TAMPEREEN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ

UUDEN ACTIVE DIRECTORY -PALVELIMEN INTEGROINTI KAUPUNGIN VERKKOYMPÄRISTÖÖN

Jari Rimmi

Tietojenkäsittelyn koulutusohjelma
Joulukuu 2008
Työn ohjaaja: Ville Haapakangas

TAMPERE 2008

Tampereen ammattikorkeakoulu

Tekijä(t)	Jari Rimmi
Koulutusohjelma(t)	Tietojenkäsittely
Opinnäytetyön nimi	Uuden Active Directory –palvelimen integrointi kaupungin verkkoympäristöön
Työn valmistumis-kuukausi ja -vuosi	Joulukuu 2008
Työn ohjaaja	Ville Haapakangas

Sivumäärä: 39

TIIVISTELMÄ

Oriveden kaupungin verkkoympäristöön kuuluu erilaisia toimipisteitä. Yhdessä kaupungin toimipisteistä, Oriveden terveyskeskuksessa, havaittiin puutteita, joiden korjaaminen on välttämätöntä. Terveyskeskuksen palvelimet ovat käyttöikänsä lopussa niin fyysisesti kuin käyttöjärjestelmien osalta. Samalla kun palvelinvaihdos toteutetaan, uusitaan terveyskeskuksen verkkoympäristön IP-osoiteavaruus. Oriveden kaupunki tarvitsi tähän muutoksien toteuttamiseen ja aiheen raportointiin ulkopuolista apua.

Opinnäytetyö on osa suurempaa kokonaisuutta, jossa vanha terveyskeskuksen verkko ja palvelimet korvataan uusilla. Palvelinvaihdoksen syynä ovat vanhat palvelinkoneet, joiden käyttöikä on kulumassa loppuun. Palvelimien käyttöjärjestelmät ja aktiivihakemistojen rakenteet ovat vanhanaikaisia eivätkä täytä nykyajan vaatimuksia. Kaupungin verkkoympäristössä siirrytään lähivuosina oman sähköpostipalvelimen käyttöön, joka otetaan huomioon muutoksessa, etenkin nimiavaruuden suunnittelussa.

Opinnäytetyö kuvaa palvelimen pystytyksen vaiheita sekä uuden verkkoalueen toteuttamista. Tavoitteena on luoda sekä uusittu verkkoalue, joka tarjoaa toimivan pohjan palvelimien ja työasemien asentamiselle ja käyttämiselle että uusittu palvelin ja toimialue, joka vastaa nykyajan ja tulevaisuuden käyttötarpeita.

Palvelinvaihdos aloitettiin tutkimalla vanhan palvelimen rooleja ja palveluita sekä aktiivihakemiston rakennetta. Tämän jälkeen tarkasteltiin myös kaupungin muiden palvelimien rooleja ja palveluita sekä aktiivihakemistojen rakennetta. Näistä saatiin hyvä pohja uuden palvelimen suunnitteluun. Työssä apuna käytettiin alan kirjallisuutta tukemaan jo olemassaolevaa tietoa sekä tarjoamaan uusia vaihtoehtoja. Myös Internetissä olevia palveluita käytettiin apuna.

Työn tuloksena saatiin uusittu verkkoalue sekä palvelin, joka vastaa nykyajan tarpeita ja vaatimuksia. Työn pohjalta on hyvä suorittaa muutostyö valmiiksi. Muutostyö sisältää kahden lisäpalvelimen asennuksen terveyskeskuksen verkkoon.

Avainsanat Aktiivihakemisto Windows Server 2003 Verkkoympäristö

Tampere Polytechnic

Author(s)	Jari Rimmi
Degree Programme(s)	Business Information Systems
Title	Integrating a new Active Directory -server into Orivesi Citys´ Network
Month and year	December 2008
Supervisor	Ville Haapakangas

Pages: 39

ABSTRACT

There were problems in a branch office of a Orivesi citys´ network environment that should be fixed. This branch office is a health center. Their server hardware and software are not updated. These systems need to be updated for example the active directory structure. At the same time when the server change happens, a new network with IP-numbers and new domain are created to the health centers´ network environment. Orivesi needed outside help with the project and documenting the whole process.

This report is a part of a larger project where all the servers, domain and network of the health center are replaced with new ones. Reasons for this change are the old server hardware and Active Directory structure that needs to be upgraded. The hardware and software don´t meet todays´ requirements for professional use. Orivesi is also planning to install a new email server in near future and that needs to be take into a consideration.

This document represents installation of the new Active Directory server, the domain and setup of the new network. It also represents the change when the workstations go under the new domain. The aim is to achieve a new network that offers good base for servers and workstations. The aim is also create a new server and domain that fulfills the expectations for professional use now and in the future.

The project started by checking server roles, services and the Active Directory structure. Then other servers in the network and their roles, services and Active Directory structures were checked. These operations worked as a base for planning the new server. Literature was also used because it gave new ideas. Internet was also a great asset.

As result, a new controllable and maintainable network and server were installed. This is a good start to finish off the project with other server installations.

Keywords Active Directory Windows Server 2003 Network environment

Sisällysluettelo

Käsitteet ja lyhenteet

Active Directory (AD) - Aktiivihakemisto

Windows 2000 server ja Windows server 2003 käyttöjärjestelmien käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista. Se mahdollistaa keskitetyn resurssien jakamisen käyttäjille ja sovelluksille.

DHCP (Dynamic host configuration protocol)

Protokolla, jonka avulla määritellään verkon laitteille TCP/IP asetukset automaattisesti.

DNS (Domain name system) - Nimipalvelu

Internetin ja intranetin nimipalvelujärjestelmä, joka muuntaa nimiä IP-osoitteiksi.

Domain - Toimialue

Ohjauspalvelinten, jäsenpalvelinten, käyttäjätilien ja tietokonetilien yhteenliittymä, jolla on toimialuenimi, esimerkiksi yritys.ad.

Domain controller (DC) – ohjauspalvelin

Palvelin, joka ylläpitää hakemistopalvelua ja tarjoaa esimerkiksi tunnistuspalvelut toimialueen käyttäjille.

FW (Firewall) – Palomuuri

Palomuurit ovat joko ohjelmistolla tai laitteistolla toteutettuja järjestelmiä, jotka valvovat tietoliikennettä verkkojen välillä. Palomuureja käytetään yleisesti suojaamaan organisaation sisäverkkoa ulkoverkosta tulevilta hyökkäyksiltä sekä rajoittamaan liikennettä eri sisäverkkoavaruuksien välillä. Palomuurin toiminnan perusedellytykset ovat, että kaikki verkkoliikenne kulkee sen läpi ja että palomuuri päästää lävitseen vain halutun kaltaisen verkkoliikenteen.

Group policy (GP) - Ryhmäkäytännöt

Ryhmäkäytännöillä tarkoitetaan järjestelmän kokoonpanoasetuksia, jotka voidaan liittää Active Directoryn objekteihin, kuten organisaatioyksiköihin. Voidaan määritellä käyttäjien ympäristöasetuksia, ohjelmien jakeluasetuksia, salasanakäytäntöjä ja muita tarvittavia asetuksia keskitetysti useille käyttäjille kerralla.

ISP (Internet service provider) – Palveluntarjoaja

Palveluntarjoaja, joka tarjoaa yrityksille tai yksityisille Internet yhteyden. Suomessa palveluntarjoajina ovat teleoperaattorit kuten Elisa ja Sonera.

LAN (Local area network) – Lähiverkko

Lähiverkko on rajoitetulla maantieteellisellä alueella toimiva tietoliikenneverkko, jolla on suuri tiedonsiirtokapasiteetti. Lähiverkko voi olla esimerkiksi yksittäisen yrityksen sisäinen verkko.

NAT (Network address translation)

Osoitteenmuunnos on Internet-tekniikka, jossa yksityisiä eli niin sanottuja harmaansarjan osoitteita muutetaan julkisiksi IP-osoitteiksi. Osoitteenmuunnos kehitettiin alun perin, kun huomattiin, että tulevaisuudessa IP-osoitteita ei riittäisi joka koneelle omaansa. Useimmiten osoitteenmuunnosta käytetään, kun Internet-yhteydellä ei ole kuin yksi IP-osoite, mutta useamman koneen tulisi päästä Internetiin. Osoitteenmuunnoksen suorittava laite on useimmiten reititin tai palomuuri.

RAID (Redundant Array of Independent Disks)

Tekniikka, jossa useita erillisiä kiintolevyjä yhdistetään yhdeksi loogiseksi levyksi. RAID-tekniikkaa käytetään etenkin levy- ja tietokantapalvelimissa, koska levyjen vasteajat tai virheettömyys ovat tärkeitä. RAID-tekniikalla pyritään estämään tietojen häviäminen kovalevyiltä laitevian sattuessa tai nopeutetaan levyn toimintaa. Yleisiä RAID-tekniikoita ovat: RAID0, RAID1, RAID0+1, RAID5 ja RAID6. Tekniikat eroavat toisistaan siinä, miten vikasietoisia ja nopeita ne ovat.

Reititin — Reititin yhdistää eri tietoverkkoja. Reitittimen tehtävä on välittää tietoa tietoverkon eri osien välillä.

Skripti — Komentojen kokoelma, joka suoritetaan komentotulkin avulla. Esimerkiksi VB-skripti (.vbs) suoritetaan skriptitulkin alaisuudessa ja komentojonot (batch) suoritetaan komentotulkin alaisuudessa.

VLAN (Virtual LAN) - Virtuaalinen lähiverkko

Tekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin osiin. Käytännössä tämä tarkoittaa sitä, että yrityksessä voidaan jakaa eri osastot omiin verkkoihin riippumatta siitä miten osastot on jaoteltu rakennukseen. VLAN jako lisää verkkoympäristön turvallisuutta.

1 Johdanto

Opinnäytetyön aiheena on ”uuden Active Directory -palvelimen integrointi kaupungin verkkoympäristöön”. Idea opinnäytetyöhön sai alkunsa työharjoittelusta, jonka suoritin Oriveden kaupungilla.

Oriveden kaupungin verkkoympäristöön kuuluvalla toimipisteellä havaittiin puutteita, joiden korjaaminen olisi välttämätöntä. Toimipiste on Oriveden terveyskeskus. Terveyskeskuksen palvelimet ovat käyttöikänsä lopussa niin fyysisesti kuin käyttöjärjestelmien osalta. Myös muita muutoksia terveyskeskuksen verkkoympäristöön tarvitaan, kuten uusi IP-osoiteavaruus. Muutoksien toteuttamiseen sekä aiheen raportointiin kaupungin atk-osasto tarvitsi ulkopuolista apua.

Opinnäytetyön tausta ja kuvaus

Palvelinvaihdos on osa suurempaa kokonaisuutta, jossa vanha terveyskeskuksen verkko korvataan uudella. Samalla, kun verkkovaihdos toteutetaan, uusitaan myös vanhan terveysverkon palvelin. Palvelinvaihdoksen syynä ovat vanhat palvelinkoneet, joiden käyttöikä on kulumassa loppuun. Palvelimien rakenteet ovat vanhanaikaisia eivätkä täytä nykyajan vaatimuksia. Kaupungin verkkoympäristössä siirrytään lähivuosina oman sähköpostipalvelimen käyttöön, joka otetaan huomioon muutoksessa, etenkin nimiavaruuden suunnittelussa.

Opinnäytetyö rajoittuu kuvailemaan pääasiassa uuden terveyspalvelimen (tk_server1) pystyttämistä ja käyttöönottoa sekä osaltaan uuden terveysverkon (uusi_tk.ad) määrityksiä. Mukana on myös kuvaus kaupungin verkkoympäristöstä sekä muista palvelimista, jotka liittyivät vaihdokseen.

Uuden terveyspalvelimen (tk_server1) rakentamisessa otettiin huomioon vanhan palvelimen aktiivihakemiston rakenteet, joiden pohjalta työtä lähdettiin suunnittelemaan. Tarkoituksena oli nykyaikaistaa palvelimen roolit ja palvelut vastaamaan tämän hetkisen ja tulevan verkon vaatimuksia. Mallina käytettiin kaupungin aktiivihakemistojen rakennetta, joka on havaittu toimivaksi kokonaisuudeksi. Verkkouudistuksen tarkoitus on uudistaa vanhan terveysverkon IP-osoiteavaruus sekä nostaa uusi toimialue kaupungin toimialueen kanssa tasavertaiseksi.

