VAASAN AMMATTIKORKEAKOULU

Juho Latva

Yritysverkon rakentaminen

Tekniikka ja liikenne

2009

ALKUSANAT

Tämä opinnäytetyö on tehty Vaasan ammattikorkeakoulun tietotekniikkaosastolle vuoden 2009 kesän aikana. Työn tilaajana toimi Vaasan ammattikorkeakoulun lehtori Antti Virtanen. Työ toteutettiin Technobotnialla.

Työn valvojana toimi lehtori Mikael Jakas.

Vaasassa 26.10.2009

Juho Latva

VAASAN AMMATTIKORKEAKOULU

Tietotekniikan koulutusohjelma

TIIVISTELMÄ

Tekijä	Juho Latva
Opinnäytetyön nimi	Yritysverkon rakentaminen
Vuosi	2009
Kieli	suomi
Sivumäärä	75+1 liite
Ohjaaja	Mikael Jakas

Tämän opinnäytetyön tarkoituksena oli rakentaa pienen yrityksen testiverkko tietotekniikan osastolle opetustarkoitukseen. Testiverkkoon kuului intraverkko ja DMZ. Verkon palomuurina käytettiin Ipcop-palomuuria. Testiverkkoon rakennettiin ohjelmisto- ja käyttäjätietokanta, sähköpostipalvelin ja levypalvelin Windowsilla ja Linuxilla käyttäen OpenSusE 11.1 -versiota, tulostinpalvelua, WWW-palvelinta ja Terminaali-palvelua.

Opinnäytetyössä käydään läpi eri autentikointimenetelmiä ja sitä miten LDAP-protokolla helpottaa käyttäjien hallintaa. Palvelimet ovat yhdellä toimialueella ja ne käyttävät tunnistautumiseen LDAP-protokollaa sekä Kerberosta.

Testiverkon rakentamisessa on huomioitava, mitä palveluita mihin laitetaan ja millä käyttöjärjestelmällä niitä käytetään. Linux-käyttöjärjestelmä aiheutti esimerkiksi ongelmia Linux-vakauden kanssa, koska eri distrot käyttäytyvät eri tavoin eri ohjelmien kanssa. Testiverkon suunnittelussa on huomioitava myös sähköpostin domain-nimi. Lähetettäessä sähköpostia koulun sähköpostiin tulee ongelmia, koska puv.fi ja botnia.puv.fi ovat samassa verkkotunnuksessa.

Asiasanat: Microsoft Server, Active Directory, Samba, Imap

VAASAN AMMATTIKORKAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Technology

ABSTRACT

Author	Juho Latva
Topic	Building a Company Network
Year	2009
Language	Finnish
Pages	75+1 appendice
Supervisor	Mikael Jakas

The objective of the research was to build a small company network for the IT department for educational purposes, including an intra network and a DMZ in this test network.The firewall program is Ipcop. The Active Directory, mail server, file server with Windows and Linux using OpenSuse version 11.1, printer server, WEB server and Terminal server were build in the test network.

Authentication with LDAP and Kerberos protocols helps users and administrators to manage user accounts. Every server and all the services are in the same Domain area. Kerberos authentication method is needed when Linux machine tries to connect to the Windows network.

There were two problems when this network was implemented. Linux machine is quite unstable and different distributions behave in different ways in the network. The other problem occurs when the user sends an email to the email system of the school. The problem is in the DNS system. In the hierarchy botnia.puv.fi is beneath puv.fi, which is the reason why the Botnia suffix disappears.

Keywords: Microsoft Server, Active Directory, Samba, Imap

LYHENNELUETTELO

AD	Active Directory Käyttäjätietokanta
APT	Advanced Packet Tool Linuxin pakettienhallintatyökalu
BDC	Backup Domain Controller Toimialueen hallitsijan varakone
DC	Domain Controller Toimialueen hallitsija
DMZ	Demilitarized Zone Demilitarisoitu alue
DNS	Domain Name System Toimialueen nimenhallintajärjestelmä
DHCP	Dynamic Host Configuration Protocol Verkkoprotokolla, joka jakaa IP-osoitteita
HTTP	Hyper Text Transfer Protocol Selaimen tiedonsiirtoprotokolla
IEEE	Institute of Electrical and Electronics Engineers Tietoliikennealan ammattilaisten yhteisö

IIS	Internet Information Services Microsoftin WWW-palvelin
IMAP	Internet Message Access Protocol Sähköpostin lukemiseen tarkoitettu protokolla
IP	Internet Protocol Internetprotokolla
KDC	Key Dictribution System Tietokanta salasanoille
LAN	Local Area Network Lähiverkko
LDAP	Lightweight Directory Access Protocol Hakemistopalveluissa käytetty tunnistusprotokolla
NAT	Network Address Translation Osoitteenmuutos
NFS	Network File System Verkkolevyn jako
NTP	Network Time Protocol Verkon aikaprotokolla
PAT	Port Address Translation Portin osoitteenmuutos

PHP	Hypertext Preprocesso Ohjelmointikieli
SMB	Server Message Block Protokolla, joka jakaa levyjä ja printtereitä verkossa
SMTP	Simple Mail Transfer Protocol Sähköpostin lähetysprotokolla
SNMP	Simple Network Management Protocol Verkonhallintaprotokolla
SSH	Secure Shell Suojattu yhteys
SSL	Secure Socket Layer Salausprotokolla
TLS	Transfer Layer Security Korvaava salausportokolla
TCP	Transmission Control Protocol Yhteydellinen kuljetusprotokolla
TS	Terminal Service Windowsin etäyhteys
URL	Uniform Resource Locator WWW-osoitteen osoittaja

WAN	Wide Area Network Laajaverkko
VOIP	Voice over IP Ääntä IP:n yli
VLAN	Virtual Local Area Network Virtuaalinen lähiverkko
VPN	Virtual Private Network Salattu etäyhteys
WWW	World Wide Web Internet

SISÄLLYS

1 JOHDANTO

Tällä hetkellä tietoliikenteen opetusohjelmassa ei käydä läpi sitä mistä yritysverkko koostuu ja minkälaisia palveluita siellä on. Yritysten verkoissa on nykypäivänä monia eri palveluja, esimerkiksi hakemistopalvelut, Voip ja intrapalvelut. Intrapalvelut ovat verkonsisäisiä palveluita, eikä niistä ei ole aukkoa ulkoverkkoon. Tässä työssä tutustutaan tietoturvaan sekä DMZ:aan (Demilitarized Zone) pienemmän yrityksen näkökannalta. Tämän päivän pienissä yritysverkoissa voi olla palveluita yhtä paljon kuin suuremman yrityksen verkossa. Pieni yritys myös tarvitsee yhtä hyvät palvelut ja toimivat ratkaisut kuin suurempi yritys, jotta henkilökunta voi keskittyä omaan työhönsä.

Tässä opinnäytetyössä rakennetaan pienen yrityksen verkko ja tutkitaan sitä. Verkkoon vaaditaan kunnon käyttäjä- ja hakemistopalvelu, tulostuspalvelu, sähköposti, WWW-palvelu sekä levypalvelu. Palveluiden rakentamiseen käytetään Microsoft Windows Server 2008 R2, OpenSuSe 11.1 -versiota. Sisäverkon, ulkoverkon ja DMZ-alueen luojana käytetään IPCOP 1.24 -palomuuriohjelmistoa. Sisäverkon reitityksen hoitaa Zyxell 5108 -kytkin, jossa on kolme VLANia. Tulostimena käytetään BROTHER NL-2150 -verkkotulostinta.

2 VERKKOTOPOLOGIA

2.1 Vaatimusmäärittely

Tässä opinnäytetyössä ensimmäisenä tehtiin vaatimusmäärittely. Tämä vaatimusmäärittely käy läpi mitä palveluja ja asetuksia asiakas haluaa. Tässä tapauksessa asiakas on Vaasan ammattikorkeakoulun tietotekniikkaosasto. Vaatimusmääritelyssä käydään läpi seuraavat asiat:

Prioriteetti 1

- verkossa tulee olla oma domainnimi
- verkossa pitää olla palomuuri
- verkossa pitää olla Intra- sekä DMZ-alue
- DNS-forwardointi
- käyttäjätietokanta ja hakemistopalvelu
- tulostuspalvelu
- tiedostopalvelimet

Prioriteetti 2

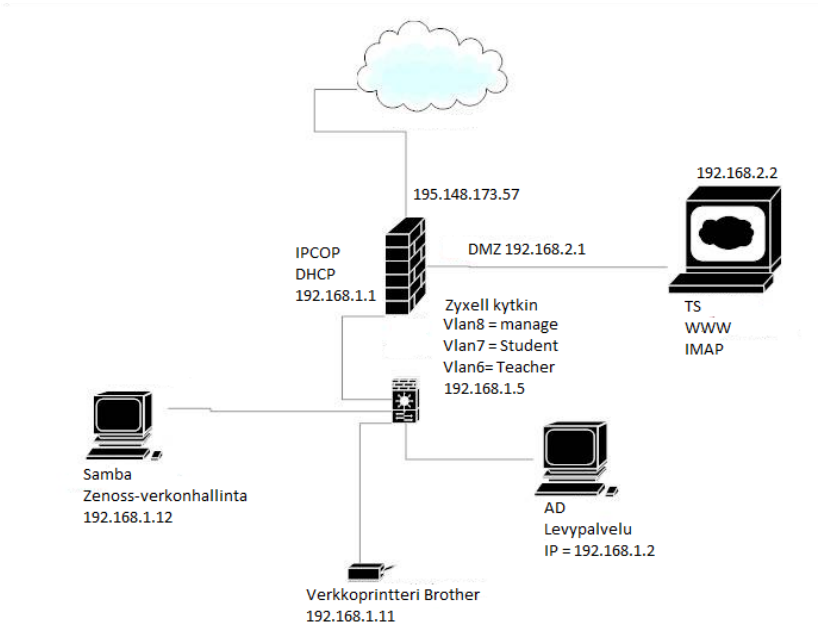
- verkonhallinta
- VLAN
- sähköpostipalvelin

Prioriteetti 3

- etäyhteys (VPN tai muu)
- oma DNS-palvelin
- IDS ja IPS
- Voip

2.2 Verkkokuvaus

Seuraavassa kuvassa (kuva 1) on kuvattu yritysverkon arkkitehtuuri.



Kuva 1 Verkkotopologia

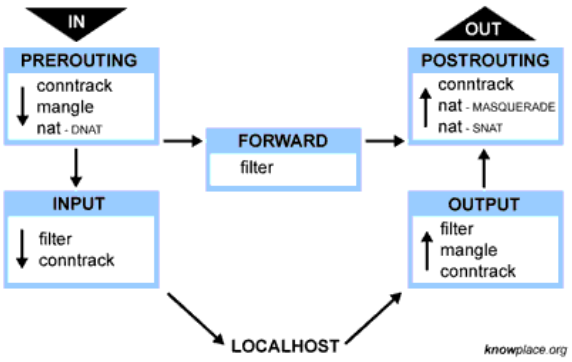
Kuvassa 1 nähdään, että ulkoinen verkko on 195.148.173.57. Osoite kuuluu Netikan osoitteisiin, jotka on reititetty ohi koulun palomuurien. Osoitteelle annetaan nimi botnia.puv.fi, joka lisätään koulun sisäiseen ja ulkoiseen DNS-palvelimeen. Näin voidaan yhdistää koulun sisältä ja ulkoverkosta botnia.puv.fi -osoitteeseen. Tämä on suora, turvaton linja ulkoverkkoon. Verkossa ei ole palomuureja eikä DNS:ää. IPCOP-palomuuriohjelmisto jakaa verkon DMZ-alueeseen sekä intra-alueeseen. DMZ-alueen osoiteavaruus on 192.168.2.1 ja intra-alueen 192.168.1.1. IPCOP-palomuurissa on myös DHCP-palvelu, joka jakaa osoitteet intraverkon laitteille.

Kuvassa on myös kerrottu, mitkä palvelut ovat milläkin koneilla ja koneiden IP-osoitteet. Laitteiden osoitteet ja kytkinten fyysiseen rakentamiseen tarvittavat tiedot on merkitty verkkotopologiakuvaan (kuva 1).

3 IPCOP

3.1 Ipcop-tekniikka

Ipcop on Linux-tyylinen palomuurisovellus, jolla voidaan estää haitallisten pakettien pääsy koneelle. Järjestelmään voidaan asentaa 4 eri verkkokorttia, mutta 2 verkkokorttia on pakollinen ratkaisu. IPCOP kutsuu eri verkkokortteja nimillä RED, GREEN, ORANGE ja BLUE. Näistä RED ja GREEN ovat pakollisia. RED tarkoittaa verkkoa, joka johtaa suoraan ulos ja GREEN sisäverkkoon johtavaa verkkoa. BLUE ja ORANGE ovat lisäpaikkoja, joilla voidaan lisätä turvallisuutta ja laajentaa verkkoa. BLUE-paikkaan voidaan lisätä erillinen verkko tai WLAN-verkko, ORANGE-lisäpaikka on ainoastaan DMZ-yhteyden luomiseen tarkoitettu. Ipcopin tekniikka perustuu ketjuihin ja tauluihin. Ketjuja on kolme: INPUT, FORWARDING sekä OUTPUT. Ketjuilla voidaan rajoittaa tiettyjä osia pakettien liikkuuvuudesta. Kuva 2 havainnollistaa paremmin pakettien liikkuvuuden. /18/



Kuva 2 /18/

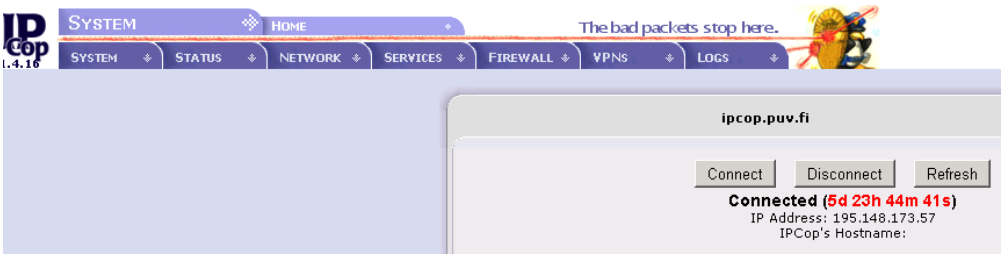
Kuvassa 2 IN tarkoittaa sisään tulevaa liikennettä ja vastaavasti OUT ulospäin menevää liikennettä. FORWARD tarkoittaa sitä, että ohjataan sisään tulevaa liikennettä toiselle koneelle.

3.2 Ipcopin edut ja haitat

Ipcop on Linux-sovellus, jossa ei ole Linuxista tuttua APT (Advanced Packet Tool) -työkalua. Tästä johtuen Ipcopia ei voi päivittää suoraan koneelta, vaan siihen pitää ladata erikseen päivityspaketit muualta. Tämä tarkoittaa myös sitä, että vaikka Ipcopissa on melko hyvä ajurituki nykypäivän verkkokorteille sekä CD-ROM asemille, uusia se ei enää tunnista. Ipcopissa on myös tunnetusti ongelmia tietokoneiden komponenttien kanssa ja varsinkin RAM-muistien kanssa. Ipcop voi saada muistivian, vaikka koneen RAM-muisti olisikin kunnossa.

Opinnäytetyössä käytettiin Ipcop-versiota 1.4.16, koska se oli sillä hetkellä toimivin järjestelmä, vaikka sitä ei ajurituen vuoksi uusille koneille saanutkaan. Ipcopin uusin versio oli vielä kokeiluversiona, joka asentui uusille koneille, mutta oli todella epävakaa. Tämän takia Ipcop-koneeksi suositellaan hieman vanhempaa konetta, josta kuitenkin löytyy RAM-muistia 2 GB ja prosessoritehoa 1.5–2.0 GHz.

Ipcopin käyttöliittymä on hyvä ja sillä hoituvat tarvittavat asetukset kätevästi ja selkeästi. Asetuksia voidaan muokata selainnäkymästä tai tekemällä omia skriptejä. Kuvassa 3 on Ipcopin selainhallintaohjelma. Selaimessa tehdyt muutokset vaikuttavat välittömästi Ipcopin toimintaan.



Kuva 3 Ipcop

Kuvassa 3 on selainhallintaohjelman etusivu. Välilehtien alla näkyy lisävalintoja, jotka ovat liitteessä 1.

3.3 Käyttöönotto

3.3.1 Asennus

Ipcop asennetaan aivan samalla tavalla kuin mikä tahansa käyttöjärjestelmä. Asennus kysyy käyttäjältä, mille kovalevyn osiolle käyttöjärjestelmä asennetaan, vai käytetäänkö koko kovaley Ipcopin käyttöön. Asennus on varsin helppo. Asennus kysyy olinpaikkaa, aikavyöhykettä ja Domain-nimeä sekä isäntänimeä. /19/

Tässä opinnäytetyössä käytetään kolmen verkkokortin asetusta eli RED, GREEN ja ORANGE. Asetukset näkyvät Taulukossa 1:
(Turvallisuussyistä tässä ei ole salasanoja.)

Taulukko 1. IPCOP-verkkokorttien asetukset

<table>
<tr><td>RED</td><td>GREEN</td><td>ORANGE</td><td>Domain nimi</td><td>Host</td></tr>
<tr><td>IP 195.148.173.57</td><td>IP 192.168.1.1
mask
255.255.255.0</td><td>IP 192.168.2.1
mask
255.255.255.0</td><td>Puv.fi</td><td>Ipcop</td></tr>
<tr><td rowspan="2">Default gateway
195.148.173.62
DNS=
193.166.140.100</td><td>DHCP päälle
Start address
192.168.1.2

End address
192.168.1.12</td><td colspan="3" rowspan="2"></td></tr>
<tr><td>Primary DNS
192.168.1.2</td></tr>
</table>

3.3.2 Asetuksien asettaminen

Opinnäytetyössä tullaan tarvitsemaan yhteydenottoa myös ulkoverkosta sisäverkkoon, sekä NAT-muutosta ja IP-forwardointia. Kuvan 4 asetukset ovat välttämättömiä asetuksia, joiden avulla verkko saadaan toimimaan kunnolla.

