutta ei niin tietoturvallinen. Salasana säilötään kunkin tunnuksen SecretStoreen.
SASL GSSAPI – LDAP-autentikointi eDirectoryyn Kerberos-tiketin avustuksella.

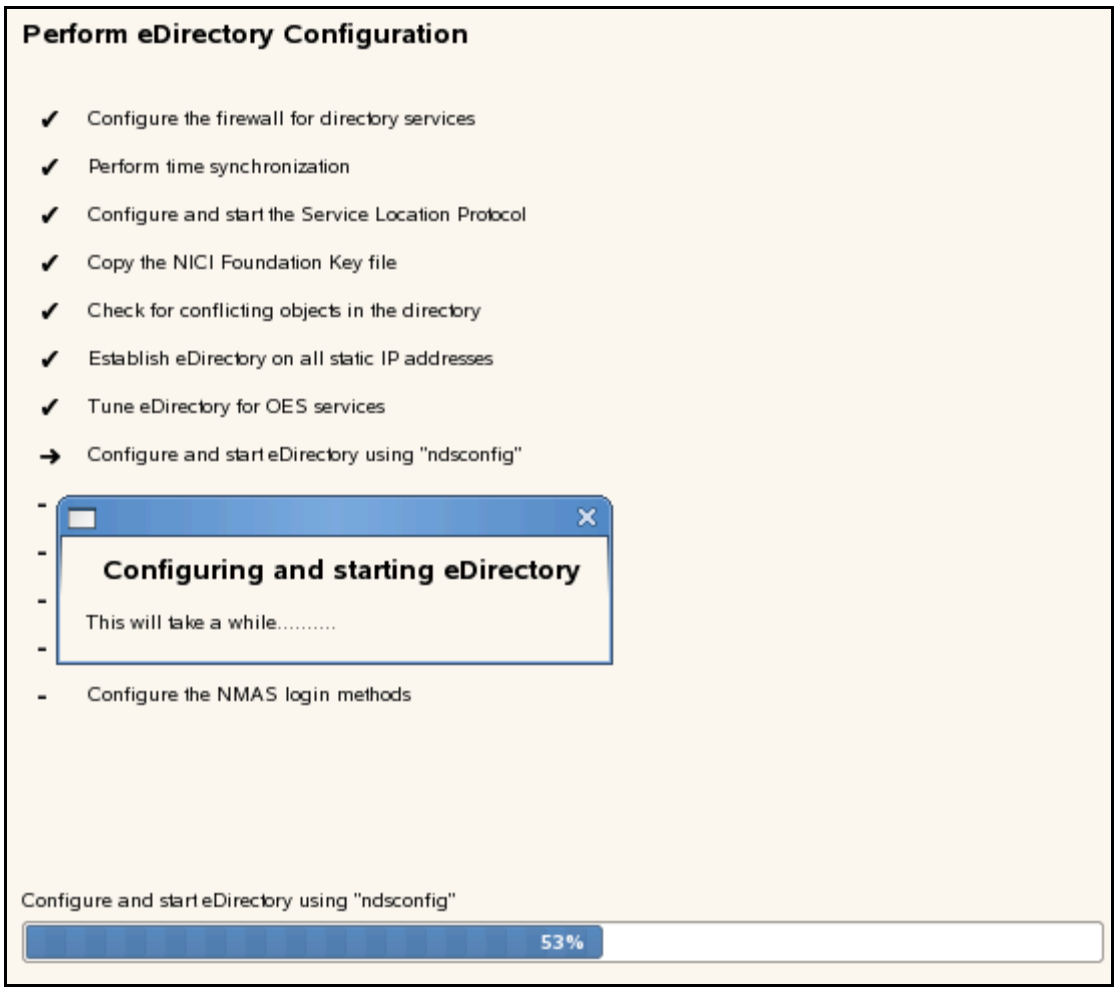
Tämä informaatio on löydettävissä eDirectoryn määritysten yhteydestä.

Oletuksena käytössä on Challenge Response ja NDS, mutta lisään tähän vielä Simple Passwordin, jotta IDM:n testaus on helpompaa. Periaatteessa normiympäristössä riittää NDS ja Challenge Response. Challenge Response oikeastaan sen takia, että unohtunut salasana on tällä mekanismilla vaihdettavissa.



KUVA 20. Yhteenveto tehtävistä konfiguraatioista

Tässä vaiheessa on vielä mahdollista tehdä muutoksia konfiguraatioihin ja mikäli konfiguraatiossa on selkeitä virheitä, ne kannattaa muuttaa tässä vaiheessa. Jälkeenpäin voi tehdä joitain muutoksia, mutta ne ovat jonkin verran haasteellisempia ja ne yleensä vaativat vähän enemmän käsityötä.



KUVA 21. Järjestelmän määrityksiä viimeistellään

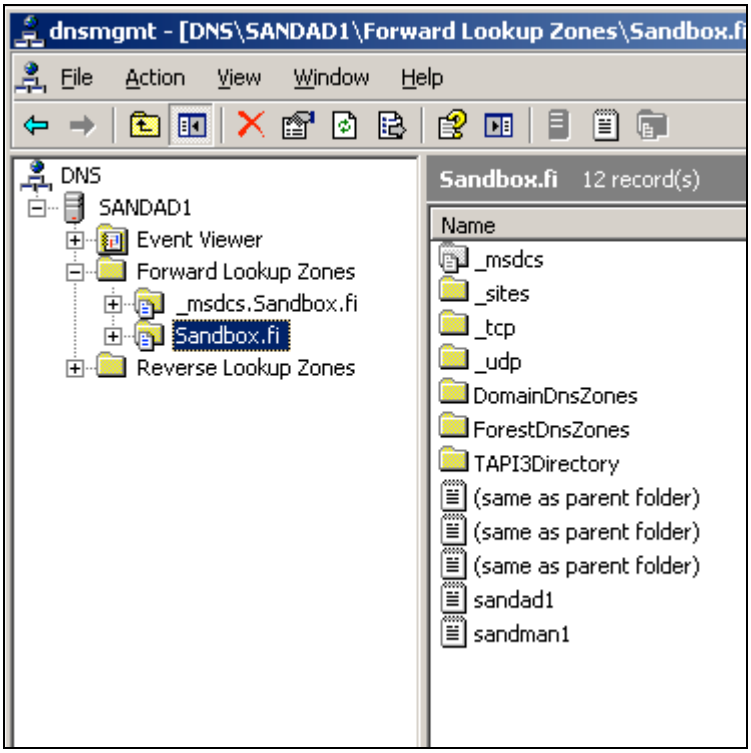
Open Enterprise Server suorittaa tarvittavat asennukset ja konfiguraatiot. Kun konfiguraatiot ovat kunnossa, asennus päättyy onnistuneesti ja eDirectory on käyttövalmis.

Linuxia ja eDirectoryn konfigurointia pidetään yleisesti hankalina osa-alueina. Edellä esitellyillä toimenpiteillä halusin osoittaa sen, että asioita on yksinkertaistettu huomattavasti. Monet asiaan vihkiytyneet hyödyntävät enemmän merkkipohjaisia sovelluksia ja komentorivejä. Itse olen sitä mieltä, että jos jossain voi säästyä ylimääräiseltä ja välttyä parametriviidakolta, ovat nämä graafiset sovellukset erinomainen valinta.

Seuraavassa luvussa esitelty Active Directoryn konfiguraatio vaatii jonkinlaisen graafisen yhteyden Windowsiin, mielellään suoraan konsoliyhteydellä. Linuxin etu kuitenkin on se, että konfiguraatiot voi tehdä merkkipohjaisesti, mikäli graafista käyttöliittymää ei jostain syystä ole käytettävissä. Monessa tapauksessa tästä on etua, kuten esimerkiksi sellaisessa tilanteessa, että järjestelmää pitäisi hallita esimerkiksi 3G-puhelimella tai pitkien etäisyyksien takaa.

5.2 Active Directoryn määritykset

En käy tässä dokumentissa läpi Active Directoryn konfigurointia, koska sen konfiguroinnin oleellisin tieto on toimialueen nimi. Mikäli DNS-palvelua ei ole määritelty, voi Active Directory –asennusohjelma luoda kyseiselle toimialueelle tarvittavan DNS-palvelun. DNS-palvelu asentuu ilman sen ihmeellisempiä toimenpiteitä ja lopputuloksena on toimiva DNS-ratkaisu.