Palvelin- ja verkkouudistuksen toteutus ei tapahdu nopealla aikavälillä, vaan uudet ja vanhat palvelimet sekä verkot tulevat toimimaan rinnakkain. Tämä mahdollistaa uuden laitteiston toimivuuden testauksen ennen vaihdoksen toteuttamista sekä palautumisen vanhaan malliin, jos kohdataan ongelmia. Mahdollisia ongelmia ovat esimerkiksi palvelinten välisten luot-

tosuhteiden toimimattomuus, ohjelmien toimintahäiriöt sekä erilaiset kommunikointi ongelmat palvelinten ja verkkojen välillä.

Palvelinvaihdoksen ja verkkomuutoksen testaamisen helpottamiseksi avuksi rakennettiin testiverkko, jonka tarkoitus oli simuloida tulevaa verkkoa mahdollisimman todenmukaisesti.

Toimeksiantaja

Työn toimeksiantajana oli Oriveden kaupunki, joka vastaa Oriveden kaupungin, terveyspalveluiden ja Oriveden seudun koulujen verkkojen ja atk-laitteistojen ylläpidosta. Terveyskeskuksen verkko kuuluu kaupungin verkkoympäristöön itsenäisenä osana.

Työssä oli mukana neljä jäsentä. Projektipäällikkönä toimi Oriveden kaupungin tietohallintopäällikkö Mikko Naaralainen. Palvelimen pystyttämisestä vastasivat ML-Soft järjestelmäasiantuntija Veikko Haavisto sekä opiskelija Jari Rimmi. Mukana oli myös Mari Halttunen, kaupungin atk- ja hallintotukihenkilö, joka vastasi käyttäjäinformaation ja käyttäjien osastojaon sekä toimenkuvien oikeellisuudesta. Hän myös päivitti vanhojen ja uusien käyttäjätunnusten linkkitietokannan. Kaikki neljä olivat mukana, kun työasemia siirrettiin uuden toimialueen alaisuuteen.

Opinnäytetyössä käytetyt IP-osoitteet ja laitteistojen nimet on vaihdettu eli ne eivät ole todenmukaisia.

2 Verkon keskeisiä elementtejä

2.1 Windows server 2003

Windows Server 2003 -tuoteperhe on nopeasti muuttuvilla markkinoilla toimiville yrityksille tarkoitettu teknisten ratkaisujen pohja. Windows Server 2003 muodostaa ainutlaatuinen tietojenkäsittely-ympäristön kaikenkokoisille yrityksille.

Windows 2000:een perustuvaan Windows Server 2003 sisältyvät kaikki asiakkaiden arvostamat Windows Server -käyttöjärjestelmän perusominaisuudet, kuten toiminnan luotettavuus, suojaus ja skaalattavuus. Lisäksi Windows Server -tuoteperhettä on parannettu ja laajennettu niin, että yritykset voivat hyödyntää kaikkia .NET-toimintoja. (http://www.microsoft.com/finland/Windowsserver2003/evaluation/overview/default.mspx)

Windows Server 2003 -tuoteperheeseen sisältyy useita erilaisia käyttöjärjestelmäversioita, joista voidaan valita tarpeisiin sopiva vaihtoehto:

- Windows Server 2003, Web edition sisältää web-palvelinympäristön toteuttamiseen tarvittavat komponentit. Se ei voi toimia ohjauspalvelimena.
- Windows Server 2003, Standard edition on päivitys Windows 2000 serverille, se voi toimia ohjauspalvelimena.
- Windows Server 2003, Enterprise edition voi toimia ohjauspalvelimena.
- Windows Server 2003, Datacenter edition voi toimia Active Directoryn ohjauspalvelimena. (Kivimäki, 2005 [2])

2.2 Active Directory

Windows server 2003:n hakemistopalvelut perustuvat Active Directoryyn. Active Directoryn tehtävänä on vähentää ylläpidettävien hakemistojen määrää, koska käyttäjätilien, tietokonetilien ja jaettujen resurssien hallinta voidaan tehdä yhtenäisillä työkaluilla. Active Directoryn ensimmäinen versio tuli Windows 2000 server -käyttöjärjestelmän mukana ja uudempi versio Windows server 2003 -käyttöjärjestelmän myötä. Windows server 2003 -version myötä Active Directoryyn tuli laajennuksia ja entistä tehokkaampia toimintoja. Windows server 2003:n Active Directory on tehokkaampi ja miellyttävämpi hallita kuin Windows 2000

serverin Active Directory. Syinä ovat järjestelmän sisäiset muutokset sekä monipuolisemmat hallinta- ja tukityökalut. (Kivimäki 2005 [1]: 1.)

2.3 Toimialueen toimintatasot (Kivimäki 2005 [1]: 53-54)

Windows server 2003 -toimialueiden Active Directory mahdollistaa useita eri toimintatasoja (functionality level) Windows NT- ja Windows 2000 -ohjauspalvelinten tukea varten. Toimintatasot olivat jo Windows 2000 server -käyttöjärjestelmässä, mutta niistä käytettiin nimitystä toimintatila (domain mode). Toimintatasot määrittelevät, minkä tyyppisen käyttöjärjestelmäversion ohjauspalvelimia toimialueella voi olla. Toimintatasoja on neljä eri tyyppistä: Windows 2000 sekatila (Windows 2000 mixed mode), Windows 2000 -natiivitila (Windows 2000 native mode), Windows server 2003 -välitila (Windows server 2003 interim mode) ja Windows server 2003 -tila (Windows server 2003 mode).

2.3.1 Windows 2000 -sekatila (Windows 2000 mixed mode)

Windows 2000 -sekatila on oletuksena, kun asennetaan uuden Active Directory -toimialueen ensimmäinen ohjauspalvelin. Tämä tila on suositeltava, jos toimialueella on Windows NT 4.0 server -varaohjauspalvelimia, Windows 2000 server -ohjauspalvelimia ja Windows server 2003 -ohjauspalvelimia. Windows NT4 -palvelin ei voi toimia toimialueen ohjauspalvelimena, vaan rooli pitää olla Windows 2000 server tai Windows server 2003 ohjaupalvelin.

Tuettuja ohjauspalvelimia ovat

- Windows NT 4.0 -varaohjauspalvelimet
- Windows 2000 server -ohjauspalvelimet
- Windows server 2003 -ohjauspalvelimet.

2.3.2 Windows 2000 -natiivitila (Windows 2000 native mode)

Kun Active Directory -toimialueella on ainoastaan Windows 2000 server- ja Windows server 2003 ohjauspalvelimia, toimialueen toimintatason voi nostaa Windows 2000 natiivitilaksi. Tästä tilasta ei voi enään palata takaisin Windows 2000 sekatilaksi.

Tuettuja ohjauspalvelimia ovat

- Windows 2000 server -ohjauspalvelimet
- Windows server 2003 -ohjauspalvelimet.

2.3.3 Windows server 2003 -välitila (Windows server 2003 interim mode)

Kun päivitetään Windows NT -toimialue Windows server 2003 -toimialueeksi, kyseeseen tulee Windows server 2003 -välitila. Välitila määritellään, kun päivitetään Windows NT -toimialueen ensisijainen ohjauspalvelin Windows server 2003 -käyttöjärjestelmään. Windows server 2003 -välitilasta on mahdollista päivittää suoraan Windows server 2003 -toimintatasolle. Tämä edellyttää, ettei toimialueella ole Windows NT -varaohjauspalvelimia.

Tuetut ohjauspalvelimet ovat

- Windows NT 4.0 -varaohjauspalvelimet
- Windows server 2003 -ohjauspalvelimet.

2.3.4 Windows server 2003 -tila (Windows server 2003 mode)

Windows server 2003 -toimintataso tukee vain Windows server 2003 -ohjauspalvelimia. Tämä tulee kyseeseen, kun päivitetään Windows 2000 server -toimialueen ohjauspalvelimet Windows server 2003 -ohjauspalvelimiksi. Ennen päivitystä täytyy Windows 2000 server -toimialueen ohjauspalvelimet valmistella adprep.exe -ohjelmalla. Kun toimitila on nostettu Windows server 2003 -toimitilaksi, ei voida palata mihinkään muuhun toimitilaan. Toimitilaan kannattaa siirtyä, jos ollaan varmoja ettei tarvita Windows NT -varaohjauspalvelimia tai Windows 2000 server -ohjauspalvelimia.

Tuettuja ohjauspalvelimia ovat Windows server 2003 -ohjauspalvelimet.

2.4 Toimialueen suunnittelu

Active Directory toimialueen toteutukseen liittyy useita tekijöitä. Pitää suunnitella nimiavaruus, joka sisältää toimialuehierarkian ja luottosuhteet. Lisäksi täytyy suunnitella organisaatioyksiköt. Toimialueen sisällä käyttäjätilit ja muut objektit tulee järjestää käyttämällä soveltuvaa organisaatioyksikköhierarkiaa. Laajemmassa verkossa täytyy suunnitella myös toimipaikat (sites), joiden avulla optimoidaan replikointi- ja sisäänkirjautumisliikennettä. (Kivimäki 2005 [1]: 8.)

2.4.1 Nimiavaruus (Kivimäki 2005 [1]: 8)

Active Directoryn nimiavaruus määrittää organisaation ylimmän tason toimialuenimen (forest root domain). Active Directoryn

nimiavaruus perustuu DNS:n nimeämisstandardeihin ja -hierarkiaan.

Yksi tärkeimmistä nimiavaruuspäätöksistä on se, käytetäänkö nimiavaruutena organisaation käyttöön jo rekisteröityä nimiavaruutta (Internet-toimialuenimi). Tähän liittyy myös se, luodaanko tai säilytetäänkö erillinen sisäinen nimiavaruus ja ulkoinen nimiavaruus vai yhdistetäänkö ne. Toimialueiden nimeäminen vaikuttaa kaikkiin Active Directoryn objekteihin. Jos käytössä oleva ulkoinen nimiavaruus on xyz.fi, niin Active Directory nimiavaruudeksi voidaan valita xyz.fi.

Julkisen verkon nimipalvelin voi vähimmillään sisältää ainoastaan web-palvelimen nimen (www.xyz.fi) ja MX-tietueen, jota tarvitaan tulevien sähköpostien ohjaamiseen oikeaan tietokoneeseen. Julkisesti käytettävät palvelut tuodaan verkon sisäisten asiakkaiden käyttöön lisäämällä ne sisäisen verkon nimipalvelimen ylläpitämään DNS-toimialueeseen osoitetietoina: molemmat DNS-toimialueet ovat xyz.fi.

Jos yrityksellä on erillinen sisäinen ja ulkoinen nimiavaruus, molemmat nimet voidaan varata Internetin DNS-rekisteröijältä. Jos molemmat nimet rekisteröidään, toinen julkinen verkko ei pysty varaamaan yrityksen sisäistä nimeä. Toinen mahdollisuus on käyttää rekisteröimätöntä sisäisen verkon nimeä, esimerkiksi ylimmän tason toimialuetunnusta .local. Tässä tapauksessa voidaan luoda erillinen sisäinen nimiavaruus. Sisäinen nimiavaruus olisi xyz.local ja Internetistä käytetään xyz.fi -nimeä ja intranetissä xyz.local.

Kun sisäisellä ja ulkoisella nimiavaruudella on eri nimet eri toimialuenimien takia, verkon sisäisten ja ulkoisten resurssien ero on selkeä. Verkon hallinta on helpompaa, kun ei tarvita päällekkäisiä ja kaksinkertaisia ylläpitoja.

Yksi haitta on se, että toimialueelle kirjautumisessa käytettävät nimet ja sähköpostinimet ovat erilaisia. Tämän pystyy ratkaisemaan muuttamalla käyttäjän UPN-jälkiliitteen ominaisuuksia niin, että tunnukset ovat samoja.

2.4.2 Toimialuerakenne

Kaikki Active Directory -toimialueet ovat liittyneet johonkin metsään (forest). Vaikka kyseessä olisi vain yksi toimialue, niin sekin muodostaa metsän. Toimialueessa on aluksi vain yksi ohjauspalvelin. Joten kaikissa Active Directory -ympäristöissä on sama lähtötilanne, yksi metsä, yksi toimialue ja yksi ohjauspalvelin. (Kivimäki 2005 [1]: 9.)

