LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

HAKEMISTOPALVELU

Suunnittelu ja käyttöönotto pienyrityksessä

LAHDEN
AMMATTIKORKEAKOULU
Tietotekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2012
Antti Tuomenoksa

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

TUOMENOKSA ANTTI:

Hakemistopalvelu
Suunnittelu ja käyttöönotto pienyrityksessä

Tietoliikennetekniikan opinnäytetyö, 52 sivua

Kevät 2012

TIIVISTELMÄ

Tämän opinnäytetyön tarkoituksena oli suunnitella ja toteuttaa Active Directory -verkkojärjestelmä. Työn toimeksiantajana on Mecatroplan Oy, joka sijaitsee Lahdessa. Yrityksessä työskentelee viisi henkeä, jotka tuottavat erilaisia mekaniikkasuunnitteluun pohjautuvia palveluita.

Opinnäytetyön tavoitteena oli luoda Mecatroplan Oy:lle heidän tarpeisiinsa soveltuva Active Directory -verkkopalvelu. Aikaisemmin yrityksen käytössä oli työryhmäkäytäntöön pohjautuva verkkoinfrastruktuuri, joka haluttiin muuttaa toimialuekäytännöksi. Toimialuekäytäntö mahdollistaa keskitetyn käyttäjien- ja tietokoneiden sekä resurssien hallinnan. Toimialuekäytäntö parantaa myös tietoturvaa Active Directoryn tarjoamien tunnistusmenetelmien sekä käyttäjäkohtaisten oikeuksien määrittämisen avulla.

Active Directoryn perusominaisuutena on tarjota tehokas hallinta verkon resursseista. Active Directoryn looginen rakenne koostuu toimialuemetsistä, toimialuepuista ja organisaatioyksiköistä. Active Directoryn fyysinen rakenne koostuu toimipaikoista ja aliverkoista. Toimialueita voidaan hallita erilaisilla työkaluilla.

Active Directoryn suunnittelu koostuu eri tekijöistä, johon sisältyy DNS-nimiavaruuden määrittäminen, organisaatioyksiköiden sekä käyttäjien- ja tietokonetilien suunnittelu. Toimialueen käyttäjien muodostaminen ja ryhmäsääntöjen luonti tapahtuu niille tarkoitetuilla hallintatyökaluilla. Työasemien liittäminen toimialueelle tapahtuu työasemien järjestelmäasetuksia muuttamalla. Toimialueelle liittyminen vaatii järjestelmänvalvojan käyttäjätunnuksen ja salasanan.

Active Directoryn etuna ovat käyttäjien, tietokoneiden, ryhmien ja verkon resurssien hallitseminen keskitetysti yhdestä paikasta. Käyttäjien hallinnassa voidaan hyödyntää ryhmäsääntöjä, jotka voidaan asettaa toimialuelaajuisesti tai organisaatioyksikkötasolle. Verkon resurssien keskittäminen yhteen paikkaan mahdollistaa resurssien helpon saatavuuden kaikille käyttäjille.

Avainsanat: Active Directory, toimialue, organisaatioyksikkö, ryhmäkäytäntö

Lahti University of Applied Sciences
Degree Programme in Information Technology

TUOMENOKSA, ANTTI:

Active Directory
Design and Introduction in a Small Business

Bachelor's Thesis in Telecommunications Technology, 52 pages

Spring 2012

ABSTRACT

The purpose of this thesis was to design and implement an Active Directory network service. The thesis was commissioned by Mecatroplan Oy in Lahti. The company employs five people who produce a variety of services based on mechanical design.

The aim of the thesis was to create an Active Directory network service for Mecatroplan Oy which would be suitable for their needs. Previously, the company had a workgroup-based network infrastructure, which they wanted to change to a domain-based network infrastructure. A domain-based infrastructure allows centralized management of users, computers and network resources. A domain-based network system also improves security because Active Directory provides the user with detection methods and user-specific determination of rights.

A standard feature of Active Directory is to provide efficient management of network resources. The logical structure of Active Directory consists of forests, domain trees and organizational units. The physical structure of Active Directory consists of sites and subnets. Domains can be managed with different tools.

The Active Directory design consists of a number of factors, which include DNS name space definition and the design of organizational units, user accounts and computer accounts. Domain users and group policies can be created with management tools which are dedicated to them. Adding workstations to the domain requires a change of system settings of workstations. Joining to the domain requires administrator username and password.

The advantage of Active Directory is that the users, computers, groups and resourses of the network can be managed from one centralized location. Group policies can be used in user management. Group Policies can be placed in domain or organizational unit levels. Centralising network resources in one place allow easy access to resources for all users.

Key words: Active Directory, domain, organization unit, group policy

LYHENNELUETTELO

ACTIVE DIECTORY

Microsoftin toteutus toimialueen aktiivihakemistopalvelusta. Aktiivihakemistopalvelu sisältää tietoja käyttäjistä, tietokoneista ja verkon resursseista.

AD DS

Active Directory Domain Services on toimialueen ohjauspalvelin

DEFAULT DOMAIN POLICY

Koko toimialueella vaikuttava ryhmäsääntö

DHCP

Dynamic Host Configuration Protocol. Palvelu, jonka avulla verkkoon yhdistyneet laitteet saavat tarvittavat verkkoasetukset.

DNS

Domain Name System, jonka avulla verkkotunnukset muutetaan IP-osoitteiksi

DOMAIN

Toimialue, joka koostuu joukosta tietokoneita. Näitä tietokoneita voidaan hallita keskitetysti yhdeltä tai useammalta Windows-palvelimelta.

FOREST

Toimialueiden muodostama kokonaisuus

FOREST ROOT DOMAIN

Metsän juuritoimialue

FQDN

Fully Qualified Domain Name, jonka avulla voidaan määrittää tarkka sijainti toimialueen nimialueen puurakenteessa.

GLOBAL CATALOG

Yleinen luettelo, jossa säilytetään tieto kaikista objekteista metsän laajuistesti

GROUP POLICY

Ryhmäsääntö, jonka avulla voidaan hallita käyttäjien ja tietokoneiden työympäristöjä

IP

Internet Protocol, joka huolehtii IP-tietoliikennepakettien toimittamisesta perille pakettikytkentäisessä Internet-verkossa

KERBEROS

Tunnistusmenetelmä, jonka avulla käyttäjät voivat tunnistautua verkossa

OU

Organizational Unit. Organisaatioyksikkö, joiden avulla toimialueen objekteja voidaan hallita tehokkaammin

PEER-TO-PEER

Vertaisverkko, jonka muodostavat samassa työryhmässä olevat työasemat

ROOT DOMAIN

Toimialueen juuritoimialue

SCOPE

Osoitealue, jota DHCP käyttää hyväkseen IP-osoitteiden jakamis essa

TCP/IP

Transmission Control Protocol / Internet Protocol on Internet-liikennöinnissä käytettävä tietoverkkoprotokollan yhdistelmä

UDP

User Datagram Protocol, jota käytetään datan kuljettamiseen Internet-verkossa

WORKGROUP

Työryhmäkäytäntö, joka on oletuksena käytössä kaikissa Windows työasemissa

SISÄLLYS

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on kehittää lahtelaisen Mecatroplan Oy yrityksen verkkoinfrastruktuuri tasolle, joka vastaa yrityksen nykyisiä tarpeita. Yrityksen lähiverkon työasemat hyödynsivät aikaisemmin Windows-työryhmäkäytäntöä (Workgroup). Työryhmäkäytäntö ei kuitenkaan vastannut yrityksen tietoturvan, hakemistopalveluiden ja hallintamahdollisuuksien vaatimuksia, jonka takia työryhmäkäytäntö päivitettiin toimialueympäristöksi (Domain). Tässä toteutuksessa käytettiin hyväksi Windows Server 2008 R2 -palvelinympäristöä sekä Active Directory -arkkitehtuuria.

Mecatroplan Oy on lahtelainen mekaniikkasuunnitteluun keskittynyt insinööritoimisto, jonka palveluksessa työskentelee viisi henkilöä. Yritys tarjoaa asiakkailleen 3D-suunnittelupalveluita koneista, laitteista ja työkaluista. 3D-suunnitteluun yritys käyttää nykyaikaisia 3D-työkaluja, kuten Solidworks 2008:a ja Customworks 2007:aa.

Työn teoriaosuudessa on käsitelty Active Directoryn perusominaisuuksia, sitä millaisia työkaluja Active Directory tarjoaa järjestelmän ylläpitäjää varten sekä mitä seikkoja tulisi ottaa huomioon Active Directorya suunnitellessa. Active Directoryn merkittävin hyöty järjestelmän ylläpitäjälle on ylläpidon keskittyminen yhteen paikkaan. Käytännössä tämä tarkoittaa käyttäjä- ja tietokonetilien tehokasta hallinnointia organisaatioyksiköittäin. Teoriaosuus käsittää myös TCP/IP -tekniikkaan tutustumista.

Työn käytännön osuudessa on käsitelty palvelinympäristön asennusta, toimialueen- ja käyttäjätilien muodostamista sekä ryhmäkäytäntöjen luontia ja tietokoneiden liittämistä toimialueeseen. Työn käytännön osuus pyrittiin tekemään mahdollisimman nopeasti, jotta pitkiltä työkatkoksilta voitiin välttyä. Yhteenvedossa on lopuksi pohdittu käyttöönoton onnistumista ja tulevaisuuden laajennusmahdollisuuksia.

2 MECATROPLAN OY

Mecatroplan Oy on mekaniikkasuunnitteluun keskittynyt insinööritoimisto, joka tarjoaa osaavia palveluitaan pienille sekä isoille yrityksille. Yrityksessä työskentelee viisi ammattitaitoista työntekijää, jotka luovat tuoteideoista valmiita laitteiden valmistus- ja kokoonpanokuvia, 3D-malleja sekä mainoslehtisiä ja internetsivuja. (Mecatroplan Oy 2012.)

Mecatroplan Oy:n tarjoamat 3D-suunnittelupalvelut tuotetaan nykyaikaisilla 3D-työkaluilla. Yrityksellä on tuotantoa varten käytössään SolidWorks 2008- ja CustomWorks 2007-suunnitteluympäristöt, CadWorks-komponenttikirjasto sekä PDM Works-revisiointi ja tiedostonhallintaohjelmisto. 3D-laitteistolla suunnittelu mahdollistaa tuotteen helpon kustomoinnin, konfiguraatioiden käytön sekä helposti hallittavan revisioinnin. Mecatroplan Oy on keskittynyt suunnittelussaan koneiden, laitteiden ja työkalujen mekaniikkasuunnitteluun. (Mecatroplan Oy 2012.)

Mecatroplan Oy ei vain suunnittele tuotteita vaan myös tarjoaa yrityksille apua arkipäivän ongelmiin ja kehitykseen tuotantokehityksen, projektienhallinnan ja tuotantokehityksen saralla, kuten logistiikan järjestelyissä tai laitteiden osittaisessa modernisoinnissa. Nämä palvelut auttavat muita yrityksiä saavuttamaan näyttäviä säästöjä sekä parempia ja turvallisimpia työympäristöjä. (Mecatroplan Oy 2012.)

Mecatroplan Oy:n henkilöstön osaaminen kohdistuu myös mainonnan ja imagon osa-alueelle. Visualisointipalveluiden avulla yritys tuottaa asiakkailleen näyttäviä 3D-mallinnuksia ja -animaatioita, Internetsivustoja, tuote- ja yritysesitteitä sekä tuote- ja yrityslogoja. Mecatroplan Oy käyttää useita eri tekniikoita luodessaan visualisointipalveluitaan, jolloin niiden käyttö on hyvin monipuolista eri markkinointikanavia käytettäessä. Kehittyvä teknologia tuo Mecatroplan Oy:lle uusia keinoja luoda asiakkaan yrityksestä ja sen tuotteista näyttävä kokonaisuus. (Mecatroplan Oy 2012.)

3 ACTIVE DIRECTORY

Active Directory, eli aktiivihakemisto on Microsoftin toteutus internet -standardien mukaisesta toimialueen hakemistopalvelusta (Directory Service), jonka avulla voidaan tehokkaasti hallita verkon resursseja. Active Directory toimii Windows Server 2008 R2 keskeisenä palveluna ja sisältää tietoja käyttäjistä, tietokoneista ja verkon resursseista. (Kivimäki 2009, 651.)

Ensimmäisen kerran Active Directory tuli käyttöön Windows 2000 Server -käyttöjärjestelmässä, jonka jälkeen Active Directorysta on julkaistu uudet versiot aina uuden palvelinkäyttöjärjestelmän myötä. Windows Server 2008 R2 -käyttöjärjestelmän myötä uusina Active Directoryn ominaisuuksina tulevat esimerkiksi vain-luku-tyyppiset ohjauspalvelimet (Read-Only Domain Controller), käyttäjäryhmä- tai -tilikohtaiset salasanakäytännöt (Password settings Object, PSO) ja Active Directoryn roskakori (Windows Server 2008 R2 -version Recycle Bin). (Kivimäki 2009, 651.)

Active Directory käyttää DNS-järjestelmää (Domain Name System) sekä toimii IP-protokollien (Internet Protocol) avulla. DNS on standardi Internetin palvelu, joka organisoi tietokonejoukot toimialueiksi. DNS:ää voidaan käyttää isäntäkoneiden nimien muuntamisissa numeerisiksi TCP/IP-osoitteiksi (Transmission Control Protocol/Internet Protocol). Active Directory -toimialuehierarkia voidaan määrittää DNS:n kautta Internetin laajuisesti tai toimialuehierarkia voi olla erillinen ja yksityinen. (Stanek 2003, 133.)

Active Directoryn avulla vähennetään ylläpidettävien hakemistojen määrää. Järjestelmävalvojan kannalta Active Directoryssa on kysymys hajautetun järjestelmän keskitetystä hallinnoinnista, joka tarkoittaa loogisesti yhdessä paikassa sijaitsevien objektien käsittelyä erilaisilla hallintatyökaluilla. Hallittavat objektit koostuvat käyttäjä- ja tietokonetileistä sekä verkon resursseista. Active Directoryn objektit tallennetaan omaan tietokantaansa. (Kivimäki 2005, 6; Kivimäki 2009, 65.)

Perinteisen määrityksen mukaan hakemistopalvelu eroaa hakemistosta (directory) siten, että sisältämällä hakemiston tiedot eli tietovaraston (tietokannan) se myös

tarjoaa palvelut (services), jolla tietovarastoon päästään käsiksi. (Kivimäki 2009, 651.)