KUVA 22. Windows 2003 Serverin DNS-hallinta

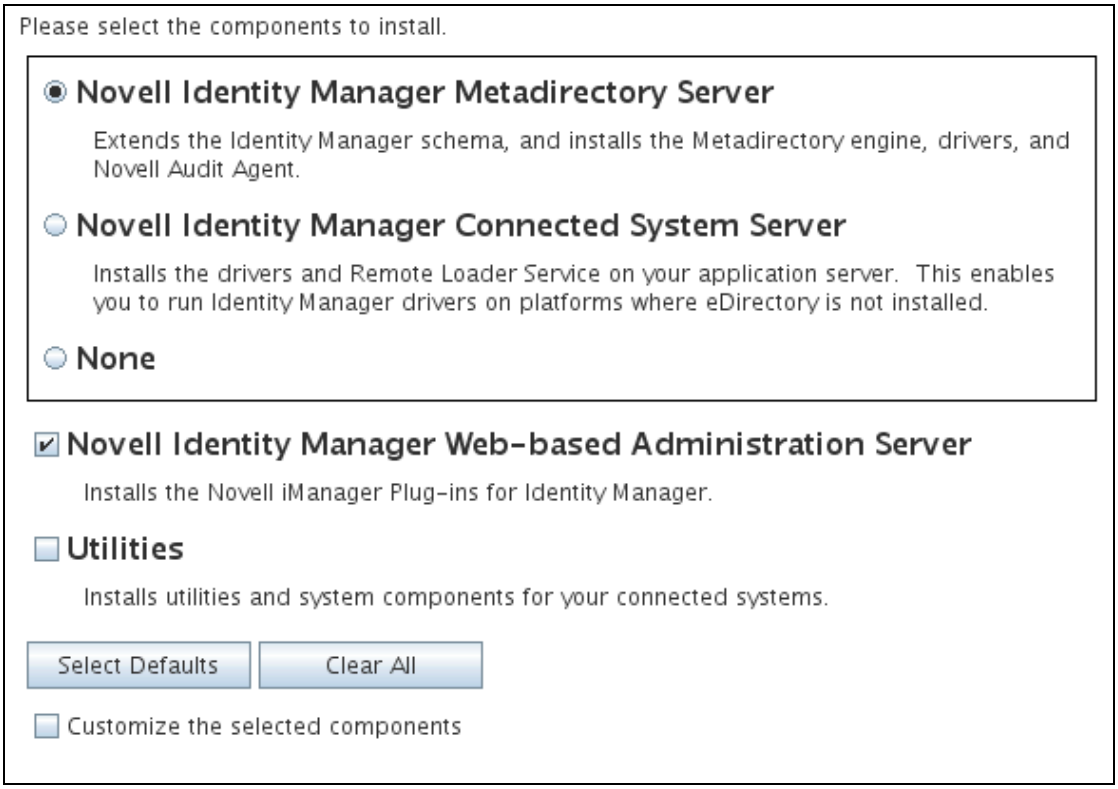
Active Directoryn asennuksen yhteydessä luodaan myös DNS-palvelu, mikäli sitä ei ole aiemmin luotu. Käytännössä mitään erityistä ei tarvitse tietää DNS:stä, jotta se voidaan luoda. Itse DNS-palvelimen ylläpitotyö on sitten kokonaan oma osa-alueensa, enkä siihen tässä keskity sen tarkemmin. Helpotan kuitenkin verkossa toimimista ja luon jokaiselle verkkoa käyttävälle palvelimelle tai työasemalle DNS host –määritykset.

DNS:n lisäksi voi määritellä myös DHCP-palvelun (Dynamic Host Control Protocol). DHCP-palvelu jakaa verkossa oleville työasemille määritellyn osoitealueen mukaisesti verkko-osoitteen, jolla työasema kommunikoi muiden verkossa olevien päätelaittei-

den kanssa. DHCP-palvelu on kätevä, mikäli työasemia on paljon ja halutaan säästää ylläpidossa. Testissäni käytän kiinteitä IP-osoitteita, koska en näe näin pienessä ympäristössä DHCP-palvelulle tarvetta.

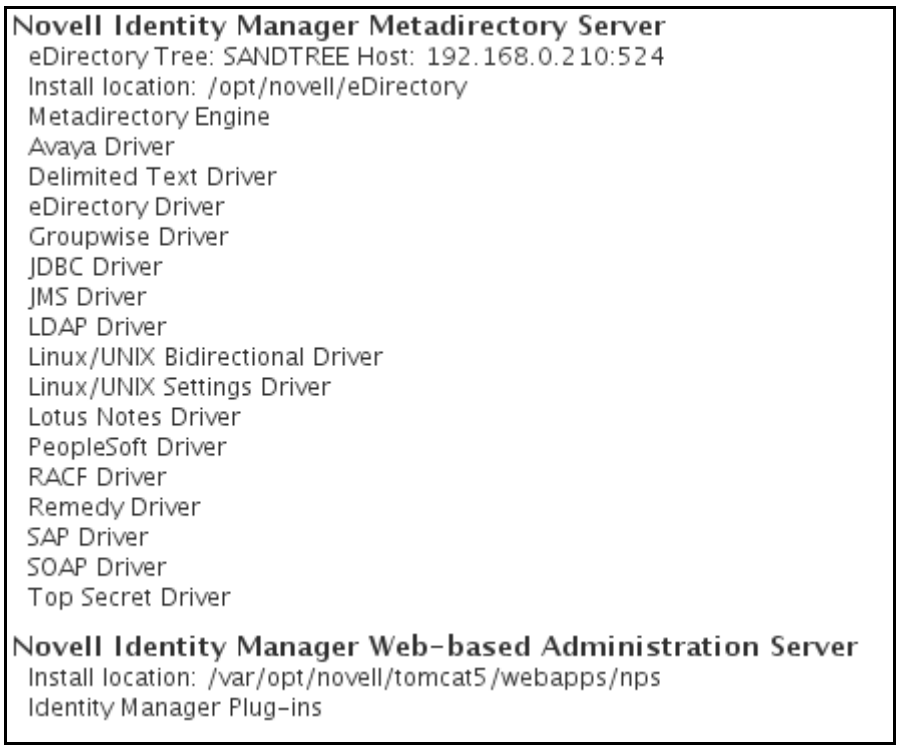
5.3 Identiteetinhallinnan määritykset

Kun käytetään Active Directorya ja eDirectorya yhdessä, tulee niissä olla yhtenäiset tiedot muun muassa käyttäjistä. Tätä varten asensin testiympäristön eDirectory-palvelimeen myös Identity Management 3.6.1 –lisäosat. Kerron tässä luvussa hiukan niistä määrityksistä mitä IDM-ympäristöön piti tehdä.



KUVA 23. IDM-asennus

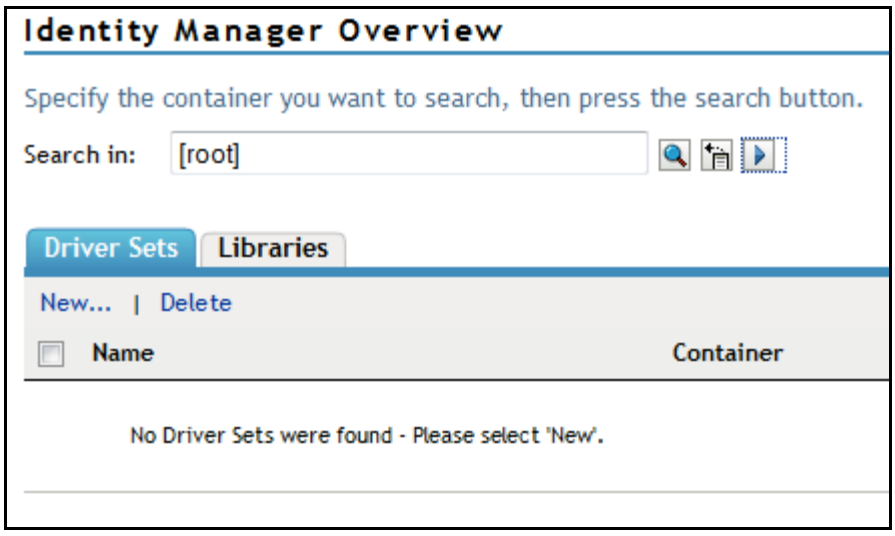
Asennusvaiheessa valittiin Metadirectory Server. Tämä siksi, koska kyseessä on se yksi ja ainoa eDirectory-palvelin. IDM-tarvitsee Active Directoryn yhteyteen myös Remote Loader –palvelun, jotta yhteys Active Directoryn ja eDirectoryn välille on luotavissa. Novell iManager Plug-ins on syytä asentaa, jotta identiteetinhallinnan määrityksiä pääsee kätevästi tekemään web-käyttöliittymän kautta.



KUVA 24. Listaus erilaisista IDM-ajureista

Kuvassa 24 näkyy Novell IDM 3.6.1:n tukemat identiteetinhallinta-ajurityypit. Novellin identiteetinhallinta on kytkettävissä kohtuullisen moneen erilaiseen ympäristöön. Asennuksen päätyttyä eDirectory-palvelin toimii nyt myös identiteetinhallinnan metahkaemistona, josta käyttäjätiedot on tarkoitus synkronoida myös Active Directoryn käyttöön. Yksinkertaisimmillaan identiteetinhallinnan ajuri voidaan luoda siten, että se synkronoi käyttäjätunnuksen ja salasanan, ei muuta informaatiota. Myös nimi- ja sijaintitiedot on järkevää synkronoida, jotta tiedetään mistä tunnuksesta on kyse. Tässä projektissa yksilöivä tekijä on käyttäjätunnus (cn, common name), mutta se voisi olla myös henkilönumero (employeeNumber) tai vastaava ID-numero (UID).