Ensimmäisenä metsään asennetaan juuritoimialue (forest root domain), joka on nimiavaruuden ensimmäinen toimialue. Metsän juuritoimialueella on erityinen asema metsässä, koska siellä sijaitsevat järjestelmänhallinan kannalta tärkeimmät ryhmät; Enterprise admins ja Schema admins. Enterprise admin -ryhmän jäsenellä on oikeus hallinnoida kaikkia metsän ohjauspalvelimia ja schema admins -ryhmän jäsenillä on oikeus käsitellä Active Directoryn rakennetta eli kaavaa (schema). (Kivimäki 2005 [1]: 9.)

2.4.3 Organisaatioyksiköt

Organisaatioyksiköitä käytetään Active Directoryn objektien hallitsemisessa. Tarkoituksena on pystyä hallitsemaan objekteja järkevästi kokonaisuuksina. Organisaatioyksiköiden tulisi heijastaa yrityksen liiketoiminnan rakennetta. Organisaatioyksiköiden rakenteen voi muodostaa vaikka toimipisteiden tai osastojen mukaan. (Kivimäki 2005 [1]: 10.)

Organisaatioyksiköihin voi linkittää ryhmäkäytäntöobjekteja (group policy object). Näin voidaan jakaa esimerkiksi ohjelmapäivityksiä, jotka kohdistuvat vain tiettyihin käyttäjiin tietyssä organisaatioyksikössä. Organisaatioyksiköt perivät toimialueen tai ylemmän tason organisaatioyksikön asetukset ja suojauskäytännöt, ellei toisin määrätä. (Kivimäki 2005 [1]: 10.)

2.4.4 Toimipaikat (sites)

Active Directory -verkkoympäristön fyysiseen rakenteeseen tulee kiinnittää huomiota. Fyysisen rakenteen rajat määritellään toimipaikoilla (sites), ne eivät kuulu Active Directoryn nimiavaruuteen. Toimipaikat muodostuvat yhdestä tai useammasta IP-aliverkosta. Toimipaikkojen rajat ovat yleensä samat kuin lähiverkon tai nopean WAN-verkon rajat. Active Directoryn replikointijärjestelmässä tapahtuva toimipaikan sisäinen liikenne on yleensä suurempaa kuin toimipaikkojen välinen liikenne. (Kivimäki 2005 [1]: 10.)

Toimipaikkojen vaikutus AD:n toimintaan

Käyttäjien kirjautuessa toimialueelle Active Directorya tukevat tietokoneet yrittävät löytää toimialueen ohjauspavelimen siitä toimipaikasta, jossa työasema on, näin kirjautumispyyntöjen käsittely on tehokkaampaa. Käyttäjän etsiessä resursseja Active Directorysta esimerkiksi kirjoittimia, ohjataan haku lähimmälle yleistä luetteloa pitävälle ohjauspalvelimelle. Hakujen käsittelystä tulee tehokkaampaa.
Toimialueiden välillä tapahtuvan replikoinnin aikataulu ja reitti voidaan määritellä. Toimipaikan sisäiselle replikoinnille näin ei voida tehdä. (Kivimäki 2005 [1]: 10.)

2.5 Ryhmäkäytännöt

Ryhmäkäytännöillä tarkoitetaan järjestelmän kokoonpanoasetuksia, jotka voidaan liittää Active Directoryn objekteihin, kuten organisaatioyksiköihin. Ryhmäkäytännöissä järjestelmänvalvojat voivat määrittää käyttäjien ympäristöasetuksia, ohjelmistoasetuksia ja suojausasetuksia. Ryhmäkäytännöt itse ovat objekteja (group policy object, GPO), joihin asetukset tallennetaan. (Kivimäki 2005 [1]: 527.)

Ryhmäkäytäntöjen hallintaa ja toteuttamista on parannettu Windows server 2003:een. Hallintakonsolin group policy -laajennus on uudistunut ja mukana on kaksi uutta hallintakonsolia (resultant set of policy ja group policy management console). Ryhmäkäytännöt ovat joustavampia muutosten ansiosta (esimerkiksi WMI-suodatus ja metsienvälinen tuki). Ryhmäkäytäntöjä on laajennettu ja ne on organisoitu uudelleen. (Kivimäki 2005 [1]: 527.)

Active Directory -toimialueilla on lisäksi toimialueen oletusryhmäkäytäntö sekä ohjauspalvelimien oletusryhmäkäytäntö. Toimialueen organisaatioyksiköihin ja toimipaikkoihin voidaan lisäksi määritellä ryhmäkäytännöt. Ryhmäkäytännöt käsitellään järjestelmän käynnistyessä ja sammutuksessa sekä käyttäjän kirjautuessa järjestelmään ja pois järjestelmästä. (Kivimäki 2005 [1]: 527.)

2.6 Luottosuhteet

Luottosuhteiden toiminnan tarkoituksena on sallia toimialueen käyttäjille toisen toimialueen resurssien käyttö. Normaalisti käyttäjä kirjautuu sille toimialueelle, jossa käyttäjätili sijaitsee. Luottosuhteen ansiosta käyttäjä voi kirjautua myös toiselle toimialueelle, johon luottosuhde on muodostettu. Toimialueluettelo nähdään kirjautumisikkunan yhteydessä olevasta valikosta. (Kivimäki 2005 [1]: 87.)

Luottosuhteiden avulla voidaan määritellä ryhmien jäsenyyksiä. Toisen toimialueen domain users -ryhmä voi olla toisen toimialueen paikallisen users -ryhmän jäsen. Kirjautumalla toiselle toimialueelle domain users -ryhmän käyttäjätilillä, pystytään käyttämään resursseja, jotka on sallittu toisen toimialueen paikallisen users -ryhmän jäsenille. (Kivimäki 2005 [1]: 87.)

Metsän sisällä luottosuhteet muodostuvat automaattisesti ylemmän ja alemman tason toimialueiden (parent domain ja child domain) välille. Myös metsän ylimmän tason toimialueet (domain tree root domain) luottavat toisiinsa automaattisesti. (Kivimäki 2005 [1]: 87.)

Windows server 2003 -käyttöjärjestelmän uusi ominaisuus on metsien liittäminen toisiinsa. Tämä edellyttää, että metsät toimivat Windows server 2003 -toimintatasolla. Tällöin ne voidaan liittää toisiinsa siten, että kerberos tunnistusmenetelmä on käytössä metsän laajuisesti kaikissa metsän toimialueissa. (Kivimäki 2005 [1]: 87.)

2.7 Replikointi

Jokaisella Active Directory -toimialueella on yksi tai useampia palvelimia, jotka toimivat toimialueen ohjauspalvelimina (domain controller). Toimialueita tai metsiä voi olla yksi tai useampi, tässä tapauksessa on yksi metsä ja kaksi toimialuetta. Active Directory käyttää multimaster-replikointia, joka tarkoittaa että toimialueen ohjauspalvelimet ovat tasavertaisia. Active Directoryssa jokaisessa toimialueen ohjauspalvelimessa on täydellinen toimialueen tietokanta ja jokainen ohjauspalvelin on osaltaan vastuussa toimialueen tietokantaan tehtävien muutosten ja päivitysten hallinnasta. (Kivimäki 2005 [1]: 647.)

Active Directory muodostaa automattisesti ohjauspalvelinten välille yhteyksiä replikoinnin suoritusta varten. Tämän rakenne (topologia) muistuttaa rengasta. Se määrittää polun, jota pitkin päivitykset suoritetaan ohjauspalvelimesta toiseen, kunnes kaikkien ohjauspalvelinten hakemistot on päivitetty. Ohjauspalvelimilla on tuleva (replicate from) ja lähtevä (replicate to) replikointiyhteys. Rengasrakenteella varmistetaan, että käytettävissä on joka tilanteessa ainakin kaksi toimialueen ohjauspalvelimelta toiselle johtavaa polkua. Jos yksi ohjauspalvelin on pois käytöstä, replikointi jatkuu muiden ohjauspalvelinten välillä. (Kivimäki 2005 [1]: 647.)

2.8 Ohjauspalvelinten roolit (operations master)

Active Directory -toimialueiden ohjauspalvelimet suorittavat tärkeitä tehtäviä. Käytännössä ohjauspalvelimet ovat tasaveroisia. Osa ohjauspalvelimista ylläpitää Active Directoryn suorittamia tehtäviä, joita muut ohjauspavelimet eivät suorita. Voidaan sanoa, että ne ylläpitävät jotain roolia tai omaavat roolin ja ovat siten toimintopalvelimia (operations master). Rooleja on viisi erilaista ja jokaisessa toimialueessa on kolmen tyyppisiä rooleja sekä kaksi metsäkohtaista roolia. (Kivimäki 2005 [1]: 63.)

Toimialuekohtaiset roolit

- Primary domain controller (PDC) emulator: PDC-emulaattori -roolissa oleva ohjauspalvelin käsittelee kaikki replikointipyynnöt Windows NT 4.0 -varaohjauspalvelimilta sekä kaikki salasanapäivitykset

asiakastietokoneilta, joissa ei ole Active Directorya tukevaa asiakasohjelmistoa. Se ylläpitää päiväystä ja kellonaikaa toimialueella ja on pääselaaja (domain master browser).

- Relative identifier (RID) master: RID-master roolissa oleva ohjauspalvelin varaa suhteellisia suojaustunnisteita (RID) kaikille ohjauspalvelimille ja varmistaa, että kaikilla suojauspääobjekteilla, kuten käyttäjätileillä, on yksilöllinen tunnus.

- Infrastructure master: Tämän roolin omaava ohjauspalvelin ylläpitää luetteloa toimialueen ulkopuolisista suojauspääobjekteista. (Kivimäki 2005 [1]: 64-65.)

Metsäkohtaiset roolit

- Schema master: Hallitsee kaikkia Active Directoryn rakenteeseen eli kaavaan (schema) tehtäviä ja muutoksia.

- Domain naming master: Lisää ja poistaa metsän toimialueita. (Kivimäki 2005 [1]: 64-65.)

Muita rooleja

- Metsän juuritoimialuetta luotaessa (forest root domain) luodaan kaavan ja configurointitietojen säiliöt. Ensimmäiselle ohjauspalvelimelle määritellään kaikki tarvittavat roolit: PDC-emulaator, RID master, domain naming master, schema master ja infrastructure master.

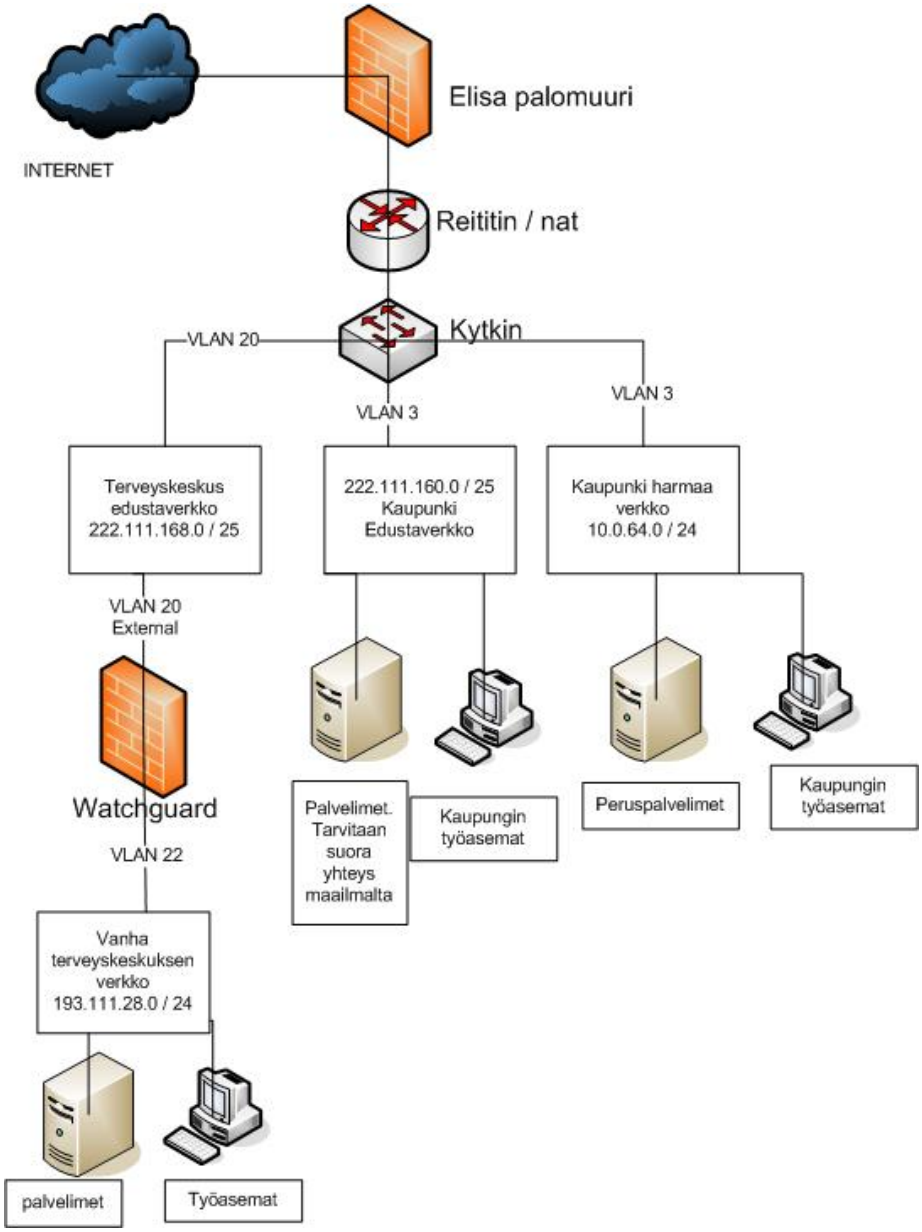
- Lisäksi ohjauspalvelin ylläpitää yleistä luetteloa. (Kivimäki 2005 [1]: 64-65.)