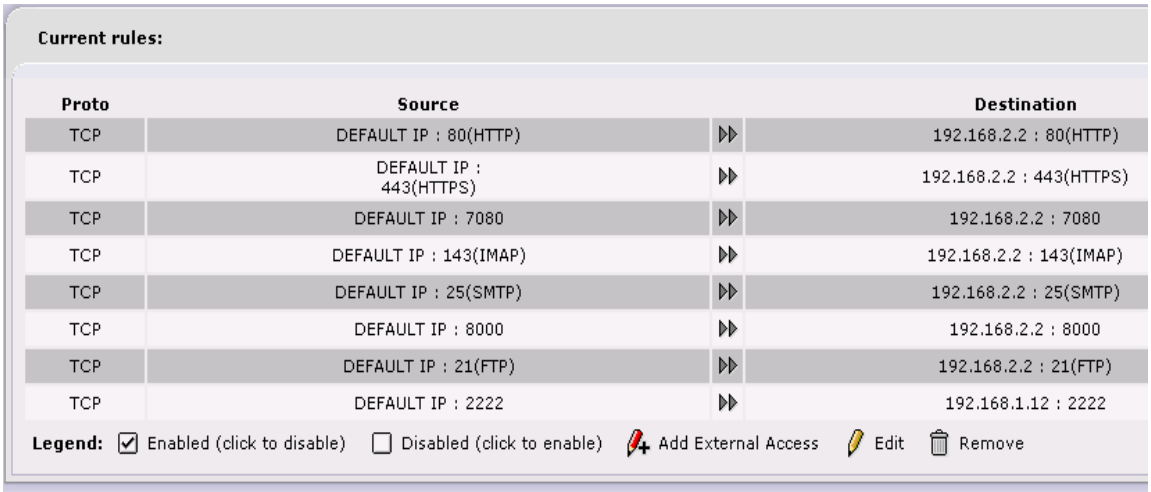
```
/sbin/iptables -P INPUT ACCEPT
/sbin/iptables -P FORWARD ACCEPT
/sbin/iptables -P OUTPUT ACCEPT



iptables -A INPUT -p ICMP -i eth1 -j ACCEPT

iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to 195.148.173.57
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Kuva 4 Iptables

Ensimmäisenä hyväksytään kaikki yhteydet ja IP-forwardointi. Tämän jälkeen kirjoitetaan sääntö, joka hyväksyy IP-forwardoinnin sekä IP-masqueraden (one to many). Tämän avulla saadaan ne koneet, jotka sijaitsevat Ipcopin intraverkossa, yhdistämään internetiin. Tämä on kuin NAT, mutta Linux-palomuurien maailmassa sitä myös kutsutuaan IP-masqueradeksi. Default-asetuksessa on vain ketjut määritetty auki siten, että yhteys sallitaan vain intra-verkosta.

iptables – A INPUT –p ICMP –i eth1 –j ACCEPT on esimerkkisääntö, joka hyväksyy ICMP-pakettien sisääntulon verkkokortille 1. Sääntöä luetaan seuraavasti: Hyväksytään sisääntuleva liikenne, protokolla ICMP interface eth1 ja hyväksytään tämä sääntö. Säännön voi myös estää, jolloin viimeisen ACCEPT:in tilalle tulee DROP. Palomuurissa on eth0- ja eth1-verkkokortit, joista pitää tarkasti katsoa, kumpi osoittaa ulkoverkkoon eli internetiin ja kumpi on taas sisäverkossa. Näin säännöt saadaan oikeiksi ja verkko toimii halutulla tavalla.

Ipcopin selainhallintaohjelmaan otetaan sisäverkosta asiakas koneelta http://192.168.1.1:445. Ohjelma kysyy käyttäjänimeä ja salasanaa, jotka ovat admin ja ****. Opinnäytetyön verkossa tarvitaan ulkoverkosta ohjaus DMZ-alueelle, ja DMZ-alueelta tarvitaan yhteys sisäverkkoon eli intraan. DMZ-alueen reiät ja porttien ohjaukset on kerrottu kuvissa 5 ja 6. /19/



Current rules:

Proto	Source		Destination
TCP	DEFAULT IP : 80(HTTP)	⏩	192.168.2.2 : 80(HTTP)
TCP	DEFAULT IP : 443(HTTPS)	⏩	192.168.2.2 : 443(HTTPS)
TCP	DEFAULT IP : 7080	⏩	192.168.2.2 : 7080
TCP	DEFAULT IP : 143(IMAP)	⏩	192.168.2.2 : 143(IMAP)
TCP	DEFAULT IP : 25(SMTP)	⏩	192.168.2.2 : 25(SMTP)
TCP	DEFAULT IP : 8000	⏩	192.168.2.2 : 8000
TCP	DEFAULT IP : 21(FTP)	⏩	192.168.2.2 : 21(FTP)
TCP	DEFAULT IP : 2222	⏩	192.168.1.12 : 2222

Legend: ☑ Enabled (click to disable) ☐ Disabled (click to enable) Add External Access Edit Remove

Kuva 5 External Access

Kuvassa 5 on Port forwardointiin tehdyt säännöt. Säännöt tarkoittavat sitä, että mistä tahansa IP-osoitteesta tuleva kysely, joka esimerkikisi kysyy portista 2222, ohjautuu tällöin sisäverkon koneelle IP-osoitteeseen 192.168.1.12. Esimerkkinä on HTTP-liikenne: kun käyttäjä tulee http://botnia.puv.fi-sivustolle, Ipcop ohjaa käyttäjän 192.168.2.2-koneelle, jonka WWW-palvelin on DMZ-alueella.

Proto	Net	Source		Net	Destination
UDP		192.168.2.2	⏩		192.168.1.2 : 123(NTP)
UDP		192.168.2.2	⏩		192.168.1.2 : 88(KERBEROS)
UDP		192.168.2.2	⏩		192.168.1.2 : 138(NETBIOS-DGM)
TCP		192.168.2.2	⏩		192.168.1.2 : 135(EPMAP)
TCP		192.168.2.2	⏩		192.168.1.2 : 49152:65535
TCP		192.168.2.2	⏩		192.168.1.2 : 389(LDAP)
TCP		192.168.2.2	⏩		192.168.1.2 : 53(DOMAIN)
UDP		192.168.2.2	⏩		192.168.1.2 : 53(DOMAIN)
TCP		192.168.2.2	⏩		192.168.1.2 : 636(LDAPS)
TCP		192.168.2.2	⏩		192.168.1.2 : 3268
TCP		192.168.2.2	⏩		192.168.1.2 : 3269
TCP		192.168.2.2	⏩		192.168.1.2 : 5000
TCP		192.168.2.2	⏩		192.168.1.2 : 88(KERBEROS)
UDP		192.168.2.2	⏩		192.168.1.2 : 389(LDAP)
TCP		192.168.2.2	⏩		192.168.1.2 : 636(LDAPS)

Legend: ☑ Enabled (click to disable) ☐ Disabled (click to enable) Edit Remove

Kuva 6 Port Forwarding

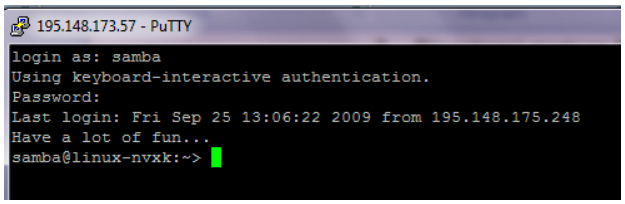
Kuvassa 6 on määritetty seuraavat aukot DMZ-alueelta sisäverkkoon. Portit, jotka ovat auki, kuuluvat Windows Server 2008 Domainiin, ja ilman näitä aukaisuja puv.fi-domainiin pääsy olisi mahdotonta. Normaalisti DMZ-alueelta ei ole pääsyä sisäverkkoon, mutta tässä opinnäytetyössä on, koska WWW-palvelin tarvitsee pääsyn domainverkkoon, joka selviää myöhemmin. Verkossa on pieni tietoturvariski, kun tietyt portit ovat auki, mutta silti vähäinen, koska portit käyttävät vain tiettyä palvelua.

3.4 Testaus

Toimivuutta testataan kolmella eri tavalla:

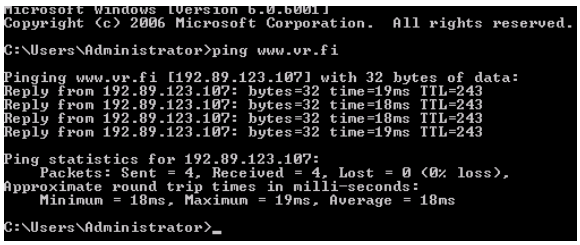
- Otetaan SSH-yhteys ulkoverkosta.
- Pingataan tai avataan internetsivu sisäverkosta (www.vr.fi).
- Liitetään WWW-palvelin Domainiin.

SSH-yhteys otetaan Putty-ohjelmalla. Otetaan yhteys 195.148.173.57 porttiin 2222. Kirjoitetaan salasansa ja käyttäjänimi. Kuvassa 7 on onnistunut yhteydenotto.



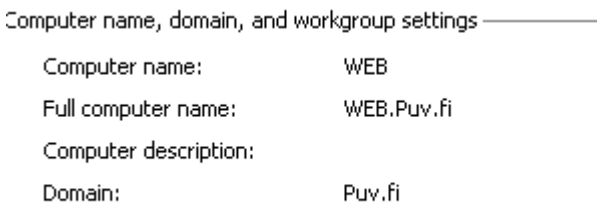
Kuva 7 Linux-kone

Ipcop on porttiohjannut SSH-yhteyden oikeaan koneeseen kun yhteys on otettu ulkoverkosta.



Kuva 8 Pingaus

Pingaus on onnistunut eli yhteys sisäverkosta toimii.



Kuva 9 Domain

WWW-palvelin on saatu Domainiin.

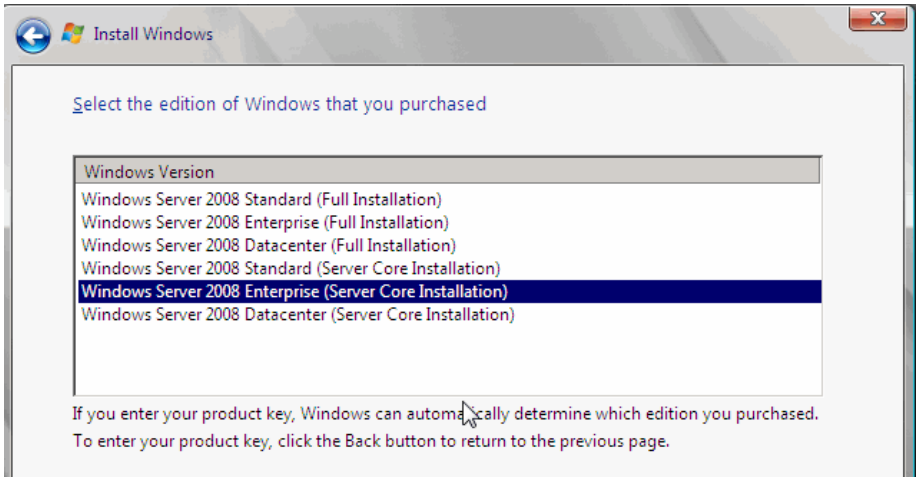
4 MICROSOFT SERVER (”Longhorn”)

4.1 Microsoft Server lyhyesti

Microsoft Server 2008 on uusin julkaisu Microsoftilta. Microsoft Server 2008 on palvelinohjelmisto, jolla yritykset voivat luoda helposti uusia palveluja, kuten WWW-palvelut ja virtualisoinnin. Microsoft on tehnyt paljon uudistuksia palvelimeensa. Lisää palveluja on tuotu ja vanhoja parannettu tuomalla niihin uusia ominaisuuksia ja parantamalla niiden toimivuutta. Microsoft Server 2008 on lisännyt toimivuuttaan virtualisoinnissa uudistamalla HYPER-V-tekniikan, joka on nopeampi ja helpommin hallittavissa kuin aiemmat. Opinnäytetyössä tullaan huomaamaan, että Microsoftin uudistukset pyrkivät taistelemaan Citrix- ja VPN-tekniikoiden kanssa. Yleiseltä kannalta katsottuna Microsoft on lisännyt kaikkien palvelujen hallitsemista ja toimivuutta. Microsoft Server 2008:aa käytetään tässä opinnäytetyössä, koska asiakkaan koneet tulevat olemaan Windows 7- ja Vista-koneita. Microsoft Server 2008:lla on pidempi tuotetuki kuin Microsoft Server 2003:lla. Jatkossa tullaan tutustumaan sen uusiin ominaisuuksiin. Vastaavaa pakettia ei ollut tarjolla ja Linux- puolella vielä odotetaan Samba 4:ää, jossa olisi AD:ta vastaava palvelu. /16/, /17/

4.1.1 Asentaminen

Microsoft Server 2008 asentaminen tehdään samalla tavalla kuin Microsoftin eri Windows-versiotkin. Asennus käynnistetään CD:ltä. Asennus kysyy samat tiedot kuin Desktop-puolella, mutta palvelinpuolella on muutamia asioita, jotka pitää ottaa huomioon. Asennuksen aikana kysytään minkä version haluat asentaa. Kuvassa 10 on näytetty mahdollisuudet.



Kuva 10 Windowsin asennus

Tässä työssä valittiin Windows Server 2008 Enterprise (FULL Installation). Ostetuissa lisensseissä asennus antaa sen vaihtoehdon johon lisenssi oikeuttaa. Asennuksen valmistuttua asetetaan salasanat, sitten asennus on valmis. Koneen nimeksi valittiin AD, koko DNS suffix on AD.PUV.FI

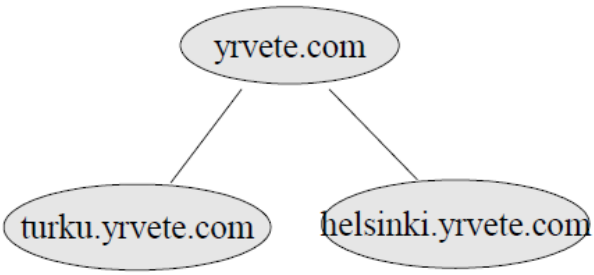
4.1.2 Microsoft Management Console

Microsoftin tuotteissa MMC:n (Microsoft Management Console) avulla voidaan muokata kaikkia Microsoftin tuotteiden asetuksia. Asetukset löytyvät helposti Add/remove snap in -valikosta. Palvelimien asennuksen aikana ja muiden säätöjen tekemiseen konsoli on erittäin kätevä työkalu.

4.2 Active Directory

Active Directory on käyttäjätietokanta ja hakemistopalvelu. Active Directory -verkossa voidaan luoda ryhmiä ja antaa eri ryhmille erilaisia oikeuksia. Palvelulla voidaan yhtenäistää eri ryhmien palveluja, turvallisuutta, työpöydän asetuksia ja ohjelmistoja sekä antaa kaistaa heille, jotka sitä eniten tarvitsevat. AD-verkolla voidaan myös yhdistää yritysten tietokannat samaan juurisolmuun, vaikka maantieteellisesti matkat olisivat pitkiä. Kuvassa 11 on kuvattu

esimerkkitopologia yrityksen verkosta, jossa on kaksi toimipistettä eri maantieeteellisessä paikassa. /6/

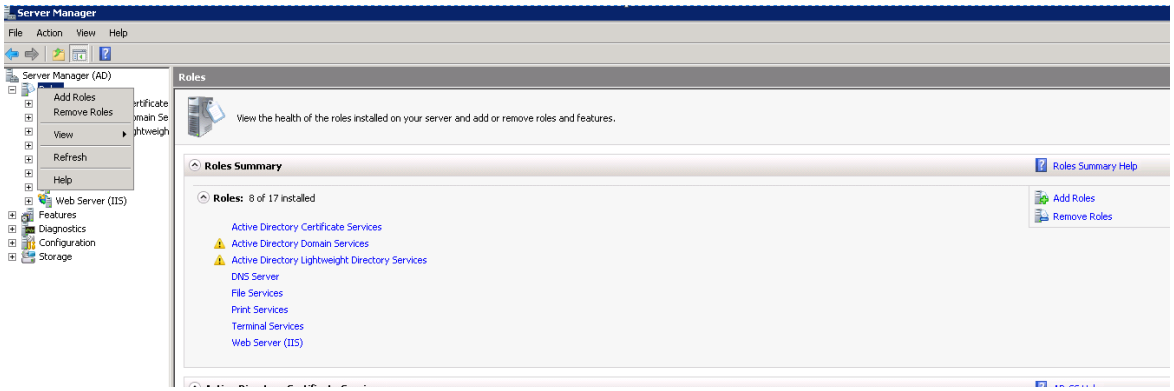


Kuva 11 Node

Kuvassa 11 juurinode on yrvete.com, ja sillä on kaksi eri toimipaikkaa Turussa ja Helsingissä. Kone, johon asennetaan Active Directory -palvelu, on tämä Primary Domain Controller eli PDC. PDC jakaa ja tarkistaa käyttäjäoikeuksia toimialueella. PDC:n rinnalle voidaan listä Backup Domain Controller (BDC). Jos PDC kaatuu tai se ei voi suorittaa tehtäviään, toimii BDC tällöin PDC:nä. Koko toimialueella eli domain-metsässä voi olla vain yksi PDC.

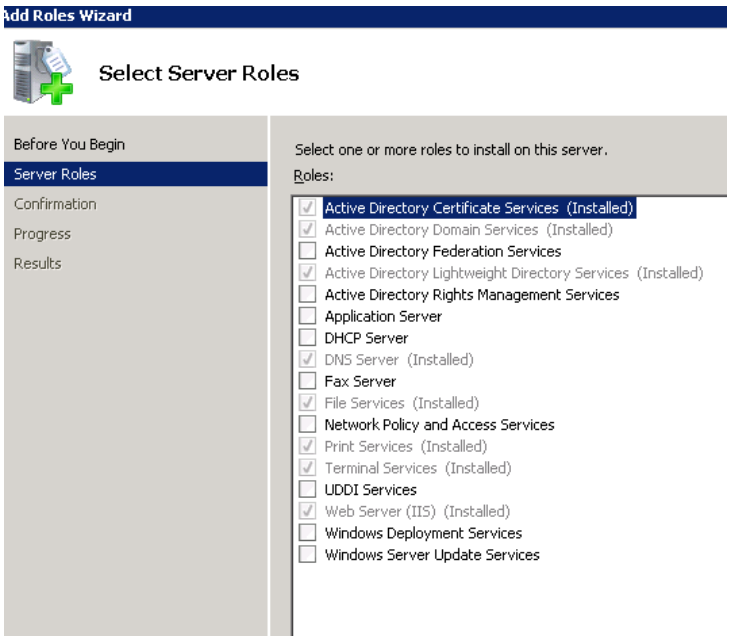
4.2.1 AD-verkon asennus

AD-palvelu asennetaan samalla tavalla kuin muutkin palvelut Windows Server 2008 -palvelimissa. Kaikki asennukset ja poistot tapahtuvat Server Manager -ohjelmassa. Server Manager näyttää myös ohjelmien tilan 24 tunnin ajalta. Kuvassa 12 näytetään, miten lisätään palvelu.



Kuva 12 Server Manager

Kuvassa 12 on Server Manager -hallintakonsoli. Palvelimen roolit lisätään Add Roles -kohdasta. Palvelujen lisäominaisuudet lisätään Add Feature -kohdasta. Active Directory -palvelu lisätään Add Role -kohdasta. Tämän jälkeen uudesta ikkunasta valitaan Active Directory Domain service (katso kuva 13).



Kuva 13 Roolit

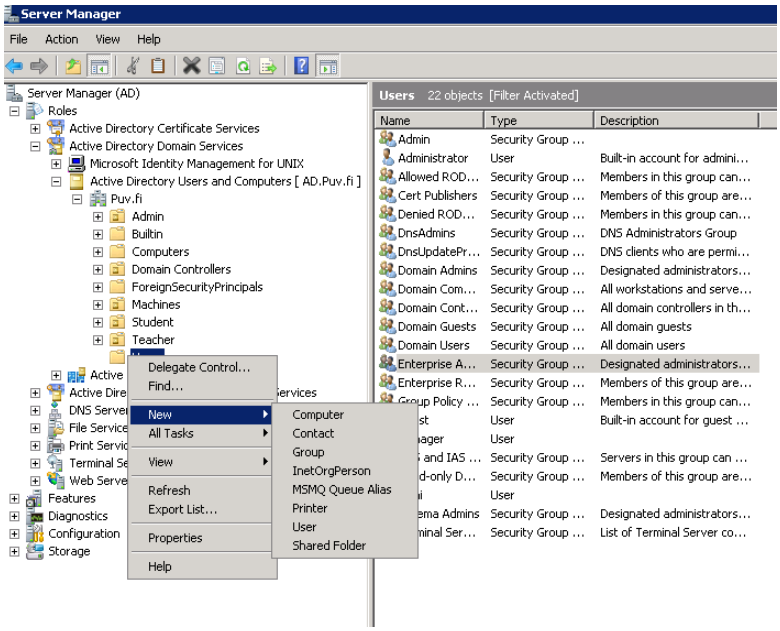
Kuvassa 13 nähdään, mitkä palvelut on lisätty tähän palvelimeen. Kuvassa rastitaan haluttu palvelu eli Active Directory Domain Service. Tämän jälkeen painetaan Next. Valitaan Advanced, jotta voidaan vaikuttaa paremmin asetuksiin. Asennus pyytää domain-nimeä, joka on puv.fi. Tämän jälkeen kysytään NetBios-nimeä, joka on TECH. Tämän jälkeen asennus on valmis. Tämän toimialueen nimi on puv.fi, mutta käyttäjälle se näkyy nimellä TECH.

4.3 Käyttäjä- ja ryhmäprofiilit

Käyttäjät lisätään toimialueelle Active Directory User and Computer -ohjelmassa Add User -valikossa. Isompien organisaatioiden käyttäjät lisätään erilaisten skriptien kautta suoraan eri tietokannoista tai Excel-taulukoista. Tässä työssä on käyttäjiä vain muutama, joten ne lisätään manuaalisesti Add User -valikosta. On suositeltavaa tehdä käyttäjäryhmät, koska ne auttavat hallitsemaan eri ryhmiä ja mahdollistavat käyttäjien oikeuksien jakamisen helposti. Käyttäjärymät lisätään samasta paikasta kuin käyttäjät. Tässä käytetään Add Group -komentoa. Käyttäjäryhmien tarkoituksena on estää tai sallia käyttäjän oikeuksia toimialueella. Toimialueella voidaan käyttäjä lisätä valmiseen esimerkkiryhmään tai tehdä hänelle uusi käyttäjäryhmä ja tehdä uudelle ryhmälle omat oikeutensa. Esimerkkinä administrator-ryhmällä on kaikki oikeudet, mutta Domain Adminilla ja Domain Controllerilla eri oikeudet.

4.3.1 Käyttäjäryhmien luominen

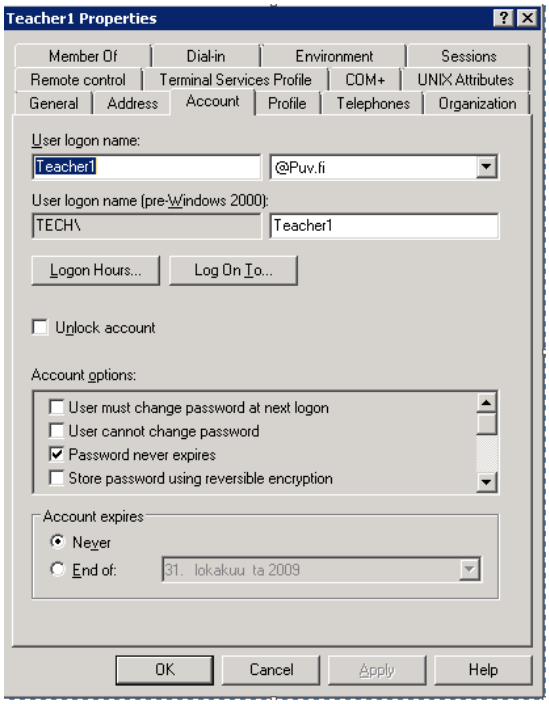
Avataan Server Manager -> Active Directory Domain Services ja Domain Users and Groups (katso kuva 14).



Kuva 14 Active Directory

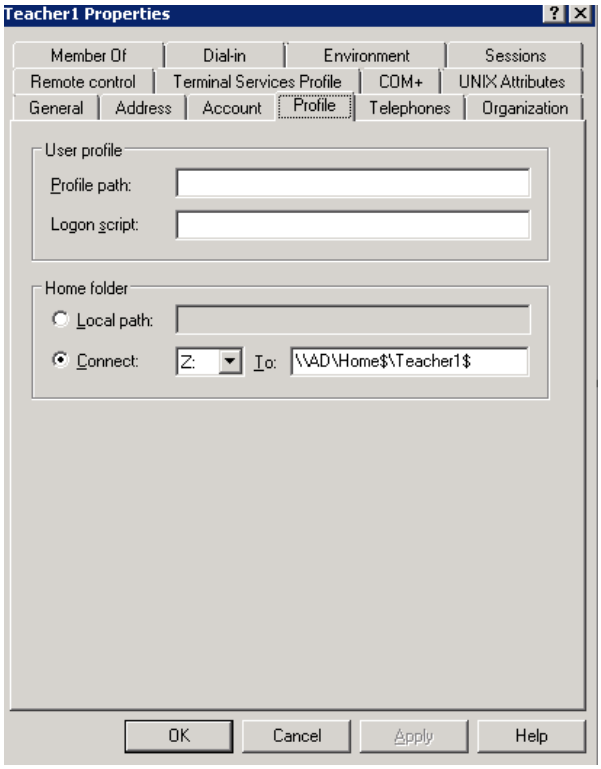
Kuvan 14 Active Directory Users and Group -valikossa hallinnoidaan toimialueen käyttäjiä sekä koneita. Kansioita, käyttäjiä, ryhmiä jne. luodaan tässä valikossa. Työssä luotiin kaksi Teacher-käyttäjää ja kaksi Student-käyttäjää ja niille omat ryhmänsä.

Kuvassa 15 on esimerkki Teacher1-käyttäjätilin tiedoista.



Kuva 15 Teacher properties

Kuvassa Teacher1 on @Puv.fi toimialueella ja käyttäjälle tämä näkyy TECH\Teacher1. Salasana on asetettu ja se ei vanhene, kuten ei vanhene käyttäjätilikään. Käyttäjän Teacher1-kotikansio asetetaan Profile-välilehdessä (katso Kuva 16).



Kuva 16 Home folder

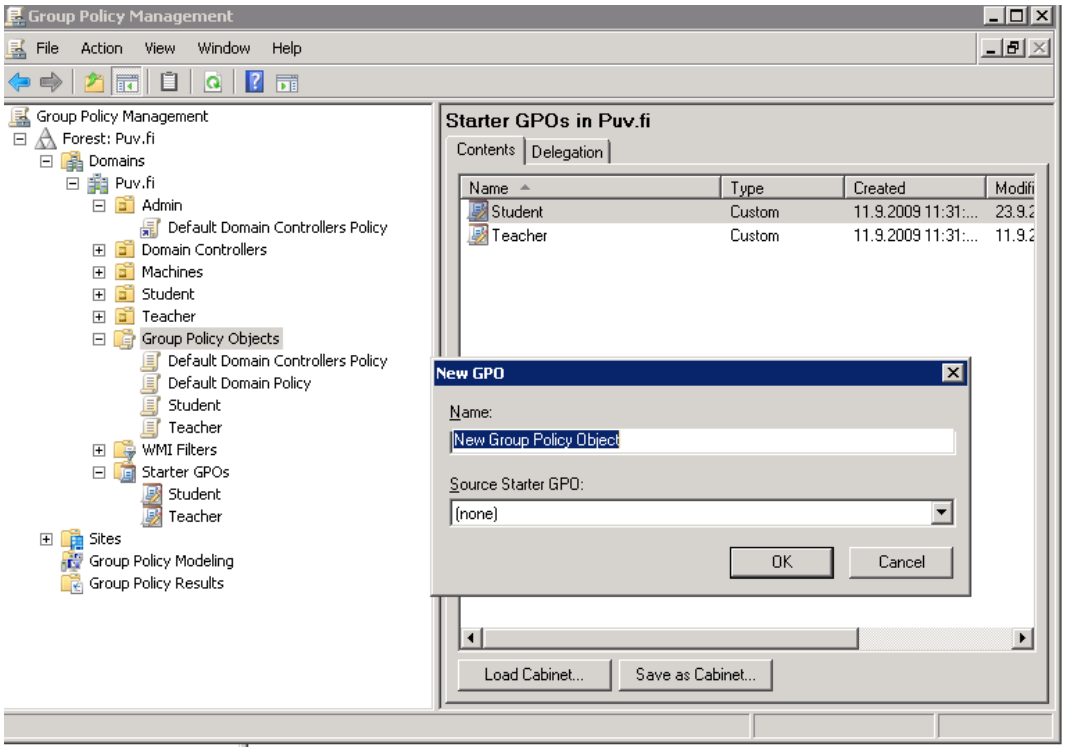
Kuvassa Teacher1-kotikansio on asetettu Z:\-levylle, joka sijaitsee AD-palvelimella kansioissa Home$. \\AD\Home$\Teacher1$ voidaan korvata \\AD\Home$\%Username%$, jolloin tietokone lisää itse kansion nimen oikeaksi. $-merkin takoitus on piilottaa kansio muilta käyttäjiltä.

4.3.2 Käyttäjäoikeudet

Käyttäjäoikeuksien hallinta tapahtuu Microsoft-oikeuksien hallinnassa. AD-palvelussa on esiasennettuna Default Domain Policy -tiedosto, joka koskee kaikkia toimialueen käyttäjiä. Default Domain Policy -tiedostoa muokkaamalla

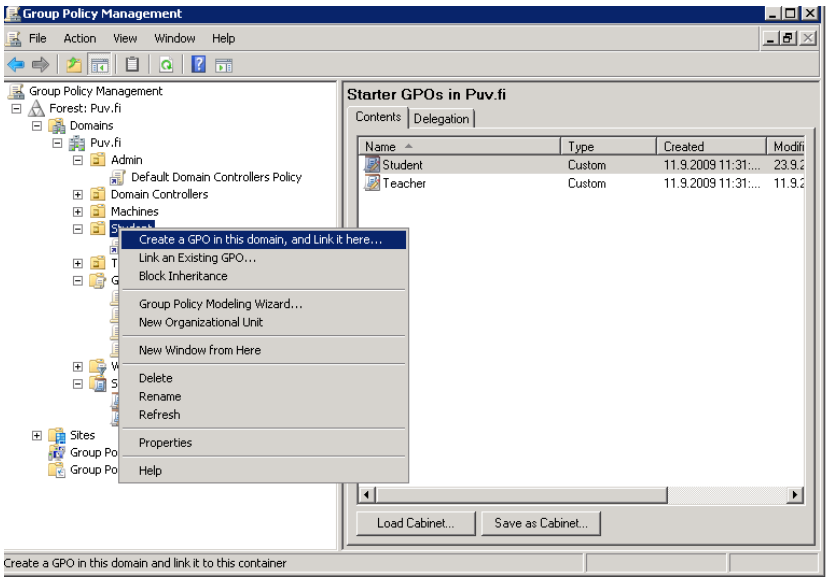
voidaan vaikuttaa kaikkien käyttäjien oikeuksiin. Kuitenkin esimerkikisi Domain Controllereilla on oma oikeustiedosto, joka jakaa tälle käyttäjäryhmälle oikeuksia. Myös Default Domain Policy jakaa eri oikeuksia.

Käyttäjäoikeuksia on helppo hallita kun käyttäjäryhmät on luotu. Jokaiselle käyttäjäryhmälle luodaan omat käyttäjäryhmäoikeudet. Ryhmäoikeudet tehdään ryhmäoikeushallinnassa (katso kuva 17).



Kuva 17 Domain policy

Ensimmäisenä luodaan uusi ryhmäoikeusobjekti. Tämän jälkeen uusi tiedosto linkitetään johonkin käyttäjäryhmään (katso kuva 18).

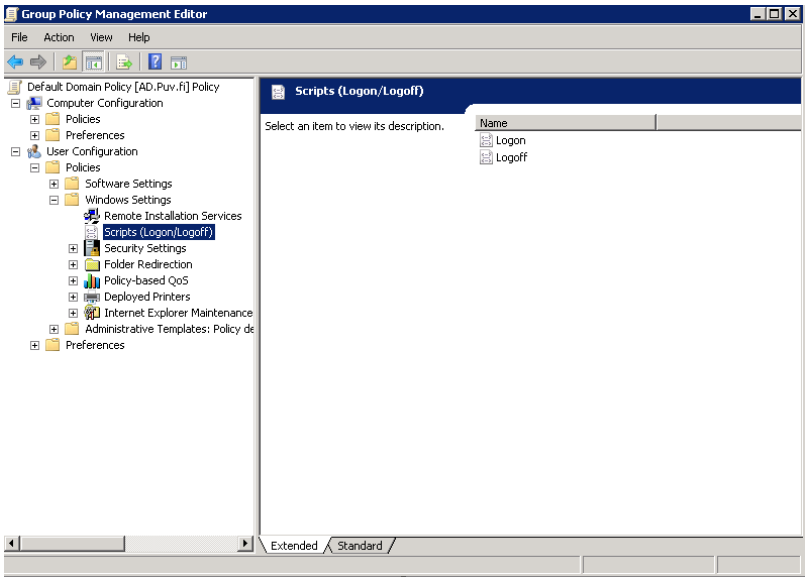


Kuva 18 Group policy

Kuvassa 18 linkitetään Student-ryhmälle tehty käyttäjäoikeustiedosto. Näin eri käyttäjäryhmille voidaan tehdä omat käyttöoikeusobjektit.

4.3.3 Logon script

Logon scriptiä käytetään, kun toimialuuen käyttäjä kirjautuu tietokoneella toimialueesen. Tällöin käynnistyy komentosarja, joka tunnistaa käyttäjän ja lisää sille kuuluvat verkkolevyt sekä tulostimen. Logon- ja logoff scriptejä on useita erilaisia. Scriptejä voidaan tehdä Visual Basic script -kielellä, tai käyttää net use -komentoja. Scriptit lisätään Default Domain policyyn (katso kuva 19).



Kuva 19 Scripts

Kuvassa 19 on lisätty logon script Default Domain Policyn käyttäjäasetuksien hallintaan. Eri logon scriptejä voidaan linkittää muille käyttäjäoikeusryhmille, mutta myös Default Domain Policyn script lisää verkkolevyt sekä tulostimet, joten tässä voi tulla päällekkäisyyksiä.

Tässä työssä käytetään Visual Basic script-ohjelmointikieltä skriptien tekemiseen, näin saadan parempi hallitavuus eri käyttäjäryhmien kirjautumiseen. VBS-scriptit ovat hankalampia tehdä kuin käyttää net use -komentoja, mutta käytettävyys on huomattavasti parempi. Taulukossa 2 on tämän työn logon script.

Taulukko 2. Logon script