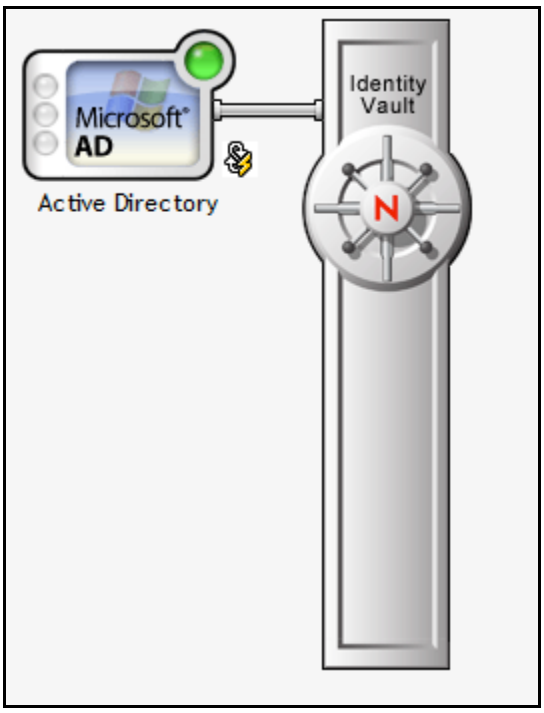
Tein loput konfiguraatiosta iManagerilla, koska Novell Identity Manager – asennusohjelma asensi siihen automaattisesti IDM:n hallintaan tarvittavat lisäosat. Seuraavassa on esitelty ajurin luomisprosessi pääpiirteissään. Kun tämän opinnäytetyön ideana ei ollut käydä itse identiteetinhallintaa läpi, vaan sen hyödyntämistä, en sen tarkemmin panosta itse konfiguraatioihin. Pyrin kuitenkin nostamaan oleelliset asiat esille, jotta itse idea tulisi selväksi.



KUVA 25. Identiteetinhallinnan ajurit

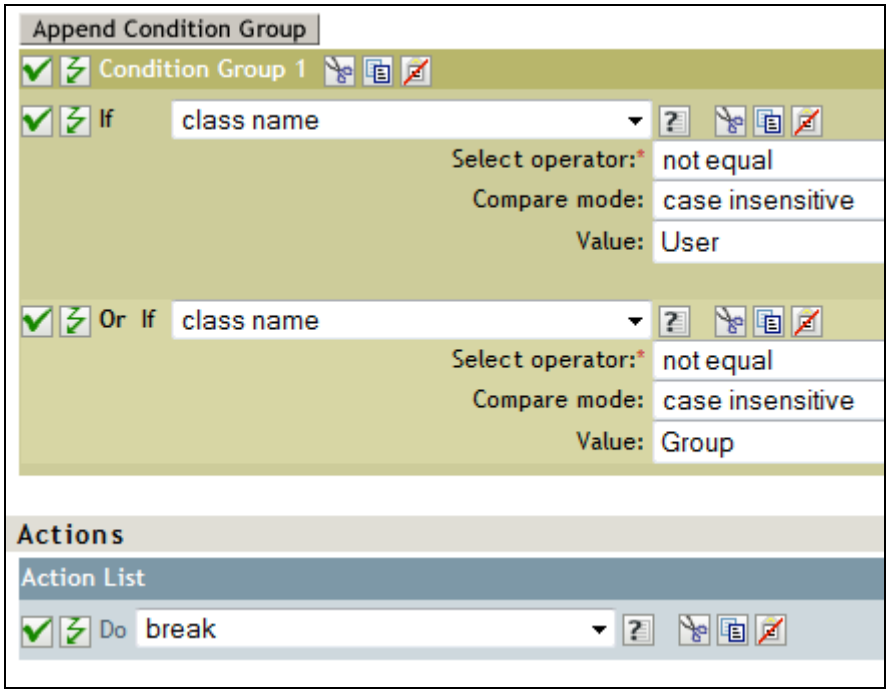
Alkutilassa tilanne on kuvan 25 mukainen. Uusi ajuri pitää luoda, jotta tietoja voidaan synkronoida hakemistopalveluiden välillä. Kun ajuri luodaan, pitää ajurin luontivaiheessa tietää missä käyttäjätunnukset sijaitsevat ja luonnollisesti tunnukset, millä käyttäjätunnuksia luodaan molempiin hakemistopalveluihin. Novellin suositus on, että testivaiheessa voi käyttää Active Directoryn Administrator-tunnusta, mutta myöhemmässä vaiheessa kannattaa luoda oma tunnus käyttäjätietojen synkronointiin. Käytän testeissäni Administrator-tunnusta, sekä eDirectoryn pääkäyttäjätunnusta. Lisäksi olisi hyvä, että metahakemistopalvelimella olisi nimitiedot toimialueesta ja toimialueen ohjainkoneesta. Tästä syystä myös metahakemistopalvelimen DNS-määritykset olisi hyvä olla kunnossa. Mikäli DNS-määrityksissä on epäselvää, kannattaa käyttää DNS-nimien sijasta suoraan IP-osoitteita. Itse olin määrittänyt DNS-palveluun kaikki tarvittavat tiedot, joten pystyin käyttämään DNS-nimiä konfiguroinneissa. Konfiguraation luomisessa täytyy olla tarkkana. Itse tein ajurin luontivaiheessa virheen, jonka paikallistamiseen meni turhaa aikaa. Tästä syystä kannattaa kerätä konfiguraatiotiedot johonkin dokumenttiin ja siitä sitten siirtää ne ajurin luontiprosessiin.

Kun ajuri on valmis, se ei käynnisty automaattisesti, vaan se pitää käynnistää. Seuraavassa kuvassa näkyvä vihreä pallo osoittaa ajurin olevan käynnissä, mikä ei vielä takaa sitä että ajuri toimisi oikein.



KUVA 26. Ajuriasetelma

Ajuriasetelma (Driver Set) on kokonaisuus joka pitää sisällään Identity Vaultin (meta-hakemisto) ja ajurin Active Directoryyn. Identity Vault on säilö käyttäjäobjekteille, joista sitten siirretään paikasta toiseen tunnuksia, joiden ajureihin merkityt säännöt toteutuvat. Oletuksena ajuri ei siirrä esimerkiksi ryhmäobjekteja, vaan tämä toiminnallisuus pitää lisätä ajurin Creation Policy –käytäntöön.



KUVA 27. Käyttäjätunnuksen ja ryhmän luontisääntö

Alun perin ajurin toiminta pysähtyi siihen, jos kyseessä oli jokin muu objekti kuin käyttäjä. Jotta sain myös ryhmäobjektit siirtymään, lisäsin toisen OR-ehdon ehtoryhmään (Condition Group 1):

Select operator = not equal
Compare mode = case insensitive
Value = Group

Tämän jälkeen ajuri voi pudottaa loput objektit, kuten Actions-kentässä onkin määriteltynä *break*.

Ajuri itsessään on nyt valmis. Toinen toimenpide mikä piti tehdä, oli salasanakäytäntöjen luominen. IDM-ajuri synkronoi salasanat Distribution Passwordin avulla, joten sen synkronointi Universal Passwordin kanssa pitää olla aktivoituna salasanakäytännöissä. Loin siis salasanakäytännön (Password Policy) ja liitin sen siihen käyttäjäkontekstiin, missä käyttäjät sijaitsivat.

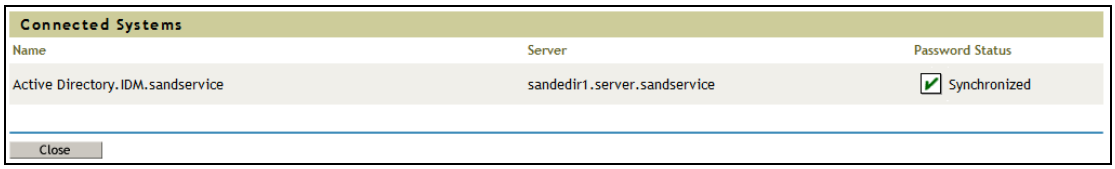
Password Policy Summary

Name	UserPasswordPolicy	
Description		
Universal Password		
Options	Enable Universal Password	true
	Enable the Advanced Password Rules	true
	Synchronize NDS password when setting Universal Password	true
	Synchronize Simple Password when setting Universal Password	true
	Allow user to retrieve password	false
	Allow admin to retrieve passwords	false
	Allow the following to retrieve passwords	false
	Synchronize Distribution Password when setting Universal Password	true
	Verify whether existing passwords comply with the password policy (verification occurs on login)	false

KUVA 28. Salasanakäytännöt

Jotta salasanan synkronointi toimisi, tulee Universal Password –toiminnon olla käytössä. Kun tunnus luodaan ja tunnuksen luontivaiheessa tarkastetaan käyttäjäkontekstista, että onko salasanakäytäntöjä, tulee kuvassa 28 kuvattu sääntö voimaan. Tällöin

tunnukseen tulee käyttöön Universal Password, joka synkronoituu Distribution Passwordin kanssa. Salasanan synkronointi on helppo tarkastaa iManagerin kautta.



KUVA 29. Salasanan synkronoituminen

Kuten kuva 29 näyttää, on testitunnuksen salasana synkronoitunut järjestelmien välillä. Password Status näyttäisi tilana Not Synchronized, mikäli salasana jostain syystä ei synkronoituisi.

5.4 Windows XP –työaseman toiminta

Windows XP –testityöasemaan olen asentanut Novell Client 4.91 SP5 –sovelluksen, joka hoitaa kommunikaation eDirectoryn kanssa. Aiemmin mainitsin siitä, että käyttäjien kotihakemistot sijaitsevat Novellin NSS-tiedostojärjestelmässä eDirectory-palvelimella. Tämä tarkoittaa sitä että, jotta pääsisin käsiksi kotihakemistoihin, täytyy työaseman autentikoitua eDirectoryyn ja luoda NCP (Netware Core Protocol) -yhteys palvelimeen. NCP on Novellin oma protokolla, jonka kautta siirretään käyttäjädataa eli esimerkiksi levy-yhteydet eDirectoryyn. Novell Clientin asetuksiin määritin yhteyden eDirectoryn palveluihin, kuten LDAP-autentikointiin.