3 Kaupungin verkkoympäristö

3.1 Alkuperäinen verkko

Kaupungin sisäverkko on jaettu loogisiin osiin, joista suurimmat ovat terveyskeskukselle jakautuva verkko, kaupungin hallintoverkko ja koulujen verkot. Kaupungin ydinverkko lähtee palveluntarjoajan palomuurilta VLAN3:sta pitkin ja jakautuu niin sanotuksi edustaverkoksi ja harmaaksi verkoksi 10.0.64.0 osoiteavaruudella. Kaupungin hallintoverkon palvelimet sijaitsevat tässä verkon osassa. Verkkoympäristön laitteet pääsevät Internetiin Elisan palomuurin kautta.

Vanha terveyskeskuksen verkko sijaitsee verkkoympäristössä omana osanaan erillisen palomuurin takana. Liikenne ohjataan palomuurilta VLAN:ien avulla Watchguard-palomuurille, joka toimii rajalaitteena terveysverkolle. Erillisellä palomuurilla saadaan rajoitettua kaupungin ja terveyskeskuksen verkon välistä liikennettä, esimerkiksi terveyskeskuksen verkkoresurssien käyttö saadaan estettyä kaupunkikäyttäjiltä. Kuva 1 esittää graafisessa muodossa kaupungin alkuperäisen verkkoympäristön. Kuvassa on muutetut IP-osoitteet ja toimialuenimet.



Kuva 1. Kuva kaupungin alkuperäisestä verkkoympäristöstä.

3.2 Testausvaiheen verkko

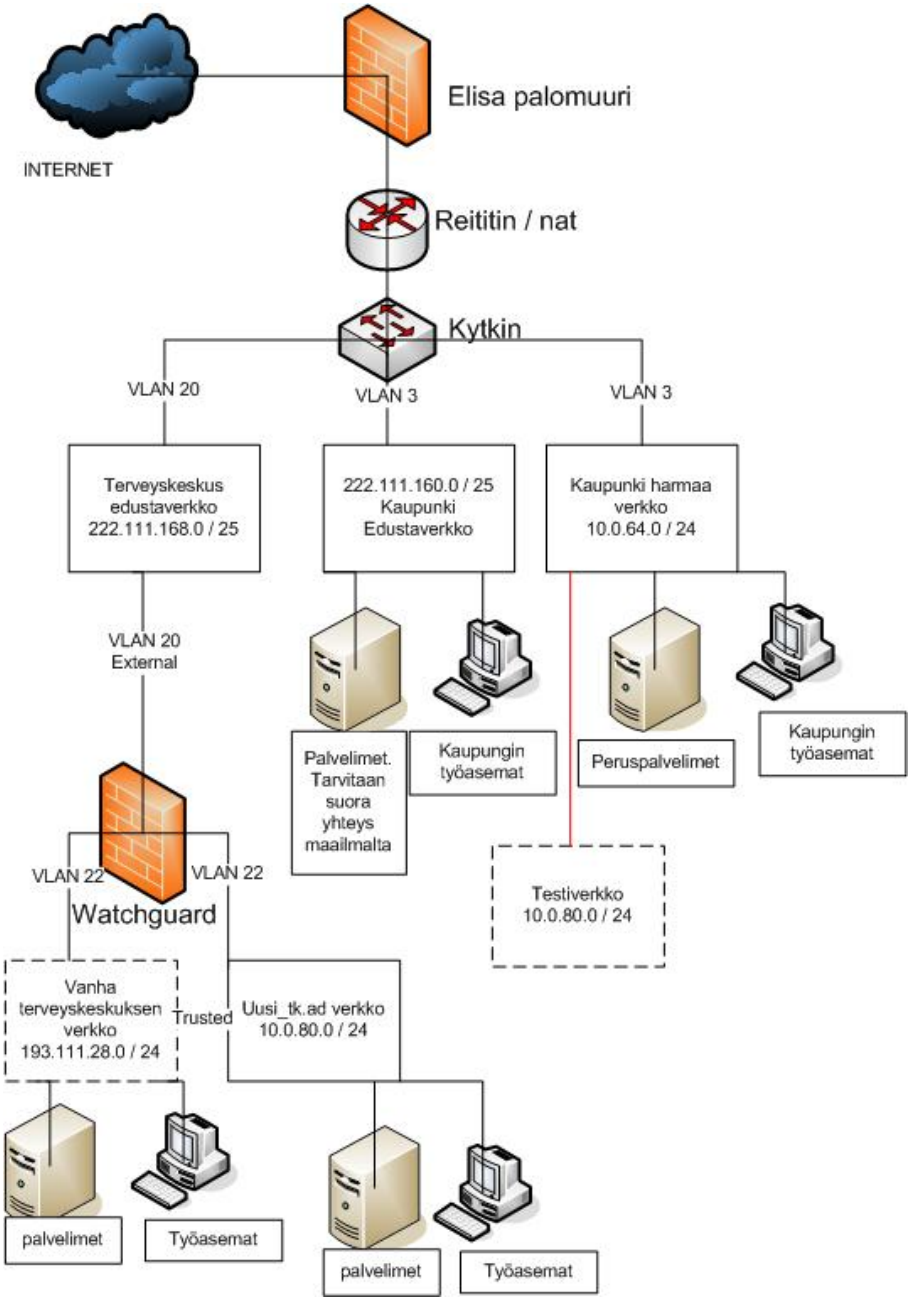
Testausvaiheen verkkoympäristöllä tarkoitetaan verkon osia, jotka luotiin käytettäväksi palvelimen pystytyksen aikana ja jotka poistettiin tuotantoverkkoon siirtymisen yhteydessä. Aluksi tk_server1-palvelin sijaitsi kaupungin verkkoon tehdyssä harmaassa verkossa. Verkon rajalaitteena toimi Watchguardin soho 5 palomuurilaite, jonka ulkoverkon portissa oli kaupungin verkon osoite 10.0.64.17 ja sisäverkko muodostui 10.0.80.0 /24 osoiteavaruudesta. Palomuurilaite toimi verkon rajalla NAT -kääntäjänä. Laitteelle tehtiin sääntö, jotta verkon muut laitteet näkisivät tk_server1:n omalla osoitteellaan 10.0.80.2.
Verkkoon tuli kuitenkin reititysongelma, koska oikean palomuurin sisäpuolelle oli määritelty samainen 10.0.80.0 verkko ja testiverkosta lähtevä liikenne ei osannut palata oikeaan paikkaan takaisin. Reitityssäännöillä liikenne saatiin kulkemaan oikeaan

10.0.80.0 verkkoon. Kaupungin palvelimille server1 ja server2 luotiin route add komennolla reitti oikeaan verkkoon.

3.3 Uusittu verkko

Tavoitetila verkkoympäristössä on silloin, kun uudet osat on kytketty ja vanhat poistettu käytöstä. Uusittuun verkkoympäristöön tuli uutena osana uusi_tk.ad verkkoalue, johon terveyskeskuksen verkkotoiminta siirtyy. Verkko sijaitsee Watchguard palomuurin takana, kuten vanha terveysverkko. Koska palvelinten siirtoa ei voitu toteuttaa yhtenä kokonaisuutena, molemmat vanha ja uusi terveyskeskuksen verkko, toimivat rinnakkain vaihdon aikana. Koska molempien toimialueiden palvelinten pitää päästä kommunikoimaan keskenään verkot ovat rinnakkaisia ja luottavat toisiinsa. Luottosuhde mahdollistaa liikenteen kulkemisen ja resurssien jakamisen verkkojen kesken. Myös uusi_tk.ad verkossa pätee samat palomuurisäännöt, kuin vanhassa, eli liikennettä rajataan niin, etteivät kaupunkikäyttäjät pääse käyttämään verkon resursseja.

Lopulliseen muotoon verkkoympäristö tulee, kun kaikki vanhan terveyskeskuksen palvelimet saadaan siirrettyä uusi_tk.ad-verkkoon ja vanha verkkoalue voidaan poistaa käytöstä. Kuva 2 näyttää kaupungin verkkoympäristön uudistusten jälkeen. Poistuvat verkko-osat on merkitty katkoviivoilla.



Kuva 2. Kuva kaupungin uudistetusta verkkoympäristöstä.

4 Palvelinympäristö

Kun palvelinvaihdosta suoritetaan, on selvää, että muutos vaikuttaa myös muuhun verkkoympäristöön sekä muihin palvelimiin. Palvelimen rakenteen ja palveluiden suunnittelussa lähdettiin liikkeelle vanhaan palvelinkalustoon tutustuen. Myös kaupunkiverkon palvelimet olivat tarkastelun alla ja etenkin uusittavien palvelimien suunnittelussa näitä käytettiin apuna. Oli helpompaa käyttää jo olemassa olevaa mallia apuna, kuin aloittaa suunnittelu kokonaan puhtaalta pöydältä. Kaupungin palvelinten ja uusi_tk.ad -verkon palvelinten toimintaperiaatteet, roolijaot ja tehtävät tulevat olemaan samankaltaisia. Myös kotihakemistot ja osastojen verkkokansiot toimivat samalla periaatteella. Koska palvelinten toimintaperiaatteet muistuttavat toisiaan, hyväksi havaitun mallin käyttäminen valmiista mallista on perusteltua.

4.1 Kaupungin palvelimet

Yritys.ad on kaupungin toimialue ja se on metsän ensimmäinen toimialue, joten se on myös metsän juuritoimialue. Uusi toimialue pystytetään tasavertaiseksi yritys.ad toimialueen kanssa, mutta silti yritys.ad toimialue on metsän ensisijainen toimialue. Lisäksi Yritys.ad-toimialueella sijaitsee ohjauspalvelinten metsäkohtaiset schema master ja domain naming master roolit.

Server1

Server1 on metsään ensimmäisenä asennettu ohjauspalvelin. Sillä on aktiivihakemistopalvelut, kuten myös metsäkohtaiset roolit, se ylläpitää tietoja toimialueiden nimeämisistä (domain naming master) ja ylläpitää aktiivihakemiston kaavaa (schema master). Se on PDC-emulaattori ja toimialuekohtaisista rooleista se on Rid-master ja yleinen leuttelo (global catalog). Se toimii nimipalvelimena kaupungin työasemille. Server1 -palvelimella on käyttäjien kotihakemistot.

Server2

Server2 on myös ohjauspalvelin, jolla on aktiivihakemistopalvelut. Toimialueen rooleista sillä on infrastructure master (IM) rooli. Palvelimella pyörii DHCP-palvelu, joka jakaa osoitteita kaupungin työasemille. Verkkoasemista server2:lla on osastokohtainen data ja sovellukset.