```
Option Explicit

// ohittaa virheen
On Error Resume Next

Dim objADSysInfo        Määritetään objektit
Dim objCurrentUser
Dim strGroups
Dim wshNetwork


Private strDomain
Private strUserName
Set wshNetwork = WScript.CreateObject("WScript.Network")
strDomain = wshNetwork.UserDomain
```

```
strUserName = wshNetwork.UserName
WScript.Echo "Welcome " &  strUserName & "." // tervetuloa teksti

                  //Käyttäjäryhmät
Const Students          = "cn=students"
Const Teacher           = "cn=teacher"
Const Admin             = "cn=admin"


// määritelee objektit ja tunnista käyttäjän
Set objADSysInfo = CreateObject("ADSystemInfo")
Set objCurrentUser = GetObject("LDAP://" & objADSysInfo.UserName)
Set wshNetwork = CreateObject("WScript.Network")


If Not IsArray(objCurrentUser.MemberOf) Then
strGroups = lcase(objCurrentUser.MemberOf)
Else
strGroups = LCase(Join(objCurrentUser.MemberOf))
End If


//Määritellään mitä levyjä tietty ryhmä saa

If InStr(1, strGroups, Students) Then
        wshNetwork.MapNetworkDrive "s:","\\AD\Students"
        wshNetwork.MapNetworkDrive "l:","\\AD\Common"

        wshNetwork.AddWindowsPrinterConnection "\\AD\Brother"
         wshNetWork.SetDefaultPrinter "\\AD\Brother"

ElseIf InStr(1, strGroups, Teacher) Then

        wshNetwork.MapNetworkDrive "t:","\\AD\Teacher"
        wshNetwork.AddWindowsPrinterConnection "\\AD\Brother"
         wshNetWork.SetDefaultPrinter "\\AD\Brother"

ElseIf InStr(1, strGroups, Admin) Then

         wshNetwork.MapNetworkDrive "x:","\\AD\Admin$"
         wshNetwork.MapNetworkDrive "s:","\\AD\Students"
         wshNetwork.MapNetworkDrive "t:","\\AD\Teacher"
         wshNetwork.MapNetworkDrive "u:","\\AD\Public"
         wshNetwork.MapNetworkDrive "z:","\\AD\Home$\%username%$"
         wshNetwork.MapNetworkDrive                "p:","\\Linux-
nvxk\Linuxshare"

         wshNetwork.AddWindowsPrinterConnection "\\AD\Brother"
         wshNetWork.SetDefaultPrinter "\\AD\Brother"


