TEKNIIKKA JA LIIKENNE

Tietotekniikka

Tietoverkot

Insinöörityö

VIRTUAALIYMPÄRISTÖN SUUNNITTELU JA TESTAUS MICROSOFT WINDOWS SERVER 2008 ACTIVE DIRECTORYN KONFIGUROINTI –KURSSIA VARTEN

Työn tekijät: Aleksi Renvall
Työn ohjaajat: Janne Salonen

Työ hyväksytty: ___. ___. 2009

Janne Salonen
Yliopettaja

ALKULAUSE

Tämä insinöörityö tehtiin Metropolia Ammattikorkeakoululle. Yliopettaja Janne Salosen Microsoft Configure Windows Server 2008 Active Directory kurssia varten. Kiitän Janne Salosta ja laboratorioinsinööri Tapio Wikströmiä pitkäjännitteisyydestä ja joustavuudesta sekä ammattimaisista ohjeista ja neuvoista.

Helsingissä 30.11.2009

Aleksi Renvall

TIIVISTELMÄ

Työn tekijä: Aleksi Renvall	
Työn nimi: Virtuaaliympäristön suunnittelu, luominen ja testaus Microsoft Windows Server 2008 Active Directoryn konfigurointi -kurssia varten	
Päivämäärä: 30.11.2009	**Sivumäärä:** 43 s.
Koulutusohjelma: Tietotekniikka	**Suuntautumisvaihtoehto:** Tietoverkot
Työn ohjaaja: Yliopettaja Janne Salonen	

Tämä insinöörityö käsittelee Windows Server 2008 Active Directoryn konfiguroimista virtuaaliympäristössä kurssia varten, virtuaaliympäristön sunnittelua ja testausta. Työ tehtiin Metropolia Ammattikorkeakoululle. Työssä esitellään käytetyt laiteet, ohjelmistot ja kerrotaan työympäristöstä. Työssä esitellään myös Microsoft Windows Server 2008 ja Active Directory versiohistorioineen sekä ominaisuuksineen.

Työtä varten suunniteltiin ja toteutettiin virtuaalikoneiden vaatimukset ympäristöä varten. Työn aikana suunniteltiin, millä virtuaalikoneiden asetuksilla kurssi tullaan suorittamaan ja mitkä harjoitukset Microsoftin materiaalista otetaan mukaan kurssille. Kaikki kurssille otetut harjoitukset testattiin virtuaalikoneella ja ongelmien varalle luotiin laboratoriomanuaali tarkentamaan harjoitusmateriaalissa esiintyviä virheitä tai antamaan lisäohjeita.

Virtuaaliympäristön konfiguroinnin valmistuttua luotiin 24 virtuaalikonetta tarvittavin asetuksin kurssia varten. Virtuaalikoneille suunniteltiin ja luotiin osoiteavaruus ja ne laitettiin koulun verkkoon. Virtuaaliympäristö otettiin käyttöön kurssin alkaessa marraskuussa 2009.

Avainsanat: Windows Server, Active Directory, virtuaalikone

ABSTRACT

Name: Aleksi Renvall

Title: Planning, creating and testing virtual environment for Configuring Microsoft Windows Server 2008 Active Directory

Date: 30.11.2009 **Number of pages:** 43 p.

Department: Information Technology

Study programme: Data Networks

Instructor: Janne Salonen

This final project examines configuring Microsoft Server 2008 Active Directory, creating and testing a virtual environment for the course. Project was accomplished for Metropolia. Project introduces used equipments, softwares and working environment. Project also introduces Microsoft Windows Server 2008 and Active directory with version history and some features.

Requirements of virtual machines was planned and tested. During the project was tested which properties of virtual machines were needed to complete the course and what exercises were taken to the actual course. All the exercises taken to course were tested with virtual machine. For the problem situations and extra instruction for the course was laboratory manual created.

After finishing virtual environment configuring 24 virtual machines were created with all the specific requirements. Address space for the virtual machines was planned and created in Metropolia's network. Virtual machine environment was taken to use in November 2009.

Keywords: Windows server, Active Directory, virtual machine

SISÄLLYS

1 JOHDANTO

Tämän työn tarkoituksena on testata harjoitukset materiaalista Microsoft Windows Server 2008 Active Directory Self-paced Training –kit. Niiden pohjalta luotiin virtuaaliympäristö koulun *palvelinklusteriin*, jossa harjoituksia tullaan tekemään VMware-virtuaalikoneella. Virtuaaliympäristöllä tulee olemaan 24 käyttäjää samanaikaisesti. Kaikkien käyttäjien tulee pystyä samanaikaiseen itsenäiseen työskentelyyn.

Työ esittelee ohjelmiston, laitteiston sekä palvelinalustan. Työ esittelee myös yleisesti Windows Server 2008 -palvelimen, jonka ominaisuus Active Directory on. Pääpaino työssä on Active Directoryn uusien ominaisuuksien, sekä Training Kit –harjoitusten esittely.

Suunnitteluosa syventyy verkkoympäristön rakentamiseen ja virtuaalikoneiden luomiseen. Suunnitteluosassa kerrotaan myös virtuaalikoneiden alustamisesta oikeilla asetuksilla kurssia varten. Harjoitukset, jotka kurssilla on tarkoitus tehdä, tullaan testaamaan. Niiden pohjalta luodaan laboratoriomanuaali mahdollisten policy–ohjeissa ilmenevien virheiden varalle. Laboratoriomanuaali toimii myös lisäohjeena harjoitusten onnistuneeseen suorittamiseen.

2 KÄYTETYT OHJELMAT JA LAITTEISTOT

Ympäristönä työlle käytettiin VMware ESX –järjestelmää, joka on asennettu Metropolian palvelimien muodostamaan alustana toimivaan palvelinklusteriin. Järjestelmää käytetään WMvare Infrastructure Client -ohjelman kautta. Virtuaalikoneisiin on myös mahdollista ottaa yhteys Remote Desktop Connection –ohjelman avulla.