4.2 Terveyskeskuksen vanha toimialue

Terveysk.local on terveyskeskuksen vanha toimialue, joka poistuu käytöstä muutoksen valmistuttua. Terveysverkko sijaitsee omassa metsässä kaupungin verkkoympäristössä. Liikenne yritys.ad:n ja terveysk.local:in välillä on kulkenut luottosuhteen ansiosta. Liikennettä on rajoitettu palomuurilla, siten etteivät

kaupunkikäyttäjät pääse terveyspuolen resursseihin käsiksi. Toimialueella on ollut kolme palvelinta, joista yksi on ollut ohjauspalvelin sisältäen aktiivihakemiston ja kaksi muuta ovat jäsenpalvelimia.

Terveyspalvelin

Terveyspalvelimen käyttöjärjestelmänä on Windows 2000 server. Se on terveysverkon ainoa ohjauspalvelin ja sisältää aktiivihakemistopalvelut, joten sillä on kaikki toimialuekohtaiset roolit. Se on infrastructure master, RID-master, PDC-emulaattori ja yleinen luettelo (global catalog) palvelin. Sillä on DNS- ja DHCP-palvelut sekä se ylläpitää luottosuhteita. Käyttäjien kotikansiot sekä jaettu levyasema X sijaitsevat palvelimella. Ohjelmista terveyspalvelimella oli muutoshetkellä MDtitania.

Muut palvelimet

Muita toimialueeseen kuuluvia palvelimia ovat ORIAPP02 sekä ORIAPP03. Ne ovat molemmat jäsenpalvelimia, eivätkä siis ylläpidä aktiivihakemistoa tai omaa toimialuerooleja. Palvelimilla on ohjelmia, kuten Physiotools, Liinos6 ja Mediatri.

4.3 Terveyskeskuksen uusi toimialue

Uusi_tk.ad-toimialue tulee uutena toimialueena verkkoympäristöön. Se pystytetään juuritoimialueeksi yritys.ad toimialueen kanssa, Yritys.ad toimialueen pysyessä metsän ensisijaisena juuritoimialueena. Uusi_tk.ad-toimialue korvaa vanhan terveysverkon, mutta siirron aikana ne toimivat rinnakkain ja vasta siirron lopuksi vanha toimialue poistetaan kokonaan käytöstä. Uusi toimialue ja uudet palvelimet tulevat tehtäviltään muistuttamaan vanhan toimialueen palvelimia, mutta nykyaikaa vastaavilla toiminnoilla. Palvelimien rakenteissa on käytetty mallina yritys.ad-toimialueen palvelimia, koska valmista ja toimivaa mallia haluttiin hyödyntää. Osa toiminnoista on pitänyt suunnitella uusiksi vastaamaan terveyskeskuksen olosuhteita.

Tk_server1

Tk_server1 korvaa vanhassa terveysverkossa olleen terveyspalvelimen. Tk_server1 on toimialueensa ensimmäinen ohjauspalvelin ja tämän vuoksi sille on annettu suuri osa toimialuekohtaisista rooleista, kuten PDC-emulaattori, RID-master ja yleinen luettelo. Palvelimelle asennettiin myös DHCP-palvelu, joka oli käytössä testaamis- ja siirtymävaiheessa. Palvelimella toimii lisäksi vielä nimipalvelu ja aktiivihakemisto. Käyttäjien kotihakemistot sijaitsevat tällä palvelimella.

Tk_server2

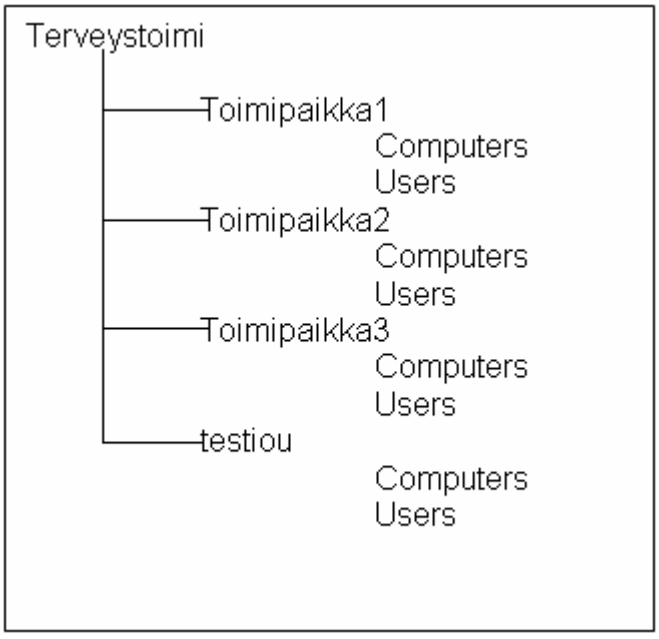
Tk_server2 on uusittu versio vanhassa terveysverkossa olleesta ORIAPP02-palvelimesta. Tk_server2 on myös aktiivihakemiston omaava ohjauspalvelin. Toimialue kohtaisista rooleista se on infrastructure master. Sillä on nimipalvelu ja se on varalla oleva DHCP-palvelin. Palvelimella sijaitsee osastokohtainen data ja sovellukset.

4.4 Tk_server1:n suunnittelua

Vanhan terveyspalvelimen idea ja suunnitelma on perusajatukseltaan samankaltainen kuin uuden palvelimenkin. Erona on esimerkiksi käyttöjärjestelmän vaihtaminen Windows Server 2003:een ja sen tuomat muutokset. Koska Tk_server1:n rakenne tulisi muistuttamaan vanhaa, suunnittelu oli hyvä aloittaa tutkimalla vanhan terveyspalvelimen rakennetta ja yrittää tehdä asiat vielä paremmin. Ensinnäkin aktiivihakemiston rakenteeseen tulee paljon muutoksia, sillä vanhassa verkossa organisaatioyksiköiden rakenne on olematon. Käyttäjät sijaitsevat kaikki samassa yksikössä, jossa on myös built-in -käyttäjät, ryhmäobjektit ja erityistarpeisiin tehdyt käyttäjätunnukset. Käytännössä rakenne tulisi muistuttamaan paljon kaupungin palvelimien aktiivihakemistojen rakennetta, joiden mallia hyödynnettiin suunnittelussa ja toteutuksessa.

4.4.1 OU - organisaatioyksiköt

Vanhalla palvelimella ei ollut minkäänlaista erillistä OU rakennetta käyttäjä- ja tietokone objekteille. Uudelle palvelimelle oli siis mahdollisuus rakentaa kokonaan uusi rakenne kyseisten kohteiden osalta. Samalla kun organisaatio yksiköiden lopullista muotoa suunniteltiin, oli mahdollista jakaa käyttäjät ja tietokoneet työpisteiden ja tehtävien mukaan järjestykseen aktiivihakemistoon. Tämä tapahtui siten, että terveyskeskus käyttäjät saisivat oman organisaatioyksikön ja muut toimipisteen mukaan omansa. Ylimpänä OU:na terveydenhuoltopalveluille toimii terveystoimi, jonka alle alatoimipisteet sijoitetaan. Kuva 3 näyttää organisaatioyksiköiden rakenteen.



Kuva 3. Organisaatioyksiköiden rakenne

4.4.2 Ryhmät

Vanha ryhmäjako oli tehty pääasiassa ohjelmien mukaan. Jos käyttäjä tarvitsi tiettyä ohjelmaa, hänet laitettiin asianmukaiseen ryhmään. Mitään jakoa toimialoittain tai työpisteittäin ei siis ollut. Uudet ryhmäjaot tulevat muistuttamaan vanhoja siltä osin, että ohjelmien osuus tulisi pysymään samana. Käyttäjä, joka kuului jonkin ohjelman ryhmään, tulee olemaan siinä vieläkin. Uudistuksen myötä tehtiin lisäksi toimipisteiden mukaan ryhmät. Tämä mahdollistaa verkossa olevien osastokohtaisten jaettujen hakemistojen oikeuksien määrittelyn helpommin. Kun käyttäjä kuuluu terveyskeskus-ryhmään, hänellä on oikeus käyttää jaettua verkkohakemistoa nimeltä terveyskeskus. Samalla saadaan työntekijät laittamaan yhteisiä tiedostoja verkkoasemille, jotka ovat kaikkien samaan ryhmään kuuluvien työntekijöiden nähtävillä. Kotikansioiden lisäksi tämä toimenpide vähentää tietojen tallennusta paikallisen koneen kovalevylle, joka taas estää tietojen häviämistä laitevian sattuessa, koska palvelimen tiedot varmuuskopioidaan säännöllisin väliajoin.

4.4.3 Nimiavaruus

Kaupungin metsässä käytetään yhteistä orivesi.fi nimiavaruutta. Vanhassa terveysverkossa ei pystynyt kirjautumaan toimialueelle muuta kuin omalla tunnuksella. Uuteen toimialueeseen lisättiin mahdollisuus kirjautua myös orivesi.fi päätteisellä kirjautumisnimellä. Yhteinen nimiavaruus helpottaa tulevaisuudessa vaihdettavaan sähköpostipalvelimeen siirryttäessä.

Nimiavaruuden suunnittelussa lähdettiin siitä, että uuden toimialueen ensimmäiselle ohjauspalvelimelle laitettaisiin nimipalvelut. Tämä palvelin käsittelisi uusi_tk.ad-toimialueen koneilta tulevat nimikyselyt ja jos palvelin ei osaa vastata se lähettää kyselyn edelleen palveluntarjoajan nimipalvelimelle. Yksi vaihtoehto olisi ollut ohjata nimikyselyt kaupunki-toimialueen nimipalvelimelle, mutta tämä ruuhkauttaisi verkkojen välistä liikennettä, joka pyrittiin pitämään mahdollisimman pienenä. Kaupungin palvelimille lähetetään yritys.ad-päätteiset kyselyt. Nimiavaruus itsessään integroidaan kaupungin verkon nykyiseen ympäristöön, vaikka se toimii omana itsenäisenä osana.

4.4.4 Toimialuerakenne ja luottosuhteet

Kaupungin verkkoympäristö muodostui ennen uuden toimialueen lisäämistä kahdesta metsästä, joissa molemmissa oli oma toimialue. Uusi toimialue liitetään kaupungin metsään tasavertaisena toimialueena jo olemassa olevan yritys.ad toimialueen rinnalle. Juuritoimialueena verkkoympäristössä toimi yritys.ad toimialue, joka myös omistaa järjestelmänhallinnan kannalta tärkeimmät tehtävät eli enterprise admins ja schema admins ryhmät. Tämä tarkoittaa sitä, että enterprise admins -ryhmään kuuluvalla tunnuksella on oikeus hallinnoida kaikkia metsän oh-

jauspalvelimia ja schema admins -ryhmän jäsenillä oikeus käsitellä aktiivihakemiston rakennetta.

Uusi_tk.ad-toimialue nostetaan tasavertaiseksi yritys.ad-toimialueen kanssa, eli molemmat ovat niin sanottuja juuritoimialueita (tree-root domain). Juuritoimialueiden välille muodostuu automaattisesti transitiivinen, kaksisuuntainen luottosuhde. Molemmat toimialueet luottavat toisiinsa. Käytännössä tämä tarkoittaa sitä, että molempien toimialueiden käyttäjät pystyvät kirjautumaan toiselle toimialueelle ja käyttämään toisen toimialueen resursseja. Kaikkien resurssien käyttö, kuten levy- tai kirjoitin mäppäys on kuitenkin estetty palomuurisäännöillä, ellei erikseen määritellä poikkeussääntöjä.

Palvelinvaihdoksessa tärkeänä osana on vielä tk_server1 ja vanhan terveyspalvelimen välisen liikenteen ja palveluiden keskinäinen toimivuus. Koneiden vaihdon ja käyttäjien tekemisen yhteydessä uuden palvelimen pitää pystyä hakemaan tietoa vanhan palvelimen aktiivihakemistosta sekä ORIAPP03-palvelimelta, pitää näiden toimialueiden välille rakentaa erikseen luottosuhde. Luottosuhteen tulee olla kaksisuuntainen.