Active Directory ei varsinaisesti näy loppukäyttäjälle. Loppukäyttäjä voi kuitenkin hyödyntää Active Directoryn tarjoamia resurssien etsimistä ja käyttöä helpottavia toimintoja, kuten verkkohakemistojen käyttö ja käyttäjien kirjautumisessa käytettäviä tunnistuspalveluita (LAN-Manager ja Kerberos). (Kivimäki 2005, 1.)

4 ACTIVE DIRECTORYN LOOGINEN RAKENNE

4.1 Yleistä AD:n loogisesta rakenteesta

Active Directory on hajautettu tietokanta, joka tallentaa ja hallitsee tietoja verkon resursseista sekä sovelluskohtaisia tietoja hakemistoon hyväksytyistä sovelluksista. Active Directory sallii järjestelmänvalvojien organisoida verkon kohteita, (kuten käyttäjiä, tietokoneita ja laitteita) hierarkkiseksi rakenteeksi, jota kutsutaan loogiseksi rakenteeksi. Loogisessa rakenteessa ylimmän tason looginen säiliö on metsä (forest). Metsä sisältää toimialueet, jotka taas sisältävät organisaatioyksiköt. (Microsoft TechNet 2012d.)

Active Directoryn looginen rakenne tarjoaa monia etuja verkkopalveluiden ja resurssien käyttöönotossa, hallinnassa ja turvaamisessa. Yhtenä etuna on verkon tietoturvan parantuminen. Verkon looginen rakenne voi siis tarjota turvatoimia kuten itsehallintaa yksittäisille ryhmille tai täydellistä eristystä tietyistä resursseista. Hyvin toteutettu looginen rakenne yksinkertaistaa myös verkon hallinnointia konfiguroinnin ja valvonnan näkökulmasta sekä helpottaa järjestelmänvalvojaa hallitsemaan käyttäjä- ja ryhmätilejä. Toimialueiden ja metsien looginen rakenne sekä niiden väliset luottosuhteet yksinkertaistavat resurssien jakamista organisaatioihin. Loogisen rakenteen etuihin kuuluu vielä kokonaiskustannuksien aleneminen, sillä loogisen rakenteen käyttö vähentää verkon hallinnan kustannuksia ja verkon resurssien kuormitusta. (Microsoft TechNet 2012d)

Active Directoryn loogiset rakenteet (Microsoft TechNet 2012d.):

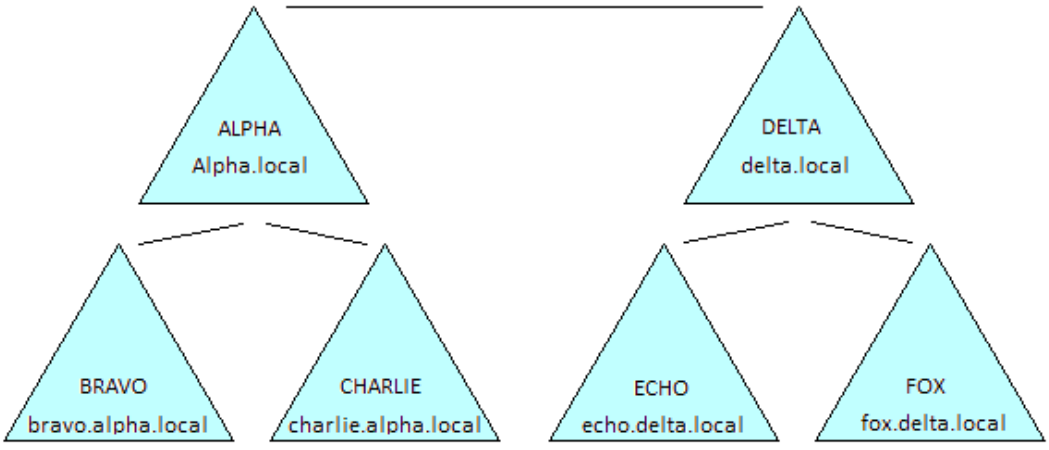
- Toimialuemetsät
- Toimialuepuut
- Toimialueet
- Organisaatioyksiköt.

4.2 Toimialuemetsä

Active Directory -toimialueet sijaitsevat jossain metsässä (forest). Toimialuemetsä on yhden tai useamman toimialueen muodostama ryhmä. Metsän ensimmäinen asennettu toimialue on metsän juuritoimialue (forest root domain). Tällä toimialueella on enemmän valtuuksia ja tärkeämpi merkitys, kuin muilla metsän toimialueilla. Toimialueella voi toimia vain yksi ohjauspalvelin. (Kivimäki 2005, 9; Microsoft TechNet 2012d.)

Kaikki samaan toimialuemetsään kuuluvat toimialueet omaavat yhteisiä ominaisuuksia. Toimialueet jakavat yhteisen loogisen rakenteen, joka tarjoaa monia etuja verkkopalveluiden ja resurssien osalta. Toimialueiden yhteisenä ominaisuutena on myös Kerberos-tunnistusmenetelmä, joka sallii käyttäjän kirjautumisen mihin tahansa metsän toimialueelle, millä tahansa toimialueen käyttäjätilillä. Käyttäjille voidaan myös määrittää käyttöoikeuksia muiden toimialueiden resursseihin. (Kivimäki 2005, 51.)

Muita toimialuemetsän yhteisiä ominaisuuksia ovat yleinen luettelo (Global Catalog), josta voidaan etsiä mitä tahansa metsän toimialueella sijaitsevaa objektia, sekä Enterprise Admins -ryhmä, joka on oletuksena mukana kaikkien toimialueiden paikallisessa Administrator-ryhmässä. Toimialuemetsien liittäminen toisiinsa voidaan tehdä luottosuhteiden avulla. (Kivimäki 2003, 11; Kivimäki 2005, 51,52.) Kuviossa 1 on esitetty toimialuemetsän ja toimialueiden välisiä suhteita.



KUVIO 1. Toimialuemetsän ja toimialueiden väliset suhteet

4.3 Toimialuepuut

Toimialuepuut koostuvat toimialueista, jotka ovat muodostuneet hierarkkisiksi rakenteiksi. Toimialuepuut jakavat yhtenäisen nimiavaruuden (DNS) toimialuepuussa sijaitseville toimialueille. Juuritoimialueet (root domain) voivat sisältää useita alitoimialueita (child domain). (Microsoft TechNet 2012c.)

Kuviossa 1 juuritoimialueena on alpha.local, jonka alitoimialueina toimivat bravo.alpha.local ja charlie.alpha.local. Delta.local muodostaa oman toimialuepuunsa, johon on liittyneenä echo.delta.local- ja fox.delta.local-juuritoimialueet. Kaikki toimialueet kuuluvat kuitenkin samaan toimialuepuuryhmään, jonka juuritoimialueena toimii alpha.local. (Microsoft TechNet 2012c.)

4.4 Toimialueet

Toimialueet ovat ryhmä tietokoneita, jotka jakavat yleisen hakemistotietokannan. Active Direcotryn nimiavaruus määrittää yrityksen ylimmän tason toimialuenimen. Active Directoryn toimialuenimien täytyy olla yksilöllisiä. Esimerkiksi kahta alpha.local-toimialuetta ei voida muodostaa, mutta alpha.local-toimialueen alle voidaan luoda lapsitoimialueita, kuten bravo.alpha.local ja charlie.alpha.local. Toimialueiden muodostamiskäytäntöä voidaan tarkastella kuviossa 1. (Kivimäki 2003, 13; Stanek 2003, 134–135.)

Toimialuetta luodessa yksityiseen verkkoon, tulee toimialuenimen määrityksessä huomioida mahdolliset ristiriitaisuudet samassa verkossa olevan toimialueen nimen kanssa. Luotaessa toimialuetta maailmanlaajuisesti, ei toimialuenimi saa olla ristiriidassa minkään Internetiin kuuluvan toimialuenimen kanssa. Näillä käytännöillä varmistetaan toimialueen nimen yksilöllisyys ja vältytään ongelmilta. (Stanek 2003, 134–135.)

Jokaisella toimialueella on omat suojauskäytännöt ja luottosuhteensa muiden toimialueiden kanssa. Juuritoimialueen ja sen alitoimialueiden välisen luottosuhteen ansiosta resurssit ovat koko toimialuepuun käytettävissä. Toimialueet voivat ulottua useampaan fyysiseen paikkaan, jolloin ne voivat sisältää useita palvelinjouk-

koja, jotka taas voivat sisältää useita aliverkkoja. Toimialueen hakemistotietokanta sisältää objekteja, jotka määrittävät käyttäjä-, ryhmä ja tietokonetilit sekä jaetut resurssit, kuten tulostimet ja kansiot. (Kivimäki 2003, 16; Microsoft TechNet 2012c.)

4.5 Organisaatioyksiköt

Organisaatioyksiköt (OU) ovat toimialueiden sisällä olevia aliryhmiä, joiden tulisi heijastaa yrityksen liiketoimintaa tai organisaation rakennetta. Organisaatioyksiköitä voidaan luoda, kun halutaan delegoida käyttäjäryhmiä, käyttäjiä ja resursseja koskevia järjestelmänhallinnallisia oikeuksia. Organisaatioyksiköt perivät toimialueen tai ylemmän tason organisaatioyksikön suojakäytännöt, ellei toisin määritellä. (Stanek 2003, 137; Kivimäki 2003, 17.)

Organisaatioyksiköiden käyttö ei kuitenkaan ole välttämätöntä. Käyttäjätilit voidaan lisätä toimialueen Users-kansioon ja tietokonetilit Computers-kansioon. Näihin kansioihin ei kuitenkaan voida liittää ryhmäkäytäntöjä (Group Policy), jolloin tilien ja käyttäjien hallinta heikentyy. (Kivimäki 2009, 368.)

Organisaation liiketoiminnalliseen tai toiminnalliseen rakenteeseen liittyvien objektien organisoiminen on helpompaa organisaatioyksiköiden avulla. Tämä ei kuitenkaan ole ainut syy käyttää organisaatioyksiköitä. Organisaatioyksiköiden avulla voidaan myös määrittää ryhmäkäytännöt toimialueen resurssijoukkoa varten, ilman ryhmäkäytäntöjen käyttöönottoa koko toimialueessa. Tämä tapa mahdollistaa ryhmäkäytäntöjen paremman asettamisen ja hallinnan organisaation eri tasoilla. Toinen merkittävä syy organisaatioyksiköiden käyttöön liittyy resurssien hallinnan parantuminen, sillä organisaatioyksiköt mahdollistavat hakemisto-objektien luonnin pienempiin näkymiin. Organisaatioyksiköiden avulla voidaan myös delegoida valtuuksia sekä ohjata helposti toimialueresurssien hallinnallista käyttöä. Organisaatioyksiköt lisäävät myös tietoturvaa. Käyttöoikeusluetteloilla mahdollistetaan resurssien rajoitettu näkyvyys, jolloin käyttäjät näkevät vain ne objektit, joihin heillä on oikeudet. (Stanek 2003, 138.)

5 ACTIVE DIRECTORYN FYYSINEN RAKENNE

5.1 Toimipaikka

Active Directoryn fyysinen rakenne koostuu toimipaikoista ja aliverkoista. Toimipaikka koostuu joukosta tietokoneita, jotka kuuluvat yhteen tai useampaan IP-aliverkkoon. Toimipaikat vaikuttavat Active Directoryn toimintaan monilla tavoilla. (Kivimäki 2003, 17.)

Kun käyttäjä kirjautuu toimialueelle, Active Directorya tukevat tietokoneet yrittävät ensisijaisesti löytää toimialueen ohjauspalvelimen siitä toimipaikasta, jossa käyttäjän työasemakin on. Tämän avulla mahdollistetaan kirjautumispyyntöjen käsittelyjen tehokkuus. Toinen toimintaan vaikuttava tekijä on Active Directorys-sa sijaitsevien objektien hakeminen. Hakujen käsittely tehostuu, kun haut ohjataan lähimmälle yleistä luetteloa ylläpitävälle ohjauspalvelimelle. Yhtenä vaikuttavana tekijänä voidaan pitää myös toimialueiden välillä tapahtuvaa hakemistojen replikointia. Replikointi voidaan tilanteen mukaan aikatauluttaa sekä toimialueiden välinen reitti konfiguroida. Toimipaikan sisäisessä replikoinnissa ei voida hyödyntää aikataulutusta ja reitin konfigurointia. (Kivimäki 2003, 17.)

5.2 Aliverkot

Aliverkon voidaan ajatella olevan ryhmä verkko-osoitteita. Toisin kuin toimipaikat, jotka voivat sisältää useita IP-osoitealueita, aliverkoilla on tietty IP-osoitealue ja aliverkon peite. Aliverkotuksella voidaan vähentää verkossa kulkevaa yleislähetysliikennettä, helpottaa verkon hallintaa ja parantaa verkon suorituskykyä. (Stanek 2003, 138–139.)

Aliverkkojen nimet muodostetaan verkko-osoitteesta ja bittimaskista, kuten esimerkiksi 192.168.19.0/24. Tässä verkko-osoite 192.168.19.9 ja aliverkon peite 255.255.255.0 muodostavat yhdessä aliverkon nimen 192.168.19.0/24. Jokaisella verkkoon liittyneellä tietokoneella on oltava määritettynä verkko-osoite ja aliverkon peite. (Stanek 2003, 138–139.)

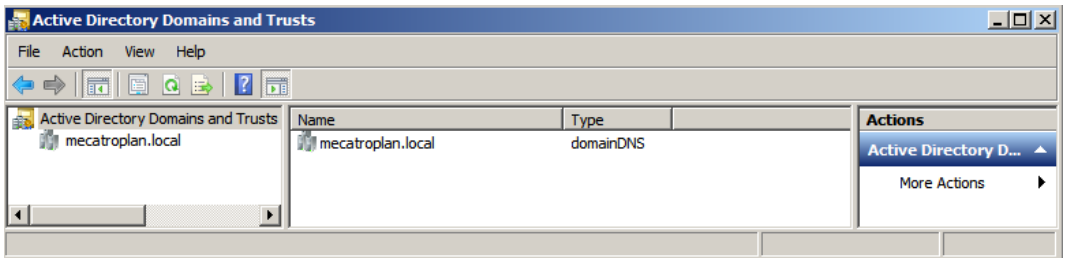
6 ACTIVE DIRECTORYN TOIMIALUEEN HALLINTA

Ensimmäisen ohjauspalvelimen asentamisen jälkeen voidaan Active Directoryn toimialueeseen suorittaa päivittäisiä hallintatoimenpiteitä erilaisilla työkaluilla. Työkaluja voidaan käyttää joko Server Manager -hallintakonsolin kautta tai suoraan Administrative Tools -valikosta. Toimialueen hallintaan tarkoitettuja työkaluja ovat (Kivimäki 2005, 33–34.):

- Users and Computers -hallintakonsoli
- Domains and Trusted -hallintakonsoli
- Sites and Services -hallintakonsoli
- Group Policy Management -hallintakonsoli.