Metropolian palvelinklusterina toimiva alusta virtuaalikoneille koostuu kuudesta korttipalvelimesta. Kolme palvelinta on Dell PowerEdge 1855 ja kolme Dell PowerEdge 1955 palvelimista. 1855–sarjan palvelimissa on jokaisesa kaksi Xeon-prosessoria, jotka toimivat 3 GHz:n kellotaajuudella ja sisältävät muistia kahdeksan gigatavua. 1955-sarjan palvelimissa taas on kaksi Xeon E5345 2.33GHz –prosessoria ja 16 gigatavua muistia. 1855–sarjan palvelimille on varattu leyvytilaa 1,3 teratavua ja 1955–sarjan palvelimille 1,4 teratavua. Palvelinklusterien välille on varattu 900 gigatavua ylimääräistä muis-

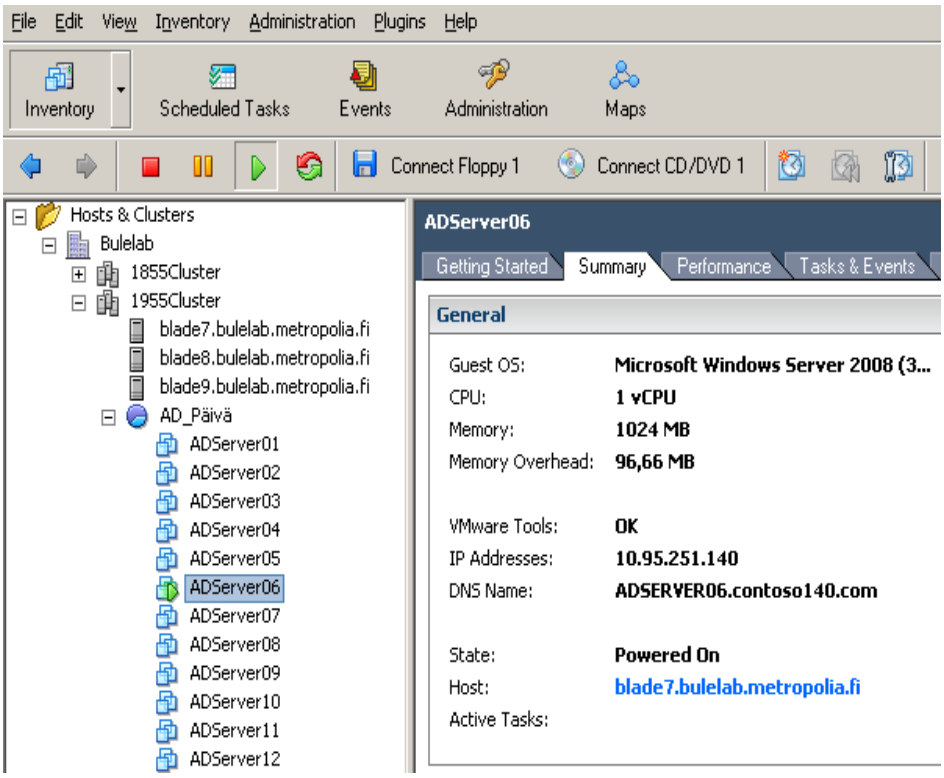
tia. Palvelimien yhteysprotokollana levyjärjestelmiin toimii Internet Small Computer System Interface (iSCSI). [11.]

Kuva 1. Dell Power Edge kehikko [14]

Kussakin palvelmisessa on kaksi verkkokorttia, jotka ovat yhteydessä kehikon takana sijaitseviin kahteen kytkimeen. Toinen kytkimistä toimii verkkoliikenteen ylläpitäjänä ja toinen on liitetty Dell AX 150i–levyjärjestelmään. Virran systeemiin tuo kolme kytkettyä virtalähdettä. Neljäs virtalähde on varalla ongelmatilanteita varten. [11.]

2.1 VMware ESX

Palvelimissa toimii omalla VMkernelillä toimiva itsenäinen käyttöjärjestelmä VMware ESX, joka on suunniteltu palveluiden virtualisointiin. Alustana ESX mahdollistaa kymmenien virtuaalikoneiden samanaikaisen käytön. Käyttöjärjestelmä kykenee itse jakamaan fyysisen koneen resursseja virtuaalikoneiden käyttöön koneiden tarpeiden mukaisesti. ESX:ää hallitaan VirtualCenter -työkalulla, VirtualCenterillä voidaan hallita useaa ESX–serveriä samanaikaisesti. [7.]



Kuva 2. Nykymä kurssin virtuaalikoneista VMware:lla

VMware mahdollistaa isäntäkoneesta riippumattomat täysin simuloidut virtuaalikoneet. Systeemi virtualisoi järjestelmän oleellisimman laitteiston, kuten verkkosovittimet, kiintolevyn, näytönohjaimet ja äänilaitteet. Myös USB-laitteen voi sillata simuloituun virtuaalikoneeseen. VMware:lla on mahdollista simuloida myös ylimääräisiä laitteita. CD- tai DVD–aseman voi liittää ISO-levykuvana esimerkiksi kovelevyksi. Isäntäkoneelle ei ole virtuaalikoneista minkään suuruista riskitekijää. [7.]

2.2 Remote Desktop Connection

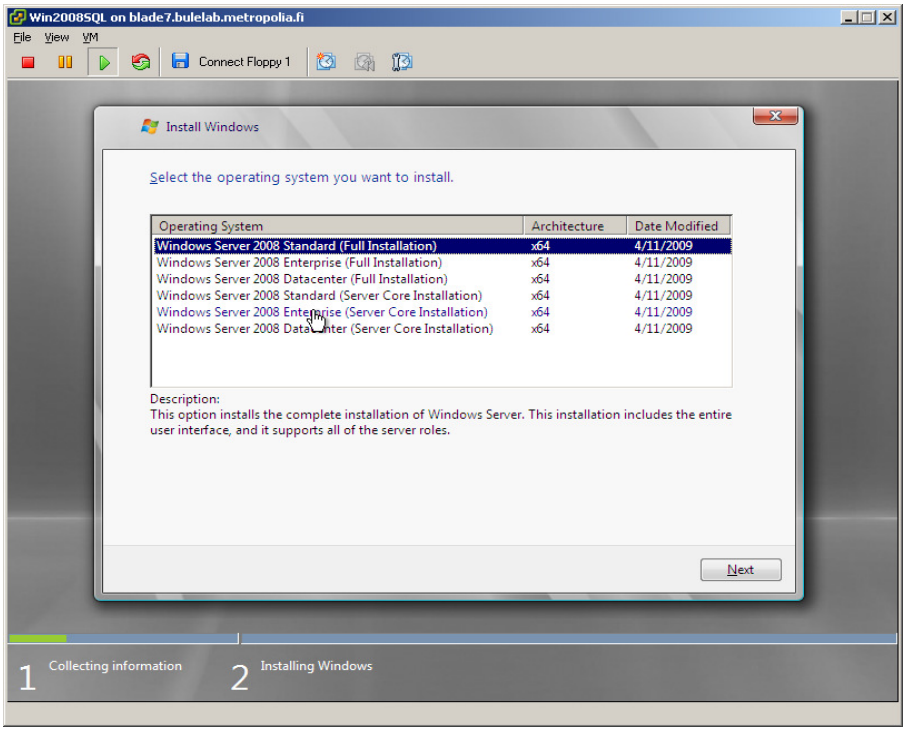
Toinen tapa ottaa yhteys virtuaalikoneisiin Metropolian palvelinklusterissa on Remote Desktop Connection (RDC). Remote Desktop Connection on sisällytetty Microsoftin Windows -käyttöjärjestelmiin. Sovellus sallii käyttäjän etäyhteyden koneeseen. Etäyhteys voi olla luotu palvelinklusteriin fyysisesti tai virtuaalisesti. Virtuaalikoneen käyttöjärjestelmästä tulee sallia *Remote Desktop Connection -toiminto* ennen kuin yhteydenotto on mahdollista. Virtuaalikoneeseen saadaan yhteys syöttämällä koneen IP-osoite (Internet Protocol) Remote Desktop Connectionin kirjautumissivulla. [8.]