4.4.5 Toimipaikat

Toimipaikat vaikuttavat replikoinnin onnistumiseen ja sen tehokkuuteen. Tk_server1-palvelimen toimipaikkoihin on määritelty yritys.ad- ja uusi_tk.ad-toimialueen keskeisten palvelinten tiedot, koska turhaa liikennettä halutaan välttää. Replikointiyhteydet tulevat kaupunkitoimialueen server1- ja server2-palvelimilta sekä uusi_tk.ad-toimialueen tk_server1- palvelimelta. Lähtevät replikointiyhteydet on ohjattu server1- ja tk_server2-palvelimille.

5 Uuden Active Directory -palvelimen asennus

5.1 Palvelimen asennus

Palvelimen pystytys aloitettiin sen kokoamisella sekä perusasetusten tekemisellä. Palvelimen asennusvaiheen aikana tehtyjä huomioitavia asioita ovat RAID-asetusten tekeminen, käyttöjärjestelmän asennus ja perustyökalujen sekä päivitysten asentaminen.

Päivitykset

Palvelimelle tehtiin päivitykset ennen käyttöjärjestelmän asentamista. Palvelimelle päivitettiin firmware, array, ILO-laitteisto sekä BIOS online. Käyttöjärjestelmän asentamisen jälkeen palvelimelle päivitettiin Windowsin peruspäivitykset, joihin kuuluivat lisäksi Framework- ja RDP v6- päivitys. Palvelimelle asennettiin c:\util-kansioon perustyökaluja kuten adminpak, support tools sekä reskit. Paketit sisältävät toiminnan kannalta tärkeitä työkaluja.

ILO

Integrated lights-out on palvelimen ominaisuus, jolla palvelinta pystytään hallitsemaan etänä. ILO-kortilla on oma verkko-osoite palvelimessa. ILO-kortin avulla pystytään käynnistämään palvelin uudelleen, vaikka se olisi sammutettu. Tämä on käytännöllistä, jos palvelimen oma verkkokortti ei vastaa. Sillä pystytään kaappaamaan kuvaruutu ja käyttämään CD/DVD-asemaa.

Raid-asemien hallinta

Palvelimen kovalevyt jaetaan loogisiin kokonaisuuksiin, jotta yhden levyn hajottua ei menetetä kaikkea tietoa, jota levyllä on. Palvelimessa on kaksi levykokonaisuutta, järjestelmäosio ja dataosio. Järjestelmäosio koostuu kahdesta 72 gigatavun kovalevystä, jotka on yhdistetty RAID1-tekniikalla. Tieto peilataan molemmille levyille. Jos toinen hajoaa, sama data löytyy myös toiselta levyltä. Dataosioon kuuluu kolme 146 gigatavun kovalevyä, jotka on yhdistetty yhdeksi kokonaisuudeksi RAID5-tekniikan avulla. RAID5-tekniikka pakkaa levyt kokonaisuudeksi niin, että yksi levy voi hajota ilman, että tietoa menetetään.

5.2 Roolit ja palvelut

Tk_server1:en rooleja suunniteltaessa mietittiin parhaita mahdollisia ratkaisuja tehdä verkosta mahdollisimman vikasietoinen, toimiva ja käytännöllinen. Roolien oikean sijoittamisen tulisi sopia myös tulevaisuuden tarpeisiin, joihin kuuluu todennäköisesti sähköpostipalvelimen tuleminen verkkoympäristöön. Koska uusi_tk.ad-toimialueelle tulisi myös kaksi lisäpalvelinta oli mahdollista jakaa tehtävät nykyaikaisen verkon tarpeisiin sopiviksi.

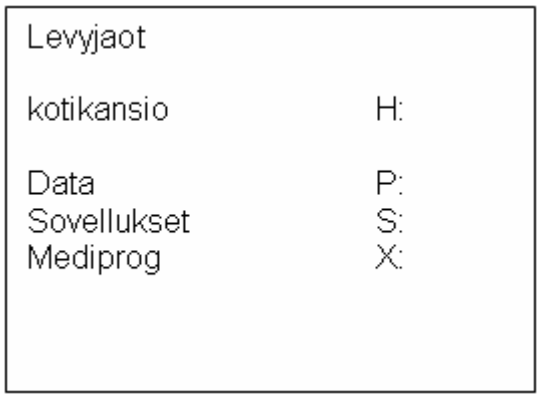
Koska tk_server1 tulee olemaan toimialueensa ensimmäinen palvelin, sille jouduttaisiin antamaan väliaikaisesti myös muita tehtäviä. Sijoitusten takana oli ajatus siitä, että tehtävät jakautuisivat tasaisesti kahden ohjauspalvelimen välille.

Tk_server1 on ohjauspalvelin, joka ylläpitää aktiivihakemistoa. Sen kautta pystytään ylläpitämään käyttäjätietokantaa ja ryhmäasetuksia. Toimialuekohtaisista rooleista se on PDC-emulaattori (primary domain controller), RID-master (relative identifier) ja ylläpitää yleistä luetteloa (Global catalog). Infrastructure master (IM) rooli sijaitsee tk_server2:lla, koska yleistä luetteloa ja IM-roolia ei suositella samalle palvelimelle. Metsäkohtaiset roolit kuten Schema master ja domain naming master roolit ovat server1:llä. Tk_server1:llä on myös nimipalvelimen rooli ja sillä oli väliaikaisesti DHCP-palvelu. Lopullisesti osoitepalvelu tulee kolmannelle uudelle palvelimelle, mutta palvelimen siirto oli vielä suunnitteilla, joten se laitettiin väliaikaisesti tk_server1:lle.

Toimialuekohtaisten roolien lisäksi piti päättää verkkoasemien sijainnit. Kotihakemistot, sovellukset ja osastojen verkkokansiot täytyi saada jaettua tasaisesti palvelimien kesken. Ratkaisussa päädyttiin käyttämään samaa mallia, joka on jo käytössä yritys.ad-toimialueessa. Kotihakemistopalvelut jaetaan toiselle palvelimelle ja sovelluksia koskeva data sekä osastodata toiselle palvelimelle. Näin toisen palvelimen hetkellinen poissaolo ei kadota kaikkia verkkoasemia. Ylläpidon kannalta ratkaisu on myös hyvä, koska kotihakemistot ovat server1:llä sekä kaupungin että uusi_tk.ad-verkon puolella ja taas vastaavasti muut verkkoasemat server2:lla.

Kotikansiot

Jokaisella käyttäjällä oma kotikansio, jokainen kansio on jaettu $, joka tarkoittaa piilotettua jakoa. Jako on yksinkertaisempi, kuin yksi kotikansiojako. Huonona puolena on jakojen suuri määrä. Malli on sama kuin yritys.ad:n kotikansiorakenteissa. Kuvassa 4 on kuvattu levyjaot ja niiden kirjaimet.



Kuva 4. Verkkoasemat

5.3 Ohjauspalvelimen asennus ja toimialueen pystytys

Valmistelu

Ennen kuin palvelimelle voidaan lisätä ohjauspalvelimen rooli ja uusi toimialue asentaa täytyy metsään tehdä muutamia toimenpiteitä. Windows 2000-toimialue on ensin valmisteltava Windows server 2003 -ohjauspalvelimen asentamista varten. Myös metsän yhteinen schema master -ohjaupalvelin, sekä jokaisen toimialueen infrastructure master -ohjauspalvelimet käsitellään adprep.exe-ohjelmalla ennen kuin Windows server 2003 -ohjauspalvelin voidaan asentaa. Metsän schema master -palvelimena toimii kaupunki toimialueen server1 ja infrastructure-palvelimina server2 ja vanha terveyspalvelin.

Asennus

Ohjauspalvelimen asennus tapahtuu Dcpromo-työkalulla. Se sijaitsee administrative tools -valikossa configure your server wizard -kohdassa, Domain controller (Active Directory), toinen vaihtoehto on kirjoittaa komentokehotteessa dcpromo. Kummallakin tavalla aukeaa ohjattu asennus -toiminto.

Aluksi valitaan ohjauspalvelin uudelle toimialueelle, koska toimialue pystytetään samalla. Toimialueen paikka on uusi toimialue valmiissa metsässä. Toimialue nimetään sekä sen koko DNS-nimellä (uusi_tk.ad) että netbios nimellä (uusi_tk). Palvelimelle määritetään kansiot, joissa tietokannat ja lokitiedot sijaitsevat. Kansio on oletuksena tarjottu C:\WINDOWS\NTDS -kansio. Myös julkisten tietojen sijainnit määritetään oletuksena tarjottuun kansioon C:\WINDOWS\SYSVOL. Palvelimelle asennetaan nimipalvelut, vaikka ne ovat jo pystyssä. Palvelin on itsessään nimipalvelin. Permissions -ikkunassa määritetään yhteensopivuus asetukset aiempien käyttöjärjestelmien kanssa. Koska käytössä on vain Windows server 2003 ja 2000 palvelimia, valitaan vaihtoehdoista tämä. Directory Services Restore Mode administrator password -ikkunassa määritetään pääkäyttäjän salasana, jonka avulla palvelin voidaan käynnistää Directory Services Restore Mode -tilassa. Salasana on paikallinen eikä koske toimialuekohtaisia asetuksia. Lopuksi tarkastetaan yhteenveto tilanteesta ja tarkistetaan tietojen paikkaansapitävyys. Varsinaisen hakemiston asennus tapahtuu vasta tässä kohtaa.

5.4 Nimipalvelut ja DHCP

Nimipalvelut

Suunnitelman mukaan nimipalvelimena toimii tk_server1. DNS-asennus toteutettiin asennusvelhon avulla. Nimiavaruus määriteltiin toimialueen nimen mukaisesti eli uusi_tk.ad. IP-osoiteavaruutena käytetään uusi_tk.ad-toimialueelle tarkoitettua osaa kaupungin harmaansarjan verkosta joka on c-luokan osoite 10.0.80.0/24. Asetuksissa osoite on muodossa 10.0.80, joka tarkoittaa, että käytössä ovat osoitteet 10.0.80.0 - 10.0.80.255. Molemmat asetukset määritellään ensisijaisiksi, jotta ne hyväk-

syisivät automaattisia päivityksiä. Jotta automaattiset päivitykset toimisivat, ne täytyy vielä laittaa päälle. Tämä tapahtuu DNS-asetuksista, molemmat alueet erikseen sekä forward että reverse, valitaan automaattisten päivitysten hyväksyminen.

Jotta nimiasetukset olisivat kunnossa, tarvitsee vielä asentaa nimiosoitukset (forwarder). Nimiosoituksien tehtävänä on lähettää nimikyselyt eteenpäin, jos kyseinen nimipalvelin ei tiedä vastausta. Konditional forwarder, eli jos loppu on yritys.ad, asetetaan server1:ksi ja server2:ksi (10.0.64.4 ja 10.0.64.10). Seuraavat osoittimet laitetaan osoittamaan palveluntarjoajan nimipalvelimille.

WINS-palvelu hoitaa toimialueen nimenkäännöstapahtumia netbios-nimien perusteella. Netbios-nimenkäännöstä käyttävät pääasiassa vanhemmat käyttöjärjestelmät ja exchange palvelin 2000 ja 2003. WINS-asetukset määriteltiin tulevaisuuden tarpeita ajatellen eli mahdollista sähköpostipalvelimeen siirtymistä varten. Tk_server1 ja tk_server2 replikoivat keskenään WINS-asetuksia.

Testiverkossa ja ennen tuotantoverkkoon siirtymistä käytettiin nimipalveluiden toimimisen varmistamiseksi host-tiedostojen apua. Host-tiedostoihin määritellään muiden palvelimien ip-osoite- ja nimitiedot. Näin varmistetaan muiden palvelimien löytyminen lyhyen DNS-nimen avulla. Esimerkki tietojen syöttämisestä: 10.0.0.4 Server1. Host-tiedostoja käytetään vain pakon edessä, eivätkä ne ole lopullisia.

DHCP

DHCP-palvelun pystyttäminen jouduttiin tekemään tk_server1:lle, koska tk_server2:ta ei ollut vielä pystytetty, mutta työasematestauksen vuoksi koneille tarvittiin IP-osoitteet. DHCP määriteltiin käyttämään suunniteltua IP-osoiteavaruutta, joka oli 10.0.80.0 aliverkon peitteellä 255.255.255.0. Koneille jaettavat osoitteet olivat väliltä 10.0.80.130 - 10.0.80.250. Varsinaiseen tuotantoverkkoon siirryttäessä DCHP otettiin pois päältä ja lisättiin takaisin työasemien siirtämisen yhteydessä.