End If
```

Taulukossa 2 on komentosarja, jolla toimialueen käyttäjäryhmät saavat niille tarkoitetut verkkolevyt ja tulostimet.

4.4 AD-tunnistautuminen

Active Directoryn verkkoon tunnistaudutaan Microsoftin tunnistautumispalvelulla käyttämällä LDAP-protokollaa sekä Kerberos-protokollaa. Unix-pohjaisista käyttöympäristöistä voidaan kirjautua toimialueelle jompaakumpaa mentelmää käyttäen.

4.4.1 LDAP lyhyesti

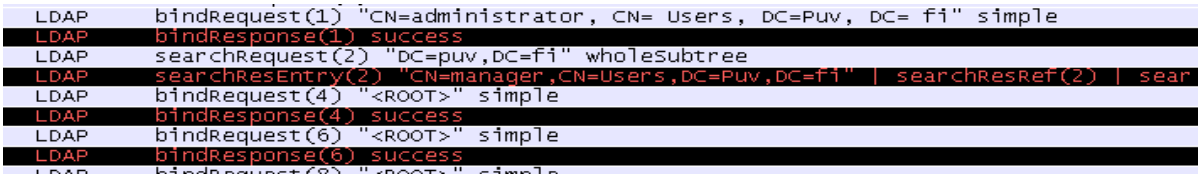
LDAP (Lightweight Directory Access Protocol) on IETF:n (Internet Engineering Task Force) määrittelemä protokolla. Nykyään käytetään LDAPv3:a, joka on kuvattu RFC 2251 -dokumentissa. LDAP:n tarkoituksena on käyttää kevyitä asiakasohjelmia, ja se voi hakea esimerkiksi sähköpostin osoitetietokannasta käyttäjän tietoja pelkän nimen avulla. Hyvä esimerkki LDAP:n toiminnasta on Vaasan ammattikorkeakoulun verkko, jossa käyttäjä voi vaihtaa missä tahansa palvelussa salasanan, jolloin salasana vaihtuu jokaiseen eri palveluun. Täten ei tarvita monia eri salasanoja, vaan voidaan käyttää vain yhtä. LDAP toimii attribuuttien avulla. Esimerkiksi puv.fi-toimialueen käyttäjä Teacher1 merkitään seuraavasti:
CN = Teacher1, OU = Teachers, DC = puv, DC = fi. LDAP hakee hierakkisesti tietoja Windowsin hakemistopalvelusta. Taulukossa 3 on kerrottu, mitä tomintoja LDAP-rajapinnalla on.

Taulukko 3. LDAP-komennot

bind	unbind	search	modify	add	delete	abandon
kytkeydy	pura yhteys	etsi	muokkaa	lisää	poista	luovuta

Taulukossa 3 olevilla komennoilla hallitaan käyttäjien ja asiakasohjelmien yhteyksiä. Bind-komennolla avataan yhteys asiakasohjelman ja palvelimen välillä.

Tällöin Palvelin tunnistaa kirjautuneen käyttäjän. Muokkaukseen tarkoitetut komennot add, modify ja delete mahdollistavat tietojen lisäyksen ja muuttamisen hakemistossa kuten salasanojen vaihdon. Search-komennolla ohjelma etsii tietoa palvelimen tietokannasta, esimerkiksi käyttäjätietoja. Kuvassa 20 on kuvattu yhteydenotto sekä hakuja tietokannassa. /4/, /7/

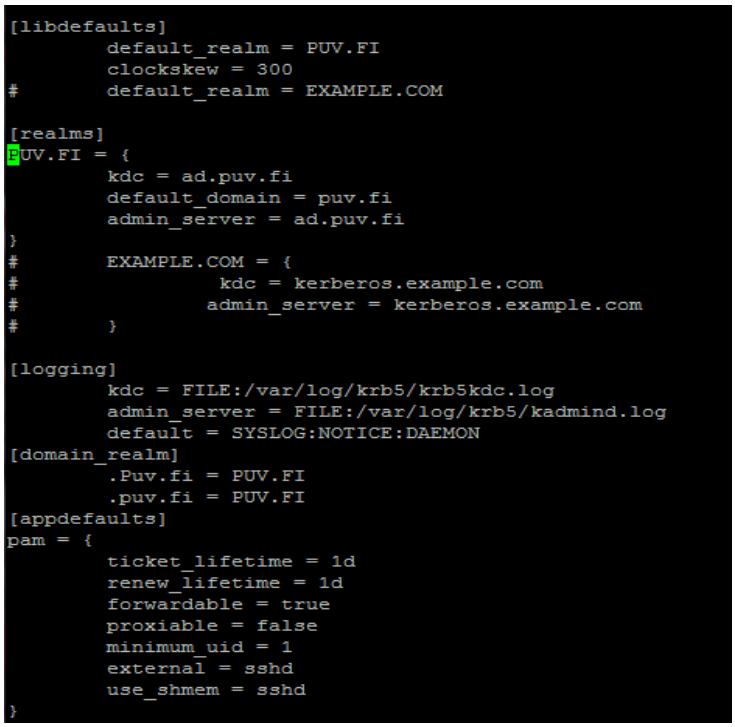


Kuva 20 LDAP

Kuvassa yhteyttä pyytää administrator, joka etsii manager-käyttäjää aloittaen hierarkkisen järjestelmän juurelta.

4.4.2 Kerberos lyhyesti

Kerberos on tunnistusprotokolla, joka aikanaan kehitettiin Unix-maailmaan. Windows Server 2008 käyttää uusinta Kerberos 5 -protokollaa, joka on kuvattu RFC 1510 -dokumentissa. Kerberos on tunnistusprotokolla, joka käyttää tikettejä tunnistamiseen. Nämä tiketit on salattu. Kerberos ei lähetä salasanoja verkossa, vaan tunnistaa käyttäjän ilman niitä. Kerberos-autentikointia on helpompi lähestyä Linuxin kautta. Linux-koneita saadaan liitettyä Windows-verkkoon Kerberoksen avulla (kuva 21). /5/



Kuva 21 Kerberos

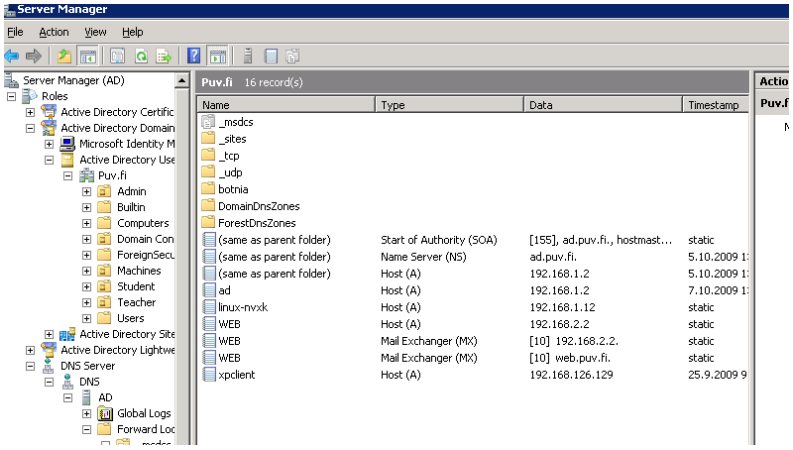
Kuvassa 21 on Linux-koneen krb5.conf -tiedosto. Tiedostossa on myönnetty tiketti jolla Kerberos voi hakea yhteyspyyntöä Key Distribution Centre:stä (KDC). KDC:tä hallitsee toimialueen DC. Yhdessä tiketissä voi olla vain yksi KDC-serveri. Kerberos autentikoi myös yhteyden palvelimeen, jotta käyttäjä ei yhdistä väärän palvelimeen. Kerberos-protokollaa voi käyttää hyvin myös suojaamattomassa verkossa.

4.5 Toimialueelle kirjautuminen

4.5.1 DNS

Domain Controllerissa on DNS (Domain Name System), joka hallitsee toimialueen nimitietokantaa. DNS-järjestelmän asentaminen tapahtuu automaattisesti toimialueen asennuksen aikana, koska toimialue tarvitsee DNS-palvelua toimiakseen. Toimialueen DNS-palvelin ei hoida nimikyselyjä muualla kuin intraverkossa. WWW (World Wide Web) -kyselyihin toimialue tarvitsee

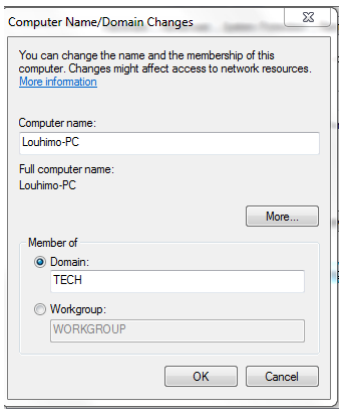
ulkopuolisen, oikean DNS-palvelimen toimiakseen. Kuvassa 22 on toimialueen DNS-palvelin. /8/



Kuva 22 DNS

4.5.2 Kirjautuminen

Toimialueelle kirjautuminen tapahtuu asiakaskoneella kuvan 23 mukaisesti.



Kuva 23 Kirjautuminen

Kuvassa 23 liitetään kone TECH-toimialueelle. Koneen liittävät toimialueelle vain ne käyttäjät, joilla on oikeus siihen. Esimerkiksi Domain Controller saa lisätä koneita toimialueellensa. Asiakaskoneella, joka liitetään toimialueelle, pitää olla sama kellonaika, jotta koneen lisääminen toimialueelle on mahdollista.

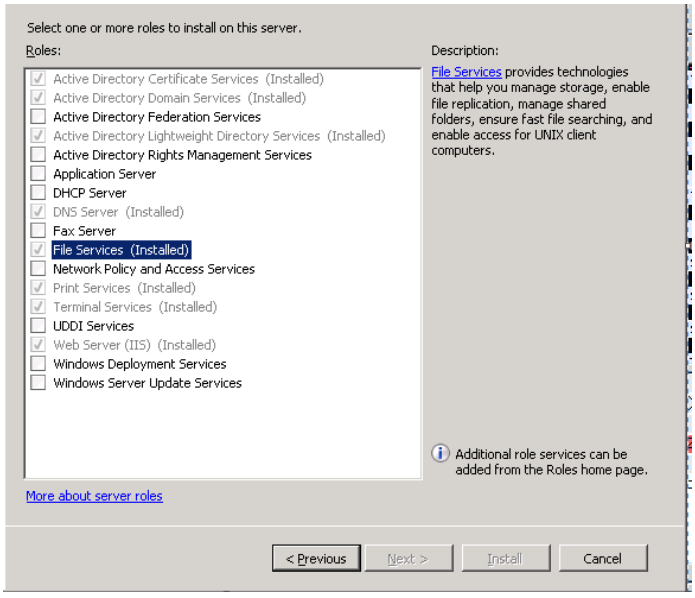
4.6 Microsoft-levypalvelu

4.6.1 Yleistä levypalveluista

Levypalvelimilla saadaan organisaation työympäristön tietoturvaa paremmaksi. Parannuksia saadaan varmuuskopioimalla jaettuja verkkolevyjä. Näin ollen yritysten tietohallintotyöntekijöiden ei tarvitse tulla työpisteille ottamaan varmuuskopionteja eikä lisämään kiintolevytilaa koska kaikki on keskitetysti verkossa. Nykyisissä levypalvelimissa käytetään myös QUOTA-palvelua, jolla saadaan suuren levyn kapasiteettia jaettua käyttäjien kesken. Esimerkiksi Vaasan ammattikorkeakoulun oppilaskäyttäjillä on omaa tilaa käytettävissä 200 MB. Työssä asennetaan SMB- levyjako sekä NFS, koska SMB-jakoa voidaan käyttää Linux-koneissa hyvin Samban avulla ja NFS-protokollalla tehtyä jakoa voidaan käyttää monella eri alustalla, esim. Macillä.

4.6.2 Asennus

Microsoftin levypalvelin asennetaan lisäämällä rooli (add role). Kuva 24



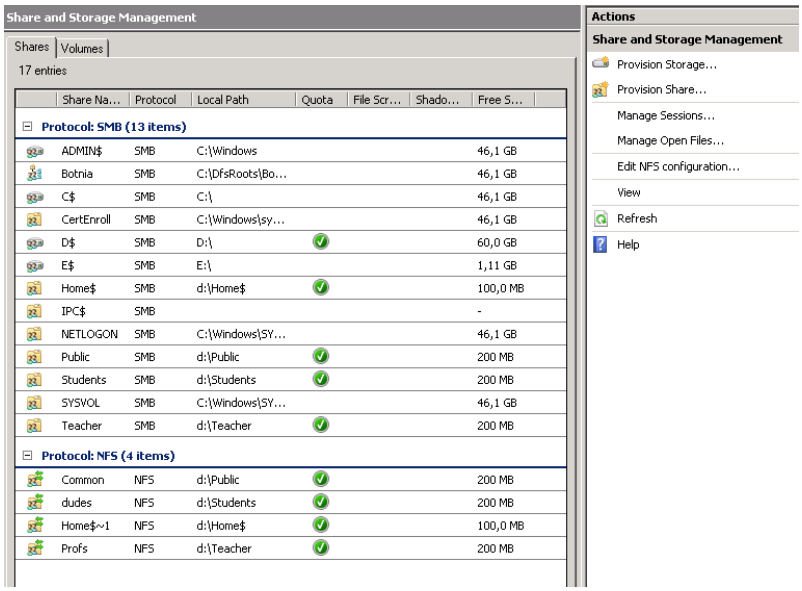
Kuva 24 Microsoft-levypalvelu

Kuvassa 24 on roolien lisäämiskeskus, josta rastitaan File Services. Asennuksen aikana asennus kysyy muita lisäpalveluita, joista valitaan DFS (Distributed File

System), File Server Resources Manager sekä Networ File System. Tämän jälkeen asennus on valmis. Levypalvelimen nimi on AD\\.

4.6.3 Levyjaon käyttöönotto

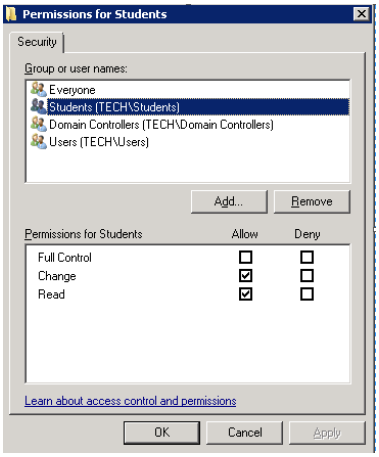
Levyjakoa hallitaan Share and Storage Managementistä, joka löytyy Server Manager → File Services -välilehdestä. Kuvassa 25 on Share and Storage Management -pääsivu, josta nähdään kaikki jaot ja jossa voidaan hallita levynjakojärjestelmää. /11/



Kuva 25 Verkkojaot

Kuvassa 25 on kaikki jaot ja levyn kapasiteetit sekä Quota-tiedot. Levyjakoja tehdään Action-paneelin Provision Share -kohdasta.

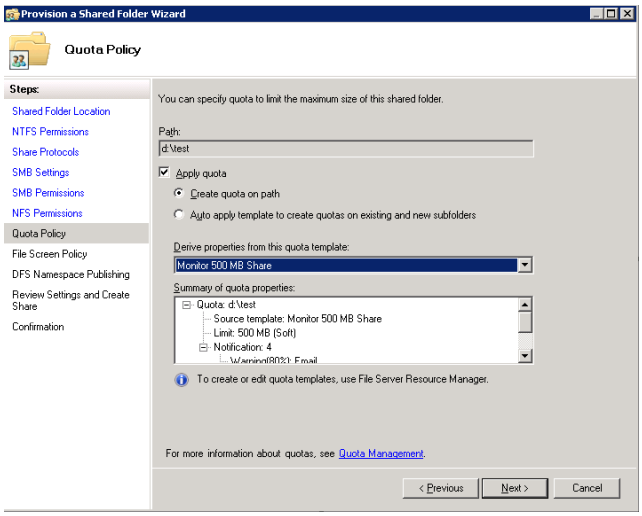
Verkkolevyn luonnin aikana on tärkeää tietää kenelle tai mille ryhmälle kansion verkkojako tehdään. Esimerkiksi opinnäytetyössä luotiin Students-kansio. Kansion tarkoitus on luoda oppilaille oma yhteinen verkkolevy. Tällöin kansion asetuksien tulee olla seuraavat (katso kuva 26).



Kuva 26 Student policy

Kuvassa 26 on säännöt annettu niin, että Students-käyttäjäryhmällä on oikeus hallita, luoda kansioita ja lukea tietoja verkkolevyllä. Muilla käyttäjillä on vain oikeus lukea, poislukien Administrator ja Domain Controller, joilla on täydet oikeudet kansioihin. Seuraavaksi asennus kysyy, millä protokollalla levy jaetaan. Tässä työssä valitaan kummatkin vaihtoehdot, eli SMB (Server Message Block) ja NFS (Network File System). Network File System on protokolla, jolla voidaan jakaa verkkolevyjä verkkoon, jossa ei ole Windows-koneita. SMB on protokolla, jolla voidaan jakaa verkkolevyjä ja tulostimia Windows-verkoissa. Windows Server 2008 käyttää uudempaa SMB2-protokollaa.

Oppilas- tai opettajakäyttöön tarkoitetuille verkkolevyille on annettu 200 MB:n Quota. Quotan lisääminen tapahtuu levyjaon yhteydessä Quota-kohdassa. Kuvassa 27 on näytetty Quota-asetuskohta.



Kuva 27 Quota

Kuvassa 27 on esimerkkinä test-niminen jako, johon lisätään 500 MB jaettu Quota. Opinnäytetyössä käytetään 200 MB:n tiedostoja, joista lähtee ilmoitus käyttäjälle sähköpostitse, kun 80 % tilasta on käytetty. Microsoft-levypalvelimessa on kuusi valmista mallia, joita voi käyttää verkkolevyjaoissa. Taulukossa 4 on kerrottu valinnat.

Taulukko 4. Quota-vaihtoehdot

100 MB Limit
200 MB Limit Reports to User
200 MB Limit with 50MB Extensions
250 MB Extended Limit
Monitor 200GB Volume Usage
Monitor 500 MB Share

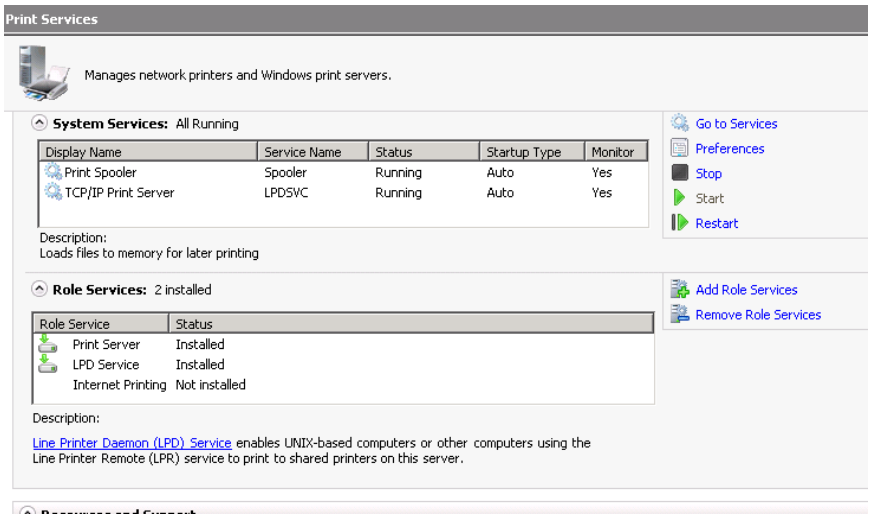
Asennus kysyy, estetäänkö audion ja videon lisääminen verkkolevyille. Tässä työssä sitä ei estetty. Tämän jälkeen verkkolevyn luonti on valmis.

4.6 Tulostinpalvelu

Tulostinpalvelulla voidaan organisaatioissa keskittää tulostimet ja jakaa tulostimet eri ryhmien kanssa. Tulostinpalvelu Active Directory -verkossa on erinomainen, koska käyttäjillä on mahdollisuus tulostaa mihin tahansa hakemistoon listattuun tulostimeen.

4.6.1 Asennus

Opinnäytetyössä käytetään Brother HL-2150N -verkkotulostinta. Tulostinpalvelu lisätään lisäämällä rooli Server Manager -ohjelmasta. Asennuksen aikana kysytään, asennetaanko tulostin paikallisena tulostimena vai verkkotulostimena. Tässä valitaan verkkotulostin. Asennus kysyy vielä, mitä muita ominaisuuksia lisätään. Tällöin valitaan LDP Service (Line Daemon Printer), joka mahdollistaa muillakin kuin Windows-koneilla tulostamisen. Brother-tulostimen paketin mukana tulee ajuri-CD, jonka asentamalla saadaan oikeat ajurit. Tulostinta hallitaan Server Manager -ohjelmassa Print Services -kohdasta. Katso kuva 28. /14/