Kuva 3. Remote Desktop Connection –ohjelmalla sisäänkirjautuminen

2.3 Windows Server 2008

Microsoft Windows Server 2008 -palvelinjärjestelmä julkaistiin 27. helmikuuta 2008. Windows Server 2008 on rakennettu perustuen NT 6.x -koodiin. Sen edeltäjä Microsoft Windows Server 2003 ehti palvella viisi vuotta ennen kuin paremmalla hallinnoinnilla, luotettavuudella ja turvallisuudella varustettu Windows Server 2008 korvasi sen. Windows Server 2008 on saatavilla useana eri versiona tarpeista riippuen. [2.]

- Windows Server 2008 Standard
- Windows Server 2008 Enterprise
- Windows Server 2008 Datacenter
- Windows HPC Server 2008
- Windows Web Server 2008
- Windows Storage Server 2008
- Windows Small Business Server 2008
- Windows Essential Business Server 2008
- Windows Server 2008 for Itanium-based Systems
- Windows Server 2008 Foundation.



Kuva 4. Windows Server 2008 Standard -version asennus

Miltei kaikki asennusmahdollisuudet tukevat sekä 32-bittistä että 64-bittistä versiota Windowsista. Windows Server 2008 on mahdollista asentaa myös Server Core -tilassa, joka ei vaadi ollenkaan Windows Exploreria, vaan toimii komentoriviltä. [3.]

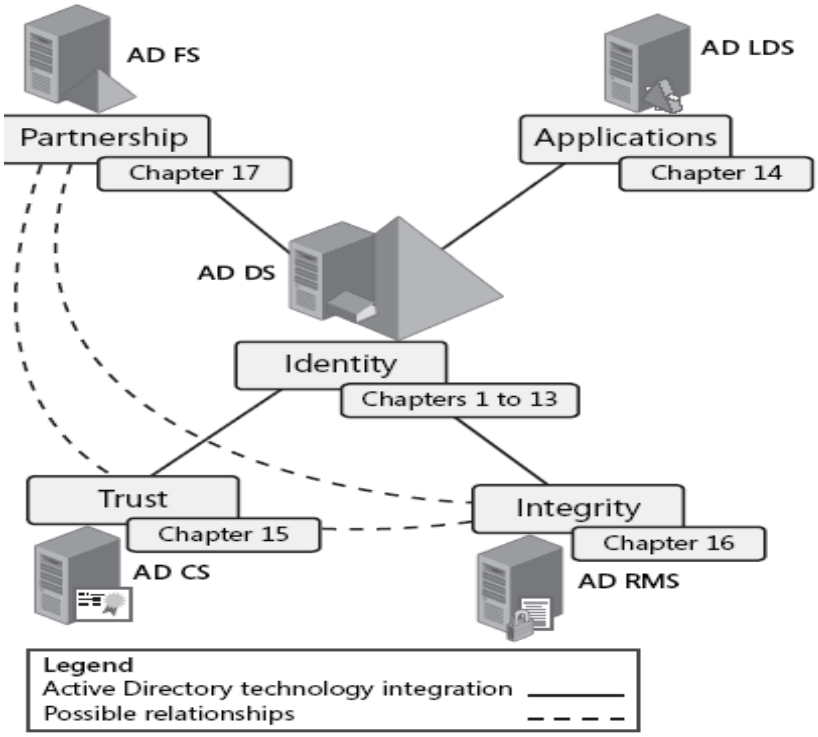
Windows Server 2008 pohjautuu Windows NT 6.0 Service Packiin, jota pidetään ensimmäisenä Service Packinä. Ensimmäinen virallinen Service Pack kantaa nimeä Servise Pack 2, joka julkaistiin 24. lokakuuta 2008. Service Pack 2 sisältää samat parannukset ja päivitykset kuin Windows Vista Service Pack 2 sekä viimeisimmän version Hyper-V 1.0:n. [3.]

Toinen julkaisu nimeltään Windows Server 2008 R2 julkaistiin 22. Heinäkuuta 2009. Tärkeimpinä uudistuksinaan kehittynyt virtaulisointikyky, sekä uudet Active Directory ominaisuudet. [3]

3 MICROSOFT ACTIVE DIRECTORY

Active Directory (AD) on teknologia, jonka Microsoft on luonut hakemistopalveluksi, autentikointiin sekä nimipalvelujärjestelmä (DNS)-pohjaiseen verkkoinformaatioon. Active Directoryn toiminta perustuu Windows–ympäristöön

ja on päätehtäviltään tietokanta verkon resursseista, käyttäjistä ja tietokoneista. Active Directory noudattaa Identity and Access (IDA)-rakennetta. Active Directory mahdollistaa yritysten ja muiden hallintaa vaatien pienten tai suurten verkkojen organisoidun ja suojatun tavan hallita käyttäjiä ja sovelluksia. Active Directory on erittäin tehokas työkalu. Sillä voi hallinnoida joko muutaman tietokoneen verkkoa tai kokonaisia eri puolille maailmaa sijoitettuja serverifarmeja. Active Directoryn hallinto (Administrator) voi lisätä toimintaohjeita, ottaa käyttöön ohjelmia sekä anoa tärkeitä päivityksiä verkolle. Active Directory on rakennettu toimimaan Microsoft Windows Server 2000:n, Microsoft Windows Server 2003:n ja Microsoft Windows Server 2008:n ominaisuutena. [4.]