Active Directory Users and Computers -hallintakonsolilla hallitaan toimialuetta ja sen ominaisuuksia, käyttäjiä, ryhmiä, tietokoneita, organisaatioyksiköitä ja ryhmäkäytäntöjä. Myös toimialueen toimitilan ja Operations Master -roolien hallinta tapahtuu tällä konsolilla. Active Directory Users and Computers -konsoli voidaan myös käynnistää komentorivillä komennolla dsa.msc. (Kivimäki 2005, 33,34.)

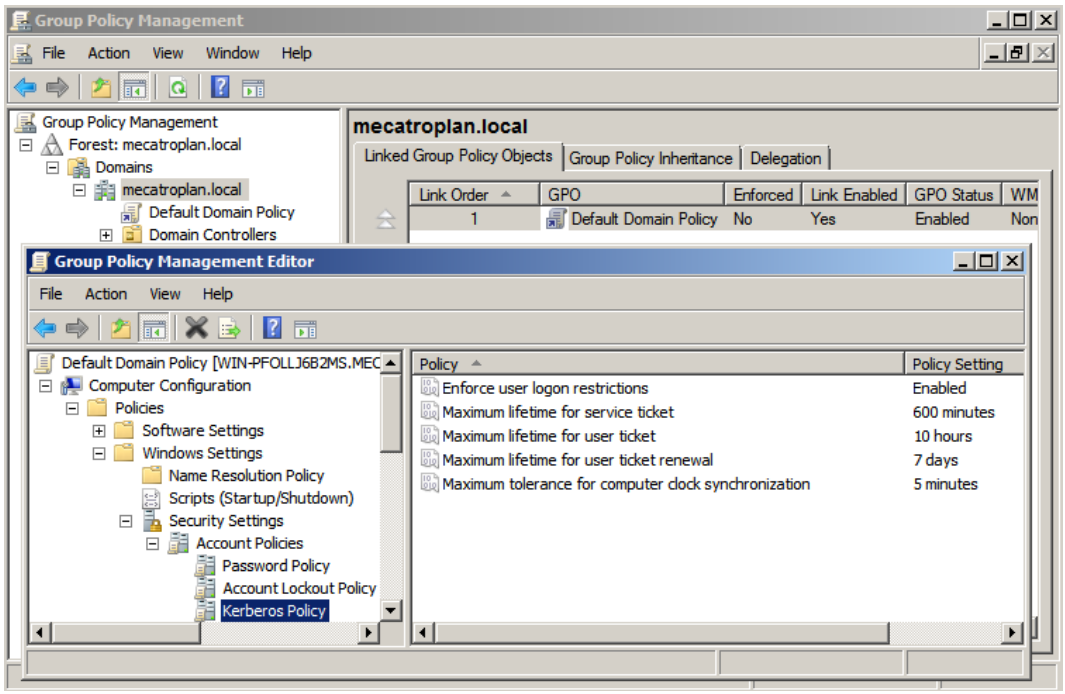
Active Directory Domains and Trusted -hallintakonsolilla (kuvio 2) hallitaan toimialueita ja metsiä. Hallinnalliset tehtävät keskittyvät luottosuhteiden hallintaan sekä toimialueen ja metsän toimitason asettamiseen. Toimialueen ja metsän toimitasot määrittävät sen, minkä käyttöjärjestelmäversion ohjauspalvelimia toimialueella voi olla. Toimitasojen korottaminen on syytä suunnitella huolella, sillä korottamisen jälkeen ei voida enää palata alkuperäiselle toimitasolle. Hallintakonsoli voidaan käynnistää komentorivillä komennolla domain.msc. (Kivimäki 2005, 33, 38, 53, 59.)



KUVIO 2. Active Directory Domains and Trusted -hallintakonsoli

Active Directory Sites and Services -hallintakonsolin avulla voidaan hallita toimipaikkoja palveluineen sekä aliverkkoja. Yleisen luettelon määrittely tehdään myös tällä konsolilla. Konsolissa voidaan myös tarkastella eri ohjauspalvelinten välisiä replikointiyhteyksiä. Active Directory Sites and Services -hallintakonsolia voidaan hyödyntää sen jälkeen kun Active Directory Domain Services rooli on asennettu toimialueelle. (Kivimäki 2005, 39.)

Active Directory Security Policy Management -hallintakonsoli on tarkoitettu toimialueen suojauskäytäntöjen hallintaa varten. Hallintakonsolissa määritetyt suojauskäytännöt kohdistuvat kaikkiin toimialueen organisaatioyksiköihin ja niiden sisältämiin käyttäjä- ja tietokonetileihin. Toimialuelaajuisesti oletuksena ovat voimassa tilikäytännöt (Password Policy, Account Lockout Policy ja Kerberos Policy). Active Directory Group Policy Management -hallintakonsolissa voidaan ryhmäkäytäntöjä määrittää myös organisaatioyksikkötasolle, jolloin käytännöt tulevat voimaan ainoastaan sen organisaatioyksikön käyttäjille tai tietokoneille. Kuviossa 3 on esitetty toimialueella oletuksena olevat Kerberos Policyn määritykset. (Kivimäki 2005, 42–43.)



KUVIO 3. Toimialueen oletus Kerberos Policy määritykset

7 TCP/IP TEKNIIKKA

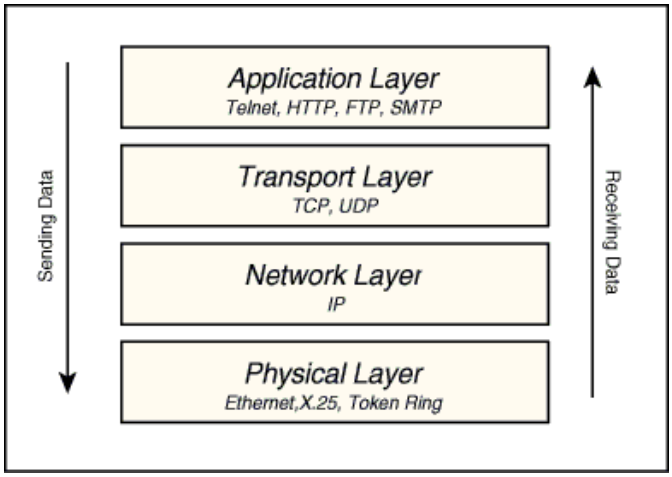
7.1 TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) on verkkoprotokollien yhdistelmä, jota käytetään Internetin välillä tapahtuvassa liikennöinnissä. TCP/IP-protokollaa voidaan käyttää myös privaateissa verkoissa, kuten intranetissä ja extranetissä. TCP-protokolla on toinen TCP/IP-maailman kuljetuskerroksen protokollista. Toinen protokollista on UDP (User Datagram Protocol). (SearchNetworking 2000; Anttila 2000, 133.)

TCP on luonteeltaan yhteydellinen ja luotettava protokolla. Se hallinnoi tiedonsiirtoyhteyksistä kahden päätelaitteen välillä sekä verkossa lähetettävien datapakettien järjestämisestä ja hukkuneiden pakettien uudelleenlähetyksestä. IP-protokolla on TCP/IP-protokollan ydin. IP-protokolla hoitaa datapakettien osoitteistamisen ja datapakettien reitittämisen oikeaan paikkaan. IP-protokolla on luonteeltaan yhteydetön, mikä tarkoittaa sitä, ettei verkkokerroksen tasolla pidetä minkäänlaista kirjaa olemassa olevista yhteyksistä. TCP/IP-protokollaperheeseen kuuluu muitakin protokollia, mutta pääosa liikennöinnistä tapahtuu TCP-yhteyksinä IP-protokollien päällä. (SearchNetworking 2000; Anttila 2000, 133; Microsoft TechNet 2012a.)

TCP/IP-protokolla-arkkitehtuuri koostuu neljästä eri kerroksesta. Ylin kerros on nimeltään sovelluskerros (Application Layer), joka käyttää alempien kerrosten tiedonsiirtopalveluita sovelluspalveluiden tuottamiseen. Esimerkkinä sovelluspalveluista ovat vaikkapa tiedostojen avaaminen, sulkeminen, kirjoittaminen ja lukeminen. Sovelluskerroksen alla on Kuljetuskerros (Transport Layer), joka taas tarjoaa yhteydellisen (TCP) ja yhteydettömän (UDP) tiedonsiirtoväylän kahden eri isäntäkoneessa toimivan prosessin välille. Kuljetuskerros huolehtii myös ylemmiltä kerroksilta vastaanotetun datan segmentoinnista ja datan välittämisestä vastaanottajalle. Kuljetuskerroksen alla on verkkokerros (Network Layer), jossa toimii muun muassa IP-protokolla. Verkkokerros huolehtii pakettien osoitteistuksesta, paketoinnista ja reititysfunktioista. Viimeisenä kerroksena on fyysinen kerros (Physical Layer), joka huolehtii kahden samaan verkkoon kytketyn solmupisteen

välisestä yhteydestä. Kuviossa 4 voidaan tarkastella TCP/IP protokolla-arkkitehtuurin eri kerroksia. (Anttila 2000, 32–34; Microsoft TechNet 2012a.)



KUVIO 4. TCP/IP-protokolla-arkkitehtuuri (Web Based Programming Tutorials 2012)

7.2 UDP

UDP on TCP:n rinnalla toimiva protokolla. Molemmat sijaitsevat protokollapinon kuljetuskerroksella, ja molempien tehtäviin kuuluu datan kuljettaminen. UDP eroaa TCP:stä siten, että se ei ole yhteydellinen, luotettava, virheenkorjaava tai kuittaava protokolla. UDP pystyy normaalin datavälityksen lisäksi multipleksaukseen, eli yksi fyysinen yhteys voi sisältää useita sessioita. (Anttila 2000, 167.)

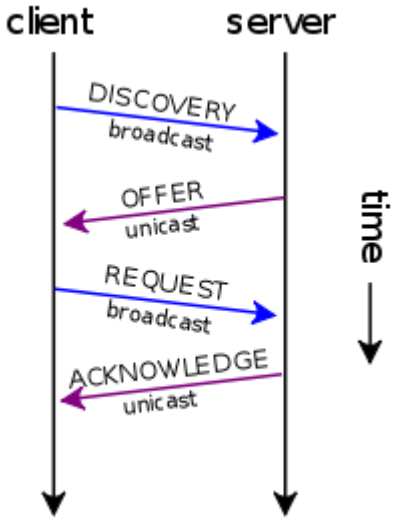
Koska UDP on yhteydetön ja epäluotettava protokolla, käytetään sitä tilanteissa, joissa välitettävän datan häviämisellä ei aiheuteta suurta vahinkoa. Nykyisistä protokollista UDP:tä käyttää muun muassa DNS- ja DHCP-protokollat (Dynamic Host Configuration Protocol). (Anttila 2000, 168.)

7.3 DHCP

DHCP (Dynamic Host Configuration Protocol) on verkkoprotokolla, jonka avulla voidaan tarjota verkkoasetuksia verkkoon liittyneille laitteille tietyksi ajaksi (lease period). Verkkoasetukset koostuvat IP-osoitteesta (IP-address), aliverkon peitteestä (Subnet mask), oletusyhdyskäytävästä (Default Gateway) ja joissain tapauksissa nimipalvelimen (DNS-server) IP-osoitteesta. Ilman DHCP:n käyttöä IP-osoite

täytyy asettaa manuaalisesti laitteen asetuksiin, jotta laitteella voitaisiin kommunikoida IP-verkossa. (Microsoft TechNet 2012e; Vicomsoft 2012.)

DHCP toimii TCP/IP-arkkitehtuurin kuljetuskerroksella ja käyttää hyväkseen yhteydetöntä UDP-protokollaa. DHCP:n toiminta perustuu käytännössä neljään eri vaiheeseen: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST ja DHCPACK. Asiakaslaite käyttää hyväkseen DHCPDISCOVER-sanomaa paikallistaakseen verkossa olevan DHCP-palvelimen. DHCP-palvelin vastaa asiakaslaitteen lähettämään DHCPDISCOVER-sanomaan DHCPOFFER-sanomalla, jolla palvelin tarjoaa IP-osoitetta asiakaslaitteelle. DHCPOFFER-sanoma sisältää asiakkaan MAC (Media Access Control)-osoitteen, vapaana olevan verkko-osoitteen, aliverkon peitteen ja mahdollisesti muita asetuksia, kuten IP-osoitteen kestoajan. DHCPREQUEST-sanomaa käytetään asiakaslaitteen vastatessa DHCP-palvelimelta tulleeseen DHCPOFFER-sanomaan. DHCPREQUES- sanoman avulla asiakaslaite pyytää DHCP-palvelimen tarjoamia verkko-asetuksia tai toisena vaihtoehtona nykyisten verkkoasetusten kestoajan pidentämistä. Kun palvelimen vastaanottaa DHCPREQUEST-sanoman, lähettää palvelin asiakkaalle DHCPACK-sanoman, jolla palvelin vahvistaa asiakaslaitteelle määritettyjen verkkoasetuksien varauksen. Kuviossa 5 voidaan tarkastella käyttäjän ja serverin välistä DHCP-viestintää. (ietf,1997; Anttila 2000, 207–208; Microsoft TechNet 2012a.)



KUVIO 5. Käyttäjän ja serverin välinen DHCP-viestintä (Wikibooks 2011)

DHCP:n käytöllä voidaan järjestelmänvalvojan hallinnallisia tehtäviä helpottaa monelta eri osin. DHCP:n avulla voidaan manuaalisesti tehtyjen asetusten yhteydessä tapahtuvia virheitä vähentää. DHCP:n toimiessa keskitetysti ja automaattisesti, TCP/IP asetuksia ei tarvitse asettaa kuin yhteen paikkaan. DHCP mahdollistaa myös helpon IP-osoitteiden jakamisen sellaisille laitteille, jotka siirtyvät paikasta tai verkosta toiseen. (Microsoft TechNet 2012e.)