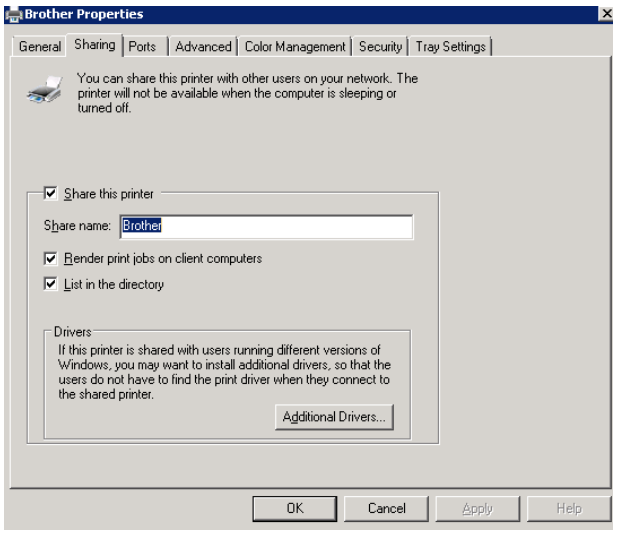


Kuva 28 Tulostinpalvelu

Kuvassa 28 on printteripalvelimen hallintasivu.

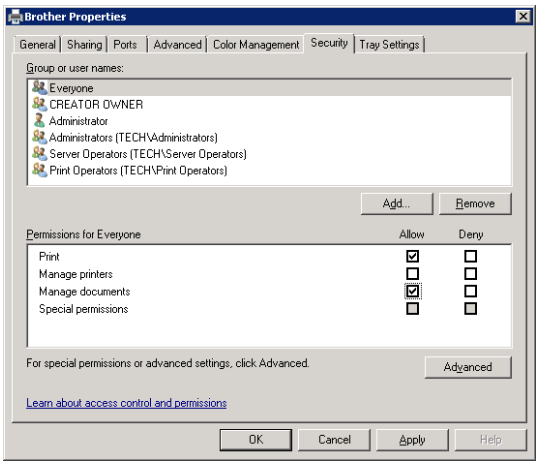
4.6.2 Asetukset

Tulostimen asetuksissa tärkeimmät kohdat näkyvät kuvassa 29.



Kuva 29 Brother-tulostin

Kuvassa 29 on tulostimen asetuksien Jako-välilehti. Välilehdeltä pitää tarkistaa, että tulostin on jaossa, ja että ruksi on siinä kohdassa, jossa tulostin listataan hakemistoon. Toimialueella on siis tällä hetkellä listattuna yksi tulostin. On myös tärkeää jakaa käyttöoikeudet niin, että käyttäjä ei saa koskea tulostimen asetuksiin, mutta saa muuttaa tulostusjonoa. Suurimmissa organisaatioissa käyttötukihenkilöt eivät muuta ehtisi tekemäänkään kuin poistamaan tulostuksia jonosta, jos käyttäjällä ei olisi lupaa poistaa omia tulostuksiaan, kun ne menevät tukkoon tai sattuu jokin muu häiriö. Kuvassa 30 on annettu jokaiselle oikeus tulostaa ja hallita dokumentteja tulostimissa. /14/



Kuva 30 Brother Properties

5 WWW-PALVELIN

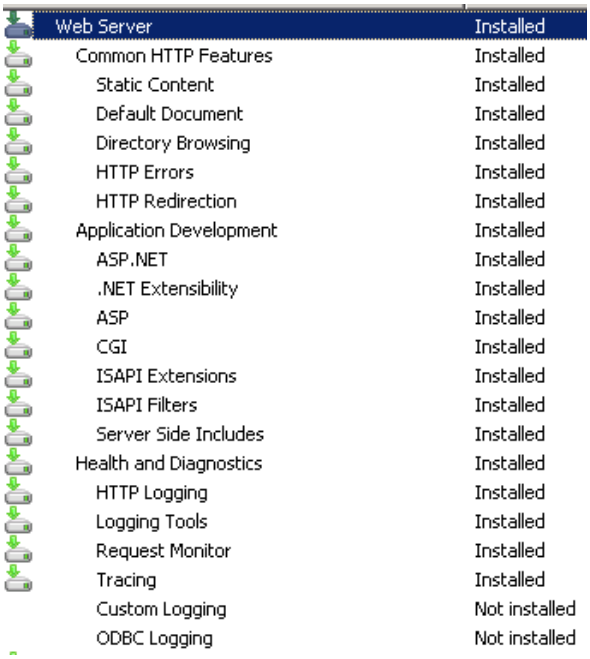
5.1 WWW-palvelin lyhyesti

WWW-palvelimen tarkoitus on tuoda HTTP-palvelut asiakkaalle. HTTP käyttää hyödykseen porttia 80 ja salatuissa yhteyksissä porttia 445. Tiedonsiirto sekä kyselyt ja vastaukset siirtyvät tcp-protokollaa hyväksi käyttäen. Windows Server 2008:ssa on uusi IIS7 web-palvelu. Microsoft on tuonut paljon uusia ominaisuuksia web-palvelimeen. Siinä on PHP- ja ASP.NET-tuki, joiden avulla PHP-ohjelmistojen käyttöönotto on helppoa. Tukena on FASTCGI-moduuli, jonka tarkoitus on edesauttaa ohjelmistojen vakautta sekä toimivuutta.

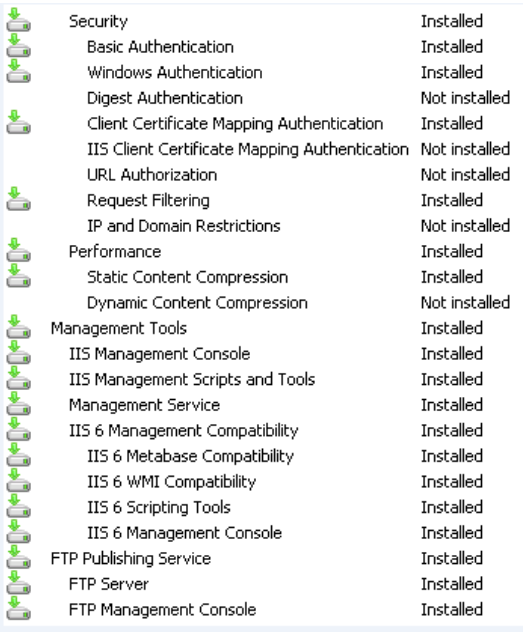
Tässä opinnäytetyössä käytetään Windows IIS7 -palvelinta, koska TS (Terminal Services) -palvelut vaativat Microsoft IIS -palvelun. /10/

5.2 WWW-palvelimen asennus

WWW-palvelin asennetaan DMZ-alueelle koneelle jonka DNS suffix on web.puv.fi. Koneeseen asennetaan WWW-palvelin samalla tyylillä kuin muutkin Windows Server -roolit, eli lisäämällä rooli Add role -valikosta. WWW-palvelin lisää automaattisesti omat tarvitsemansa komponentit, mutta WWW-palvelimen tehokäyttöön täytyy itse asentaa lisäominaisuuksia. Kuvissa 31 ja 32 näkyy, mitä palveluita tässä työssä on asennettu. /11/

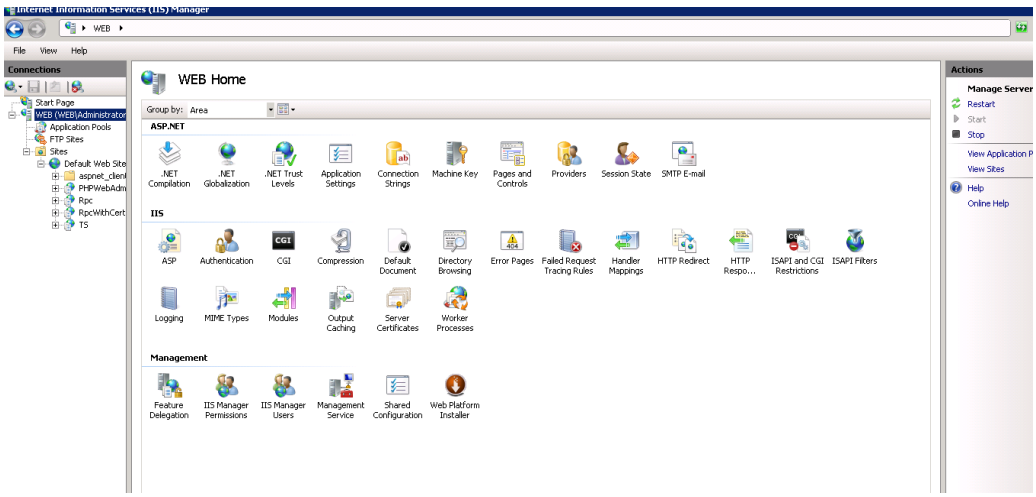


Kuva 31 WWW-roolit



Kuva 32 WWW-roolit

Kuvissa 31 ja 32 nähdään, että Web Serverillä on paljon eri palveluita käytössä. Kaikkia palveluita ei edes tulla käyttämään tämän lopputyön aikana. Osa palveluista asentuu automaattisesti kun asennetaan erillistä ohjelmistoa. Esimerkiksi, kun asentaa Terminal Service -palvelun, asennus pyytää asentamaan muutaman lisäominaisuuden WWW-palvelimelle. Microsoft IIS -hallintakonsoli on kuvattu kuvassa 33.



Kuva 33 IIS manager

Kuvassa 33 on IIS-hallintakonsoli, johon päästään Adminstrative tools → Internet Information Service Manager. Tällä sivulla hallinoidaan yleistä WWW-palvelinta ja palvelimen turvallisuutta. Palvelimen toimivuutta voidaan testata menemällä osoitteseen http://botnia.puv.fi. IIS-palvelu asettaa kotisivuksi kuvan 34 mukaisen kotisivun.

Kuva 34 IIS7-sivu

Kuvassa 34 on http://botnia.puv.fi-kotisivu ennen kuin siihen on tehty oma kotisivu.

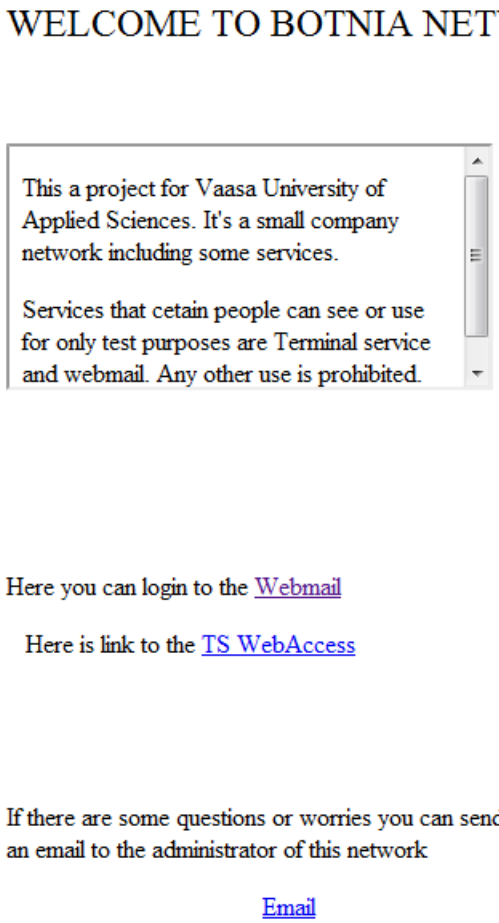
5.2.1 Oman kotisivun asettaminen

Kotisivu asetetaan IIS-ohjelman juurikansioon, joka on C:\Inetpub\wwwroot\. Kotisivutiedoston nimi voi olla mikä tahansa, mutta myös IIS-ohjelmistoon tiedoston nimi pitää käydä asettamassa. Valmiissa IIS-ohjelmistossa on monta valmista mallia, ja ne näkyvät taulukossa 4./9/

Taulukko 4. HTTP- sivujen malli tiedoston nimet.

Default.htm	iisstrat.htm
Default.asp	default.aspx
Index.htm	
Index.html	

Tässä työssä käytettiin iisstrart.htm -nimeä, ja uusi kotisivu näkyy kuvassa 35.



Kuva 35 Kotisivu

Kuvassa 35 on http://botnia.puv.fi:n uusi kotisivu.

5.3 IIS-ohjelmat lyhyesti

WWW-palvelimessa toimivat ohjelmat, jotka on tehty esimerkiksi PHP:llä, osaavat vastata HTTP-pyyntöihin. Monet ohjelmat ovat suoraan exe- tai php-tiedostoja, joita ei voida avata selaimella, ellei niitä asenneta IIS-palvelimelle ja käytetä Cgi-moduulia. Esimerkiksi PHP webAdmin tai sähköpostiohjelmat ovat kasa eri kooditiedostoja, ja Cgi-moduuli osaa tehdä näistä toimivan ohjelman. Tässä opinnäytetyössä on Terminal Service -ohjelma, joka on asennettu IIS-

palvelimen ohjelmiin. URL (Uniform Resource Locator) tälle ohjelmalle on osoite http://botnia.puv.fi/ts.

6 TERMINAL SERVICE

6.1 Terminal Servicen hyödyt

Tässä työssä tarvittiin etäyhteys. Etäyhteys päätettiin tehdä Windowsin uudella TS (Terminal Service) -ohjelmalla. Uudessa ohjelmistossa on paljon uusia ominaisuuksia, jotka helpottavat etäyhteyden luontia. Nykyään yrityksissä kuten Vaasan ammattikorkeakoulussa, käytetään VPN-yhteyksiä, kun esimerkiksi opettajat ottavat yhteyden koulun verkkoon. VPN:ssä on se huono puoli, että kun otetaan VPN-yhteys ja asiakaskone on saastunut on mahdollista, että koulun verkko saastuu samalla. VPN-yhteydessä on myös huonona puolena se, että se pitää asentaa joka koneelle erikseen. Käyttäjät eivät voi liittyä verkkoon tai käyttää työpaikan palveluja miltä koneelta tahansa.

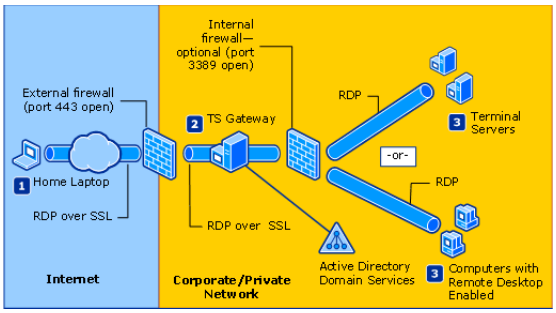
TS käyttää suojattua HTTP-yhteyttä TS Gateway -koneelle, jolloin koneille syntyy SSL/TLS tunneli portissa 443. TS Gateway -kone ohjaa liikenteen asiakaskoneille tai TS Server -koneille porttia 3389 pitkin. Tämä tekniikka auttaa käyttäjiä yhdistämään koneensa esimerkiksi yrityksen verkkoon missä tahansa ja käyttää yrityksen verkon palveluita mistä tahansa. Yritysverkkoon ei luoda kiinteää yhteyttä vaan se virtualisoidaan. TS-palvelun käyttäjille voidaan jakaa erilaisia käyttöoikeuksia. Voidaan esimerkiksi määrittää mihin palveluihin eri käyttäjäryhmät voivat kirjautua. Tietokoneita ja niiden kirjautumiskeinoja voidaan rajata. Voidaan esimerkiksi määritellä, pitääkö koneen kuulua toimialueeseen, voiko kirjautua sisään salasanalla tai pitääkö käyttää tunnistautumiskorttia.

6.2 Terminal Service -asennus

Terminal Servicellä on kolme erilaista asennusmahdollisuutta: CORE, NAP ja ISA. NAP-asennuksessa käytetään erillistä palvelinta, joka tarkistaa asiakaskoneen pätevyyden verkkoon. NAP-asetuksella lisätään turvallisuutta verkkoon; esim. asiakaskone ei pääse verkkoon, ellei siinä ole Windows Update päällä. Verkosta halutaan avoin, ja monessa koneessa ei ole Windows Update

päällä, koska erillinen ohjelma päivittää tietokoneita. NAP:in asettaminen ei ole vaikeaa. Näistä syistä NAP-asetusta ei käytetä.

ISA-asennuksessa käytetään erillistä palvelinta DMZ-alueella, josta lähtee erillinen SSL-tunnelointi intraverkon TS GATEWAY -koneelle. Laitteistoa tarvitaan enemmän, joten tässä työssä käytetään Core-asennusta. Laitteiden ja ohjelmistojen riittävyys on sopiva Core-asennukseen. Core-tyylinen asennus on nähtävillä kuvassa 36.



Kuva 36 /13/

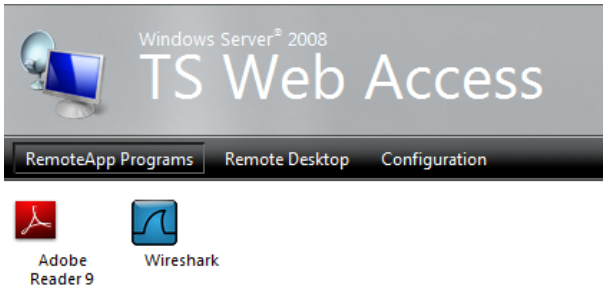
Kuvassa 36 kotitietokone pääsee yritysverkkoon portin 443 kautta. Portissa on SSL-tunnelointi. TS Gateway hyväksyy yhteyden varmentamalla käyttäjätiedot DC:ltä. Yhteyden takana voi olla erilaisia Terminal-palvelimia tai esimerkiksi työpaikan kone, johon halutaan ottaa yhteyttä. /13/

Terminal Service asennetaan lisäämällä palvelimeen rooli (add role). Koneelle, jossa on WWW-palvelin (web.puv.fi), asennetaan seuraavat Terminal Service roolit: Terminal Service, TS Gateway ja TS WebAccess. Tärkeimmät asiat, jotka asennuksen aikana pitää valita, ovat käyttäjäsäännöt sekä sertifikaatti etäyhteyspalvelulle. Sertifikaatti, joka valitaan, on botnia.puv.fi, koska on ehdottoman tärkeää, että TS Gateway ja sertifikaatti ovat samannimisiä. Käyttäjäsäännöillä valitaan, ketkä saavat yhdistää TS Gatewayn kautta. TS CAP ja TS RAP ovat autentikointi- eli käyttäjäsääntöjä. TS CAP on tarkoitettu ryhmille sekä yksittäisille käyttäjille, ja TS RAP on tarkoitettu tietokoneille. TS RAP

tarkoittaa sitä, minkä niminen tietokone saa yhdistää ja mihin. Tässä työssä käytetään vain TS CAP -sääntöä. Opettajat ja verkonhallitsijat saavat yhdistää koneensa mihin tahansa verkon palveluun. Tämän jälkeen asennus on valmis.

6.2.1 TS Web Access

TS Web Access on ohjelma, jonka avulla voi selaimella ottaa yhteyttä TS Gateway -koneelle. TS Web Access -sivulla voidaan ottaa etäyhteys verkko-ohjelmiin tai yhdistää verkossa oleville koneille. Ts Web Access -sivustoon pitää yhdistää Internet Explorerilla, koska sivusto käyttää Microsoftin TS ActiveX -plugia, joka ei toistaiseksi toimi kunnolla muilla selaimilla. Kuvassa 37 on TS WebAccess:n pääsivu.



Kuva 37 TS Web Access