Kuva 5. IDA rakentuu viidestä komponentista. [9]

3.1 Versiohistoria

Active Directory esiteltiin ensimmäistä kertaa vuonna 1999 ja julkaistiin yleiseen käyttöön vuonna 2000, Windows Server 2000:n ilmestymisen yhteydessä. Active Directoryn toiminta perustuu Windows Serverin olemassaoloon. Active Directory saa viimeisimmän päivityksen, kun Windows Serverille ilmestyy Service Pack tai uudempi versio Windows Serveristä. [4.]

Huhtikuussa 2003 ilmestenyt Windows Server 2003 toi mukanaan Active Directoryyn laajemman toimintason (Functional Level) ja kehittyneemmän hallinnallisuuden. Joulukuussa 2005 Microsoft julkisti Windows Server 2003 R2:n, jonka parannukset Active Directoryn osalta liittyivät pääosin käyttäjätileihin. [4.]

Helmikuun 27. 2008 julkistettu Windows Server 2008 ja heinäkuussa julkistettu Windows Server 2008 R2 paransivat Active Directoryn toimintaa tunnistamisessa, sertifikoinneilla ja oikeuksienhallintapalveluilla. Windows Server 2008 Active Directoryn keskeisin rooli on Active Directory Domain Services (AD DS), joka hallinnoi tietokoneille asetettuja toimintaohjeita ryhmille, käyttäjille ja tukee uusien sovellusten samanaikaisesti lisäämistä tietokoneille. Muita uusia palveluita ovat Active Directory Federation Services (AD FS), Active Directory Lightweight Directory Services (AD LDS), Active Directory Certificate Services (AD CS) ja Active Directory Rights Management Services. (AD RMS). Windows Server 2008:n myötä tuli myös nimi Active Directory Domain Services, entinen nimi Active Directory Directory Services. Vanhemmissa Microsoftin dokumenteissa nimi oli NT Directory Service (NTDS), joka voi yhä esiintyä joissain Active Directory -binääreissä. [4.]

3.2 Objektit

Active Directory käsittelee toimintaansa sekä rakentuu hierarkisista objekteista. Objekti voi olla käyttäjä, systeemi, resurssi tai palvelu. Active Directory pystyy jäljittämään useita objekteja samanaikaisesti. Haku helpottuu, koska objektit voivat jakaa yhteisiä atribuutteja. Objektit voidaan jakaa kahteen kategoriaan, resursseihin ja turvallisuusperusteisiin. Kukin objekti edustaa itsenäistä kokonaisuutta. Objektit voivat sisältää toisia objekteja, administraattorin jakamista hallintaoikeuksista riippuen. [4.]

3.3 Metsät, puut ja toimialueet

Active Directoryn rakenteen korkeimmalla tasolla on metsä (forest). Metsä on kokoelma kaikista objekteista, niiden atribuuteista ja säännöistä. Metsä koostuu yhdestä tai useammasta puusta (tree). Puu sisältää toimivia toimialueita (domain) ja on kokoelma yhdestä tai useammasta toimialueesta eli toimivasta systeemistä. Esimerkiksi, *contoso.com.* [4]

Toimialueet tunnistetaan nimipalvelinjärjestelmän avulla nimiavaruudesta (namespace). Toimialueiden objektit sijoitetaan containereihin (container) nimeltä Organizational Units (OU). OU:t luovat toimialuehierarkian, jonka administraattorilupia ja oikeuksia myöntämällä konfiguroi verkolle sopivaksi käyttäen Group Policyä. Group Policy on toimintaohje, joka koostuu Group Policy -objekteista. Myös OU voi sisältää yhden tai useamman alemman OU:n. Hallittavuuden kannalta Microsoftin toimintaohjeet suosittelevat mahdollisimman vähän toimialueita yhtä Active Directoryä kohden.

3.4 Domain Controller

Domain Controller (DC) toimii ohjauskoneserverinä Active Directoryssä. Niiden tehtävänä ylläpitää toimialueen tietokannan resursseja ja tunnistaa toimialueelle kirjautuvat käyttäjät. Ensimmäinen toimialue luodaan automaattisesti Global Catalog (GC) Domain Controlleriksi. GC-serveri on kirjoituksen salliva (writable) Domain Controller, joka replikoi objekteja servereiden välillä. [5.]

Read-only Domain Controller on uudentyyppinen Domain Controller, jonka Windows Server 2008 toi markkinoille. Sen tarkoitus on mahdollisuus sijoittaa Doamin Controller paikkaan, jossa fyysinen turvallisuus ei ole itsestään selvää. RODC mahdollistaa vain lukemisen. Sen konfiguraatiota ei voi muuttaa, joten se toimii haarakonttoreiden ohjauskoneena haastavissa sijainneissa. [6.]

4 SUUNNITTELU JA TOTEUTUS

Kurssille suunniteltiin alusta asti 24 virtuaalikonetta, yksi oppilasta kohden. Virtuaalikoneet tultaisiin luomaan Metropolia Ammattikorkeakoulun palvelinklusteriin. Virtuaalikoneisiin tultaisiin ottamaan yhteys Microsoft Remote Desktop Connection tai VMware Infrastructure Client –ohjelmilla.

Kurssilla suoritettavat harjoitukset perustuvat kirjaan Configuring Microsoft Server 2008 Active Directory Selfpaced Training-Kit. Kirja koostuu materiaalista, joka esittelee Active Directoryn ja Server 2008 mukana tulleet uudistukset. Kirjassa on 17 kappaletta, jokaisessa noin kuudesta kahteentoista harjoitusta. Materiaalia alustavasti läpi käydessä törmättiin ongelmaan. Met-

ropolian palvelinklusterin kovalevytila mahdollistaisi kunkin oppilaan käyttöön vain yhden virtuaalikoneen. Kirjan kappaleiden 1 – 8 harjoitukset onnistuttaisiin tekemään yhdellä virtuaalikoneella ja kappaleiden 9 – 17 harjoitukset vaativat kaksi tai useamman virtuaalikoneen. Käyttöön päätettiin myöhemmin asettaa toinen virtuaalikone ja testata, onko kurssille mahdollista ottaa mukaan harjoituksia kappaleista, jotka vaativat kaksi virtuaalikonetta. Testauksessa todettiin, että tähän ei ollut mahdollisuutta ja tämän insinöörityön pääpaino tulee olemaan kappaleiden 1 – 8 harjoituksissa. Loppukappaleiden ominaisuudet esitellään teoriatasolla. Kaikki harjoitukset kurssille tulevista kappaleista tehtiin, mutta suuren määrän vuoksi niistä vain oleellisimmiksi katsotuista kerrotaan tarkemmin tässä työssä.