Novell Clientin lisäksi liitin työaseman Active Directory –toimialueelle. Active Directory –autentikointi mahdollistaa itse Windowsiin kirjautumisen, mitä Novell Client ei yksinään mahdollista. Jotta työasemaan kirjautuminen onnistuisi pelkillä Novell-sovelluksilla, tarvitaan myös Novell ZENworks Desktop Management tai Novell ZENworks Configuration Management –työasemahallinnan lisäosat. Nyt näitä komponentteja ei tarvita, koska käyttäjätiedot Windowsiin saadaan toimialueelta. Ja jotta kirjautuminen olisi sujuvaa, tein yhden rekisteriasetuksen, joka poisti edellisen kirjautuneen käyttäjän tiedot kirjautumisikkunassa.

Kirjautuminen työasemaan toimi moitteetta. Käyttäjä autentikoitui sekä eDirectoryyn, että Active Directoryyn. eDirectory tarjosi käyttäjälle kotihakemiston ja Active Directory Windows-identiteetin. Viiveitä ei ollut, mikä sinänsä ei ole ihme, koska käyttäjä-

määrä hakemistopalveluissa on niin pieni. Käyttäjän salasanan vaihdossa oli sellainen ominaisuus että sitä ei voinut onnistuneesti vaihtaa kuin eDirectoryyn. Tämä ei sinänsä ole mikään ongelma, koska salasanan synkronointi järjestelmästä toiseen toimii moitteetta. Ongelmaksi muodostui salasanan kompleksisuus. Salasanaa vaihdettaessa Active Directoryyn tuli virheilmoitus jossa väitettiin, ettei salasana täytä hakemistopalvelun vaatimuksia salasanan kompleksisuudesta. Tämä ei pitänyt paikkaansa, koska olin poistanut salasanalle asetettavat vaatimukset Active Directoryn salasanakäytännöissä. Tällainen ongelma ei tällaisessa ympäristössä ole oikeastaan ongelma, vaan sellainen asia, joka pitää ohjeistaa. Sekalaisen ympäristön käyttämisessä on muutenkin haasteita.

5.5 Arvio kokonaisuudesta

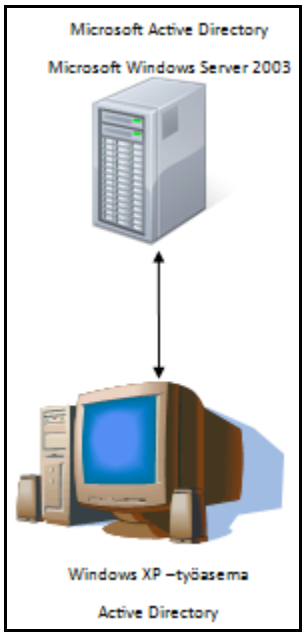
Tällaisenaan järjestelmän käyttö ei välttämättä ole kovin järkevää. Työasemaan siis täytyy asentaa Novell Client –lisäosat, määritellä eDirectory-liitännät ja pitää vielä huoli Active Directory –yhteydestä. Tällaisessa tilanteessa kannattaa miettiä sitä, että pystyykö Novell Storage Systems (NSS) –yhteyksiä hyödyntämään suoraan Windowsissa, vai onko migraatio Windowsin levypalveluihin järkevä vaihtoehto.

Jos levypalvelut ovat ainoa syy käyttää eDirectorya, kannattaa miettiä levypalveluiden migraatiota Windowsin levypalveluihin. Mielestäni eDirectoryn roolia ei kannata alkaa korostaa liikaa, kun on kyse työasemaan autentikoitumisesta. Mikäli epäilystä herättää Active Directoryn kyky hallita suuria objektimääriä, voi toimialueita luoda useampia ja niiden välille luottosuhteita. MAMKin kokoisessa organisaatiossa ei edes tarvita useita toimialueita, koska objektimäärä ei todennäköisesti nouse mitenkään kriittiselle tasolle.

Muuten edellisen kaltaisen järjestelmän rakentaminen on täysin mahdollista ja loppujen lopuksi aika yksinkertaista. Tällainen järjestelmä olisi järkevä sellaisena, että eDirectory toimisi metahakemistona, johon henkilöstöhallinnosta tulisi käyttäjätiedot. Tästä tiedot synkronoituisivat Active Directoryyn työasemien käytettäväksi. Tällainen toimintatapa kuitenkin mahdollistaisi sen, ettei välttämättä tarvitsisi ensimmäisessä vaiheessa alkaa levypalveluita siirtää paikasta toiseen. Migraatio voisi olla pidemmän tähtäimen suunnitelma ja sitä voisi tehdä pala kerrallaan.

6 DEDIKOITU ACTIVE DIRECTORY -YMPÄRISTÖ

Dedikoitu Active Directory –ympäristö on hyvin tyypillinen tapa toteuttaa verkon infrastruktuuri. Testiympäristön rakentaminen oli yksinkertainen prosessi, mutta migraatioon liittyvät haasteet vaativat enemmän työtä.



KUVA 30. Active Directory –ympäristö.

MAMKilla on jo olemassa Active Directory tiettyjä toimintoja varten, joten täysin uutta järjestelmää ei olisi tarpeen rakentaa. Puhdas Active Directory (kuva 30) on aina hyvä ratkaisu, koska Windows-työasemat tukevat parhaiten nimenomaan Active Directorya. Tuki tälle on integroituna Professional- ja Enterprise -tason käyttöjärjestelmissä. Käyn seuraavassa läpi periaatteellisella tasolla sen, mitä kaikkea vaaditaan, jotta migraatio eDirectorysta Active Directoryyn onnistuisi.

Edellisessä luvussa kävin läpi sitä, kuinka Active Directory käyttäytyy Novell eDirectoryn kanssa. Active Directory itsessään ei ole mikään vaativa asentaa ja konfiguroida, enemmän vaatimuksia tulee siitä, miten tietoa siirretään järjestelmästä toiseen. Testiympäristö on aina testiympäristö, mutta siitä saa kuitenkin viitteitä siitä mitä mahdollisia ongelmia migraatio voi tuoda tullessaan.

Dedikoitu Active Directory käytännössä tarkoittaisi sitä, että kaikki käyttäjätiedot olisivat Active Directoryn varassa. Luvussa 2.5 tehdyn vertailun perusteella Active Di-

rectory ei olisi kovin hyvä vaihtoehto suurelle käyttäjämäärälle. Tästä syystä onkin järkevä kartoittaa palvelut ja sitä kautta arvioida tarvetta esimerkiksi metahakemistolle.

6.1 Novell-verkon palveluiden kartoitus

Verkkoon tarjotaan varsin laajalla kirjolla palveluita, eikä kaikista Novell-palveluista olekaan syytä luopua. Tärkeintä on määrittää ne palvelut, joita työasemat käyttävät ja miten ne ovat siirrettävissä Microsoftin järjestelmiin. Tällaisessa tilanteessa testausympäristön rooli tulee voimakkaasti esille. Voi nimittäin olla, että joitakin palveluita ei kannata siirtää, vaan ne kannattaa luoda uudestaan uuteen järjestelmään tai antaa olla vanhassa järjestelmässä.

Vaikka onkin kyse hiukan vähemmän käytetystä hakemistopalveluratkaisusta, eli eDirectorysta, ovat sen palvelut kuitenkin tavalla tai toisella standardeja. Suurin osa on siis siirrettävissä joko sellaisenaan tai sitten pienen muunnoksen kautta järjestelmästä toiseen. Seuraavassa käyn hiukan tarkemmin läpi näitä palveluita joiden siirto olisi todennäköinen.

6.1.1 Hakemistopalvelu ja levypalvelut

Hakemistopalvelu on oleellisin osa järjestelmää. Käyttäjätunnustietoa synkronoidaan useammankin eri hakemistopalvelun välillä, kuten jo aikaisemmin mainitsin. Tästä syystä hakemistopalvelun osalta muutos ei ole kovinkaan mittava. Suurin työ onkin työasemissa, koska niistä pitäisi tällöin poistaa Novell Clientit ja liittää työasemat toimialueelle. Testattavaa riittäisi, esimerkiksi ryhmäkäytäntöjen ja levyliitosten osalta. Hakemistopalvelun informaatio on helposti siirrettävissä hakemistopalvelusta toiseen. Identiteetinhallintaratkaisuilla ongelma on helposti ratkaistavissa. Rakentamassani testiympäristössä kaikki tiedot synkronoituivat erinomaisesti hakemistopalvelusta toiseen, mikä suoraan mahdollistaisi pelkän Active Directoryn käytön työasemissa. Vaikka työasemat käyttäisivätkin pääautentikointilähteenä Active Directorya, jättäisin eDirectoryn siitä huolimatta hoitamaan metahakemiston roolia.