Kuvassa on kaksi verkko-ohjelmaa, joita voivat käyttää käyttäjät, joilla on oikeus siihen. Remote Desktop -välilehdeltä pystyy kirjautumaan joihinkin verkon resursseihin. Configuration-välilehdeltä voi vaihtaa eri Terminal Service -paikkaan. Tällä hetkellä Adobe Reader ja Wireshark on ohjattu TS Gateway -koneelta. Configuration-välilehdeltä voi vaihtaa verkko-ohjelmia kun valitsee eri tietokoneen nimen.

6.3 TS Licensing

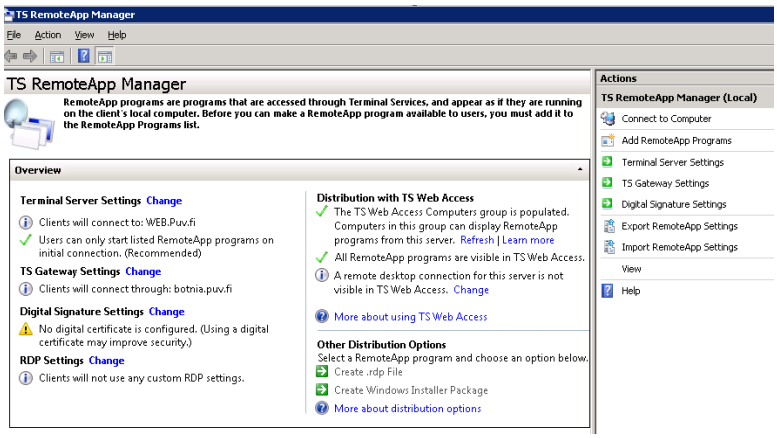
TS Licensing Manager on ohjelma, jota Terminal Services -ohjelmat käyttävät. Terminal Services -ohjelmat hakevat lisenssitietonsa sieltä. Jotta verkko-ohjelmia voidaan käyttää pitemmän aikaa kuin 120 päivää, tarvitsevat Terminal Service -ohjelmat lisenssiserverin. Microsoftilta voi ostaa lisenssejä, mutta pelkän lisenssipalvelimen asennus ja aktivointi riittää. TS Licensing asennetaan Domain Controller -koneelle. Terminal Service -tietokoneet löytävät automaattisesti verkosta lisenssipalvelimen. TS Licensing asennetaan samalla tavalla kuin muutkin ohjelmat, mutta pakettien asennusohjelmistossa Terminal Service -valikossa valitaan vain TS Licensing. TS Licensing -palvelu tulisi vain aktivoida ja TS-koneet löytävät palvelun automaattisesti.

6.4 RemoteApp

Nykypäivän yrityksissä etätyön tekeminen on mahdollista VPN- ja Citrix-ohjelmien avulla. Microsoft on tuonut markkinoille oman Citrixiä vastaavan ympäristön, joka mahdollistaa etätyöskentelyn tai muun etäkäytön. Yritykset ja organisaatiot voivat asentaa verkko-ohjelmia, joita voidaan käyttää mistä tahansa etänä.

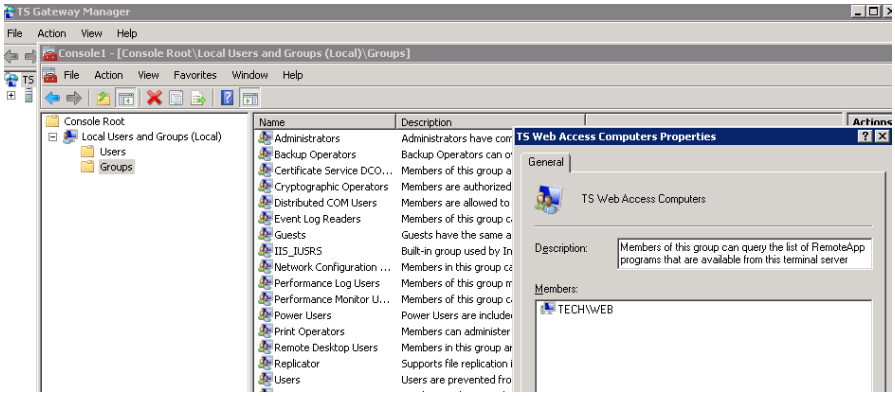
6.4.1 Asetukset

Kuvassa 38 on RemoteApp-hallintaohjelma.



Kuva 38 Remote App -ohjelma

Kaikki etäohjelmiston hallinta on kyseisellä sivustolla. Sivustolta voidaan lisätä tai poistaa sovelluksia tai muokata yhteysasetuksia. Jotta saadaan etäohjelmat näkymään TS Web Access -ohjelmistossa, on tietokoneet ensin määritettävä TS RemoteApp -ryhmään. Tietokoneet lisätään Local users and groups -hallinnasta tai DC:n Domain Users and Groups -valikosta, riippuen siitä, minkälaisella asetuksella verkko on tehty. Tässä työssä lisätään tietokoneet RemoteApp Distribution -ryhmään web.puv.fi-koneen Local Users and Groups -hallintaohjelmasta. MMC :stä valitaan Local Users and Groups -välilehti. Katso kuva 39.



Kuva 39 Gateway Manager

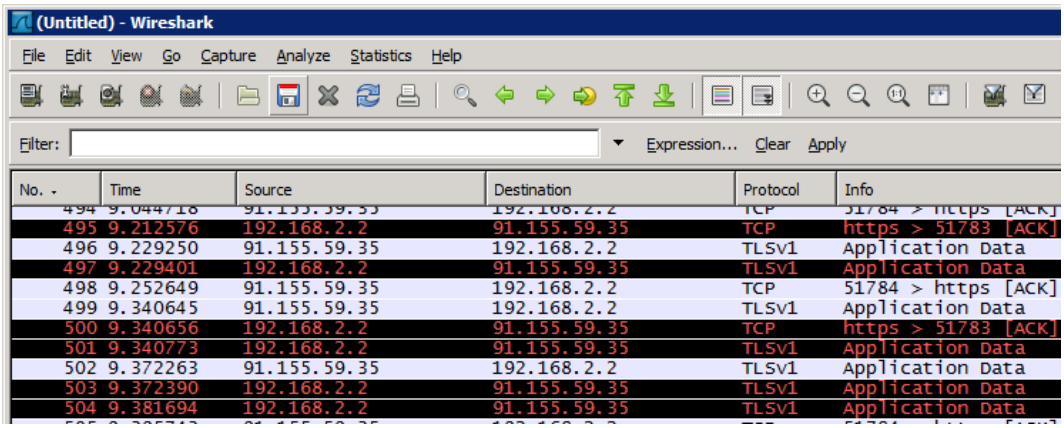
Kuvassa lisätään TECH-toimialueelta WEB-kone TS Web Access -jäseneksi. Tällöin WEB-kone voi jakaa ohjelmistoja käyttäjille. Tämän jälkeen ohjelmistoja voidaan lisätä hallintaohjelman kautta. Ohjelmia lisätään Action-paneelista Add RemoteApp -kohdasta. Verkko-ohjelmat pitää vielä lisätä näkyviksi verkkojakeluun komennolla Show in TS Web Access. Tässä työssä lisättiin Adobe Reader- sekä Wireshark-ohjelmat.

6.4.2 Testaus

Verkko-ohjelmat voi helposti testata avamaalla sivun https://botnia.puv.fi/ts. Sivustolla on nyt Wireshark- sekä Adobe Reader -ohjelmistot. Ohjelmien avautuessa kysytään käyttäjänimeä ja salasanaa, koska ohjelmisto avataan eri

paikasta kuin missä ohjelmisto on, ja käyttäjät ovat toimialuekäyttäjiä. Käyttäjänimi on syötettävä TECH\käyttäjänimi, jotta kerrotaan mikä on toimialue ja ohjelma voidaan avata.

Kuvassa 40 on onnistuneesti avattu Wireshark-ohjelma.



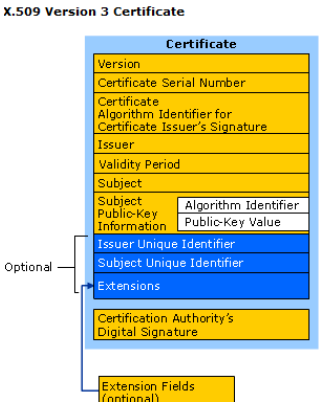
Kuva 40 Wireshark

Kuvasta nähdään, että tietokoneeseen on luotu suojattu yhteys ja Wireshark pyörii paikallisesti Vaasan Technobotnian tiloissa IP:llä 192.168.2.2. IP 91.155.59.35 tulee Saunalahden verkosta Tampereen Pyynikin kaupunginosasta.

7 VARMENNE

7.1 Yleistä varmenteista

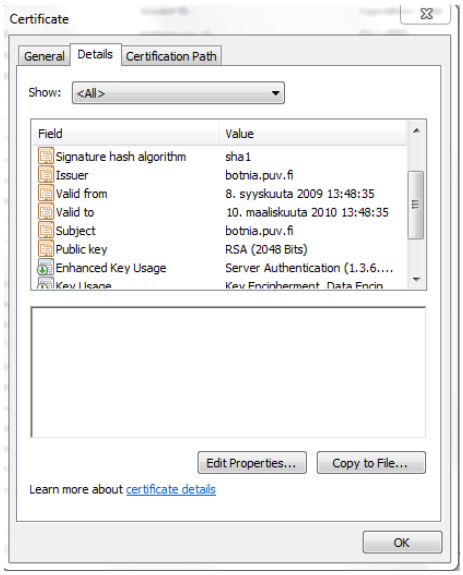
Sertifikaatilla eli varmenteelta voidaan tunnistaa käyttäjä johonkin palveluun, kirjautua koneelle tai esimerkiksi verkkokauppaan. Varmenteessa voi olla tietoja käyttäjästä tai organisaation tai yrityksen yhteystietoja. Nykyään käytetään versio kolmosta X.509, joka on ITU-T:n julkaisema. Kuvassa 40 näkyy X.509-varmenne ja sen arkkitehtuuri.



Kuva 40 /15/ Varmenteen arkkitehtuuri

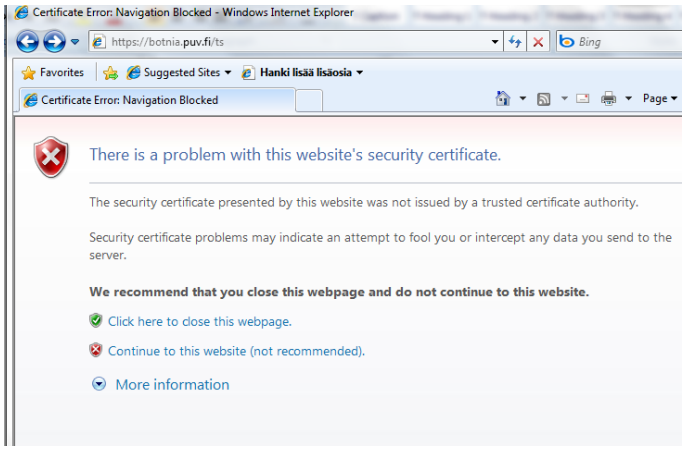
7.1.1 Varmenteen käyttö

Tässä opinnäytetyössä käytetään varmenteita TS-palveluissa. Käyttäjän ottaessa etäyhteyden palvelin pyytää botnia.puv.fi -varmenteen. Botnia.puv.fi -varmenne on niin sanottu root, jonka Certificate Authority on hyväksynyt. Certificate Authority on hierarkkisesti korkeimmalla kohdalla, joten botnia. puv.fi -varmenne on päävarmenne. Kuvassa 41 on kuva botnia.puv.fi -varmenteesta.



Kuva 41 Varmenteen asetukset

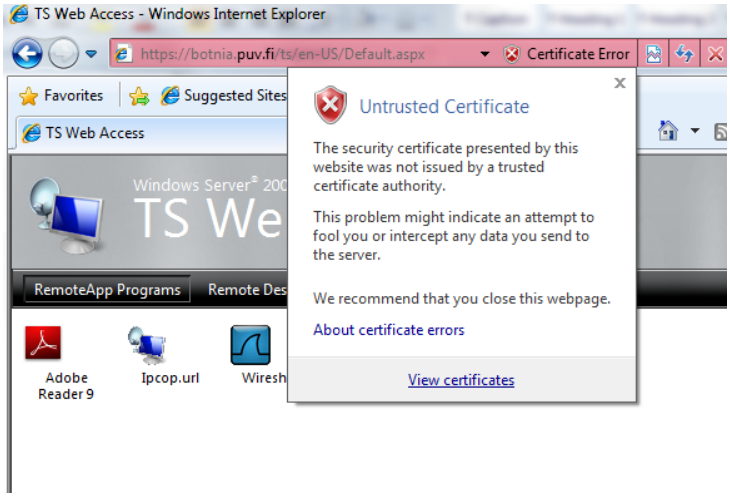
Kuvassa 41 näkyvät tärkeimmät asiat varmenteesta. Jotta varmennetta voidaan käyttää, Subjectin sekä Issuerin pitää olla samannimisiä. Tärkeää tietoa on myös se, kuinka kauan varmenne on voimassa. Työssä käytetään varmennetta tunnistamaan oikeat käyttäjät terminaalipalveluissa. Yhdistettäessä https://botnia.puv.fi/ts -sivustolle selain ilmoittaa varmennevirheestä. Katso kuva 42.



Kuva 42 Certificate Error

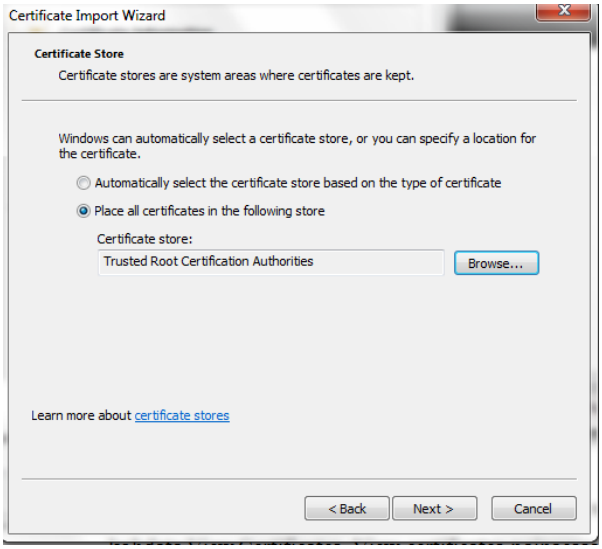
Kuvassa 42 sivusto ilmoittaa varmennevirheestä, mutta siitä pääsee eteenpäin painamalla Continue.

Ilman varmennetta ei voi käyttää terminaalipalveluita. Varmenne ladataan TS Web Acces -sivustolta kuvan 43 mukaisesti.



Kuva 43 Untrusted Certificate

Kuvassa 43 on TS Web Acces -pääsivu. Varmenteen voi ladata Certificate Error -kohdasta valitsemalla View Certificates. Valitsemalla View Certificates tulee esiin ikkuna, josta asennetaan varmenne. Varmenne asennetaan Certificate Import Wizardin avulla kuvan 44 mukaisesti.



Kuva 44 Certificate Import

Varmenne asennetaan Trusted Root Certification Authorties -kansioon, koska botnia.puv.fi -varmenne vaatii tämän toimiakseen. Asennuksen jälkeen terminaalipalvelut toimivat, mutta selain huomauttaa Ad.puv.fi- ja Web.puv.fi -varmenteista, koska varmenteet eivät ole luotettuja, eikä niitä ole Certificate Authority hyväksynyt. Ilmoituksesta pääsee eteenpäin painamalla OK.

7.2 Certificate Authority

CA (Certificate Authority) on varmennepalvelin. CA hyväksyy verkossa olevat varmennepyynnöt tai ei hyväksy niitä. Tässä työssä asennetaan Certificate Authority Enterpise Root -versio, koska se on osa toimialuetta. Se asennetaan koneelle, joka on DC-kone. Stand alone -versio voidaan asentaa myös toimialueelle tai pois siitä, ja se voi olla oma palvelimensa muualla. Certificate Authoritylle lähetetään varmennepyyntöjä IIS7:n kautta.

8 SÄHKÖPOSTI

Työssä vaadittiin yhtenä palveluna sähköpostipalvelin. Työssä tutustuttiin sekä Linux- että Windows-sähköpostipalvelimiin. Opinnäytetyössä päädyttiin käyttämään Windows-sähköpostipalvelinta.

8.1 Vaatimukset

Sähköpostipalvelimen piti toimia IMAP (Internet Message Access Protocol) -protokolla, ja siinä pitää olla Webmail. Opinnäytetyössä käytetään Axigen-ohjelmistoa. Ohjelmistoon saa vuoden kokeilulisenssin ilmaiseksi. Axigen-ohjelmistossa on Webmail- ja Imap-palvelut käytössä ja siitä löytyy myös LDAP-tuki.

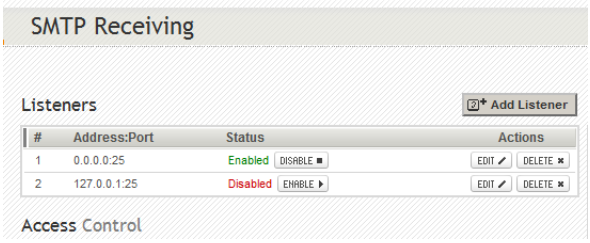
8.2 Asetukset

Ohjelma on helppo asentaa, koska siinä on oma asennusohjelmisto, joka asentaa sen automaattisesti koneelle. Domain-nimeksi asennetaan botnia.puv.fi ja admin-käyttäjäksi manager. Domain-nimi tarkoittaa sitä, että käyttäjien sähköpostit ovat tässä tapauksessa muotoa @botnia.puv.fi. Lähettävän ja vastaanottavan palvelimen nimeksi tuli botnia.puv.fi.

DNS-palvelimelle lisätään MX-tietue, joka on web.botnia.puv.fi. MX-tietue osaa ohjata sähköpostin sähköpostipalvelimelle. Palomuuriin tehdään ”reikä” portille 25, jotta sähköpostit pääsevät koneelle sekä lisätään Ipcopin ohjauspalvelimelle sääntö, joka päästää portista 25 liikkuvan datan.

8.2.1 SMTP Receiving

SMTP Receiving -välilehdessä pitää asentaa Listener kytkeytymään osoitteeseen 0.0.0.0 :25 kuvan 46 osoittamalla tavalla.



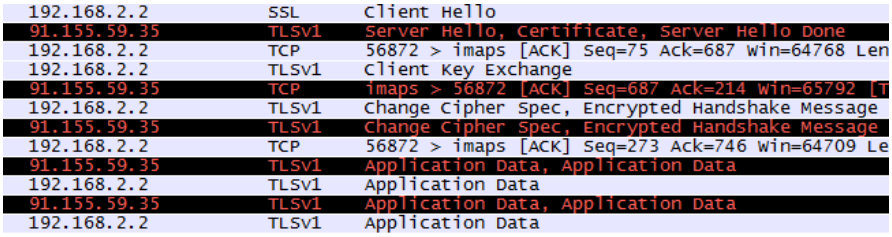
Kuva 46 SMTP

Kuvasta nähdään, että Listener-ohjelmaan on lisätty osoite 0.0.0.0: 25. Localhostin osoite 127.0.0.1:25 on sammutettu, koska sähköpostia ei voi saada omasta osoitteestaa, ellei lähetä viestiä vain itselleen.

Suojattu yhteys asetetaan SMTP Receiving -asetuksista SSL-välilehdeltä. Rastitaan suojattu yhteys päälle, muutetaan Listener kuuntelemaan porttia 465 ja tehdään muutokset palomuureihin. Tässä työssä ei käytetä suojattua yhteyttä paremman tutkimushyödyn takia.

8.2.2 Imap4 lyhyesti

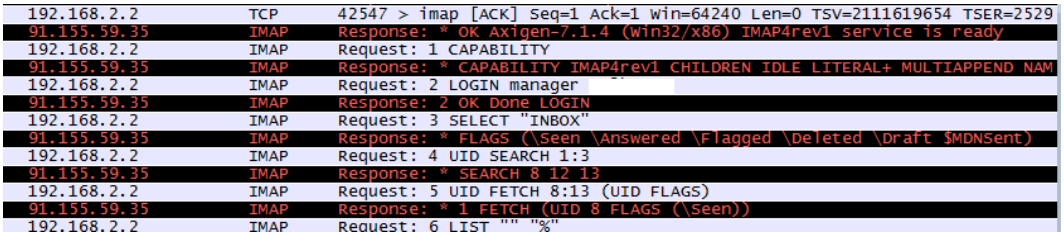
Imap4-protokolla on tällä hetkellä paljon käytetty protokolla, joka on kuvattu RFC 3501 -dokumentissa. Imap-protokollalla tehtyjä viestejä luetaan suoraan palvelimilta. POP 3 (Post Office Protocol) -protokollalla lähetettyjä viestejä vastaanotetaan suoraan omalle koneelle. Tämän takia Imap-protokolla on suositumpi ja tietoturvallisempi protokolla silloin, kun viestejä ei tallenneta koneille. Imap-protokolla käyttää porttia 143 ja suojattuna porttia 993. Tässä opinnäytetyössä ei käytetä suojattua yhteyttä, koska silloin protokollan käyttäytymistä ei voida havaita Wiresharkin avulla. Suojaamattomana käyttäjät näkevät paremmin miten Imap-protokolla toimii. Kuvassa 40 Imap-protokolla on suojattu.