4.1 Suunnittelu

Tavoitteeksi asetettiin, että kurssin alkaessa virtuaalikoneet asetuksineen olisi luotu palvelinklusteriin Windows Server 2008 valmiiksi asennettuna. Oppilaiden tulisi ensimmäisellä tunnilla asentaa itse koneisiin Active Directory Domain Services. Osana AD DS -asennusta nimipalvelin asentuisi oletusasetuksena. Harjoituksissa vastaan tulevat ohjelmat päätettiin asentaa valmiiksi virtuaalikoneen C-asemalle tehtyyn Setup–kansioon. Muutoin ongelmaksi olisi voinut koitua tiedostojen siirtäminen virtuaalikoneille.

Virtuaalikoneet suunniteltiin laitettaviksi samaan verkkoon peräkkäiin IP-osoitteisiin. Kurssin ensimmäisellä tunnilla kullekin oppilaalle jaettaisiin yksilöllinen IP-osoite, jonka mukaan otetaan yhteys omaan virtuaalikoneeseen WMvare Infrastructure Client tai Remote Desktop Connection ohjelmien -avulla. Virtuaalikoneet ja toimialueet tulisi tämän vuoksi nimetä yksilöllisesti Active Directory Domain Services asennettaessa ensimmäisellä oppitunnilla. Virtuaalikoneille päätettiin antaa seuraavat tiedot. (virtuaalikoneen numero = XX)

- IP-osoite 10.95.251.1XX (10.95.251.135 – 10.95.251.158)
- Nimi: ADServerXX
- WMvare nimi: ADServerXX
- Toimialue: contosoXX.com.

Materiaalin esimerkeissä on toimialueena contoso.com ja koneen nimenä SERVER01. Suunniteltaessa kurssia haluttiin nimien vastaavan mahdolli-

simmin paljon näitä nimiä. Harjoituksia oli helpoin seurata nimillä, jotka vastaavat mahdollisimman paljon harjoitusmateriaalin nimiä.

4.2 Alkuvalmistelut

Testaamista ja harjoitusten läpikäymistä varten luotiin virtuaalikone samaan ympäristöön palveliklusteriin, jossa kurssi tultaisiin käymään. Virtuaalikoneen luomisen jälkeen lähdettiin käymään läpi oppimateriaalia ja harjoituksia kappale kerrallaan. Ensimmäinen kappale alkaa Windows Server 2008 Standard Editionin asennuksella oikeiden asetusten mukaisesti. Minimivaatimukset asennukselle vaativat seuraavaa.

- 512 Megatavua muistia
- 10 Gigatavua kovalevytilaa
- x32 tai x64 –bittisen prosessorin.

Virtuaalikoneisiin päätettiin kuitenkin laittaa muistia ja kovalevyä kaksinkertainen määrä, jotta se varmasti riittäisi ja tarvittaessa olisi varaa asentaa uusia ohjelmia sekä tallentaa tiedostoja ja uutta tietoa koneille. Virtuaalikone nimettiin Trainin-Kit -harjoitusmateriaalin mukaisesti. IP-osoite valittiin koulun verkkoon sopivaksi.

- Toimialue: contoso.com
- Kone: SERVER01
- IP: 10.95.251.102.

4.3 Active Directory Domain Services

Active Directory Domain Services (AD DS) on koko Active Directoryn toiminnan alusta. AD DS asennetaan Windows Server 2008 -asennuksen jälkeen. Kun AD DS on asennettu, on Active Directory valmis yksityiskohtaisempaan konfigurointiin. [9.]

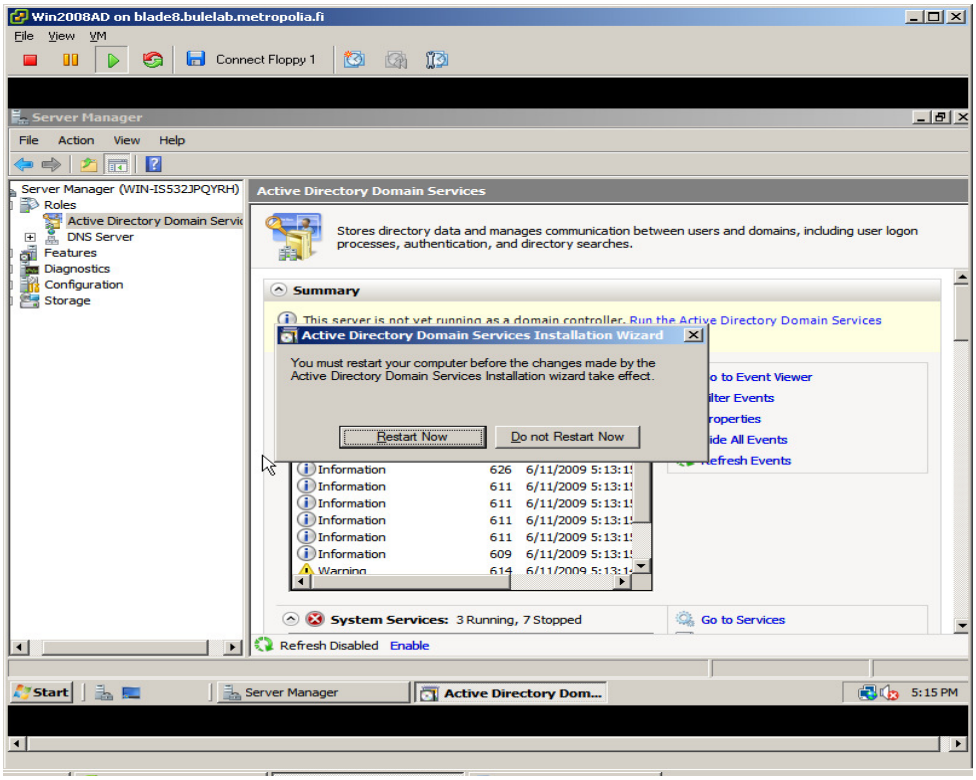
4.3.1 Active Directory Domain Services -asennus ja roolit

Windows Server 2008 Standard Editionin asentamisen jälkeen koneelle annettiin nimi SERVER01. Internet-protokollaksi valittiin TCP/IPv4 ja koneeseen asennettiin kaikki muutkin verkon vaatimat IP-osoitteet. [9.]