Levypalveluiden siirtäminen Microsoftin järjestelmään onkin sitten haastavampi osa prosessia. Pienillä epävarmoilla toimenpiteillä nykyisen Novell NSS -levyjärjestelmän

voisi ottaa käyttöön myös Windows-ympäristössä, mutta sen käytöstä ei ole kovin vakuuttavia kokemuksia eikä sen integroituvuus Active Directory -ympäristöön ole kovin hyvä. Voisi kuvitella, että tieto siirtyy ”Copy/Paste” -periaatteella, mutta totuus on se, että suurten datasiirtojen tekeminen on iso ja haastava prosessi. Mielestäni järkevin vaihtoehto tietojen migraatioon olisi varmuuskopiointi ja siitä palautus. Haasteellisin osa olisi käyttöoikeuksien siirtäminen Novell-ympäristöstä Active Directoryyn. Tämä onkin syytä käydä läpi ennen suurempia muutoksia. Testiympäristössä tietojen siirto onnistui ongelmitta. Tämä ei sinänsä ole mikään ihme, koska siirrettävän tiedon määrä oli vähäinen. Ainakin Novellilla on olemassa tuotteita, joilla käyttöoikeudet pystyy siirtämään joko datan mukana tai sitten datan siirron jälkeen. Novellilla ja Microsoftilla on hiukan erilainen lähestymistapa oikeuksien periytymiseen hakemistorakenteissa. Novellin tiedostojärjestelmissä pystyy varsin tarkkaan määrittelemään sen, mihin milläkin objektilla on oikeus. Windowsin tiedostojärjestelmässä annettu oikeus periytyy seuraaville tasoille ja näin ollen hankaloittaa tietojen yksilöimistä.

Uusien tunnusten osalta tämä ei olisi mikään ongelma, koska ne voidaan osoittaa uusiin levyalueisiin ja sitä kautta myöntää käyttöoikeudet suoraan Windowsin levyjärjestelmiin. Helpoin tapa tällaisessa olisikin luoda järjestelmä alusta alkaen uusiksi.

6.1.2 Muut tarjottavat palvelut

Myös MAMKin verkon ulkopuolelle tarjotaan esimerkiksi tiedostopalveluita, eli mahdollisuutta päästä mistä tahansa omalle kotiverkkolevylle. Mikäli tiedostopalvelut siirrettäisiin Microsoftin levypalveluihin, pitäisi Microsoftilta löytyä joku vastaava tapa päästä käsiksi henkilökohtaisiin tiedostoihin myös työpaikan verkon ulkopuolella. Mahdollisia ratkaisuja on olemassa, mutta toimivimman ratkaisun löytäminen jää käytännössä testattavaksi.

Nykyinen sähköpostijärjestelmä voitaisiin säilyttää, koska se toimii omalla käyttäjätietokannalla, joskin on hallittavissa samoilla työkaluilla kuin muukin eDirectory. Mutta mikäli sähköpostijärjestelmä pitäisi vaihtaa, vaatisi sen migraatio tarkkaa suunnittelua. Toki vaihtoehtona olisi se, että vaihdetaan järjestelmä ja käynnistetään uusi palvelu tyhjästä ja kukin käyttäjä siirtää itse haluamansa postit uuteen järjestelmään.

Verkon keskitetty hallinta on pääsääntöisesti toteutettu Novell ZENworks -työasemien hallintajärjestelmällä, joka on sidoksissa eDirectoryyn. Novell on tehnyt uuden ZENworks-tuotteen, joka ei ole sidoksissa mihinkään hakemistopalveluun, vaan on liitettävissä eDirectoryn ohella myös Active Directoryyn. Tätä uutta hallintaratkaisua on jo pilotoitu parissa luokkatilassa ja sen käytöstä on vielä hiukan hatarat kokemukset. ZENworksille vaihtoehtona on myös Microsoftin oma hallintajärjestelmä Microsoft System Center Configuration Manager, jonka edeltäjä on Systems Management Server (SMS).

Nykyinen tulostuspalvelu toimii Novell iPrint/NDPS -järjestelmässä, mikä oikeastaan voisi olla sellaisenaan ja tulostimia voisi siirtää vähitellen Active Directoryn hallitsemaksi. PCounter -tulostuksenhallintajärjestelmä ei ole riippuvainen mistään tietystä hakemistopalvelusta, joten sen pystyisi määrittelemään myös hyödyntämään Active Directoryssa olevia käyttäjätunnuksia.

6.2 Miten toteutin?

Käytännössä tällaisen toteutus on pitkä prosessi ja se on tehtävä vaiheittain. Testiympäristössä sain käyttäjätiedot siirtymään eDirectorysta Active Directoryyn. Tämä käyttäjätunnusten siirto voi olla joko kertaluontoinen toimenpide tai sitten pidemmän ajanjakson prosessi. Käyttäjätiedon synkronointi oikeastaan olikin yksinkertaisin prosessi. Enemmän ongelmia tuotti käyttäjien kotihakemistojen migraatio. Itse tietojen siirto levyltä toiselle oli yksinkertaista, mutta käyttöoikeuksien osoitukset eivät niinkään. Oikeastaan kotihakemistojen käyttöoikeudet oli helppo määritellä, koska yhdellä kansiolla oli yksi käyttäjä ja sillä käyttäjällä tietyt oikeudet kansioonsa. Mutta muiden hakemistojen, jotka sijaitsivat yhteisellä levyalueella, siirto tuotti ongelmia. Käytännössä tämä tarkoitti sitä että käyttöoikeudet piti siirtää käsin ja näin pienessä ympäristössä se vielä toimiikin niin. Kun suurempia tietomääriä pitäisi siirtää kaikkine oikeuksineen, on sitä varten olemassa maksullisia tuotteita kuten Quest NDS Migrator. Tällaista tuotetta en testannut, koska se tuli vastaan vasta hyvin loppuvaiheilla prosessia. On kuitenkin todennäköistä, että joko tuota tai vastaavaa tuotetta tullaan hyödyntämään, jos MAMKilla tehdään päätös järjestelmien migraatiosta

Tulostimien migraatiolle uskoisin olevan hyviä ja käteviä konsteja. Tutkittuani hiukan erilaisia keskusteluryhmiä, tuli vastaan joitakin tuotteita, jotka mahdollistaisivat kir-

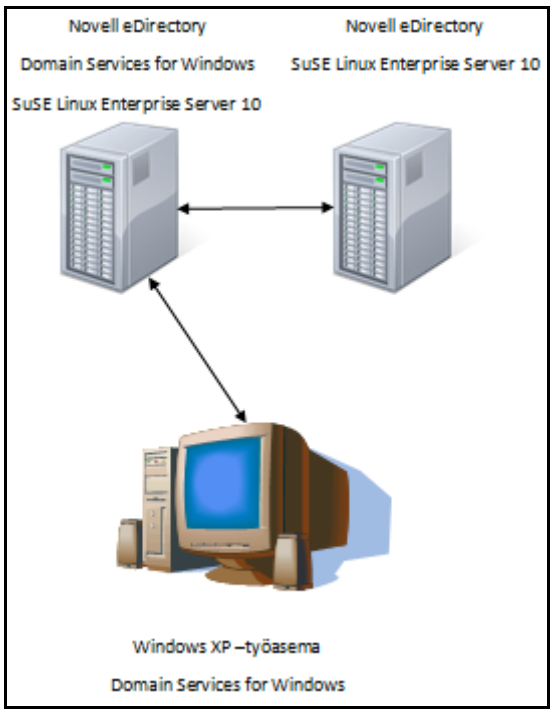
joittimien siirron iPrintistä Active Directoryyn. Yksi tällainen vaihtoehto olisi Printer Properties Pro: Migrator joka ainakin mainosten perusteella pystyy helposti siirtämään niin NDPS-tulostimet kuin iPrint-tulostimetkin.

6.3 Yhteenveto puhtaan Active Directory -ympäristön käytöstä

eDirectoryn palveluita on hankalampi siirtää sellaisenaan AD:n käyttöön. Monien palveluiden siirto varmasti onnistuukin ilman suuria ongelmia. Levy- ja tiedostojärjestelmät ovat yksi haasteellisimmista kokonaisuuksista. Ei niinkään siksi, että tiedostojärjestelmiä olisi vaikea yhdistellä toisiinsa, vaan siksi että suurien datamäärien siirrolle ei aina ole yksiselitteistä keinoa.

7 EDIRECTORYN KÄYTTÖ ACTIVE DIRECTORYNA

Tämä testiympäristö oli haastavin rakentaa ja vaatikin eniten aikaa. Aiemmin luvussa 5 esitellystä järjestelmästä hyödynnettiin eDirectory-palvelin, johon liitin vielä toisen palvelimen. Kerron tässä luvussa hiukan tarkemmin tästä kokonaisuudesta.



KUVA 31. Domain Services for Windows –ympäristö

Novell on kehitellyt järjestelmän, jolla se pystyy jäljittelemään Active Directorya. Käytännössä Novell SuSE Linux Enterprise Server 10:iin asennettuun Open Enterprise Server 2:een asennetaan Domain Services for Windows -palvelu, joka saadaan näyttämään aivan Active Directorylta (kuva 31). Windows–työasema näkee palvelun oikeana Active Directory -palvelimena, mutta tällaisessa tapauksessa voidaan hyödyntää eDirectoryssa olevia käyttäjätunnuksia sekä sen tarjoamia levypalveluita. Työasemiin ei tällöin tarvitse asentaa mitään Novellin sovelluksia, vaan voidaan hyödyntää Windowsiin integroituja komponentteja.

7.1 Vaadittavat komponentit

Kuten jo aikaisemmin mainitsin, luodaan tässä toteutustavassa palvelu osaksi eDirectorya. Tällöin mitään migraatiota hakemistopalvelusta toiseen ei tarvitse tehdä ja kaikkia eDirectoryn palveluita, joita jo luvussa 4 listasin, voidaan hyödyntää sellaisenaan.