Varsinainen DHCP-palvelu asennetaan tk_server3 -palvelimelle, kuten alunperin suunniteltiin. Koska palvelin asennetaan vasta myöhemmin, toimii tk_server1 väliaikaisesti nimipalveluna.

5.5 Luottosuhteet ja replikointi

Luottosuhteet

Luottosuhteita jouduttiin määrittelemään moneen otteeseen, koska suunnitelmat muuttuivat työn edetessä. Tämän vuoksi määrityksiä jouduttiin lisäämään muutamaan kertaan aina tarpeiden mukaan. Luottosuhteita koskevat asetukset kerrotaan

kuitenkin yhtenä kokonaisuutena yhtenäisyyden ja hahmottamisen vuoksi.

Lähtötilanteena oli vanhan terveysk.local-toimialueen ja yritys.ad-toimialueen välinen luottosuhde, jota oli tarkoitus käyttää myös uuden toimialueen kanssa. Kuten vanhan luottosuhteen, myös uuden oli tarkoitus olla käytettävissä vain toiseen suuntaan. Terveyskeskuksen käyttäjät pääsisivät käyttämään kaupungin puolen resursseja, mutta kaupunkikäyttäjät eivät pääsisi käyttämään terveyspuolen resursseja. Tähän syynä ovat tietoturvallisuuteen liittyvät seikat, kuten potilastietojen ja arkaluontoisten materiaalien sijaitseminen terveysverkon puolella. Lähtötilanteeseen tulisi lisäksi luottosuhde uuden ja vanhan terveysk.local-toimialueen välille käyttäjien siirron ajaksi, koska käyttäjäsiirron aikana käyttäjätiedot pitää varmistaa vanhalta palvelimelta oikeellisuuden takaamiseksi. Myös käyttäjäprofiilin siirtoon tarvittiin kaksisuuntainen luottosuhde.

Yritys.ad - uusi_tk.ad

Ensimmäinen luottosuhde muodostuu yritys.ad:n ja uusi_tk.ad:n välille. Tarkoitus on, että resursseja pystytään jakamaan toimialueiden välillä. Myös osa terveyspuolen käyttäjistä tarvitsee kaupunkiverkon puolella sijaitsevia ohjelmia ja verkkoresursseja, kuten verkkolevyillä sijaitsevia kansioita. Samanlaista luottosuhdetta kuin aikaisemmin oli ollut ei pystytty muodostamaan, koska molemmat toimialueet ovat juuritoimialueita (tree-root domain). Tämä tarkoittaa sitä, että toimialueiden välille muodostuu automaattisesti juuritoimialueiden luottosuhde (tree-root trust). Luottosuhde on automaattisesti transitiivinen ja kaksisuuntainen. Molempien toimialueiden käyttäjät voivat kirjautua toiselle toimialueelle ja käyttää tämän resursseja, ellei toimintaa rajoiteta muilla määrityksillä, kuten kaupungilla on palomuurisäännöillä.

Uusi_tk.ad - terveysk.local

Toinen luottosuhde rakennettiin terveysk.local-toimialueen ja uusi_tk.ad-toimialueen välille, syynä tähän oli käyttäjien siirtoon liittyvät toimenpiteet. Käyttäjien siirron aikana yksittäisen käyttäjän tunnistetiedot varmistetaan ensin vanhalta terveyspalvelimelta ja vasta tämän jälkeen siirto voidaan hyväksyä. Luottosuhde rakennettiin kaksisuuntaiseksi, jossa molemmat palvelimet luottavat toisiinsa. Luottosuhdetta ei saatu aluksi toimimaan halutulla tavalla, vaikka käyttäjävaihdoksen aikana se toimikin riittävästi. Ongelma huomattiin, kun määriteltiin käyttäjäkohtaisia oikeusasetuksia palvelimien välillä. Syynä ongelmaan oli lm_host -asetusten puutteellinen määrittely vanhalla terveyspalvelimella. Asetusten korjaamisen jälkeen luottosuhde toimi oikein ja varmennus (validate) osoitti kaiken olevan kunnossa.

Replikointi

Tk_server1-palvelimella replikointi noudattaa edellä kuvatun mukaista mallia, jossa replikointia tapahtuu uusi_tk.ad toimialueen ohjauspalvelinten välillä, sekä myös yritys.ad- ja uusi_tk.ad-toimialueiden välillä. Seuraavassa on kuvattu tk_server1:n tulevat ja lähtevät replikointireitit. Tulevia server1, server2 ja tk_server2 sekä lähtevinä server1 ja tk_server2. Replikointi ei siis pysähdy, vaikka jokin palvelimista olisi väliaikaisesti pois käytöstä ja myös toimielueiden välinen replikointi jatkuu häiriöistä huolimatta.

5.6 Tuotantoverkkoon siirtyminen

Tk_server1-palvelimen sijainti oli aluksi erikseen rakennettu testiverkko, joka sijaitsi kaupungin verkossa. Rajalaitteena testiverkossa oli Watchguardin Soho 5-palomuurilaite, jonka tehtävänä oli simuloida varsinaista palomuuria ja luoda mahdollisimman oikea kuva verkon määrityksistä. Todellisuudessa se ei ajanut täysin tehtäväänsä ja tämän vuoksi kaikkia haluttuja toimenpiteitä ei pystytty määrittelemään testiverkossa. Yhtenä ongelmana oli reititys, jota ei pystytty hoitamaan halutulla tavalla. Ongelma johtui siitä, että verkon rajalaitteena toiminut Sohon palomuurilaite ei osannut mainostaa testiverkkoa muille verkon laitteille. Reititys hoidettiinkin muille palvelimille tehdyillä reitityskomennoilla, eli kerrottiin tk_server1:n sijainti. Reititys tehtiin käyttäen apuna route add -komentoa. Asetukset poistettiin siirron jälkeen, koska Watchguard hoiti liikenteen reitittämisen ja verkon mainostamisen.

Varsinainen fyysinen siirtyminen tehtiin kaapeloimalla palvelin eri laitteeseen, joka tässä tapauksessa oli kaupungin verkon Watchguard-palomuuri-rajalaite. Myös testityöasemina toimineet kannettavat tietokoneet kaapeloitiin eri sijaintiin. DHCP-asetukset pysäytettiin tk_server1:ltä ja lisättiin vanhan terveyspalvelimen DHCP-asetuksiin uusi määritys (scope), joka hoitaisi väliaikaisesti uusi_tk.ad:n osoitteiden jakamisen. Siirron jälkeen tehtiin kattava testaus verkon palveluiden toimimiseksi, mm. nimipalvelut ja luottosuhteet sekä replikoinnin toimivuus varmistettiin.

5.7 Ryhmäkäytännöt

Koneiden ja käyttäjien hallintaan päätettiin käyttää aktiivihakemiston ryhmäkäytännöt-työkalua (group policy). Näin käyttäjiä pystytään hallitsemaan kokonaisuuksina keskitetysti, eikä jokaiseen koneeseen tarvitse erikseen määritellä asetuksia. Ryhmäkäytännöt laitettiin osoittamaan toimialueeseen kuuluville käyttäjille (default domain policy). Tarkempia määrityksiä pystyy asettamaan organisaatioyksikkötasolla, mutta tähän ei ainakaan vielä nähty tarvetta ryhtyä.

Perusasetukset ovat kaikille samat (default domain policy), käyttäjille määritettiin salasanoihin liittyvät asetukset ja tilien lukituskäytännöt. Määrityksiä tehtiin myös oletus-ohjauspalvelin käytäntöihin (default domain controllers policy), jossa tärkeimpinä olivat paikalliset käytännöt ja käyttäjien oikeusasetukset.

Kehitteillä oli myös ORIAPP03-palvelimen vaihdokseen liittyvä ryhmäkäytäntö joka saatiin valmiiksi, mutta käytännön testaaminen siirtyi suunnitelmien muututtua. Perusajatuksena oli työasemien rekisteriasetuksien muuttaminen siten, että ORIAPP03-palvelimen vaihdoksen myötä muuttuva palvelinosoite vaihdetaan vastaamaan uuden palvelimen osoitetta. Näin käyttäjien ei tarvitse tehdä mitään toimenpiteitä työasemille, vaikka palvelimen osoite vaihtuu.

Logonscript eli kirjautumiskomentojono käynnistyy, kun käyttäjä kirjautuu järjestelmään. Tarkoituksena on suorittaa tietyt peruskomentojonot aina kun käyttäjä kirjautuu toimialueelle. Perusmäärityksiä ovat esimerkiksi osasto- ja ryhmäkohtaiset verkkoasemat sekä tulostinasetukset. Komentojono on sama kaikille käyttäjille.

6 Työasemien siirto

6.1 Suunnittelu

Palvelimen siirtoon valmistautumisessa yhtenä olennaisena osana oli päättää millä tavoin työasemat siirretään uuden palvelimen alaisuuteen. Vaihdoksessa huomioon otettavia asioita olivat toimialueen vaihtoon liittyvät toimenpiteet ja työasemien paikalliset tiedostot sekä sähköpostitilien siirtäminen, koska osalla käyttäjäjistä on ollut Outlook Express -sähköpostiohjelma. Tarkoituksena oli siis siirtää paikallisten työasemien käyttäjän omat tiedostot uuden käyttäjätunnuksen alaisuuteen. Ideana ei ollut siirtää käyttäjiä vanhasta toimialueesta uuteen, koska kaikille käyttäjille muutamaa poikkeusta lukuun ottamatta luotiin täysin uusi tunnus. Ohjelmien toimivuus uudessa toimialueessa ja IP-osoiteavaruuden muuttuminen olivat huomioitavia asioita. Työasemien vaihdoksen piti tapahtua työajan ulkopuolella, eli käytännössä viikonlopun aikana. Tarvittiin siis työkalu, jolla yhteen työasemaan ei kuluisi liikaa aikaa.

Suunnitteluvaiheessa tiedossa olleista neljästä käyttötarkoitukseen sopivasta työkalusta ei ollut vielä paljon tietoa. Ainoastaan yhtä oli käytetty aikaisemmin kaupungin verkkoympäristön palvelimen vaihdoksen yhteydessä. Työkalu on nimeltään Acticve Directory Migration Tool, joka on toiminnaltaan varma, mutta hieman hidas työkalu. Ja koska ajallisesti vaihdos piti suorittaa mahdollisimman nopeasti, myös muita vaihtoehtoja piti tarkastella. Kaikista työkaluista ei löytynyt varmaa tietoa kirjoista eikä Internetistä, joten ainoa vaihtoehto oli suorittaa testejä.

Moveuser.exe

Moveuser.exe niminen työkalu oli alustavan tutkimisen jälkeen sopivan tuntuinen kyseiseen tehtävään. Tietoa työkalusta löytyi lähinnä Internetin keskustelupalstoilta, joten tiedon luotettavuus piti testata. Moveuser.exe suoritetaan Komennolla MOVEUSER [DOMAIN/]*user1* [DOMAIN/]*user2* [/c:*computer*] [/k] [/y]

User1 tarkoittaa vanhaa käyttäjäprofiilia. User2 tarkoittaa käyttäjäprofiilia, joka perii user1:n profiilin. \c:computer -tarkoittaa tietokonetta, jolla vaihto suoritetaan. Tietokone voi olla myös etätyöasema, jolloin syntaksi olisi esimerkiksi /c:\\name0123. /k säilyttää user1:n profiilin ja toimii vain paikallisessa profiilissa. /y kopioi user2:n profiilin user1:n päälle.

6.2 Testaus

Testityöasemina käytettiin kahta kannettavaa tietokonetta. Testauksen tarkoituksena oli selvittää työkalun siirtoon käyttämä aika ja sen käyttämät metodit. Lisäksi testauksella haluttiin varmistaa, ettei käyttäjiltä katoaisi tietoja siirron aikana. Kannettaville luotiin oikean tilanteen mukainen profiili, johon asennettiin ohjelmat ja testattiin niiden toimivuus, lisättiin kuvia ja isoja tiedostoja, määriteltiin Outlook Express -sähköposti, luotiin sivuhistoriat, tehtiin Microsoftin ohjelmistoihin käyttäjäkohtaiset tiedot ja asetettiin työpöytäasetukset kuntoon. Testauksen jälkeen huomattu puute oli työpöydän taustakuvan katoaminen. Rekisterimuutoksella saatiin profiilin vaihto valmiiksi ja sähköpostitilin tuominen onnistui, kunhan tilitiedot otettiin talteen etukäteen. Itse profiilin muutokseen käytetty aika oli lyhyt.