- Aliverkonmaski: 255.255.254.0

- Oletus yhteyskäytävä: 10.95.251.254
- Nimipalvelin osoite: 10.95.254.252.

Seuraavaksi asennettiin Server Managerin kautta Active Directory Domain Services -rooli. Kun Installation Wizardilla oli asennettu AD DS -rooli, ajettiin Windows Explorerissa komento Dcpromo.exe. Tämä komento laukaisee Domain Controllerin, toimialueen ja metsän luomiseen tarvittavan Installation Wizardin. Asennuksen aikana määriteltiin uusi toimialue (contoso.com) uuteen metsään. Nimipalvelin asentuu automaattisesti toimialueen nimeämisen yhteydessä. Toimintatasoksi valitaan Windows Server 2008. Valitsemalla tämä toimintataso edellyttää se kaikkien metsän toimialueiden toimivan Windows Server 2008 -toimintatasolla. Korkein toimintataso mahdollistaa Windows Server 2008 mukana tulleet uudet ominaisuudet. Domain Controller -tyypiksi valitaan Global Catalog, joka on aina ensimmäinen Domain Controller-metsässä. Uudelleenkäynnistyksen jälkeen AD DS oli valmis konfiguroitavaksi. [9.]



Kuva 6. AD DS -asennus vaatii uudelleenkäynnistyksen

4.3.2 Server Core

Maksimiturvallisuuden saavuttaminen Domain Controllerina toimivalle serverille on Server Core -asennus, joka on minimiasennus Windowsista. Server Corea hallitaan komentoriviltä ja se voidaan asentaa myös etäasetuksena. Testauksessa Server Coren asentamista harjoiteltiin virtuaalikoneella asentamalla Windows Server 2008 uudelleen alusta asti. Koska käytössä oli tässä vaiheessa vain yksi virtuaalikone, tuli Server Core -asennuksen jälkeen tehdä ensimmäinen harjoitus AD DS -asennuksesta uudelleen. Tämän vuoksi Server Coren asennus päätettiin jättää pois kurssilta.

Server Coren asennuttua CD-levyltä konfiguroitiin ipv4 toimimaan.

netsh interface ipv4 set address name="Local Area Connection"

source=staticaddress=10.95.251.102 mask255.255.254.0 gatewaynetsh 10.95.251.254 interface ipv4 set dns name="Local Area Connection" source=static address=10.95.251.102

Seuraavaksi luotiin Domain Controller.

*dcpromo/unattend/replicaOrNewDomain:replica/replicaDomainDNSName:contoso.com /ConfirmGC:Yes /UserName:CONTOSO\Administrator /Password: * /safeModeAdminPassword:P@ssword*

AD DS -roolin asennuttua serveri käynnistyy uudelleen. Server Coreen voidaan lisätä tai poistaa rooleja komennolla:

Ocsetup.exe.

Domain Controller poistettiin komennolla.

/unattend /AdministratorPassword:password

4.4 Hallinto

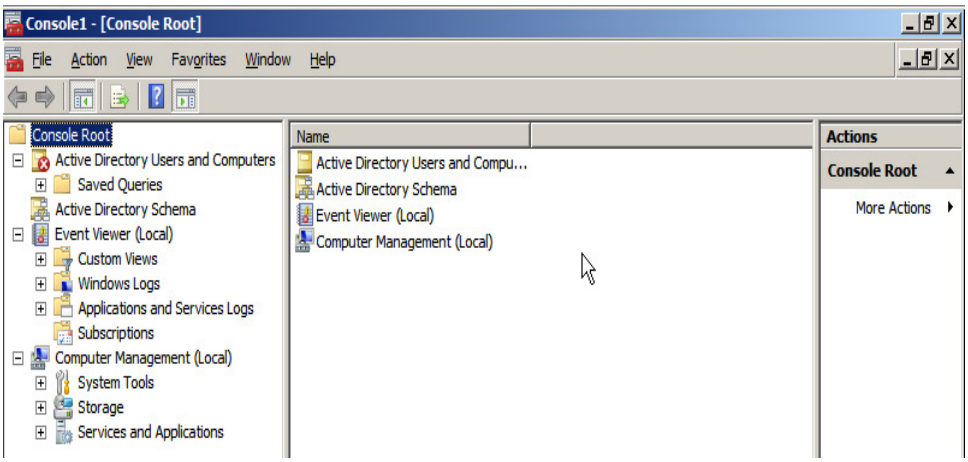
Active Directoryä hallinnoivat henkilöt eli administraattorit aloittavat hallinnoin konfiguroimalla AD DS:n Users And Computers -työkalulla. Toimialueeseen luodaan objekteja eli käyttäjiä, koneita ja ryhmiä, jotka sijoitetaan jo valmiisiin tai tässä vaiheessa luotaviin Organizanional Uniteihin (OU). Users

And Computers ja muut hallintoa edellyttävät työkalut tulee kuitenkin ensin ottaa käyttöön. Työkaluja kutsutaan nimellä snap-in. Snap-in -työkaluja voidaan lisätä tai poistaa käytöstä Microsoft Management Consolen (MMC) kautta. [9.]

4.4.1 Snap-in-työkalut

Microsoft Management Console on Windows Administrative Tool-ominaisuus, joka on asennettu oletuksena Active Directoryyn. Administraattorit rakentavat sitä kautta tarpeelliseksi katsomansa kokonaisuuden toimialueen hallinointia varten. MMC:n tärkeimpiä ominaisuus on lisätä ja poistaa snap-in työkaluja. Snap-in on yksittäinen työkalu, jolla hallitaan yhtä tiettyä asiaa. Snap-in ei toimi itsenäisesti vaan MMC:n kautta. Ensimmäinen snap-in, joka MMC:n lisätään on käyttäjiä ja koneita hallinnoiva Users And Computers. Muita lisättäviä snap-in-työkaluja olivat. [9.]

- Active Directory Schema
- Computer Management
- Event Viewer.