8 ACTIVE DIRECTORYN SUUNNITTELU

8.1 Suunnittelussa huomioitavaa

Active Directoryn toteutus koostuu monista eri tekijöistä. Suunnittelussa on huomioitava DNS-nimiavaruus, joka sisältää toimialuehierarkian, luottosuhteet ja globaalin luettelon. Tämän jälkeen on suunniteltava toimialueelle muodostettavat organisaatioyksiköt, joihin sijoitetaan käyttäjä-, tietokone- ja ryhmätilit. Lopuksi tulisi suunnitella toimipaikat replikointi- ja sisäänkirjautumisliikennettä varten. (Kivimäki 2003, 13.)

Active Directory kannattaa suunnitella mahdollisimman yksinkertaiseksi, jolloin se parantaa yleistä tehokkuutta, helpottaa mahdollisia ongelmatilanteiden ratkaisuja ja vähentää yleisesti toteutusvaiheessa tarvittavaa aikaa. Yksinkertainen Active Directoryn kokonaisuus antaa mahdollisuuden tulevaisuuden muutoksia varten.

8.2 DNS-nimiavaruus

Active Directoryn nimiavaruus määrittää yrityksen ylimmän tason toimialuenimen. Nimiavaruuden suunnittelussa tulee ottaa huomioon se, onko muodostettava Active Directoryn -nimiavaruus sama kuin yritykselle mahdollisesti rekisteröity DNS-nimiavaruus (Internet-toimialuenimi). Active Directoryn -nimiavaruus voidaan yhdistää ulkoisen nimiavaruuden kanssa tai toisena vaihtoehtona on luoda sisäinen nimiavaruus (Intranet, palomuurin sisäpuolella oleva). (Kivimäki 2005, 8.)

Verkon hallinnan kannalta helpompi vaihtoehto on luoda sisäiselle ja ulkoiselle nimiavaruudelle eri nimet, sillä tällöin ei tarvitse hallita kuin yhtä DNS-aluetta. Sisäisen nimiavaruuden muodostukseen voidaan hyödyntää ylimmän tason toimialuetunnusta .local. Sisäisen ja ulkoisen nimiavaruuden samannimisyys vaatii tiettyjen vaatimusten huomioon ottamisen. (Kivimäki 2003, 13–15.)

Sisäisen ja ulkoisen nimiavaruuden ollessa samannimiset tulee yrityksen omassa verkossa olevien työntekijöiden pystyä luomaan yhteys sekä sisäisiin että ulkoi-

siin palvelimiin. Toinen vaatimus liittyy tietoturvaan palomuurin osalta. Palomuurin ulkopuolelta ei saa olla pääsyä yrityksen sisäisiin resursseihin sekä sisäiseen nimipalveluun. Palomuurin ulkopuolelta on kuitenkin oltava pääsy julkiseen nimipalveluun. (Kivimäki 2003, 13.)

8.3 Organisaatioyksiköt

Organisaatioyksiköiden suunnittelussa tulisi huomioida, millä tavalla toimialueen objekteja halutaan hallita. Organisaatioyksiköt sisältävät verkon objekteja kuten käyttäjä- ja ryhmätilejä. Toimialueen organisaatioyksikkörakennetta voidaan tarpeen vaatiessa muokata ja laajentaa sekä niissä olevia objekteja voidaan siirtää organisaatioyksiköstä toiseen. (Kivimäki 2003, 337.)

Suunnittelussa tulisi hyödyntää tiettyjä seikkoja. Organisaatioyksikkörakenteen tulisi mahdollistaa järjestelmänvalvojien tehokas työskentely. Organisaatioyksiköt tulisi suunnitella siten, että niihin liitetyt ryhmäkäytännöt vaikuttaisivat tehokkaasti. Organisaatioyksiköiden sisäisten tasojen määrä ja rakenne eivät saisi olla monimutkaisia, sillä liika monimutkaisuus vaikuttaa negatiivisesti hallinnallisiin ominaisuuksiin. (Kivimäki 2003, 340–341.)

Organisaatioyksikköhierarkia voidaan suunnitella monella eri tavalla. Monet yritykset käyttävät toteutuksissaan mallia, joka kuvastaa liiketoiminnan rakennetta. Muita hyödynnettäviä rakenteita ovat ainakin seuraavat (Kivimäki 2005, 372.):

- järjestelmänhallintaperusteiset organisaatioyksiköt
- liiketoimintoihin perustuvat organisaatioyksiköt
- osastokohtaiset organisaatioyksiköt
- projektikohtaiset organisaatioyksiköt.

8.4 Käyttäjätilit

Käyttäjätilien avulla käyttäjät voivat kirjautua toimialueelle ja käyttää verkon resursseja tai kirjautua sisään paikalliseen tietokoneeseen ja käyttää sen resursseja. Active Directoryn käyttäjätilien huolellinen suunnittelu nopeuttaa käyttäjätilien

luontiprosessia. Huomioitavia asioita suunnittelussa ovat (Kivimäki 2003, 385, 434.):

- käyttäjätilien nimeämiskäytännöt
- käyttäjätilien voimassaoloajat
- ryhmäjäsenyydet
- salasanavaatimukset
- sallitut kirjautumisajat
- käyttäjätileihin liittyvät tilikäytännöt (Account Policies), kuten Password Policy (salasanakäytännöt), Account Lockout Policy (tilien lukitsemiskäytännöt) ja Kerberos Policy (Kerberos-käytännöt).

Käyttäjätilien nimeämisissä tulisi käyttää yhdenmukaisia käyttäjänimiä, jolloin niiden muistaminen ja etsiminen olisi helpompaa. Tilien nimeämisen turvallisuudesta vastaa salasanakäytännöt, joita voidaan muokata yrityksen tarpeita vastaaviksi. Käyttäjätilillä on näyttönimi (Display name), joka on nähtävissä käyttöliittymässä sekä kirjautumistunnus (Logon name), jolla käyttäjä kirjautuu toimialueelle. (Kivimäki 2003, 434–435.)

Käyttäjätilien voimassaoloajalla voidaan ehkäistä käyttäjän pääsy verkkoon silloin, kun hänellä ei ole enää siihen oikeutta. Tätä käytäntöä voidaan esimerkiksi käyttää silloin, kun tiedetään työntekijän työsopimuksen päättymispäivä. (Kivimäki 2003, 445.)

Käyttäjätilien kanssa käytetään salasanoja verkkoresurssien käytön valtuutuksessa. Salasanat tulisi määrittää turvallisiksi ja vahvoiksi, jolloin ehkäistäisiin tilien luvaton käyttö. Salasana-asetukset voidaan muuttaa tarpeisiin sopiviksi, jotta ne täyttäisivät minimivaatimukset. (Kivimäki 2003, 445–446.)

Käyttäjätileihin liittyvät tilikäytännöt ovat osa suojauskäytäntöjä (Security Policy). Suojauskäytännöt tulisi suunnitella toimialuetasolla, jolloin toimialueen käyttäjätilit saisivat yhdenmukaiset tilikäytännöt. Toimialuetason suojauskäytäntöjä

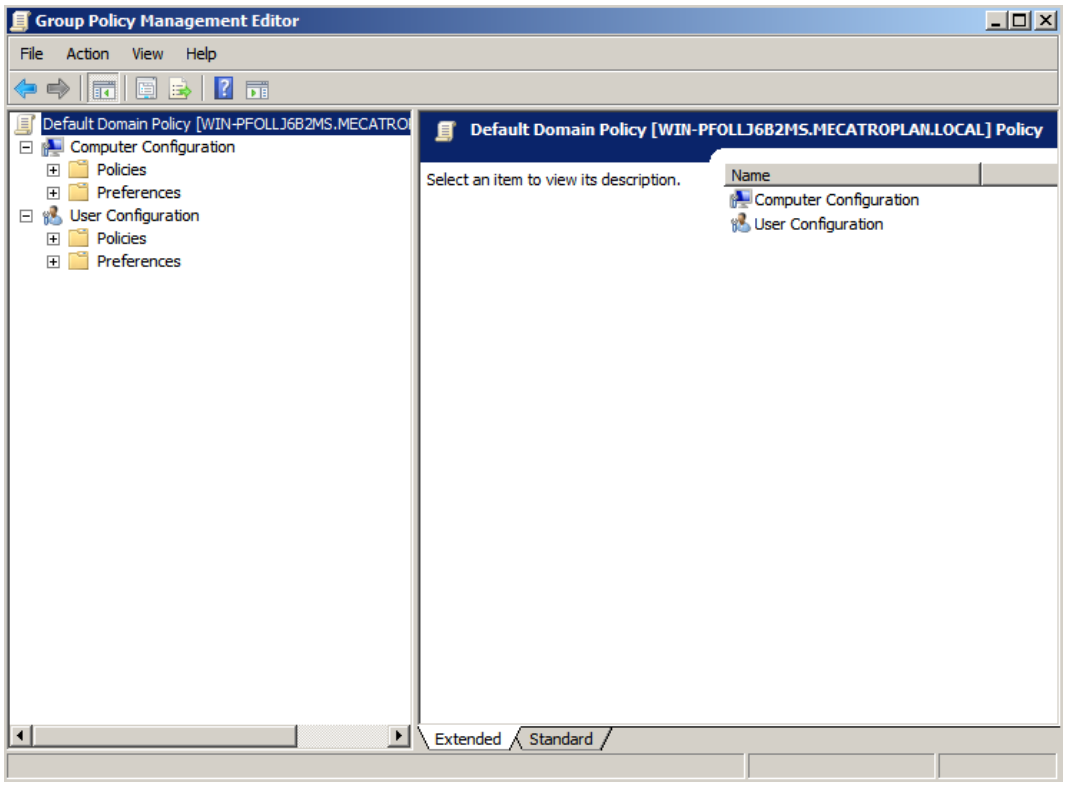
voidaan asettaa toimialueen oletusryhmäkäytännössä (Default Domain Policy). (Kivimäki 2003, 446–447.)

8.5 Ryhmäkäytännöt

Ryhmäkäytännöillä (Group Policy) tarkoitetaan järjestelmän kokoonpanoasetuksia, jotka voidaan liittää Active Directoryn objekteihin, kuten organisaatioyksikköön. Muodostetut ryhmäkäytännöt ja oletusryhmäkäytännöt käsitellään järjestelmän käynnistyksessä ja sammutuksessa sekä käyttäjän kirjautuessa järjestelmään ja järjestelmästä ulos. (Kivimäki 2003, 595.)

Ryhmäkäytäntöjä suunniteltaessa tulisi huomioida tiettyjä asioita. Yhteen tietokoneeseen tai käyttäjätiliin kohdistuvia ryhmäkäytäntöjen määrää tulisi rajoittaa. Ryhmäkäytäntöjen ryhmittelyä ja kokoamista ryhmäkäytäntöobjekteihin ei tulisi tehdä. Esimerkiksi kaikkia käyttäjätilejä koskevat tilikäytännöt voidaan määrittää toimialuetasolla, kun taas yksittäisen organisaatioyksikön käyttäjiä koskevat asetukset voidaan määritellä ryhmäkäytäntöobjektissa, joka on sijoitettu kyseiset käyttäjätilit sisältävään organisaatioyksikköön. Suunnittelussa tulisi vielä huomioida ryhmäkäytäntöjä hallitsevien järjestelmänvalvojien määrä. (Kivimäki 2003, 595.)

Ryhmäkäytännöt jakaantuvat tietokoneasetuksiin ja käyttäjäasetuksiin. Tietokoneasetuksilla (Computer Configuration) voidaan mukauttaa käyttäjän työpöydän asetuksia tai määrittää verkon tietokoneita koskevia suojauskäytäntöjä. Käyttäjäasetuksien (User Configuration) avulla voidaan käyttäjän työpöydän asetuksia mukauttaa tai määrittää verkon käyttäjiä koskevia suojauskäytäntöjä. Asetukset sisältävät kaikki käyttäjäkohtaiset määritykset, jotka vaikuttavat työpöydän ulkoasuun, sovellusten asetuksiin sekä sisään- ja uloskirjautumisskripteihin. Ryhmäkäytäntöjen jakauma on kuvattuna kuviossa 6. (Kivimäki 2003, 596–597.)



KUVIO 6. Group Policy Management -hallintakonsoli

9 ACTIVE DIRECTORYN TOTEUTUS

9.1 Tavoitteet

Opinnäytetyön tavoitteena oli tutustua Microsoft Windows Active Directory 2008 R2 toimintaan sekä suunnitella ja toteuttaa kokonaisvaltainen hakemistopalvelinratkaisu pienyrityksen käyttöön. Työhön tutustumisessa käytettiin hyväksi kirja- ja Internet lähteitä sekä virtuaaliympäristöä, joka mahdollisti käytännönläheisen tutustumisen aiheeseen.

Työn suunnittelussa pyrittiin huomioimaan kaikki tarvittava tieto sekä luomaan tarkka näkemys siitä, mitä toteutusvaihe pitää sisällään eri osa-alueissa. Toteutusvaiheen tavoitteena oli suoriutua toteutuksesta mahdollisimman nopeasti ja tehokkaasti, jotta valmis hakemistopalvelin saataisiin hyötykäyttöön sekä turhilta viivästyksiltä vältyttäisiin.

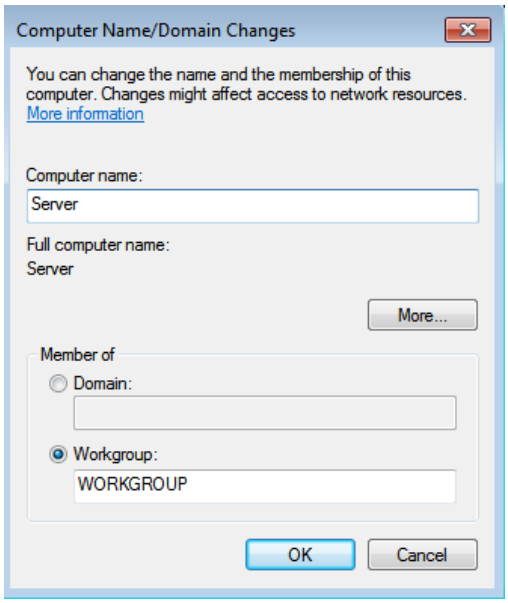
9.2 Käytössä oleva laitteisto

Active Directoryn suunnitteluvaiheessa otettiin huomioon yrityksen nykyinen palvelinlaitteisto. Tekniikaltaan nykyinen palvelinlaitteisto oli vaatimukset täyttävä, joten se soveltui mainiosti uuden palvelimen perustaksi. Tallennus- ja varmuuskopiointikapasiteettia haluttiin kuitenkin kasvattaa, jonka myötä uutta palvelinta varten hankittiin kaksi Western Digitalin 1,5 terabitin kiintolevyä sekä Hewlett Package Storageworks DAT160-nauhavarmistusasema. Aikaisemmin käytössä oli kaksi 300 gigatavun kiintolevyä ja Hewlett Package Storageworks DAT72 -nauhavarmistusasema. Uuteen nauhavarmistusasemaan päädyttiin Mecatroplan Oy:n suurten tiedostomäärien sekä aikaisemmin käytössä olleen nauhavarmistusaseman takia. Nauhavarmistus on hyvä lisäturva silloin kun tarvitaan lisävarmuutta palvelimen tietojen tallennukseen ja kun tietojen palautuksessa halutaan mahdollisuus palata pitkälle taaksepäin aiempaan tilanteeseen. Nauhavarmistuksen käyttö vaatii kuitenkin käyttäjien manuaalisia toimenpiteitä, kuten nauhan vaihtoa päivittäin.