Käyttäjätunnukset

Vanhassa terveyspalvelimessa käyttäjähallinta oli vanhanaikaista ja tunnusten sijoituksen lisäksi myös nimeämiskäytännössä oli puutteita. Käyttäjät kirjautuivat työasemille kolmikirjaimisilla tunnuksilla, joiden rakenne ei ollut yhtenäinen. Toisissa oli etunimen ensimmäinen ja sukunimen kaksi ensimmäistä kirjainta, joissakin oli kaksi kirjainta etunimestä ja yksi sukunimestä. Samalla, kun käyttäjälistat uusitaan ja turhat tunnukset poistetaan, myös tunnusten rakenne muutetaan uudenlaiseksi. Etunimestä otetaan ensimmäinen kirjain ja 7 ensimmäistä kirjainta sukunimestä, jos lyhyempi sukunimi kuin 7 kirjainta niin kyseinen määrä kirjaimia, kun muodostetaan käyttäjien kirjautumistunnukset.

Tunnusten luonti aloitettiin tarkistamalla kaikkien terveyskeskuksen työntekijöiden tunnusten ajantasaisuus. Kaikkia käyttäjätunnuksia ei ollut poistettu kun käyttäjä oli lopettanut työsuhteen. Lisäksi tarkoituksena oli, että käyttäjät voisivat käyttää samoja tunnuksia useammassa palvelussa, ettei aina kirjautuessa olisi eri tunnusta. Käyttäjien tiedot kirjattiin Excel-taulukkoon järjestyksessä niin, että ryhmittely olisi helpompaa. Käyttäjäkohtaiset tiedot laitettiin aina samalle riville. Sukunimi/etunimi/etunimi.sukunimi /salasana /kirjautumistunnus/ryhmä1/ryhmä2/ryhmä3/ryhmä4/EOL/organisaatioyksikkö. Kaikkien käyttäjien tiedot laitettiin samaan taulukkoon, josta se muutettiin tekstitiedostoksi .csv päätteellä. Itse käyttäjien luominen tapahtui skriptillä, johon muuttuvat tiedot otettiin .csv tiedostosta.

6.3 Koneiden siirto uusi_tk.ad-toimialueeseen

Työasemia, joille tomialueen vaihto toteutettiin, oli noin 80. Vielä ennen toteutuksen alkua prosessia nopeutettiin tekemällä skripti vaihdoksesta. Käsin tehtävän työn osuutta vähennettiin vielä tekemällä työjono (tkmu.bat), joka automatisoisi työtä. Toimenpiteen ansiosta suurin osa vaihdokseen liittyvästä työstä

tapahtui työjonon avulla. Vaihdokseen liittyvistä toimenpiteistä luotiin käyttöohje, joita oli yksi työasemaa kohden. Etukäteen käyttäjiä oli ohjeistettu tuomaan Outlook Express -sähköpostiohjelmasta, jos sellaista käytettiin, tilitiedot työpöydälle.

Tkmu.bat

Työjonolla pyrittiin automatisoimaan käsin tehtävää työtä. moveuser-komentojonosta tarvitsi syöttää vain käyttäjän vanha ja uusi tunnus. Toiminto nimeää profiilikansion uuden tunnuksen mukaan. Jos käyttäjällä on Outlook Express käytössä, kopioidaan osoitekirja oletuskansiostaan uuden profiilin vastaavaan kansioon ja nimetään se uudelleen uuden tunnuksen mukaan. Työjono kutsuu rekisterimuutokselle aputiedoston, joka näyttää muutettavien polkujen sijainnin. Seuraavaksi muutetaan tietokoneen nimi ja kuvaus, jonka jälkeen käyttäjää pyydetään syöttämään oikeat tiedot ja skripti hoitaa loput. Lopuksi muutetaan paikalliset oikeudet uuden toimialueen mukaisiksi.

Työasemille kirjauduttiin vanhan toimialueen administrator-tunnuksella ja tarkistettiin onko käyttäjä tuonut tilitietoja työpöydälle. IP-osoite piti olla uusi_tk.ad-toimialueeseen kuuluva osoite. Työasema pudotettiin pois vanhasta toimialueesta ja lisättiin uusi_tk.ad-toimialueeseen. Uudelle toimialueelle kirjauduttiin pääkäyttäjän tunnuksella ja komentokehotteesta käynnistettiin työjono. Käyttäjän tunnustiedot syötettiin käsin. Uudelle tunnukselle saatiin oikeudet profiilikansioon ja vaihdettiin profiilikansion nimi uudelle tunnukselle. Työasemalle tehtiin rekisterimuutos, jotta profiilikansion nimi ja käyttäjätunnus ovat samat. Käyttäjän SID:ä vastaavan avaimen sisältö korvataan uudella, esimerkiksi timotest-tunnus korvataan ttesti-tunnuksella. Tietokoneen tiedot sijoitettiin aktiivihakemistoon skriptin avulla. Tiedoista syötettiin organisaatioyksikkö, sukunimi, etunimi sekä käyttäjätunnus ja skripti sijoittaa tiedot suoraan aktiivihakemistoon. Työasemalta poistettiin vanhan toimialueen pääkäyttäjä ja tarkastettiin uusi_tk.ad-käyttäjätunnusten olemassaolo. Lopuksi kirjauduttiin käyttäjän tunnuksilla työasemalle ja tuotiin sähköpostitili Outlook Express –ohjelmaan ja myös mediatriohjelman toimivuus ja versiopäivitys tarkistettiin. Jos koneella oli useampi siirrettävä profiili, aloitettiin skripti alusta ja tehtiin rekisterimuutokset. Käyttäjien pöydälle jätettiin kirjekuori, jossa olivat uudet tunnukset ja käyttöohjeet.

7 Pohdintaa

Idean opinnäytetyön aiheeksi sain työharjoittelun aikana, jonka suoritin Oriveden kaupungilla toukokuun ja marraskuun välisenä aikana vuonna 2007. Ehdotuksen aiheesta teki Oriveden kaupungin tietohallintopäällikkö Mikko Naaralainen, joka toimi lähimpänä esimiehenä harjoittelun aikana. Aihe kuulosti mielenkiintoiselta ja antoi mahdollisuuden hyödyntää koulussa opittuja asioita sekä oppia uutta.

Palvelimen vaihto oli hyvin mielenkiintoinen ja haastava kokonaisuus, koska siihen kuului paljon muutakin kuin vain palvelimen pystytys. Huomioon otettavia asioita oli paljon ja piti osata hahmottaa kokonaisuutta jatkuvasti työn edetessä. Etenkin keskisuuren verkkoympäristön, monen palvelimen ja monen sovelluksen kanssa toimiminen antoi oman lisähaasteen työlle.

Vaikka palvelimen pystytys oli osa suurempaa kokonaisuutta, tuntui se itsessään suurelta työltä. Huomioon otettavia asioita oli todella paljon. Alussa tehty suunnitelma ei kantanut aivan loppuun asti. Eteen tuli asioita, joita ei osannut alussa ottaa huomioon ja suunnitelmiin tuli muutoksia. Etenkin työn alkuvaiheessa kohdattujen ongelmien vuoksi joudutaan suunnittelemaan osia työstä uusiksi ja miettimään muutoksien vaikutuksia koko työhön.

7.1 Toteutuksesta

Palvelimen rakennusalustana toiminut testiverkko aiheutti paljon päänvaivaa. Syynä tähän olivat reititysongelmat, joiden selvittämiseksi jouduttiin käyttämään paljon aikaa. Juuri näiden ongelmien vuoksi alkuperäistä aikataulua jouduttiin siirtämään useaan otteeseen. Eteen tuli monia asioita, joita ei aluksi osattu ottaa huomioon.

Juuritoimialueiden välinen tree-root luottosuhde aiheutti myös päänvaivaa, koska se ei kuulunut suunnitelmiin. Koska luottosuhde kaupunki- ja terveysverkon välillä on oleellinen asia toimintaympäristössä, asian ratkaisuun jouduttiin käyttämään paljon aikaa. Myös ongelmat uuden ja vanhan terveysverkon luottosuhteessa aiheuttivat ongelmia, etenkin valmistautumisessa työasemien siirtoon uudelle toimialueelle. Vaikka työasemien siirto saatiin suoritettua, luottosuhde ei toiminut aivan kuten sen oli tarkoitus, joten sen korjaamiseksi jouduttiin vielä tekemään töitä. Luottosuhteen täydelle toiminnalle ei alun perin pitänyt olla tarvetta, mutta terveyskeskuksen röntgenlaitteisto aiheutti odottamattoman tilanteen, jossa luottosuhteen piti toimia täydellisesti.

Työasemien siirto vanhasta toimialueesta uuteen sujui ehkä paremmin, kuin alunperin suunniteltiin. Moveuser.exe oli työkaluna toimiva ja erittäin nopea verrattuna vaihtoehtona olleeseen ADMT:hen (Active Directory Migration Tool), kuten haluttiinkin. Työasemien siirto saatiin tehtyä suunnitelmien mukaan, suurin osa viikonlopun aikana ja muutamat kohteet maanantaina.

7.2 Tavoitteiden saavutus

Tavoitteena oli pystyttää uusi palvelin ja lisätä se uuteen verkkoympäristöön niin, että käyttäjille koituu mahdollisimman vähän muutoksia, vaikka koko aktiivihakemiston hierarkia ja tunnuspolitiikka muuttuu täysin. Tavoite saavutettiin onnistuneesti, pieniä viivästyksiä lukuunottamatta.

Opinnäytetyön tavoite saavutettiin ja uudesta palvelimesta saatiin tavoitteiden kaltainen. Se täyttää nykyajan vaatimukset käyttöjärjestelmän osalta ja aktiivihakemiston hallittavuus parani huomattavasti vanhasta palvelimesta. Vikasietoisuus saatiin korkeammalle tasolle kuin aikaisemmassa järjestelmässä ja yhden palvelimen kaatuminen ei pysäytä koko terveyskeskuksen toimintaa. Jos jokin palvelimien palveluista kaatuu, on toisella palvelimella varapalvelu käytössä.

Kommunikointi palvelimien ja verkkojen välillä toimii niin kuin sen pitääkin. Yhteydet ovat kunnossa molempiin suuntiin yritys.ad:n ja uusi_tk.ad:n välillä. Luottosuhteet toimivat siten, että tarvittaessa päästään käyttämään toisen toimialueen resursseja. Palomuurisäännöillä estettiin kaupunkikäyttäjien pääsy uusi_tk.ad:n resursseihin kuten oli tarkoitus. Tavoitetila saavutettiin, kun uusi palvelin oli toiminnassa uudessa verkossa ja työasemat toimivat uuden toimialueen alaisena.. Edellytyksenä oli myös ohjelmien ja verkkoresurssien moitteeton toimiminen, joka saavutettiin.

Henkilökohtaisena tavoitteenani oli antaa täysi panos työlle ja sen onnistumiselle. Mielestäni onnistuin tavoitteessa hyvin. Lisäksi opin monia uusia asioita aiheen ympäriltä sekä sain itsevarmuutta toimia palvelinympäristöissä. Suurimpana puutteena oli kokemattomuus vastaavan kaltaisista töistä, joka näkyi ainakin kokonaisuuksien hallinnan puutteena. Myös työrutiini ja työtavat eivät olleet harjaantuneet tasolle, jota olisi alusta asti vaadittu.

8 Lähteet

Painetut lähteet:

Kivimäki, Jyrki 2005 [1]. Windows Server 2003 - Active Directory tehokas hallinta. Jyväskylä: Gummeruksen Kirjapaino Oy

Kivimäki, Jyrki 2005 [2]. Windows Server 2003 - tehokas hallinta. Jyväskylä: Gummeruksen Kirjapaino Oy

Sähköiset lähteet:

Microsoft [online] [viitattu 15.5.2008]
http://www.microsoft.com/finland/Windowsserver2003/evaluation/overview/default.mspx