Kuva 7. Näkymä MMC:llä asennetuista työkaluista

MMC:hen voidaan asentaa ominaisuus, joka estää käyttäjää lisäämästä tai poistamasta snap-in-työkaluja. MMC:n tiedosto-valikossa on kohta, joka mahdollistaa määrittelyn, käytetäänkö MMC:tä peruskäyttäjänä vai Administraattorina. [9]

4.4.2 Objektit ja OU:t

Active Directory toimii hakemistopalveluna, joka ylläpitää resursseja kuten käyttäjiä, ryhmiä ja koneita. Resurssit sisällytetään Organizational Uniteihin (OU) eli hallinnollisiin containereihin ja ovat nimeltään objekteja. OU:t helpottavat samankaltaisten objektien käyttöä ja hallintaa. OU:t muodostavat keskenään hierarkian Active Directoryyn. Harjoituksissa luotiin eri tarkoituksiin useampi eri hierarkiatason OU Users And Computers snap-in-työkalun avulla. Snap-in-työkalun avulla luotiin myös käyttäjiä, ryhmiä ja koneita OUiden sisälle. [9.]

Objektin luomisen aikana oli mahdollista kofiguroida vain rajatusti sen ominaisuksia. Ominaisuuksien konfiguroimiseen tullaan keskittymään seuraavassa kappaleessa. OUihin ja objekteihin luotiin suojaus, joka estää vahinkopoistamisen mahdollisuuden. Suojaus on oletusasetus Active Directorysä. [9.]

4.5 Käyttäjätilit ja ryhmät

Active Directoryn perimmäiseltä tarkoitukseltaan luotu käyttäjien olemassaolon hallintaan. Ilman käyttäjiä ei koko hakemisto olisi tarpeellinen. Käyttäjien luomiseen on käytössä useita eri vaihtoehtoja, kuten graafisesti helppo Users And Computers snap-in, komentorivi, Windows Powershell ja VBScript. [9.]

4.5.1 Käyttäjätilien luominen komentoriviltä

Käyttäjien luominen suoraan komentoriviltä onnistuu yhdellä komennolla. Harjoituksissa luotiin mm. käyttäjä Mike Fitzmaurice People OU:hun.

dsadd user ”cn=Mike Fitzmaurice, ou=People, dc=contoso, dc=com”

Käyttäjiä lisättiin komentoriviltä myös skriptin avulla. CSVDE (comma separated Value Data Exchange) toiminnossa luotiin seuraavanlainen tekstitiedosto Notepadin avulla.

DN,objectClass,sAMAccountName,sn,givenName,userPrincipalName“cn=LisaAn-
drews,ou=People,dc=contoso,dc=com”,user,lisa.andrews,Lisa,Andrews,lisa.and-

rews@contoso.com“cn=DavidJones,ou=People,dc=contoso,dc=com”,user,david.jones,David,Jones,david.jones@contoso.com

Tiedosto tallennettiin Documents -kansioon nimellä Newusers.txt. Kansion sisältö laukaistiin komentoriviltä komennolla.

csvde –i –f newusers.txt

CSVDE:n etu on usean käyttäjien samanaikaisessa lisäämisessä. Jos hallinnoidaan suurta verkkoa, on CSVDE erittäin käytännöllinen.

Käyttäjiä tuotiin myös Lightweight Directory Access Protocol Data Interchange Format eli LDIFDE -kansion avulla. LDIFDE ei pelkästään tuo uusia käyttäjiä Active Directoryyn, vaan sen avulla voidaan luoda yksityiskohtaisempaa tietoa käyttäjästä. Notepadilla luotiin Newusers.ldf tiedosta ja tallennettiin se Documents kansioon. LDIFDE laukaistaan CDVDE:n tapaan myös komentoriviltä.

```
DN: CN=April Stewart,OU=People,DC=contoso,DC=com
changeType: add
CN: April Stewart
objectClass: user
sAMAccountName: april.stewart
userPrincipalName: april.stewart@contoso.com
givenName: April
sn: Stewart
displayName: Stewart, April
mail: april.stewart@contoso.com
description: Sales Representative in the USA
title: Sales Representative
department: Sales
company: Contoso, Ltd.

DN: CN=Tony Krijnen,OU=People,DC=contoso,DC=com
changeType: add
CN: Tony Krijnen
objectClass: user
sAMAccountName: tony.krijnen
userPrincipalName: tony.krijnen@contoso.com
givenName: Tony
sn: Krijnen
displayName: Krijnen, Tony
mail: tony.krijnen@contoso.com
description: Sales Representative in The Netherlands
title: Sales Representative
department: Sales
company: Contoso, Ltd.
```

Kuva 8. Newusers.ldf-tiedosto. [9]

4.5.2 Käyttäjien luominen Windows Powershellin ja VBScriptin avulla

Windows Powershell ja VBScript ovat voimakkaita työkaluja hallinnollisten tehtävien toteuttamiseen. Kumpikin mahdollistaa skripteillä käyttäjien automaattisen luomisen. Powershell on Windows Server 2008:n uusi ominaisuus, jonka voi ladata myös vanhemmille servereille. Komentoriville Powershellissä on yli 130 komentoa. VBScript on vanhempi skriptikieli, joka on kaikissa Windowsin versioissa. Koska se on ollut olemassa jo pitkään, on sille olemassa myös laaja tuki. Kuitenkin koko ajan kehittyvä Powershell tulee olemaan tulevaisuudessa käytetympi vaihtoehto. [9]

Harjoituksissa asennettiin Windows Powershell Server Managerin avulla, Powershell asennettiin *Käynnistä*-valikkoon. Käyttäjiä luotiin Powershellin omalta komentoriviltä, joka on pitkälti Windowsin cmd:n tyylinen. Käyttäjän Mary North luominen toteutettiin seuraavalla komennolla.

$objUser=$objOU.Create("user","CN=Mary North")

Skriptin avulla käyttäjän lisäämiseen luotiin ensin notepad tiedosto nimellä ”Newusers.ps1”. Heittomerkit ovat tarpeelliset, jottei Notepad tallenna kansiota .txt-muotoon.

$objOU=[ADSI]"LDAP://OU=People,DC=contoso,DC=com"

$objUser=$objOU.Create("user","CN=Scott Mitchell")

$objUser.Put("sAMAccountName","scott.mitchell")

$objUser.SetInfo()

Seuraavaksi avattiin Powershell terminaali ja syötettiin komento laukaisemaan kansion sisältö.

.\newuser.ps1

VBScriptillä käyttäjien luominen on miltei identtinen.