Palvelinkäyttöjärjestelmäksi valittiin 64-bittinen Microsoft Windows Server 2008 R2. Käyttöjärjestelmän valintaan vaikutti Microsoftin tuotteiden helppo käytettävyys ja yhteensopivuus useiden sovellusten kanssa. Komponentit ja ohjelmisto hankittiin lahtelaisen tietotekniikkayrityksen kautta.

9.3 Lähtötilanne Mectroplan Oy

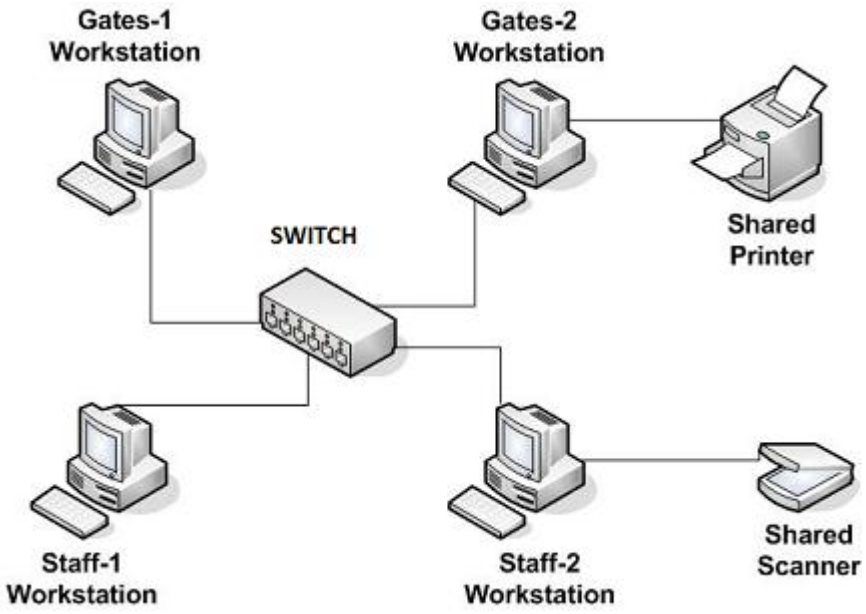
Työasemat voivat kuulua joko työryhmään tai toimialueeseen. Mecatroplan Oy:n aikaisempi tiedostopalvelin pohjautui työryhmäkäytäntöön. Tiedostojen jako tapahtui työasemalta, johon oli asennettu Windows XP Professional -käyttöjärjestelmä. Työasema oli samassa työryhmässä muiden yrityksen työasemien kanssa. Järjestelmä oli ollut Mecatroplan Oy:n käytössä vuodesta 2008. Kuviossa 7 voidaan tarkastella serverin liittymistä työryhmään.



KUVIO 7. Työryhmään liittyminen

Työryhmäkäytäntö on käytännöllinen pienille verkoille, joissa sijaitsee alle 10 työasemaa. Työryhmässä toimivat tietokoneet muodostavat vertaisverkon (Peer-to-Peer), jossa jokainen verkon tietokone toimii sekä palvelimena että asiakkaana muille tietokoneille. Työryhmäkäytäntö tarjoaa helpon tavan jakaa tiedostoja, tulostimia ja muita verkon resursseja. Hyvänä puolena työryhmässä toimimiseen on myös se, ettei siinä tarvita palvelinkäyttöjärjestelmää. Tämä tuo huomattavia sääs-

töjä ohjelmistokustannuksissa. Työryhmäkäytäntö ei myöskään vaadi ylimääräistä osaamista, sillä se on oletuksena käytössä kaikissa työasemissa. (Microsoft 2012.) Kuviossa 8 on esitetty vertaisverkon malli.



KUVIO 8. Vertaisverkon (Peer-to-Peer) malli (WebJunction 2005)

Työryhmänä toimivat tietokoneet eivät voi hallita toisiaan, mikä lisää järjestelmänvalvojan töitä. Työryhmäkäytäntö vaatii esimerkiksi käyttäjätilien ja salasanojen luonnin jokaiselle työasemalle erikseen, jos halutaan jokaisen työntekijän pystyvän tekemään töitä millä työasemalla tahansa. Käyttäjätilien luonti työasemiin vaatii paikallisen tietokoneen järjestelmänvalvojan oikeudet. (Spector CNE 2012.)

Merkittävin ero työryhmien ja toimialueiden välillä on se, miten tietokoneita ja verkkoresursseja hallitaan. Työryhmäkäytännöllä voidaan verkon tiedostoja ja hakemistoja jakaa Windowsin jako-oikeuksien mukaan. Jako-oikeudet ovat kuitenkin hyvin yksinkertaisia eivätkä tarjoa hallinnallisesti järkeviä ratkaisuja siihen, kuka pääsee käsiksi ja mihin. Työryhmää ei myöskään ole suojattu minkäänlaisella salasanalla, joka lisää tietoturvariskiä. Käytännössä jokaisella samassa aliverkossa olevalla työasemalla on pääsy jaettuihin verkkoresursseihin. (Microsoft 2012; Everyjoy 2006.)

9.4 Windows Server 2008 R2 –käyttöjärjestelmän asennus

Palvelimen uusien komponenttien asentamisen jälkeen suoritettiin palvelinkäyttöjärjestelmän asennus. Asennus tapahtui Microsoft Windows Server 2008 R2 -asennuslevykkeeltä. Käyttöjärjestelmän asennusohjelma muistutti Windows Vistan asennusohjelmaa ja oli erittäin yksinkertainen.

Asennusvaihtoehtoja olivat uusi asennus (Clean Install) tai vanhemman Windows-version päivittäminen (Upgrade). Tässä työssä asennusvaihtoehdoksi valittiin uusi asennus, sillä aikaisempaa palvelinkäyttöjärjestelmää ei ollut asennettu.

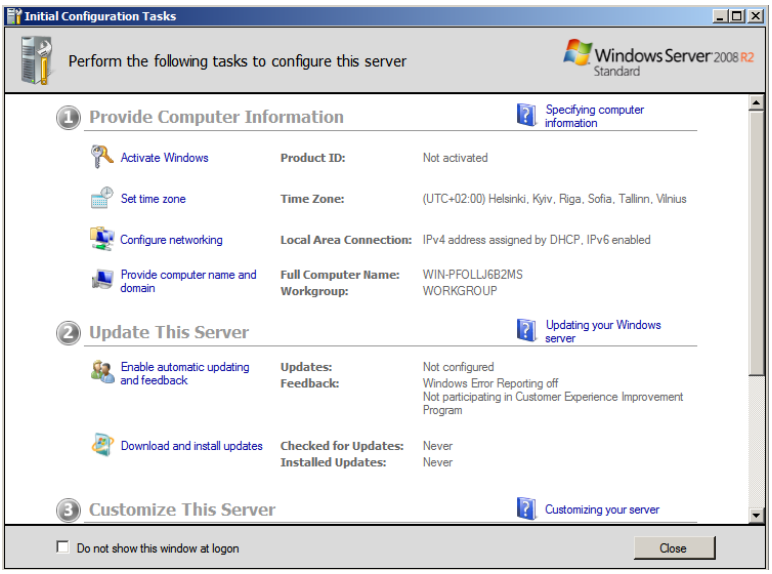
Asennusohjelman käynnistyttyä asennusohjelma latasi asennusympäristön. Tämän jälkeen avautui Install Windows -asennusikkuna, jossa kysyttiin asennuksen yhteydessä käytettäviä asetuksia. Asennettavaksi kieleksi (Language to install) valittiin suomi, ajan ja rahayksikön muodoksi (Time and currency format) valittiin Finnish sekä näppäimistöasettelu tai syöttötavaksi (Keyboard or input method) valittiin Finnish.

Tämän jälkeen päästiin varsinaiseen asennuksen aloittamiseen. Aluksi asennuksessa jouduttiin antamaan tuotetunnus, joka käyttöjärjestelmän aktivoinnin yhteydessä liitetään laitteistokokoonpanoon. Tämän jälkeen asennettavaksi versioksi valittiin Windows Server 2008 R2 Standard (Full Installation), asennettavaksi tyypiksi valittiin mukautettu asennus (Custom (Advanced)), jolloin asennus suoritetaan tyhjään ympäristöön.

Seuraavaksi valittiin levyosio, johon käyttöjärjestelmä haluttiin asentumaan. Vaihtoehtoina oli kaksi identtisistä kiintolevyistä, joista toinen valittiin. Tämän jälkeen asennusohjelman suoritus alkoi ja asennustiedostoja kopioitiin sekä purettiin. Järjestelmän asentamisen jälkeen Windowsiin tuli kirjautua ensimmäisen kerran järjestelmänvalvojana (Administrator). Ennen kirjautumista oli määritettävä järjestelmänvalvojan käyttäjätilin salasana.

Sisäänkirjautumisen jälkeen työpöydälle avautui Initial Configuration Tasks -työkalu, jonka avulla voitiin helposti suorittaa tiettyjä vaadittavia asetuksia. Tär-

keimpiä asetuksia olivat käyttöjärjestelmän aktivointi, automaattisten päivitysten käyttöönotto, saatavilla olevien päivitysten asentaminen, serverin nimen sekä kiinteän IP-osoitteen määrittäminen. Kuviossa 9 voidaan tarkastella Initial Configuration Tasks -hallintaikkunan eri kohtia.

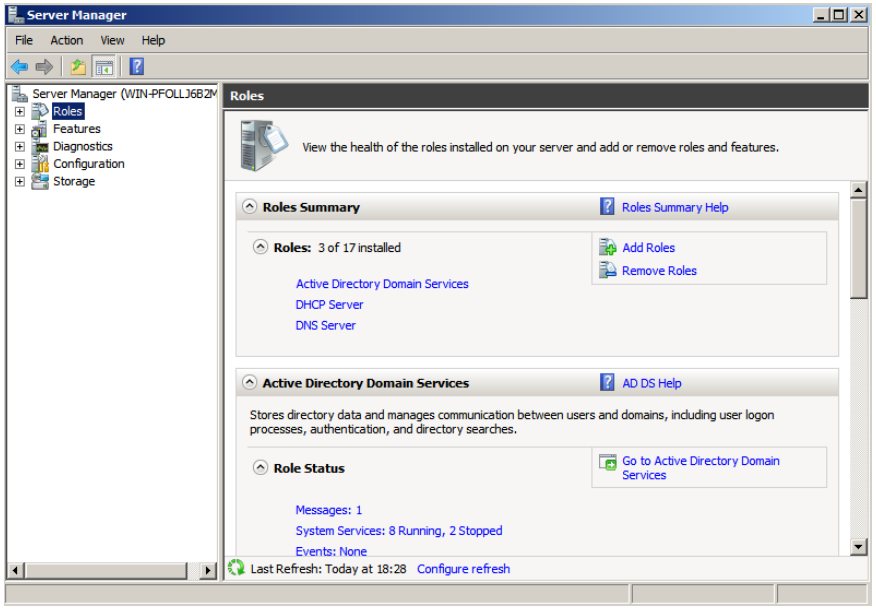


KUVIO 9. Initial Configuration Tasks -hallintaikkuna

9.5 Toimialueen roolien asentaminen

Käyttöjärjestelmän asentamisen jälkeen palvelimeen asennettavat roolit asennettiin Server Manager -hallintakonsolin avulla. Server Manager on keskitetty työkalu palvelimen hallintaan, joka tarjoaa näkymän palvelimen asetuksiin, asennettuihin rooleihin ja ominaisuuksiin sekä niihin liittyviin keskeisiin tapahtumiin. (Kivimäki 2009, 409–410.)

Palvelimen rooli (role) liittyy kokoelmaan käyttöjärjestelmän ohjelmistokomponentteja, jotka mahdollistavat järjestelmän palveluiden tarjoamisen verkon käyttäjille ja toisille tietokoneille. Kuviossa 10 on näkymä Server Manager -hallintaikkunasta. (Kivimäki 2009, 409–410.) Järjestelmään asennettavia rooleja olivat Active Directory Domain Services, DNS server ja DHCP server.



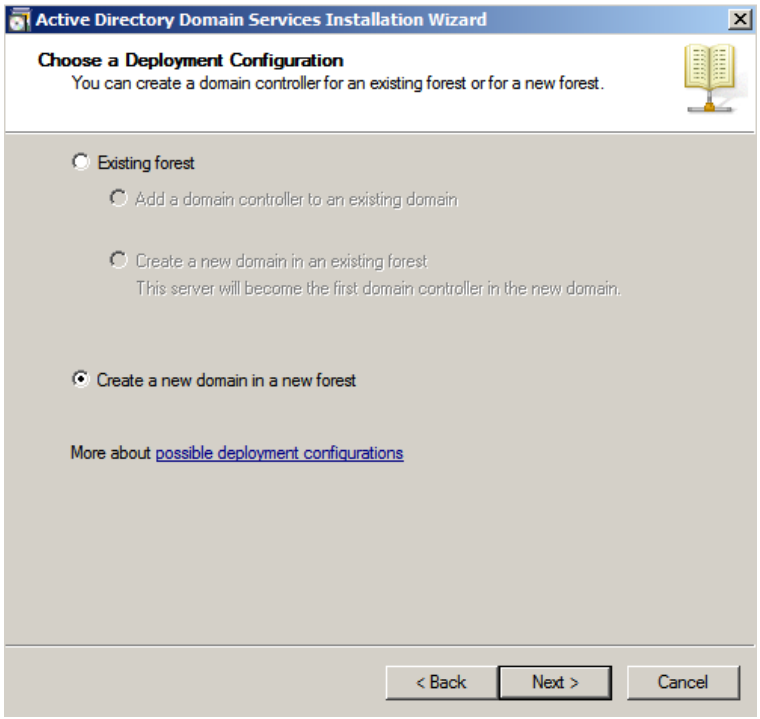
KUVIO 10. Server Manager -hallintakonsoli

9.6 Metsän ja toimialueen toteutus

Active Directory Domain Services -rooli (AD DS) on perinteinen Active Directory -ohjauspalvelin, joka tarjoaa tunnistuspalvelut, hakemistopalvelut ja tallennuspalvelun erilaisista objekteista (Kivimäki 2009, 421). Käyttämällä AD DS -roolia Windows Server 2008 R2 -käyttöjärjestelmässä, voidaan luoda skaalautuva, turvallinen ja hallittava infrastruktuuri käyttäjiä ja resurssien hallintaa varten. AD DS roolin käyttö tarjoaa myös kattavan tuen hakemistopohjaisille sovelluksille, kuten Microsoft Exchange serverille. (Microsoft TechNet 2012f.)