On kuitenkin muutamia asioita, joita tulee ottaa huomioon otettaessa käyttöön Domain Services for Windows (DSfW) -palvelua. Ensinnäkin, hakemistopalvelun skeema pitää laajentaa vastaamaan DSfW:n vaatimuksia. Toisekseen, on syytä tehdä tuotantoympäristöstä tarkka kopio testiympäristöön, jotta tuotantoympäristö ei sotkeudu mahdollisten epäonnistuneiden konfiguraatioiden takia. Novell eDirectory on sikäli kuitenkin turvallinen hakemistopalvelu tehdä muutoksia, että skeeman laajennukset voidaan poistaa ja *Hot Continuous Backup* hoitaa varmistuksen sen mukaan mitä tarve on. Kolmantena asiana on itse varmistus. On syytä ottaa myös koko hakemistopalvelu varmistusnauhalle, jotta tietokanta voidaan palauttaa sellaisenaan takaisin. Suosituksena on, että DSfW eriytetään omalle palvelimelle, jotta muut komponentit (kuten IDM) eivät syystä tai toisesta vikaantuisi. Muutenkin eriyttäminen on suotavaa, koska kyseessä on hyvin erityyppinen palvelu muihin Novell-palveluihin verrattuna. Toisekseen, DSfW tarjoaa sellaista roolia verkkoon, joka ei täysin ole Novell-palvelu.

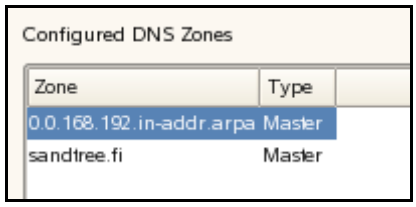
DSfW asentaa myös DNS:n, joten myös DNS-palvelun täytyy olla kunnossa. DSfW on toimialueen ohjauskone, joten on loogista, että myös DNS-määritykset ovat kunnossa, erityisesti tällaisessa tapauksessa, jossa kyseessä on ensisijainen palvelin toimialueella. Linuxin mukana tuleva named-nimipalvelu on helppo konfiguroida ja sitä kautta järjestelmä saa kätevästi nimitiedot kaikkialle missä niitä tarvitaan.

DSfW on siis osa Novell Open Enterprise Server 2 –lisäosaa, joka on asennettavissa SuSE Linux Enterprise Server 10 SP3:een. Domain Services for Windows asennetaan käynnistämällä Open Enterprise Server –tuotteiden asennus ja konfiguraatio YaST –järjestelmänhallintatyökaluilla. Käytän työssäni graafisia työkaluja, koska tällöin saa selkeän kuvan siitä mitä pitää tehdä ja toisekseen, näkee suoraan sen mitä on tekemässä ja mitä valintoja pitää tehdä.

7.2 DNS-nimipalvelun määritykset

Koin tarpeelliseksi ottaa tässä kantaa myös DNS-määrityksiin, koska järjestelmä on käytännössä riippuvainen sen olemassa olosta. DSfW:n asennuksessa asentuu oikeastaan kaksi nimipalvelua, Linuxin oma named-nimipalvelu ja Novellin oma novell-named –nimipalvelu. Novell-named –nimipalvelu tosin hyödyntää varsinaista Linuxin nimipalvelua, mutta novell-named on konfiguroitavissa myös iManager-hallintasivuston kautta. Käytin kuitenkin Linuxin omaa työkalua, joka löytyy YaST:n Network Services –osiosta.

DNS-palvelimen määrityksissä on oltava ainakin DNS Forward Lookup Zone, mutta myös Reverse DNS on hyvä olla olemassa, jotta IP-osoitteet saadaan käännettyä nimelle. Omassa DNS-ympäristössäni loin molemmat zonet.



KUVA 32. DNS zonet

Forward Lookup Zone on käytännössä se toimialue, jossa DSfW on käytössä. Testiympäristööni loin zonen nimellä sandtree.fi, koska se toimi myös toimialueeni nimenä DSfW:ssä. Reverse DNS nimetään aina IP-osoiteavaruuden perusteella, kuten omassa DNS-palvelussani olen nimennyt sen 0.0.168.192.in-addr.arpa. DNS-merkinnät ovat kummallakin zonella hiukan erilaiset ja Linuxin tapa tulkata näitä on jonkin verran monimutkaisempi verrattuna Windowsin DNS-palveluun.

```
$TTL 2D
@               IN SOA          sanddsfw1.sandtree.fi.
root.sanddsfw1.sandtree.fi. (
                                2010110210      ; serial
                                3H              ; refresh
                                1H              ; retry
                                1W              ; expiry
                                1D )            ; minimum

sandtree.fi.    IN NS           sanddsfw1.
sanddsfw1       IN A            192.168.0.214
sandedir1       IN A            192.168.0.210
```

KUVA 33. Sandtree.fi –DNS-toimialueen merkinnät

Edellisessä kuvassa on merkittynä tärkeimmät palvelut, joita halutaan kutsua nimellä. Kuva 33 on sandtree.fi –zonen konfiguraatiotiedostosta, joka sijaitsee Linux-palvelimella kansiossa /var/lib/named/master/. Erityisen tärkeä oli tämä sanddsfw1, koska se toimi myös itse nimipalvelimena. Sandedir1 näkyy listassa siksi, koska määritin työasemien Novell Client –asetukset siten, että niitä kutsuttiin nimellä. Yksi tärkeä merkintä on *sandtree.fi. IN NS sanddsfw1.,* koska se kertoo nimipalvelulle, mikä palvelin toimii DNS-palvelimena.

```
$TTL 2D
@               IN SOA          sanddsfw1.sandtree.fi.
root.sanddsfw1.sandtree.fi. (
                                2010110210      ; serial
                                3H              ; refresh
                                1H              ; retry
                                1W              ; expiry
                                1D )            ; minimum

0.0.168.192.in-addr.arpa.       IN NS           sanddsfw1.sandtree.fi.
214             IN PTR          sanddsfw1.sandtree.fi.
sandtree.fi.    IN NS           sanddsfw1
```

KUVA 34. 0.0.168.192.in-addr.arpa –DNS-toimialueen merkinnät

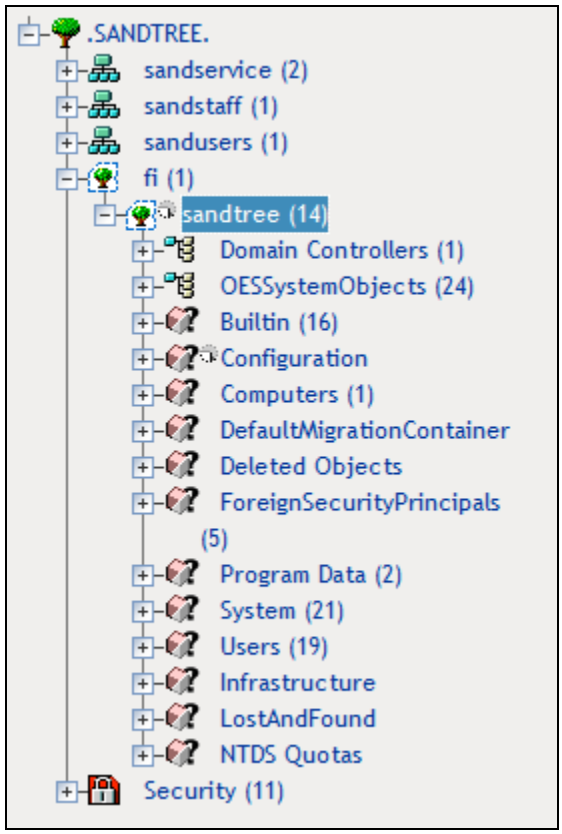
Käänteisessä nimipalvelussa on omat mielenkiintoiset piirteensä. Host-kohtaiset merkinnät tulevat pelkällä IP-osoitteen viimeisellä oktetilla, kuten *214 IN PTR sanddsfw1.sandtree.fi.* on merkittykin.

7.3 Open Enterprise Serveriin tehtävät määritykset

Open Enterprise Server pitää valmistella DSfW:tä varten. DSfW ei asennu Open Enterprise Serveriin oikein, mikäli eDirectory on etukäteen asennettuna. eDirectory ja

DSfW konfiguroidaan yhdessä. Nimipalvelusta pitää löytyä tiedot uudesta DSfW-toimialueesta sekä palvelimesta jossa DSfW-komponentit ovat.

Konfigurointivaiheessa tulee tietää eDirectoryn asetukset, kuten eDirectoryssa jo olevan palvelimen IP, pääkäyttäjätunnus ja salasana, sekä sijainti palvelinobjekteille. Lisäksi täytyy luoda eDirectoryyn domain (dc), joka viittaa luotavaan DSfW-toimialueeseen.



KUVA 35. Hakemistopalvelun rakenne

Kuvassa 35 näkyy koko hakemistopalvelun rakenne. DSfW:n kannalta oleellinen osa-alue on kuvassa laajennettuna näkyvä dc=fi,dc=sandtree –konteksti. Konfigurointi rakentaa edellä mainitun kontekstin alle kuvan mukaisen hakemistorakenteen. Näiden objektien sijaintiin ja nimiin ei pysty vaikuttamaan. eDirectoryn konfigurointivaiheessa DSfW-palvelimen sijainti oli ou=server,o=sandservices, mutta DSfW-provisiointi siirsi palvelimen sille tarkoitettuun paikkaan.