Kuva 47 Salattu yhtes

Kuvassa 47 käyttäjä ei saa tietoonsa muuta kuin palvelimen ja sähköpostiohjelman varmennetervehtimisen.

Kuvassa 48 yhteyttä ei ole suojattu.

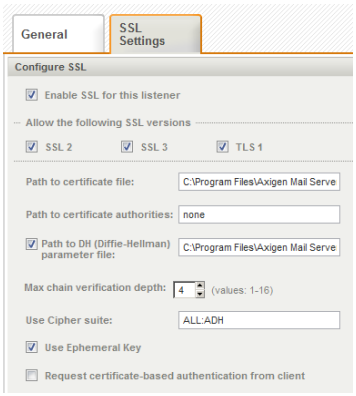


Kuva 48 Avoin yhteys

Kuvassa 48 suojaattomalla yhteydellä käyttäjä voi tutkia huomattavasti paremmin Imap-protokollan toimintaa.

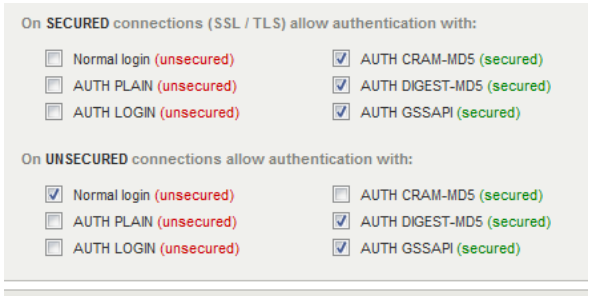
8.2.3 Imap-asetukset

Imap-palvelimelle tehdään samanlainen asetus. Lisätään Listener-asetukselle osoite 0.0.0.0 :143 ja Imap-asetuksista rastitaan Normal login päälle. SSL-suojatun yhteyden luomiseen tarvitsee kuvan 49 mukaiset asetukset.



Kuva 49 SSL-asetukset

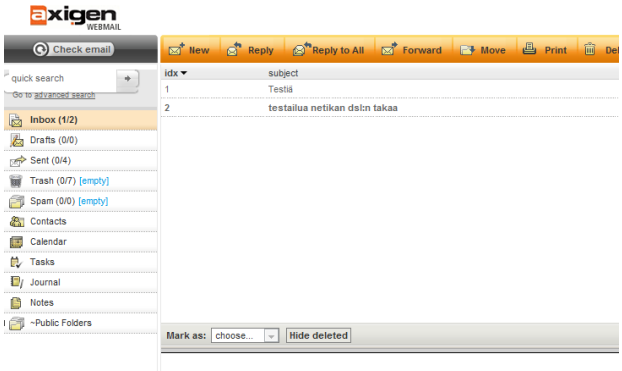
Kuvassa 49 on SSL-yhteys asetettu päälle. Imap-asetuksista asetetaan vaadittavat kirjautumissuojat päälle kuvan 50 mukaisesti. Listeneriä pitää muuttaa kuuntelemaan porttia 993 sekä tekemään muutos Ipcop:iin ja palvelimen palomuuriin.



Kuva 50 SSL/TLS-asetukset

8.3 Webmail

Yritysverkon Webmailiin pääsee osoitteesta http://botnia.puv.fi:7080 .Webmailia ei tarvitse lisätä IIS-palvelimelle, koska Webmail käyttää Axigenin sisäistä palvelintaan. Webmail-asetuksiin ei ole koskettu, koska käyttäjät saavat itse päättää, minkälaisen sähköpostin he haluavat. Sähköpostin asetuksia ei voi muuttaa, mutta ulkoasua ja sen tyyliä saa muokata. Kuvassa 51 on Webmailin pääsivu kun käyttäjä on kirjatunut sisään.



Kuva 51 Axigen

8.4 Testaus

Sähköpostia testataan kahdella tavalla. Tehdään sähköpostitili Nokia N95 -kännykkään ja lähetetään sähköpostitse puhelimella. Lähetetään sähköpostia ja luetaan sähköposti Axigen Webmailista.

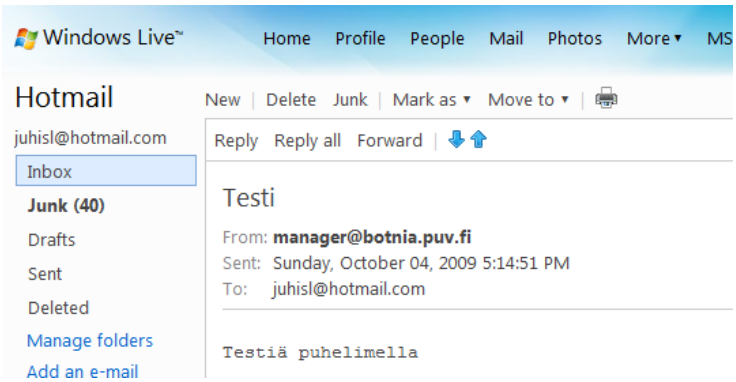
8.4.1 N95

Asetetaan taulukon 6 mukaiset asetukset puhelimeen. Saapuvan sähköpostin asetuksia ei tässä testissä tarvita, mutta käyttäjän halutessa sähköpostin puhelimeen ovat asetukset tarpeelliset.

Taulukko 6. Sähköpostiasetukset

Saapuva sähköposti		Lähtevä sähköposti	
Käyttäjänimi	manager	Käyttäjänimi	manager
Vastaanottava palvelin	botnia.puv.fi	Lähettävä palvelin	posti.saunalahti.fi
Postilaatikon tyyppi	Imap	Suojaus	ei käytössä
Suojaus	ei käytössä	Portti	25
portti	143		

Lähetetään puhelimesta sähköposti aiheella Testi osoitteeseen Juhisl@hotmail.com. Kuvassa 52 on Hotmail-sähköposti, johon viesti lähetettiin.

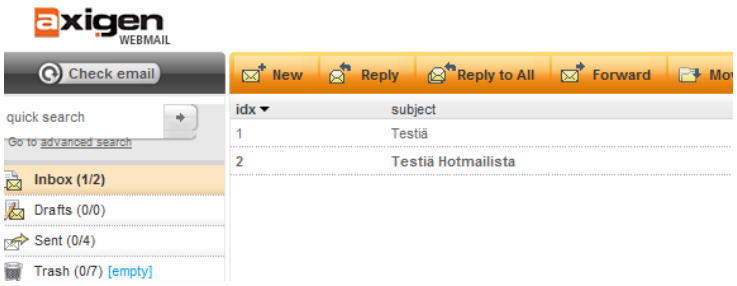


Kuva 52 Hotmail

Kuvassa 52 on saapunut viesti Manager@botnia.puv.fi -osoitteesta eli sähköpostin lähetys on onnistunut.

8.4.2 Webmail

Lähetetään Hotmail-palvelusta sähköpostia käyttäjälle Manager. Kuvassa 53 on Axigen Webmail.



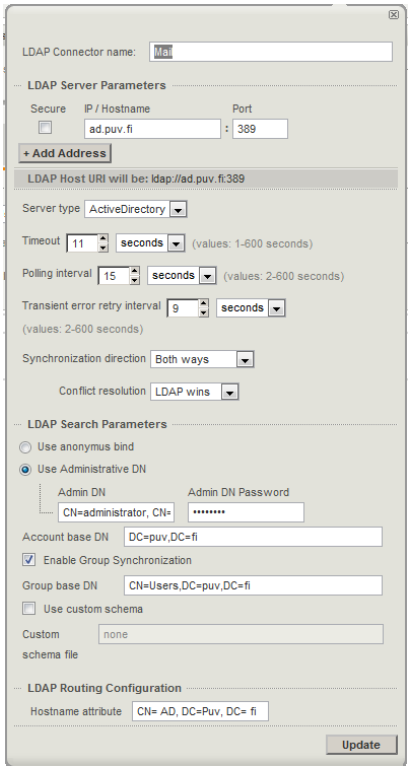
Kuva 53 Axigen Webmail

Kuvasta 53 nähdään, että sähköposti on on onnistuneesti saapunut perille.

8.5 LDAP-asetukset

LDAP-asetukset asetetaan Clustering-kohdasta kuvan 54 mukaisesti. Clustering-asetuksista luodaan connector, joka liitetään LDAP-asetuksiin. Clustering tarkoittaa sitä, että liitetään toinen kone sähköpostipalvelimeen. Connector

sähköpostipalvelimessa on pelkkä yhteysnimi, jolla liitetään sähköpostipalvelin DC-koneeseen LDAP:n avulla.



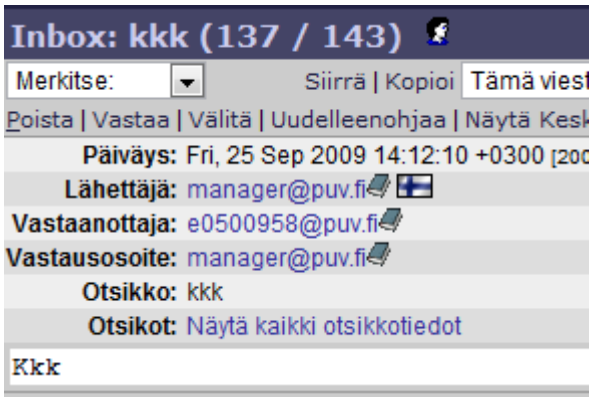
Kuva 54 LDAP-asetukset

Tämän jälkeen Connector liitetään LDAP-asetuksiin. Avataan Domain & Accounts → edit botnia.puv.fi ja sivun alalaidasta LDAP synchronization -kohdasta lisätään LDAP-connectoriin juuri luotu sähköpostiviesti.

8.6 Ongelmat

Sähköpostin valinnassa oli kaksi vaihtoehtoa. Voitiin käyttää Linux-puolen sähköpostipalvelinta tai Windows-puolen sähköpostipalvelinta. Ensimmäisenä lähdettiin rakentamaan Linux-sähköpostipalvelinta. Sähköpostipalvelimeksi valitsin Courier mail serverin, jossa oli PostgresQL -tietokanta sekä Squirrelmail Webmail. Squirrelmailia päästiin projektin aikana testamaan kerran. Tämä johtui Linuxin epävakaisuudesta sekä aikarajasta.

Ongelmia tulee myös kun lähetetään sähköpostia koulun osoitteisiin. Kuvassa 55 on lähetetty käyttäjälle Manager sähköposti osoitteeseen e0500958@puv.fi.



Kuva 55 Koulun sähköposti

Kuvassa manager@botnia.puv.fi osoite on lyhentynyt manager@puv.fi. Ongelma johtuu siitä, että botnia.puv.fi-verkko on suoraan hierarkkisesti puv.fi-verkon alapuolella ja näin ollen botnia-pääte katoaa matkalla.

9 OPENSUSE

Työssä käytetään Opensuse 11.0 -versiota. OpenSuse on SUSE-Linuxin ilmainen versio. Opensuse ja Suse on kehitetty Novell-verkkoihin, joten Opensuse on tässä tapauksessa hyvä valinta, koska sitä tullaan käyttämään toimialueella. OpenSusen tarkoituksena tässä työssä on käyttää sitä levypalvelimena sekä verkonhallintakoneena. Verkonhallinassa tullaan käyttämään Zenoss-verkonhallintaohjelmistoa ja levypalvelimessa käytetään Samba-palvelua.

9.2 Asennus

Asennus on OpenSusSen graafisen käyttöympäristön takia samanlainen kuin asennettaisiin Windows-ympäristön koneita. Asennus hoituu automaattisesti, mutta asennus kysyy käytetäänkö KDE- vai Gnome-ympäristöä. Tässä työssä käytetään Gnome-ympäristöä.

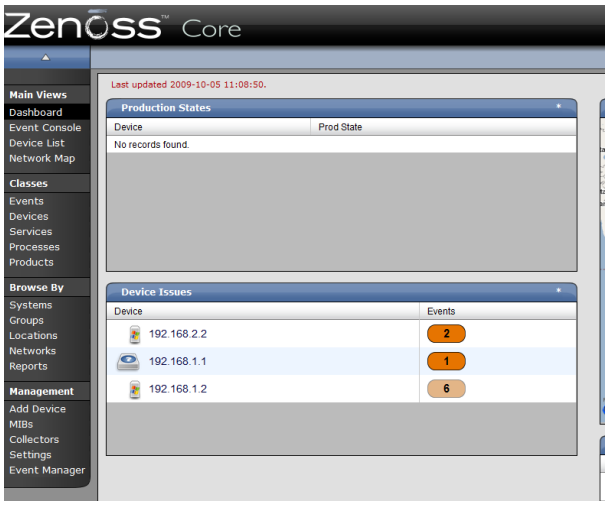
OpenSuse-käyttöjärjestelmässä on asennettu tähän työhön tarvittavat ohjelmat valmiiksi lukuun ottamatta Zenoss-ohjelmaa.

9.2.1 Zenossin asentaminen

Zenoss-ohjelman bin-tiedosto haetaan Zenoss-ohjelman kotisivuilta. Zenoss asennetaan tietokoneelle antamalla ajo-oikeus tiedostolle ja käynnistämällä tiedosto ./Zenoss.bin. Asennuksen jälkeen Zenoss-ohjelma avataan selaimella http://localhost:8080.

9.2.2 Zenossin käyttö

Zenoss-ohjelmalla voidaan katsella verkon tilaa SNMP:n (Simple Network Management Protocol) avulla. Asiakaskoneet ilmoittavat tilastaan SNMP-kutsujen avulla. Esimerkiksi kytkimen portti voi sulkeutua. Silloin kytkin lähettää hälytyksen Zenoss-ohjelmalle, joka kertoo sähköpostilla Managerille tapahtuneesta. Zenoss hakee automaattisesti verkosta laitteita ja palvelimia. Kuvassa 56 on Zenoss-käyttöliittymä.



Kuva 56 Zenoss

9.3 Samba

Samba-ohjelmalla voidaan Linux- tai Unix-koneisiin lisätä Windows-verkkojakoja sekä tulostimia. Verkkolevyjä ja tulostinpalveluja voidaan tehdä Samba-ohjelmalla myös Windows-koneille. Tässä työssä käytetään Samba 3 -versiota. /2/

9.3.1 Samban asetukset

OpenSuSe Linuxissa on valmiiksi asennettu Samba, joten ainoa asia, jota pitää muokata, on smb.conf -tiedosto, johon asetetaan kaikki tarvittavat tiedot levyjakoa varten Seuraavassa taulukossa 7 on smb.conf -perussäännöt, joita käytetään kun LDAP-protokollalla. /1/, /3/

Taulukko 7. Samba-palvelimen asetustiedosto

[global] workgroup = TECH realm = PUV.FI security = user use kerberos keytab = true winbind use default domain = yes	Asetetaan Samba Tech työryhmään ja toimialueeseen Puv.fi. Käyttää kerberos protokollaa Winbind on ominaisuus Sambassa jolla voidaan kirjautua Linuxiin

winbind separator = +	Windows verkon tunniksilla.
idmap uid = 1000-59999	Windbind seperator tarkoittaa, että
idmap gid = 1000-59999	toimialue käyttäjät merkitään
winbind enum users = yes	TECH+ käyttäjä.
winbind enum groups = yes	
deadtime = 10	
winbind cache time = 10	
winbind nested groups = yes	
template homedir = /home/%D/%U	Kotipolku
template shell = /bin/bash	
client use spnego = yes	spnegeo käytetään kun asiakkas
socket options = TCP_NODELAY SO_RCVBUF=16384 SO_SNDBUF=16384	koneen palveluja käytetään toisilla koneilla.
idmap backend = ldap:ldap://ad.puv.fi	Ldap admin asetuksia.
ldap idmap suffix = ou=Idmap	
ldap admin dn = cn=maanger, cn=users,dc=puv,dc=fi	
ldap suffix = dc=Puv,dc=fi	
dns proxy = no	
domain master = No	
max log size = 100	
log file = /var/log/samba/%m.log	
printing = cups	Tulostinpalvelun asetuksia
printcap name = cups	
printcap cache time = 750	
cups options = raw	
map to guest = Bad User	
include = /etc/samba/dhcp.conf	
logon path = \\%L\profiles\.msprofile	
logon home = \\%L\%U\.9xprofile	
logon drive = P:	
usershare allow guests = yes	

add machine script = /usr/sbin/useradd -c Machine -d /var/lib/nobody -s /bin/false %m$ domain logons = Yes winbind refresh tickets = yes usershare max shares = 100 ldap group suffix = ou=Groups ldap machine suffix = ou=Machines ldap passwd sync = Yes ldap user suffix = ou=Users passdb backend = ldap-sam:ldap://ad.puv.fi	Ldap käyttäjä asetuksia

Taulukossa 7 olevat asetukset kertovat Samba-ohjelmalle, miten Windows-käyttäjät voivat käyttää Linux-levypalvelinta ja miten Samba yhdistää itsensä Windows-verkkoon.

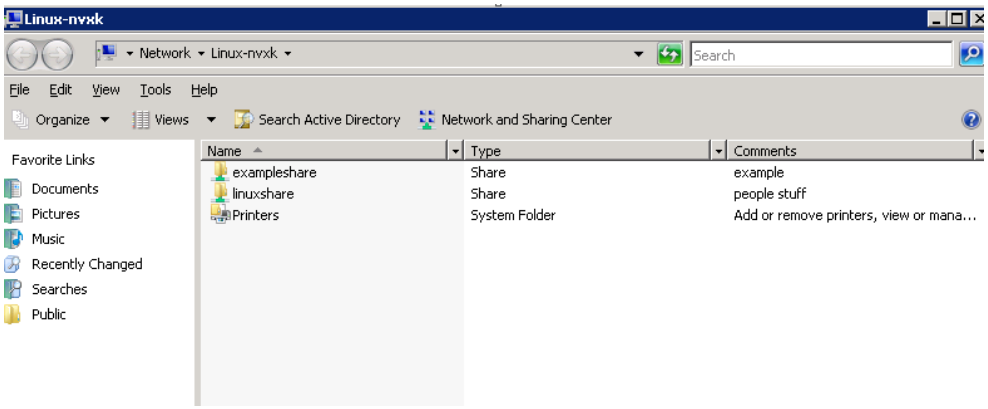
Asetuksista muutama tulee valmiina, mutta suurimman osan joutuu itse muokkaamaan. Taulukossa 8 on esimerkkinä Samba-jako.

Taulukko 8. Samba-jako

[linuxshare] comment = people stuff inherit acls = Yes