Active Directory Domain Services -roolin asentamisen jälkeen varsinainen ohjauspalvelin täytyy konfiguroida erikseen ohjatun toiminnan avulla. Konfigurointi suoritettiin ohjatulla Active Directory Domain Services Installation Wizard -toiminnolla. Ohjattu toiminto käynnistettiin komentorivissä Dcpromo.exe-komennolla.

Asennusvelhon käynnistyttyä, Choose a Deployment Configuration -ikkunassa kokoonpanoksi valittiin Create a new domain in a new forest. Tämä toiminto loi uuden toimialueen uuteen metsään (kuvio 11).



KUVIO 11. Uuden toimialueen muodostus uuteen metsään

Name the Forest Root Domain -ikkunassa annettiin toimialueen DNS-nimi (FQDN, Fully Qualified Domain Name). Toimialueen DNS-nimeksi määritettiin mecatroplan.local.

Tämän jälkeen metsän ja toimialueen toimitasoiksi (Forest- and Domain Function Levels) määritettiin Windows Server 2008 R2. Toimialuetason määrittäminen alimmasta oletuksena olevasta toimitasosta (Windows 2000 Native Mode) ylimpään toimialuetasoon (Windows Server 2008 R2) mahdollistaa kaikkien ominaisuuksien käyttämisen. Toimialuetason määrittämisen jälkeen vanhempia käyttöjärjestelmällä varustettuja toimialueen ohjauskoneita ei voi tuoda toimialueelle. (Petri IT Knowledebase 2009.)

Additional Domain Controller Options -ikkunassa voitiin antaa asennuksen lisävalintoja. Lisävalinnaksi valittiin DNS server, joka on Active Directoryn edellyttämä DNS-palvelin. Global Catalog valinta on oletuksena valittuna ensimmäistä ohjauspalvelinta asennettaessa.

Location for Database, Log Files and SYSVOL -ikkunassa valittiin hakemiston tietokannan (Database folder) ja lokien (Log files folder) sijainniksi %System-root%\Ntds-kansiot sekä System Volume hakemiston sijainniksi %System-root%\SYSVOL-kansiot. SYSVOL hakemisto tarjoaa standardin tallennussijainnin tärkeille elementeille, kuten ryhmäkäytäntöobjekteille ja skripteille. (TechNet 2012b.)

Asetuksien määrittämisen jälkeen varsinainen Active Directoryn asennus käynnistyi. Asennuksen jälkeen ensimmäinen ohjauspalvelin oli myös muodostunut oletustoimipaikan nimeltä Default-First-Site-Name. Palvelimen uudelleenkäynnistämisen jälkeen ohjauspalvelimeen asennettuja rooleja voitiin tarkastella Server Manager -konsolilla.

9.7 DHCP-roolin toteutus

DHCP-palvelin (DHCP server) on DHCP-asiakas/palvelinprotokollaa käyttävä palvelin, jonka tarkoituksena on tarjota automaattisesti IP-osoitteet ja muut konfigurointiasetukset asiakastietokoneille. DHCP:n avulla hallitaan keskitetysti IP-osoitteita ja muita TCP/IP-asetuksia (Kivimäki 2009, 601). DHCP server roolin asennus suoritettiin Server Manager -hallintakonsolin kautta. Asennusvaiheessa Select Server Roles -ikkunassa valittiin DHCP Server.

Select Network Connection Bindings -ikkunassa valittiin käytettäväksi verkkoliittymäksi serverin verkkoliittymä. Specify IPv4 DNS Server Settings -ikkunassa annettiin DNS-toimialueen nimeksi mecatroplan.local ja käytettävän ensisijaisen IPv4 DNS-palvelimen osoitteeksi serverin IP-osoite.

Add or Edit DHCP Scopes -ikkunassa DHCP-palvelimelle luotiin osoitealue (Scope), jota DHCP-palvelu käyttää osoitteiden jakamisessa. Add Scope -ikkunassa osoitealueelle (Scope Name) määritettiin kuvaava nimi. Ensimmäiseksi jaettavaksi osoitteeksi (Starting IP Address) ja viimeiseksi jaettavaksi osoitteeksi (Ending IP Address) annettiin toisistaan riittävän suurella välillä olevat IP-osoitteet. Tämän avulla varmistettiin IP-osoitteiden riittävyys lähiverkkoon liitty-

ville laitteille. Lopuksi määritetiin aliverkon peite (Subnet mask) ja oletusyhdyskäytävän (Default Gateway) IP-osoite.

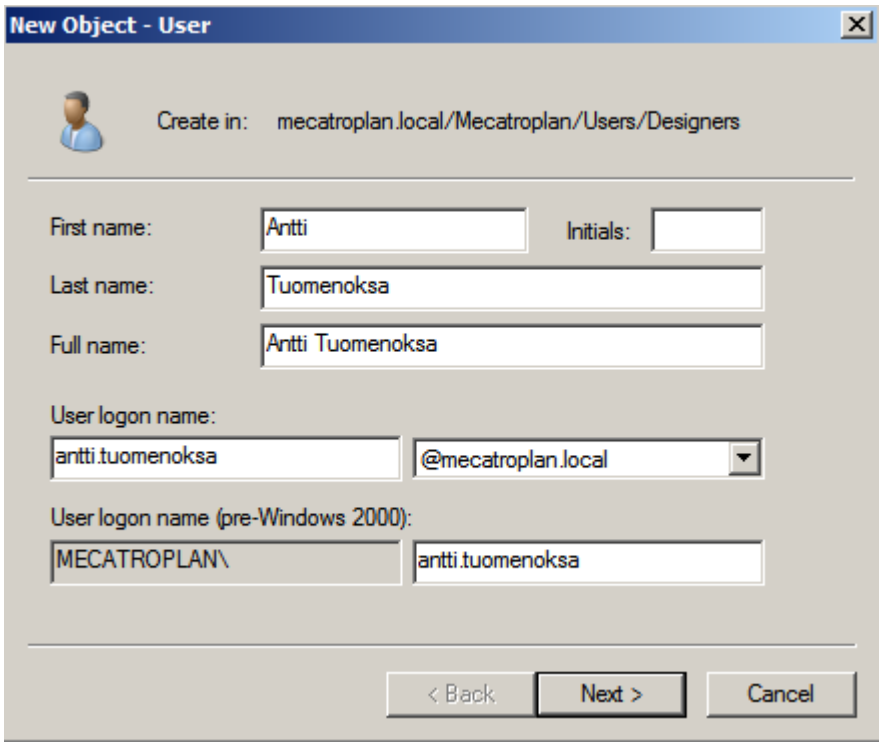
Authorize DHCP Server -ikkunassa DHCP-palvelin ja palvelimen jakamat osoitealueet valtuutettiin. Toimialueella sijaitseva DHCP-palvelin on valtuutettava, jotta palvelimen tuottamia dynaamisia IP-osoitteita voidaan hyödyntää toimialueessa. Valtuutuksella ehkäistään myös luvattomien DHCP-palvelimien toiminta toimialueella. Tämä myös varmistaa, että verkkotoiminnot toimivat sujuvasti. DHCP-palvelin valtuutettiin käyttämällä kirjautuneen käyttäjän tunnistetietoja.

9.8 Käyttäjätilit

Toimialueen käyttäjät luotiin Active Directory Users and Computers -hallintakonsolilla. Mecatroplan Oy yrityksen työntekijöiden vähäisen määrän takia, jokainen käyttäjätili luotiin erikseen käyttäjälle tarkoitettuun organisaatioyksikköön, eikä luonnissa käytetty minkäänlaisia skriptejä tai komentojonoja.

Toimialueelle luotu organisaatioyksikkörakenne rakentuu Mecatroplan organisaatioyksikön alle. Mecatroplan organisaatioyksikkö jakautuu Computers- ja Users-ali-organisaatioyksiköhin, jotka erottavat tietokoneet ja käyttäjät toisistaan. Computers organisaatioyksikkö jakaantuu vielä Desktop- ja Laptop -organisaatioyksiköihin. Users-organisaatioyksikkö jakaantuu Designers-, Lead Designers- ja Managing Director -organisaatioyksiköihin. Kuviossa 13 voidaan nähdä muodostettu organisaatioyksikkörakenne.

Luontiprosessissa käyttäjälle määritettiin käyttäjän etunimi (First name), käyttäjän sukunimi (Last name), käyttäjän koko nimi (Full name), joka näkyy käyttäjää etsittäessä organisaatioyksiköstä ja käyttäjän yksilöllinen käyttäjänimi (User logon name). Käyttäjien yksilölliset käyttäjänimet muodostettiin nimiyhdistelmälyhenteistä, jolloin niistä saatiin helposti muistettavat sekä samankaltaiset muihin käyttäjiin nähden. Kuviossa 12 on tarkasteltu käyttäjän luontiprosessia.



KUVIO 12. Toimialueelle muodostettavan käyttäjän luontiprosessi

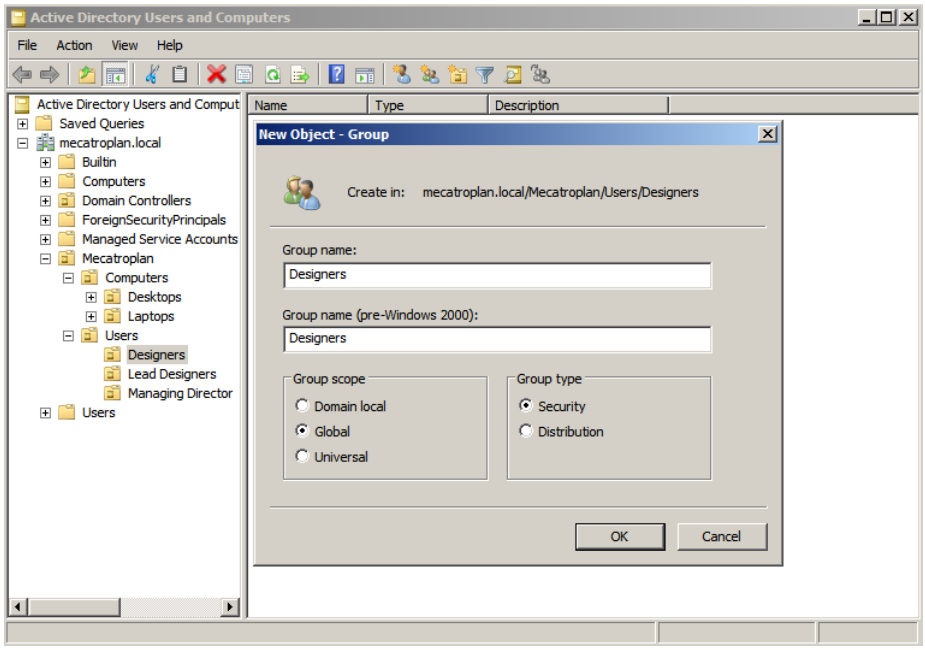
New Object User -ikkunassa käyttäjälle määritettiin käyttäjätilin salasana. Salasanan määrityksessä tuli ottaa huomioon toimialueella vaikuttavan Default Domain Policyn salasanavaatimukset, jotka määrittävät muodostettavan salasanan minimipituuden ja erikoismerkkien käytön. Salasanan asetusvalinnoista otettiin käyttöön User must change password at next logon, jolloin käyttäjän oli muutettava salasanansa ensimmäisen kirjautumisen yhteydessä. Tällä määrityksellä varmistettiin, että kun käyttäjä luo uuden salasanan, on salasana vain käyttäjän omassa tiedossaan. Muita vaihtoehtoisia määrityksiä olivat User cannot change password, Password never expires ja Account is dissabled. Näille määrityksille ei kuitenkaan ollut tarvetta.

Käyttäjän luomisen jälkeen käyttäjätiliä muokattiin properties-ikkunassa. Profiles-välilehdessä määritettiin profiilin asetukset käyttämällä Username-ympäristömuuttujaa. Määritettäviä alueita olivat käyttäjäprofiilin sijainti (Profile path) ja kotikansio (Home folder).

Käyttäjäprofiili on kokoelma kansioita ja tiedostoja, joihin on tallennettu käyttäjän nykyiset työpöydän ja sovellusten asetukset sekä käyttäjän henkilökohtaiset ase-

tukset. Kotikansio on käyttäjälle luotu kansio, johon käyttäjällä on mahdollisuus tallentaa omia tiedostojaan. (Kivimäki 2003, 511.)

Active Directory Users and Computers -konsolin avulla jokaiseen organisaatioyksikköön luotiin myös käyttäjäryhmät. Käyttäjäryhmät voivat sisältää käyttäjiä, kontakteja, tietokoneita tai muita ryhmiä. Ryhmien käyttö yksinkertaistaa ja tehostaa järjestelmänhallintaa, koska käyttöoikeudet voidaan myöntää käyttäjäryhmälle sen sijaan, että ne myönnettäisiin erikseen jokaiselle käyttäjätilille. Designers-ryhmän muodostus Designers-organisaatioyksikköön on kuvattu kuviossa 13.