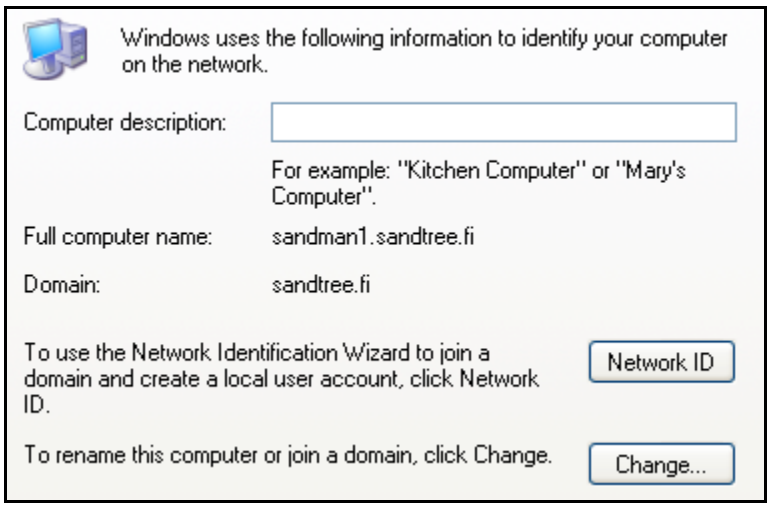
Kun DSfW-palvelussa on kaikki tarvittavat komponentit ja eDirectorykin on ajan tasalla, täytyy DSfW-palvelut provisioida eDirectoryyn. Tätä toimintoa varten on DSfW Provisioning Wizard. Ohjattu toiminto käy läpi kaikki DSfW:n vaatimat osa-alueet ja

luo sille objektit eDirectoryyn (kuva 35). Ennen tätä vaihetta viimeistään pitää DNS-määritysten olla kunnossa ja /etc/resolv.conf-tiedostosta löytyä oikeat DNS-palvelinmääritykset.

DSfW-palvelu toimii itse asiassa aika loogisesti. Halutaan luoda olemassa olevaan hakemistopalveluun toimialuepalvelut Windowsille, mutta palveluita ei suoranaisesti haluta sotkea muiden palveluiden sekaan. Tällöin oman toimialueen luonti (dc=fi,dc=sandtree) on järkevä ratkaisu ja se eriyttää kätevästi toimialuepalvelut eDirectoryn palveluista.

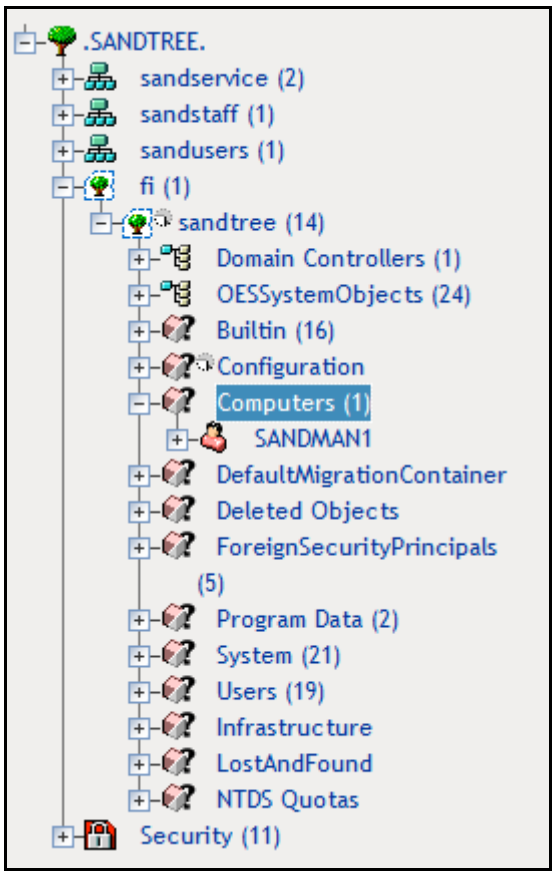
7.4 Työaseman määritykset ja käyttäytyminen

Poistin työaseman toimialueelta jota olin aikaisemmin käyttänyt eDirectoryn ja Active Directoryn yhteiskäytön testauksessa. Tämän jälkeen määritin työaseman DNS-määrityksiin uuden DSfW-palvelimen IP-osoitteen ensisijaiseksi DNS-palvelimeksi. Tämä takasi sen, että siinä vaiheessa kun tein toimialueliitosta, löytyi siihen tarvittavat nimitiedot varmasti. Kun DNS-määritykset olivat kunnossa, liitin työaseman DSfW-toimialueelle.



KUVA 36. Työaseman toimialuetiedot

Kuvassa 36 näkyy nyt, että työasema on toimialueella. Windows XP ei missään vaiheessa tiedä sitä, mikä palvelin toimialuetta ohjaa, se toimii kuten Active Directory –ympäristössä.



KUVA 37. Työaseman sijainti eDirectoryssa

Edellisen kuvan perusteella voimme huomata sen, että työasemaobjekti löytyy myös eDirectorysta ja juuri sieltä minne sen on suunniteltu menevänkin. Jotta kirjautuminen DSfW:n avulla onnistuu, on käyttäjätunnusten löydyttävä Users-kontekstista.

7.5 Arvio kokonaisuudesta

Ideana DSfW on fiksu, mutta sen konfigurointi vaatii asialle vihkiytymistä ja on monesti aika hankala. Useasti kävi kyllä mielessä, ettei tällaisen käyttöönotossa ole mitään järkeä, vaan oikean Active Directoryn rakentaminen on huomattavasti kivuttomampaa ja nopeampaa. Lopputulos kuitenkin oli hyvä ja sain toteutettua sen mihin pyrin. Novell eDirectorya on mahdollista käyttää työasemien autentikointiin ilman Novell Client –asiakasohjelmia. Tämä voi monessa tilanteessa olla helpotus ja säästyyhän siinä ylimääräisen migraation vaivalta, joka odottaisi siirtymisessä eDirectorysta Active Directoryyn.

Haasteellisinta tässä projektissa oli nimipalvelu. Periaatteessa olisin voinut hyödyntää Active Directoryssa olevaa nimipalvelua, mutta se olisi ollut ristiriidassa määrittele-

mäni toimialueen kanssa. Active Directoryn toimialue oli Sandbox.fi ja DSfW:n toimialue oli Sandtree.fi. Rakensin siis uuden DNS-palvelun, joka kohtuullisen monimuotoisen konfiguraatioviidakon kautta lähti toimimaan niin kuin pitikin.

Käytettäessä Linuxia palvelinalustana täytyy varautua siihen, etteivät toiminnot ole kovin suoraviivaisia. Monen asian konfigurointi vaatii Linux-osaamista, mutta se myös mahdollistaa sen, että asioita pystyy varsin monimuotoisesti konfiguroimaan. Olin kuitenkin yllättynyt siitä, miten vakaasti Linux-palvelimet toimivat niinkin monimuotoisten palveluiden käytössä.

Tällaista järjestelmää en välttämättä ottaisi käyttöön, mikäli siihen ei olisi riittävän hyvää syytä. Mielestäni parempi ratkaisu olisi hyödyntää Novell IDM:ää ja yhdistää eDirectoryn ja Active Directoryn voimat, kuten sitä asiaa luvussa 5 esittelin. DSfW menisi erinomaisesti pienessä ympäristössä, jossa halutaan hyödyntää Novell eDirectoryn monipuolista käyttäjätunnistusta, mutta ilman Novell Client –sovellusta.

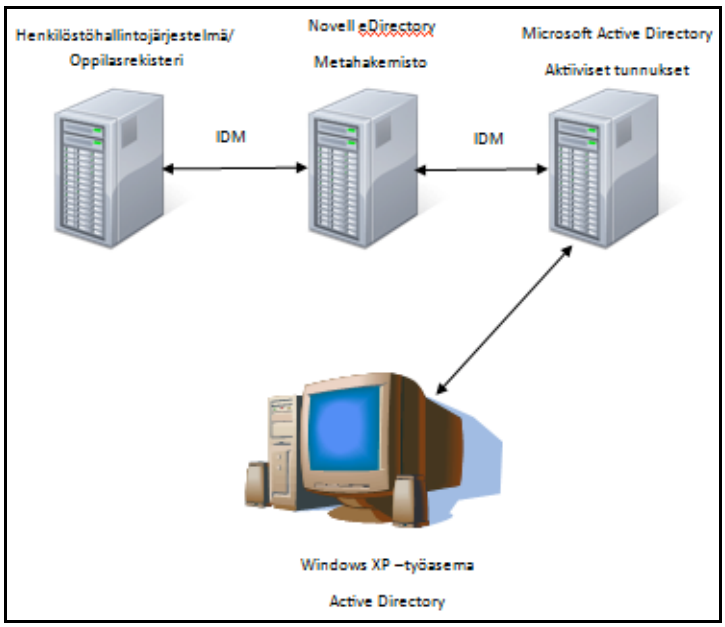
8 LOPPUPÄÄTELMÄT

Tulin siihen tulokseen, että hakemistopalvelut on kätevintä hyödyntää yhdessä. Ei ole järkevää siirtää palveluita järjestelmästä toiseen vaan pyrkiä integroimaan ne keskenään. Active Directory tulee olemaan oleellisessa osassa MAMKin kehitystä, siitä ei pääse mihinkään. Sitä luonnollisesti pitää miettiä, että mistä esimerkiksi levypalvelut tulevat. Kun on kyse identiteettien siirtämisestä järjestelmästä toiseen, ei oikeastaan ole yksinkertaista tapaa suorittaa sitä. Perusasioiden siirto onnistuu mainiosti ilman suurempaa perehtymistä, mutta kun halutaan tarkemmin yksilöidä asioita ja tehdä jopa omia attribuutteja siirrettävien identiteettien ominaisuuksiin, tarvitaan silloin huomattavasti enemmän perehtyneisyyttä.