```
path = /home/Common
read only = No
valid users = TECH + admin, TECH + Student, TECH + Teacher
```

Taulukossa 8 on luotu Linuxshare-niminen kansio, johon käyttöoikeudet ovat toimialueen henkilöillä. Kuvassa 57 on Windows-verkossa näkyvät Samba-jaot.



Kuva 57 Samba

9.4 Ongelmat

Ongelmat kohdistuvat eniten OpenSuSe-ohjelmistoon, joka on epävakaa järjestelmä, koska OpenSuSe hukkaa Root-salasanan, jos käyttäjä muokkaa yhteysasetuksia suoraan Linux Terminalista. OpenSuSe-järjestelmä käyttää Yast-ohjelmistoa, joka on ohjelmiston hallintatyökalu. Yastin voi ottaa tietyistä sovelluksista pois, mutta sama ongelma syntyy silloinkin, eli Root-salasanan hukkaaminen.

Linux-palvelimen valinnassa tuli myös muita ongelmia esille. Ensimmäisenä yritettiin käyttää Ubuntua Linux-palvelimena, mutta silloin ilmeni ongelmia toimialueelle kirjautumisessa. Ubuntun sai kirjautumaan toimialueelle, mutta se ei pysynyt siellä.

10 YHTEENVETO

Nykyään jo pienemmissäkin yrityksissä käytetään Active Directory -palveluita käyttäjien hallintaan. Käyttäjien hallinta on yksinkertaista ja helppoa. Verkonhallitsijat voivat lisätä tai poistaa käyttäjän nopeasti ja lisätä hänet tiettyyn ryhmään. Ryhmille voidaan antaa erilaiset oikeudet tai eri levyjaot. Levyjakoon sekä tulostinjakoon skriptien käyttö on erittäin toimiva ratkaisu. Yhdellä skriptillä voidaan hallita kaikkien käyttäjien automaattisesti toimivaa tulostimen ja levyjen jakoa.

Opinnäytetyössä piti rakentaa pienen yrityksen verkko, jossa on kaikki vaadittavat palvelut. Työ onnistui mielestäni hyvin, vaikka kaikki järjestelmät eivät toimi niin automaattisesti kuin olisin halunnut. Työssä oli paljon vertailua ja päätöksenteko, piti esimerkiksi päättää, minkälaisia ratkaisuja ja mitä tekniikoita käytetään. Työssä tuli vastaan paljon sellaisia uusia tekniikoita ja protokollia, joihin en ollut aikasemmin törmännyt. Varsinkin autentikoinnit ja varmenteet olivat uusia ja hankalia asioita oppia.

Opinnäytetyö oli mielenkiintoinen, vaikka sen aihe oli hyvin laaja. Eri palveluita oli vain muutama, niiden toiminnan ymmärtäminen oli haasteellista. Microsoft Windows 2008 oli minulle uusi käyttöjärjestelmä, joka piti opetella. Aihetta ei myöskään tehnyt helpommaksi se, että käyttöjärjestelmästä ei ollut vielä ilmestynyt kirjaa, vaikka sen piti tulla kesän aikana.

WWW-palvelimena Microsoft Windows IIS7 on helppo hallita, mutta mielestäni Apache-palvelin on helpompi ymmärtää. Toki IIS7:ssä on paljon uusia ominaisuuksia, ja asetukset voidaan hiirellä klikata, mutta asetuksia on monessa eri paikassa ja niitä on paljon. Käyttäessäni Apachea asetukset oli helpompi sisäistää ja niitä muokatessa tiesin, mitä asetuksia säädin. Opinnäytetyö oli todella haastava mutta mielenkiintoinen.

LÄHTEET

/1/ Software Freedom Conservancy 2009. Samba configure[online] [Viitattu 7.10.2009] Saatavilla www-muodossa: <URL:http://samba.org/samba/docs/man/Samba-Guide/>

/2/ Software Freedom Conservancy 2009. Samba install [online] [Viitattu 7.10.2009] Saatavilla www-muodossa <URL:/http://samba.org/samba/docs/man/Samba-HOWTO-Collection/install.html>

/3/ Software Freedom Conservancy 2009. Samba start[online] [Viitattu 7.10.2009] Saatavilla www-muodossa <URL:http://samba.org/samba/docs/man/Samba-HOWTO-Collection/install.html#id2552921>

/4/ Korenius, Kalle 1997. LDAP (Lightweight Directory Access Protocol) [online][Viitattu 7.10.2009] Saatavilla www-muodossa: <URL:http://www.tml.tkk.fi/Studies/Tik-110.300/1997/Essays/ldap.html >

/5/ Massachusetts Institute of Technology 2009.[online] [Viitattu 7.10.2009] Saatavilla www-muodossa: <URL:http://web.mit.edu/Kerberos/#what_is>

/6/ Microsoft Corporation 2009. Active Directory [online] [Viitattu 7.10.2009] Saatavilla www-muodossa: <URL: http://technet.microsoft.com/en-us/library/cc731053(WS.10).aspx>

/7/ Microsoft Corporation 2009. AD LDS [online] [Viitattu 7.10.2009] Saatavilla www-muodossa: <URL:http://technet.microsoft.com/en-us/library/cc794857(WS.10).aspx>

/8/ Microsoft Corporation 2009. DNS [online]
[Viitattu 7.10.2009] Saatavilla www-muodossa:
<URL:http://technet.microsoft.com/en-us/library/cc772774(WS.10).aspx>

/9/ Microsoft Corporation 2009. HTTP-asetukset [online]
[Viitattu 7.10.2009] Saatavilla www-muodossa:
<URL:http://technet.microsoft.com/en-us/library/cc730716(WS.10).aspx>

/10/ Microsoft Corporation 2009. IIS 7[online]
[Viitattu 7.10.2009] Saatavilla www-muodossa:
<URL:http://technet.microsoft.com/en-us/library/cc753198(WS.10).aspx>

/11/ Microsoft Corporation 2009. IIS7 asentaminen[online]
[Viitattu 7.10.2009] Saatavilla www-muodossa:
<URL:http://technet.microsoft.com/en-us/library/cc732382(WS.10).aspx>

/12/ Microsoft Corporation 2009. Levypalvelin[online]
[Viitattu 7.10.2009] Saatavilla www-muodossa:
<URL:http://technet.microsoft.com/en-us/library/cc770740(WS.10).aspx>

/13/ Microsoft Corporation 2009. Terminal Service[online]
[Viitattu 7.10.2009] Saatavilla www-muodossa:
<URL:http://technet.microsoft.com/en-us/library/cc754252(WS.10).aspx>

/14/ Microsoft Corporation 2009. Tulostinpalvelin[online]
[Viitattu 7.10.2009] Saatavilla www-muodossa:
<URL:http://technet.microsoft.com/en-us/library/cc753109(WS.10).aspx>

/15/ Microsoft Corporation 2009. Varmenteet[online]
[Viitattu 7.10.2009] Saatavilla www-muodossa:
<URL:http://technet.microsoft.com/en-us/library/cc776447(WS.10).aspx#w2k3tr_certs_how_xebx>

/16/ Microsoft Corporation 2009. Windows Server 2008[online] [Viitattu 7.10.2009] Saatavilla www-muodossa: <URL:http://technet.microsoft.com/en-us/library/dd443520(WS.10).aspx>

/17/ Microsoft Corporation 2009. Windows Server 2008 toiminnat[online] €[Viitattu 7.10.2009] Saatavilla www-muodossa: <URL:http://technet.microsoft.com/en-us/windowsserver/default.aspx>

/18/ Tzen, Shane 2008.IPTABLES[online][Viitattu 7.10.2009] Saatavilla www-muodossa: <URL:http://www.knowplace.org/pages/howtos/firewalling_with_netfilter_iptables.php>

/19/ Walker, Peter 2009. Ipcop Installation manual [online][Viitattu 7.10.2009] Saatavilla www-muodossa: <URL:http://www.ipcop.org/1.4.0/en/install/html/>

LIITE 1

System

- Home
- Update
- Passwords
- Ssh Access
- Gui settings
- Backup
- Shutdown
- Credits

Status

- Network status
- System status
- System Graphs
- Traffic Graphs
- Connections

Network

- Dialup
- Upload
- Modem
- Aliases

Services

- Proxy
- DHCP-server
- Dynamic DNS
- Timer Server
- Traffic Shaping
- Intrusio Detection

Firewall

- Port Forwarding
- External Access
- DMZ pinholes

VPNs

- VPN

Logs

- Log settings
- Log summary
- Firewall logs
- IDs logs
- System logs