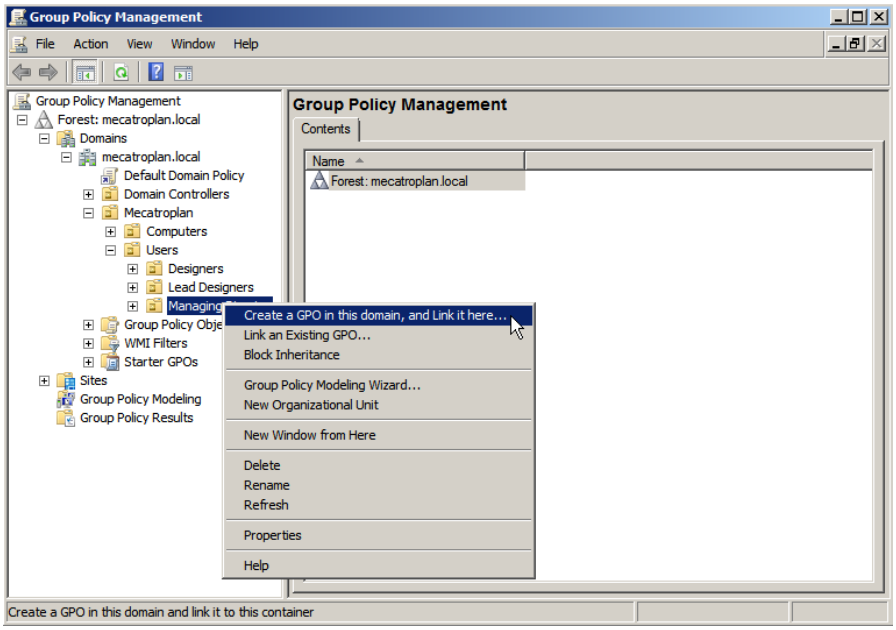


KUVIO 13. Designers-ryhmän muodostus

Käyttäjäryhmien luonnissa ryhmälle annettiin kuvaava nimi (Group name), ryhmän vaikutusalueeksi (Group scope) määritettiin Global, jolloin ryhmä voi toimia vain sille määritetyllä toimialueella, sekä ryhmän tyypiksi (Group type) Security. Security-määritys sallii järjestelmänvalvojan hallita käyttäjien ja tietokoneiden pääsyä jaettuihin kansioihin. Muodostettuihin käyttäjäryhmiin lisättiin sen organisaatioyksikön käyttäjät. Käyttäjien lisääminen tapahtui ryhmän properties -ikkunan Member Of -välilehdessä.

9.9 Ryhmäsäännöt

AD-palvelimelle muodostetut tiedostokansiot tuli jakaa työntekijöiden käyttöön verkkolevynäkyminä. Verkkolevynäkymien käyttö helpottaa huomattavasti työntekijöiden työskentelyä, sillä työntekijöillä on niiden avulla nopea pääsy palvelimen tarjoamiin tiedostoihin sekä mahdollisuus tallentaa omia tiedostojaan palvelimelle. Tiedostokansioiden jakamisessa käytettiin hyväksi ryhmäsääntöjä. Ryhmäsäännöt muodostettiin suoraan organisaatioyksiköihin käyttäen hyväksi Group Policy Management -hallintakonsolia. Ryhmäsäännön muodostaminen Managing Director -organisaatioyksikköön on kuvattu kuviossa 14.

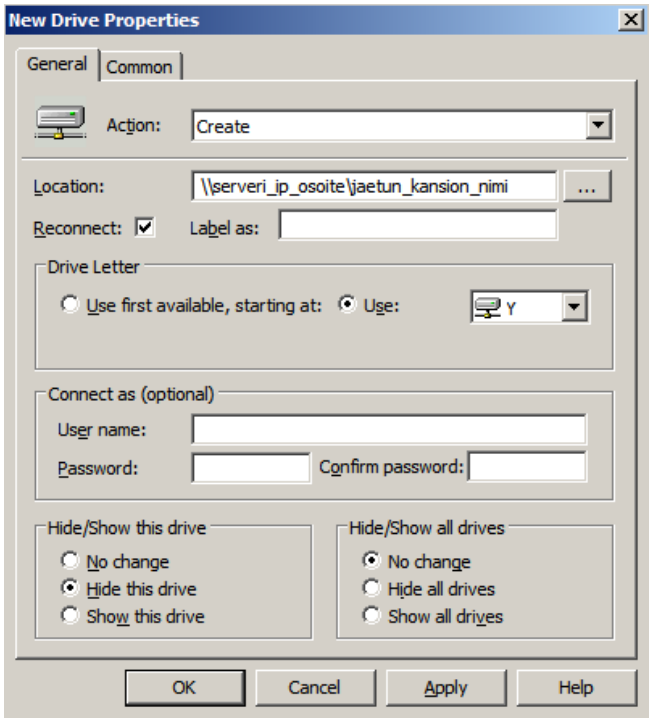


KUVIO 14. Ryhmäsäännön muodostaminen Group Policy Management -hallintakonsolin avulla

Ryhmäsäännön muodostamisen jälkeen säännölle tuli asettaa tarvittavat määritykset. Määritysten teko tapahtui editoimalla sääntöä, jolloin avautui Group Policy Management Editor -ikkuna. Group Policy Management Editor -ikkunassa valittiin User Configuration | Preferences | Windows-settings -haaran Drive Maps -käytäntö. Drive Maps -käytäntö mahdollisti uuden verkkolevynäkymän luonnin.

Valitsemalla New | Mapped Drive päästiin luomaan uusi verkkolevy. Properties-ikkunassa määritettiin Action-luettelosta halutuksi toiminnoksi Create. Create-

valinta määritti verkkolevyn luonnin. Location-kohdassa kansion sijaintipoluksi määritettiin halutun kansion sijainti. Sijainniksi annettiin kansion sijainti palvelimella. Drive Letter -kohdassa valittiin Use ja kirjainluettelosta haluttu kirjain, joka kuvasti verkkolevyä. Tämän jälkeen Drive Maps -käytäntö oli luotu. Uuden verkkolevyn asetuksien määritykset on kuvattuna kuviossa 15.



KUVIO 15. Muodostettavan verkkolevyn määritykset

Tarvittavien ryhmäsääntöjen luonnin jälkeen varmistettiin sääntöjen voimaanastuminen syöttämällä komentokehotteessa komento gpupdate /force. Tämä komento suoritti uusimpien ryhmäsääntöjen käyttöönoton välittömästi. Yhtenä ongelmana huomattiin verkkolevynäkymien puuttuminen käyttäjiltä, kirjauduttaessa Mecatroplan Oy:n neuvotteluhuoneen kannettavalle tietokoneelle. Tilanne oli erikoinen, sillä verkkolevynäkymät ilmestyivät normaalisti muille työasemille. Ongelmaa yritettiin ratkaista yksinkertaisen sisäänkirjautumisskriptin avulla, joka liitettiin käyttäjille heidän profiiliasetuksissa. Skriptin tarkoituksena oli muodostaa verkkolevynäkymät käyttäjän kirjautuessa toimialueelle. Havaintojen perusteella skriptin ajo käynnistyi käyttäjän kirjautumisen yhteydessä, mutta verkkolevyt eivät kuitenkaan ilmaantuneet käyttäjälle. Ratkaisua asiaan ei saatu, ja päätelmät viittasivat kannettavan tietokoneen Windows XP Professional -käyttöjärjestelmän

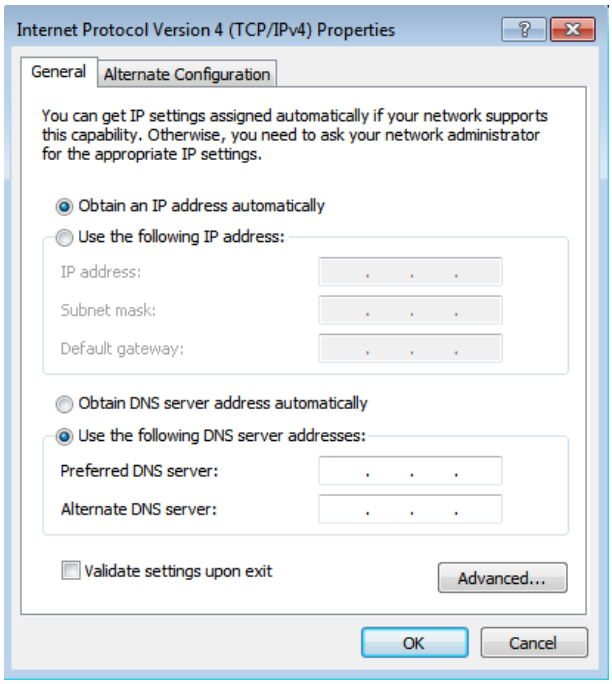
yhteensopivuusongelmaan toimialueella muodostettujen ryhmäsääntöjen osalta. Neuvotteluhuoneen kannettavan tietokoneen verkkolevynäkymät jouduttiin määrittämään jokaiselle käyttäjälle paikallisesti Windowsin omaa Map Network Drive -hallintaa käyttäen.

Organisaatioyksikköihin liitetyt käytännöt tulivat voimaan kaikille siinä organisaatioyksikössä oleville käyttäjille. Käytäntöjen liittämisessä tuli huomioida työntekijöiden asema yrityksessä ja siten rajoittaa tiettyjen verkkolevynäkymien luontia. Tiettyihin kansioihin pääsyä rajoitettiin myös käyttäjäkohtaisilla oikeuksilla. Rajoitukset koskivat pääsääntöisesti yrityksen luottamuksellisia tiedostokansioita.

Muita merkittäviä ryhmäsääntöjä ei luotu, sillä niille ei ollut tarvetta. Kenenkään työntekijän työpöytänäkymää tai Windowsin asetuksia ei muokattu ryhmäsääntöjen avulla. Käytännössä jokaisen Mecatroplan Oy työntekijän tuli saada työasemalleen samanlaiset asetukset ja näkymät kuin muillakin, poislukien muutamia tiettyjä kansioita. Toimialuelaajuisesti vaikuttavaa Default Domain Policy -ryhmäsääntöä kuitenkin muokattiin tilikäytäntöjen osalta. Tilikäytäntöjen Password Policyt määritettiin yrityksen vaatimustasojen mukaisiksi. Vaatimuustasot käsittivät salasanojen minimipituuksien ja voimassaoloaikojen määrittämisen sekä salasanoissa käytettävien erikoismerkkien käyttöönoton. Näillä Password Policy -ryhmäsääntöjen muutoksilla saavutettiin parempi toimialueen tietoturva.

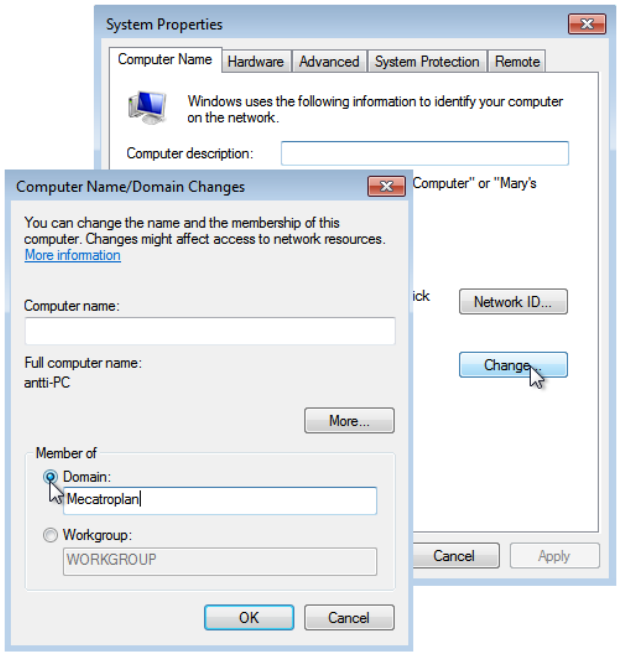
9.10 Työasemien liittäminen toimialueeseen

Mecatroplan Oy yrityksen työasemien liittäminen toimialueeseen tehtiin työntekijöiden poissa ollessa, jolloin mahdollisilta työkatkoksilta vältyttiin. Ennen kuin työasemat voitiin liittää toimialueeseen, tuli niiden verkkoasetuksia muokata DNS-osoitteen osalta (kuvio 16). DNS-osoitteeksi tuli määrittää DNS-palvelimen IP-osoite, jotta työasema osaisi keskustella sen kanssa. Työasemille ei määritetty staattisia IP-osoitteita vaan IP-osoitteet saatiin palvelimeen asennetusta DHCP-palvelusta.



KUVIO 16. Työasemien DNS-määritykset

Työaseman liittäminen toimialueeseen tapahtui järjestelmä-ikkunassa. Computer name, domain and workgroup settings -kohdassa valittiin Change settings, jolloin esille saatiin järjestelmän ominaisuusikkunan Computer Name -välilehti. Tietokoneen toimialuetta päästiin muuttamaan painamalla Change-painiketta. Valitsemalla Member of -valinta ja antamalla oikea toimialueen nimi (mecatroplan) domain kohtaan ilman .local-päätettä saatiin työasema ottamaan yhteyden palvelimelle muodostettuun toimialueeseen. Toimialueelle liittyminen vaati vielä järjestelmävalvojan käyttäjätunnuksen ja salasanan antamisen. Kuviossa 17 voidaan tarkastella työaseman liittämistä mecatroplan.local -toimialueelle.



KUVIO 17. Työaseman liittäminen mecatroplan -toimialueelle

Mecatroplan.local-toimialueelle liitetyt työasemat ilmestyivät toimialueen Computers-kansioon. Sieltä ne siirrettiin niille tarkoitettuun organisaatioyksikköönsä, jolloin niiden hallitseminen muuttui järjestelmällisemmäksi ja tehokkaammaksi.

9.11 AD:n edut

Active Directoryn suurimpina etuina ovat käyttäjien, tietokoneiden, ryhmien ja verkon resussien hallitseminen keskitetysti yhdestä paikasta. Hallittavia käyttäjiä ja tietokoneita voi olla tuhansia. Käyttäjien ja tietokoneiden hallinnassa voidaan käyttää ryhmäsääntöjä, jotka voidaan liittää toimialuelaajuisiksi tai organisaatioyksikkötasolle. Ryhmäsäännöillä voidaan esimerkiksi määrittää pääsy hakemistoobjekteihin tai verkon resursseihin. Käyttäjätilien ja tietokonetilien asetuksia voidaan myös muokata ryhmäsääntöjen avulla. Resurssien keskittäminen yhteen paikkaan mahdollistaa resurssien helpon saatavuuden kaikille käyttäjille.