Domain Services for Windows on ihan kätevä tuote, joskaan en oikein ymmärrä sen käyttötarkoitusta. Ymmärrän toki sen, että jos pieni organisaatio haluaa välttämättä ottaa puhtaalta pöydältä käyttöön nimenomaan Novell eDirectoryn ja hyödyntää samalla perinteistä toimialue autentikointia, on DSfW silloin ratkaisu. Muutoin tällainen järjestelmä vaikuttaa lähinnä pakolliselta lisältä Novellin tuotteiden sekaan. Todellisuudessa järjestelmä kannattaa rakentaa siten, että suuret käyttäjätunnusmassat (aktii-

viset, poistuvat ja poistettavat) sijaitsisivat esimerkiksi eDirectoryssa ja pelkästään aktiiviset tunnukset Active Directoryssa. Erilaisilla identiteetinhallintatyökaluilla aktiivisten identiteettien siirtely hakemistopalveluista toiseen olisi erittäin yksinkertaista.

Itse rakentaisin järjestelmän siten, että alusta alkaen identiteetit tulisivat jostakin tietokannasta, jota ylläpitää henkilöstöhallinto tai opintotoimisto. Nämä ovat sellaisia järjestelmiä, joita joka tapauksessa ylläpidetään ja opiskelijan ensimmäinen kontakti koulun kanssa on nimenomaan opintotoimisto. Sama toki pätee henkilöstöönkin, henkilöstöhallinto hoitaa työntekijälle henkilönumeron ja lisää hänet palkkalistoille. Kun edellä mainituista järjestelmistä on yhteys Meta-hakemistoon, voidaan sieltä sitten siirtää haluttua tietoa myös Active Directoryyn (kuva 38). Active Directoryn rooli olisi merkityksellinen työasemille. Käyttäjät kirjautuisivat Active Directoryyn ja saisivat sitä kautta tarvittavan levyrajapinnan ja mahdollisesti tulostuspalvelut. Olisin edelleen Novell GroupWise –sähköpostijärjestelmän kannalla. GroupWise on osoittanut omat vahvuutensa ja sen ylläpitäminen on loppujen lopuksi aika yksinkertaista ja nopeata.



KUVA 38. Visio MAMKin tietojärjestelmästä

Oma konseptini MAMKin järjestelmistä siis tukeutuisi enemmän Active Directoryyn ja eDirectoryn rooli työasemilla ja loppukäyttäjillä olisi melko pieni. eDirectory olisi osa identiteetinhallintaa ja se säilö jokaiselle identiteetille. Kumpaakaan hakemistopalvelua ei ole syytä väheksyä, koska molemmilla on vahvuutensa. Isommissa käyttä-

jäkannoissa yhden hakemistopalvelun hyödyntäminen ei välttämättä ole hyvä ratkaisu ja se asettaakin omat haasteensa tällaisten kokonaisuuksien implementoinnille.

Miksi sitten päädyin tällaisiin ratkaisuihin? MAMKilla on erilaisia projekteja käynnissä erilaisten uusien teknologioiden parissa. Yksi suuri käyttöön otettava teknologia on työasemavirtualisointi, Virtual Desktop Infrastructure (VDI). VDI-ympäristöissä on hyvin tavallista, että käyttäjäidentiteetti haetaan Active Directorysta. Tämä vaikutti siihen, että oli syytä tutkia mekanismeja, joilla identiteetit olisivat niin Active Directoryssa kuin eDirectoryssakin. Joitakin toteutuksia on, mutta suurimpana haasteena on nimenomaan autentikointi. Työasemat keskustelevat eDirectoryn kanssa, mikä hankaloittaa esimerkiksi VMware View –järjestelmän käyttöä. VMware View –järjestelmässä virtuaalikoneiden pitää olla toimialueella, jotta käyttäjä pystytään autentikoimaan ja tätä kautta yhdistämään oikea virtuaalikone oikealle käyttäjälle. Virtualisointi tulee olemaan oleellinen osa jokaista isompaa organisaatiota ja siksi onkin syytä tehdä ratkaisuja, jotka tukevat monipuolista VDI-konseptitarjontaa. MAMK otti käyttöön Oraclen VDI –ratkaisun, joka ei sido käyttämään mitään tiettyä hakemistopalvelua. Tietyt osa-alueet ovat paremmin tuettuja Active Directoryn autentikoinnin kanssa, mutta perustoiminta (virtuaalityöasemien vienti päätteille) on hakemistopalveluriippumatonta.

Hakemistopalveluiden kanssa riittää siis haasteita. Pyrin työssäni MAMKilla luomaan parhaita käytäntöjä ja luomaan erityisesti loppukäyttäjille ratkaisuja, joita heidän on mahdollisimman helppo käyttää. Yksinkertaisilla hallintamalleilla saadaan säästöjä konesaliin tehtävillä hankinnoilla ja luonnollisesti myös hallintaan tarvittavalla ajansäästöllä. Mahdollisimman dynaaminen ympäristö mahdollistaa asioiden yksinkertaistamisen, joskin dynaamisen ympäristön rakentaminen vaatii kaksinkertaista työtä. Joka tapauksessa implementaatiovaiheessa annettu panos näkyy sitten tuotantovaiheessa ja uskoisinpa niin, että asennuksen resursointi maksaa itsensä takaisin.

9 SANASTO

CIFS = Common Internet File System. Tiedostojärjestelmä joka on tuettuna useassa eri järjestelmässä. Mahdollistaa muun muassa Novell-levypalveluiden käytön Windowsissa ilman Novell Client –lisäohjelmia.
DHCP = Dynamic Host Control Protocol. Järjestelmä joka mahdollistaa esimerkiksi työasemien automaattiset verkkoasetukset (IP-osoite, DNS-palvelimet ja yhdyskäytävän)
DNS = Domain Name System. Järjestelmä joka mahdollistaa internetin ja verkon sisäisten palveluiden käyttämisen palveluiden nimellä eikä niiden IP-osoitteilla.
IDM = Identity Management. Identiteetin hallintajärjestelmä. Mahdollistaa esimerkiksi käyttäjätietojen synkronoinnin Active Directoryn ja eDirectoryn välillä.
ISO = International Organization for Standardization. Kansainvälinen standardoimisjärjestö. Tämän työn yhteydessä käytetty käsite ISO-image viittaa virtuaaliseen CD tai DVD –imageen. Käytännössä vastaa fyysistä CD tai DVD –levyä.
NCP = NetWare Core Protocol. Hallinnoi yhteyksiä NetWare/Novell-palvelimien ydintoimintoihin.
NDPS = Novell Distributed Printing Service. Novellin verkkotulostusjärjestelmä. iPrint-tulostuspalvelu tukeutuu NDPS-järjestelmään.
NMAS = Novell Modular Authentication Service. Erilaisten autentikointitapojen palvelu, jossa on mahdollista käyttää jotain tiettyä autentikointitapaa tai yhdistellä erilaisia tapoja lisätietoturvan saavuttamiseksi.
NTP = Network Time Protocol. Järjestelmä joka tarjoaa verkkoon täsmällistä aikaa.
OSI = Open Systems Interconnection. Tiedonsiirtoprotokollien yhdistelmä.
SLP = Service Location Protocol. Sijaintiprotokolla, joka mahdollistaa palveluiden paikallistamisen lähiverkossa.
SP = Service Pack, Support Pack. Päivityskokonaisuus, joka on tarkoitettu joko sovellukseen tai käyttöjärjestelmään.

LÄHTEET

Clines, Steve & Loughry, Marcia 2008. Active Directory For Dummies. Indianapolis: John Wiley & Sons.

Dean, Tamara 2005. Network+ 2005 In Depth. Boston: Course Technology.

Honeycutt, Jerry 2003. Introducing Microsoft Windows Server 2003. Redmond: Microsoft Press.

Howes, Timothy A., Smith, Mark C. & Good, Gordon S. 1999. Understanding and deploying LDAP directory services. Indianapolis: Macmillan Technical Publishing.

Hudson, Sally & Hatcher, Eric 2010. Improving IT Staff Efficiency, Reducing Costs, and Boosting User Productivity with Novell Identity and Access Management (IAM). PDF-dokumentti. http://www.novell.com/docrep/2010/03/IDC_ROI_Final.pdf. Päivitetty 1.4.2010. Luettu 29.10.2010.

IBM Redbooks 2004. Understanding LDAP - Design and Implementation. Austin: IBM.

Karjalainen, Harri 2010. Haastattelu 22.9.2010. Järjestelmäasiantuntija Citius.net.

Kivimäki, Jyrki 2003. Inside Active Directory: verkonhallinta. Helsinki: IT Press.

Novell 2004. Active Directory vs. eDirectory. PDF-dokumentti. http://whitepapers.zdnet.com/abstract.aspx?docid=92320&promo=508&tag=nl.e508. Ei päivitystietoa. Luettu 24.10.2010.

Novell Communities 2009. eDirectory Version Chart. WWW-dokumentti. http://www.novell.com/communities/node/8600/edirectory-version-chart. Päivitetty 7.7.2009. Luettu 29.10.2010.

Sapman, Pekka 2010. Haastattelu 29.9.2010. Järjestelmäasiantuntija. Mikkelin ammattikorkeakoulu Oy.

LIITE 1.

NDS:n/eDirectoryn versiokehitys (Novell Communities 2009)