Käyttäjien autentikointi on keskeinen Active Directoryn tarjoama turvaominaisuus. Autentikoinnissa käytetään Kerberos-tunnistusprotokollaa. Käyttäjät voivat kirjautua toimialueelle mistä tahansa toimialueen työasemasta, mikä helpottaa järjestelmänvalvojan töitä.

Active Directory tarjoaa myös helpon skaalautuvuuden. Active Directory koostuu yhdestä tai useammasta toimialueesta. Jos toimialueita on useita, voidaan toimialueet yhdistää toimialuepuiksi ja toimialuepuut toimialuemetsiksi. Skaalautuvuus tuo mahdollisuuden tehokkaampaan toimialueiden hallintaan sekä tarjoaa helpon resurssien jakamisen toimialueiden välillä.

9.12 Työryhmä ja toimialue

Työryhmä- ja toimialueympäristön ominaisuudet sekä hallinta eroavat toisistaan monella eri tavoin. Työryhmässä tietokoneet muodostavat vertaisverkon, jonka avulla työasemat voivat keskustella suoraan toistensa kanssa sekä jakaa helposti resurssejaan. Työryhmäympäristö on edullinen ja helppo rakentaa, eikä se vaadi järjestelmänvalvojan ylläpitoa. Työryhmäympäristössä toimiviin työasemiin joudutaan hallinnalliset tehtävät suorittamaan paikallisesti. Esimerkiksi käyttäjätilin ja salasanan luonti tulee suorittaa kaikkiin työasemiin, joissa käyttäjän halutaan pystyvän työskentelemään. Tietoturvariskiä kasvattaa se, ettei työryhmäympäristöä ole suojattu millään salasanalla. Tämä tilanne mahdollistaa minkä tahansa samassa aliverkossa toimivan laitteen pääsyn verkon resursseihin. (Microsoft 2012.) Taulukossa 1 voidaan tarkastella työryhmäympäristön ominaisuuksia.

Toimialueympäristö koostuu ohjauspalvelimena toimivasta palvelintietokoneesta, johon muut verkon työasemat ovat yhdistyneet. Työasemat jakavat yhteisen hakemistotietokannan sekä tietoturvakäytännöt. Toimialueympäristössä käyttäjien, työasemien ja verkon resurssien hallinta on keskitetty yhteen palvelintyöasemaan. Tämä vähentää järjestelmänvalvojan töitä ja lisää verkon tehokkuutta sekä tietoturvaa. Käyttäjät voivat kirjautua toimialueelle mistä tahansa työasemalta ja saada heille tarkoitetut resurssit käyttöönsä. Toimialueympäristössä voidaan käyttää ryhmäsääntöjä, joilla voidaan verkon resursseja ja käyttäjäkohtaisia asetuksia määrittää. (Microsoft 2012; Difference Between 2012.) Taulukossa 1 voidaan tarkastella toimialueympäristön ominaisuuksia.

TAULUKKO 1. Työryhmän ja toimialueen vertailua

Työryhmä	**Toimialue**
Käytetää yleensä alle 20 tietokoneen verkoissa	Toimialue voi sisältää tuhansia tietokoneita
Tietokoneet muodostavat vertaisverkon	Toimialueella on yksi tai useampi palvelin tietokone, johon muut työasemat ovat liittyneet
Tietokoneet eivät voi hallita toisiaan	Käyttäjiä, tietokoneita ja ryhmiä hallitaan keskitetysti toimialueen palvelimelta
Jokaiseen tietokoneeseen tulee asettaa käyttäjätili. Jos käyttäjiä on enemmän, tulee jokaisen tili olla kyseisessä tietokoneessa	Toimialueelle muodostettu käyttäjä voi kirjautua mihin tahansa toimialueella olevaan tietokoneeseen omalla käyttäjätunnuksella ja salasanalla
Verkon resurssien jakaminen on helppoa	Verkon resurssit ovat helposti käyttäjien saatavissa. Resurssien jakamista voidaan rajoittaa käyttäjien käyttöoikeuksien mukaan
Työryhmää ei ole sisällä salasanaa, joka heikentää tietoturvaa	Toimialueelle liittyminen vaatii järjestelmänvalvojan salasanan asettamisen

10 TULEVAISUUDEN MAHDOLLISUUDET

10.1 Microsoft Exchange Server

Microsoft Exchange Server 2010 on Microsoftin yhdistettyjen viestintäratkaisujen perusosa. Exchange Server 2010 tarjoaa yritystason sähköposti-, kalenteri- ja yhteystietopalveluita. Exchange Server 2010:n avulla saavutetaan luotettava, tehokas ja yksinkertainen viestintäympäristö. Exchange Server 2010:n tarjoamia palveluita voidaan käyttää monilla viestintätyökaluilla, kuten asiakasohjelmilla työasemissa, selaimilla sekä mobiililaitteilla. (Microsoft 2011.) Microsoft Windows Server 2008 R2 -käyttöjärjestelmäympäristö ja Active Directoryn tarjoamat tunnistuspalvelut sekä tietokannat mahdollistavat tulevaisuudessa Mecatroplan Oy:n hakemistopalvelimen toiminnan laajentamisen sähköpostipalveluiden osalta.

Exchange server 2010 on kiinteästi integroitu AD:hen. Exchange Server hyödyntää AD:n tarjoamia tietokantoja tallentaakseen sen omia tietojaan ja tarkastellessaan käyttäjien tietoja, kuten sähköpostiosoitteita. Exchange Server käyttää myös AD:n reititystopologiaa päättämään, kuinka viestit kulkevat organisaatiossa. AD:n tarjoamat tunnistuspalvelut mahdollistavat käyttäjien kirjautumisen omille sähköpostitileilleen ja Internetistä saapuvien sähköpostiviestien tarkastamisen vastaanottajien osalta. (Stanek 2012, 17.)

10.2 AD:n käyttö yleisesti

Monien yritysten kohdalla AD:n käyttö tulee varmasti yleistymään pienissä ja suurissa yrityksissä, sen tarjoamien monipuolisten ja tehokkaiden ominaisuuksien myötä. AD:n ominaisuudet tarjoavat järjestelmänvalvojalle helpon ja kustannustehokkaan tavan hallita verkon resursseja. Verkon resurssien hallintaa voidaan tehostaa esimerkiksi AD:n tarjoamien ryhmäsääntöjen avulla.

Verkon käyttäjät hyötyvät AD:n käytöstä autentikoinnin kohdalla. Toimialueen työasemille voidaan kirjautua, millä tahansa toimialueen käyttäjätunnuksella, jolloin saadaan sille käyttäjälle tarkoitetut resurssit käyttöön. Tämä vähentää käyttä-

jätunnuksien määrää, helpottaa järjestelmänvalvojan työtä sekä luo toimivan ympäristön.

11 YHTEENVETO

Tämän opinnäytetyön tavoitteena oli luoda Active Directory -verkkojärjestelmä Mecatroplan Oy:lle, joka soveltui yrityksen tarpeisiin. Työn teoriaosuudessa käsiteltiin Active Directoryn perusominaisuuksia, huomioitavia seikkoja toteutusta suunniteltaessa, järjestelmänvalvojaa helpottavia toimialueen hallintamahdollisuuksia sekä TCP/IP-tekniikkaa.

Active Directoryn suunnittelu aloitettiin syksyllä 2011 Mecatroplan Oy -yrityksen johtohenkilökunnan kanssa. Suunnittelu koostui DNS-nimiavaruudesta, organisaatioyksikkörakenteesta, käyttäjistä ja ryhmäsäännöistä. Suunnittelu vietiin huolellisesti loppuun, minkä jälkeen toteutus oltiin valmiina suorittamaan.

Mecatroplan Oy:llä aikaisemmin käytössä ollut Windows-työryhmäkäytäntö ei vastannut yrityksen tarpeita, joten toimialuekäytäntöön siirtyminen oli hyvä ratkaisu. Uuden järjestelmän myötä merkittävimpiä muutoksia vanhaan järjestelmään oli käyttäjien ja resurssien hallinta, oikeuksien määrittäminen ja yleisen tietoturvan kasvaminen. Oikeuksien määrittämisellä varmistettiin käyttäjien pääsy vain heille tarkoitettuihin hakemistoihin.

Mecatroplan Oy:n looginen rakenne koostui yhdestä toimialueesta, joka muodosti myös toimialuemetsän. Yksi toimialue yksinkertaisti verkon hallinnointia, eikä toimialueiden välistä replikointiliikennettä tarvinnut ottaa huomioon. Toimialueen muodostuksessa käytettiin hyväksi ylimmän tason toimialuetunnusta .local, jolloin hallinnan tarve saatiin rajoitettua vain sisäiseen nimiavaruuteen.

Mecatroplan Oy:n toimialueen käyttäjille määritettiin yhdenmukaiset käyttäjänimet, jolloin saavutettiin helpompi käyttäjien muistaminen ja etsiminen toimialueelta. Toimialueen organisaatioyksikkörakenne määritettiin kuvastamaan Mecatroplan Oy:n organisaatiota. Organisaatioyksikön käyttäjät ja tietokoneet erotettiin toisistaan, jolloin hallinta saatiin paljon tehokkaammaksi.

Kokonaisuudessaan Active Directory -projekti onnistui tavoitteiden mukaisesti. Ongelmat projektin aikana olivat vähäiset, mistä voitiin päätellä, että suunnittelu-

työ oli tehty oikein. Yhtenä ongelmana oli käyttäjien verkkolevynäkymien ilmaantuminen neuvotteluhuoneen tietokoneelle. Ongelma jouduttiin ratkaisemaan luomalla verkkolevynäkymät erikseen paikallisesti.

Tulevaisuudessa Mecatroplan Oy:llä on mahdollisuus laajentaa hakemistopalvelintaan sähköpostipalvelun osalta. Windows Server 2008 R2 -palvelinkäyttöjärjestelmä ja Active Directory-arkkitehtuuri tarjoavat sähköpostipalvelulle toimintaympäristön, tunnistusmenetelmät ja tietokannat. AD:n tarjoamat palvelut ovat hyvin käyttäjäystävällisiä ja tulevaisuudessa palveluita tullaan kehittämään yhä käyttäjäystävällisemmiksi, jolloin palveluiden ominaisuudet ja tehokkuus paranevat.

LÄHTEET

Anttila, A. 2000. TCP/IP tekniikka. Juva: WSOY-kirjapainoyksikkö.

Difference Between 2012. Difference Between Workgroup and Domain [viitattu 28.2.2012]. Saatavissa: http://www.differencebetween.net/technology/difference-between-workgroup-and-domain/

Everyjoy 2006. Workgroup vs Domain: What´s the difference? [viitattu 7.2.12]. Saatavissa: http://everyjoe.com/technology/57-2/

IETF 2012. RFC 2131, Dynamic Host Configuration Protocol [viitattu 21.2.2012]. Saatavissa: http://www.rfc-editor.org/rfc/rfc2131.txt

Kivimäki, J. 2003. Inside Active Directory, Verkonhallinta.
Helsinki: Edita Prima Oy.

Kivimäki, J. 2005. Windows Server 2003, Active Directory
Jyväskylä: Gummerus.

Kivimäki, J. 2009. Windows Server 2008 R2, Tehokas hallinta.
Hämeenlinna: Kariston Kirjapaino Oy.

Mecatroplan Oy 2012. [viitattu 2.2.12]. Saatavissa:
http:// http://www.mecatroplan.com/index.php

Microsoft 2011. Exchange Server [viitattu 26.2.2012]. Saatavissa: http://www.microsoft.com/businessproductivity/fi/fi/products/exchange-server.aspx

Microsoft 2012. Miten toimialue, työryhmä ja kotiryhmä eroavat toisistaan? [viitattu 7.2.12]. Saatavissa: http://windows.microsoft.com/fi-FI/windows7/What-is-the-difference-between-a-domain-a-workgroup-and-a-homegroup

Microsoft TechNet 2012a. How TCP/IP Works [viitattu 21.2.2012]. Saatavissa: http://technet.microsoft.com/enus/library/cc786128%28v=ws.10%29.aspx

Microsoft TechNet 2012b. Introduction to Administering SYSVOL [viitattu 13.2.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/cc778037%28WS.10%29.aspx

Microsoft TechNet 2012c. Using Active Directory Service [Viitattu 17.1.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/bb726976.aspx

Microsoft TechNet 2012d. What Are Domains and Forests? [Viitattu 16.1.2012]. Saatavissa: http://technet.microsoft.com/dede/library/cc759073%28WS.10%29.aspx#w2k3tr_logic_what_orxw

Microsoft TechNet, 2012e. What Is DHCP? [viitattu 21.2.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/cc781008%28v=ws.10%29.aspx

Microsoft TechNet 2012f. Active Directory Domain Services Overview [viitattu 2.2.2012]. Saatavissa: http://technet.microsoft.com/enus/library/cc731053%28WS.10%29.aspx

Petri IT Knowledgebase 2009. Understanding Windows Server 2008 Active Directory Domain and Forest Functional Levels [viitattu 13.2.2012]. Saatavissa: http://www.petri.co.il/understanding-windows-server-2008-active-directory-domain-and-forest-functional-levels.htm

SearchNetworking 2000. TCP/IP (Transmission Control Protocol/Internet Protocol) [viitattu 21.2.2012]. Saatavissa: http://www.searchnetworking.techtarget.com/definition/TCP-IP

Spector CNE, 2012. Domain vs Workgroup [viitattu 7.2.12]. Saatavissa: http://www.spectorsoft.com/products/spectorcne_windows/help/v43/deployment/Domain_vs_Workgroup.htm

Stanek W. R. 2003. Microsoft Windows Server 2003. Asiantuntijan käsikirja. Helsinki: Edita Prima Oy.

Stanek W. R. 2010. Microsoft Exchange Server 2010. Administrator´s Pocket Consultant.
Redmond, Washington: Microsoft Press.

Vicomsoft 2012. DHCP [viitattu 21.2.2012].
Saatavissa: http://www.vicomsoft.com/learning-center/dhcp/

Web Based Programming Tutorials 2012. TCP/IP Network Architecture [viitattu 21.2.2012]. Saatavissa: http://www.webbasedprogramming.com/Java-Unleashed-Second-Edition/f23-1.gif

WebJunction 2005. Illustration of a peer-to-peer network [Viitattu 9.2.12].
Saatavissa: http://www.webjunction.org/networking/articles/content/437741

Wikibooks 2011. CCNA Certification/Application Layer [viitattu 21.2.2012].
Saatavissa:
http://upload.wikimedia.org/wikipedia/commons/2/28/DHCP_session_en.svg