Set objOU=GetObject("LDAP://OU=People,DC=contoso,DC=com")

Set objUser=objOU.Create("user","CN=Linda Mitchell")

objUser.Put "sAMAccountName","linda.mitchell"

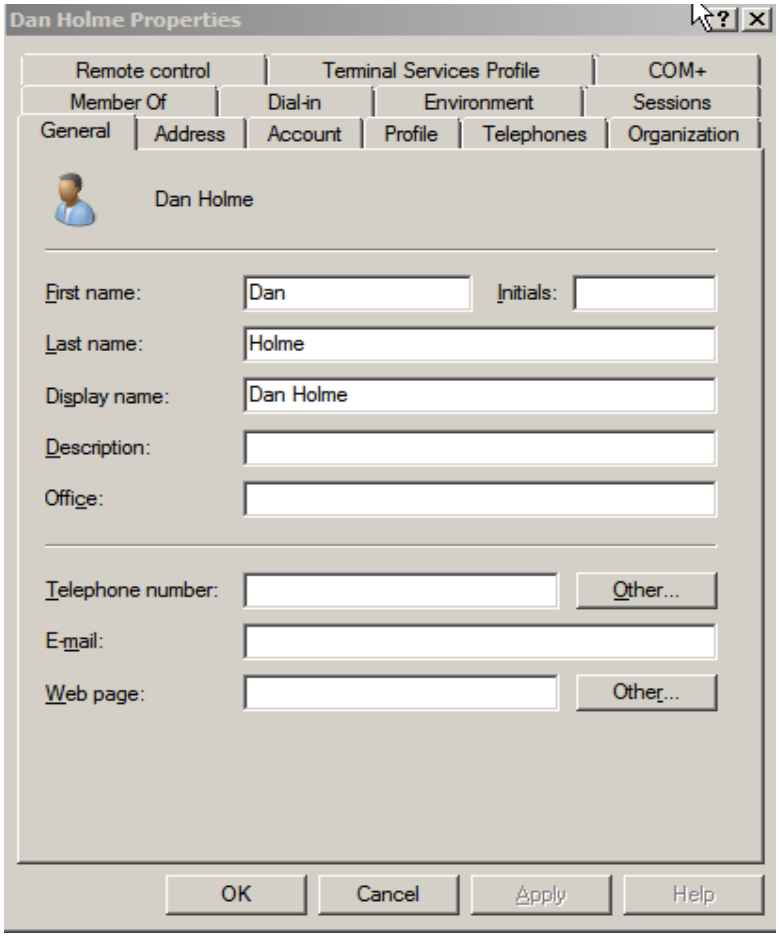
objUser.SetInfo()

Skripti tallennettiin Notepadilla ”Newusers.vbs”. Avattiin komentorivi ja laukaistiin skriptin sisältö komennolla.

cscript.exe newuser.vbs

4.5.3 Atribuuttien konfiguroiminen

Käyttäjien luomisen jälkeen täytyy konfiguroida atribuutteja jotka määrittelevät käyttäjätilien ominaisuuksia ja turvallisuutta. Käyttäjän atribuutteja voi konfiguroida jonkin verran komentoriviltä. Powershellissä ja VBSripteissä suositaan skriptien avulla konfiguroimista. Visuaalisesti helpoin ja tehokas tapa atribuuttien konfiguroimiseen on kuitenkin Users And Computers snap-in. Klikkaamalla hiiren oikeaa näppäintä halutun käyttäjän kohdalla ja valitsemalla ominaisuudet (properties) avataan ikkuna, joka näyttää käyttäjän sen hetkiset ominaisuudet. [9.]



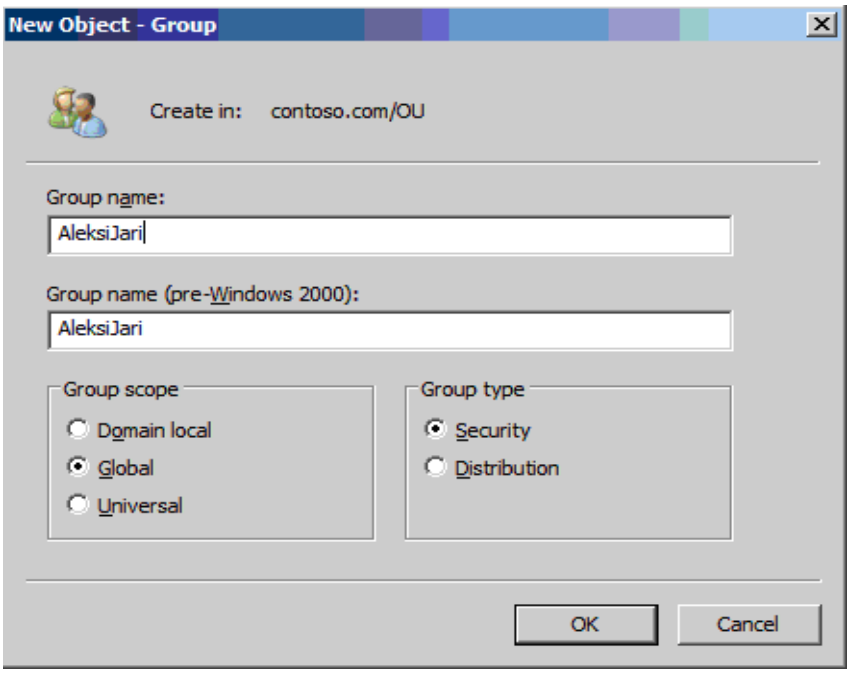
Kuva 9. Käyttäjän ominaisuudet -valikko

Ominaisuudet valikosta pystytään lisäämään tai poistamaan käyttäjän attribuutteja. Tätä kautta voidaan konfiguroida lukuisia asiota kuten sisäänkirjautumissäännöt, henkilökohtaista informaatiota, jäsenyystietoja, etähallintakonfiguraation, ja useita muita asioita. Usean käyttäjän samanaikainen konfiguroiminen on myös mahdollista valitsemalla useampi käyttäjä control–näppäimen avulla. Powershellissä ja VBScriptissä vastaava konfigurointi tehdään skriptien avulla. [9.]

4.5.4 Ryhmät

Käyttäjien parempaa hallintaa varten Active Directory tarvitsee ryhmiä. Hallinnolliset tehtävät on kätevä jakaa ryhmiin ja antaa ryhmille oikeuksia sekä lupia. Active Directoryssa on kahdenlaisia ryhmiä. Jakeluryhmiä (distribution), jotka on pääosin sähköpostisovellusten käyttöön ja turvallisuusrymiä

(security), jotka nimensä mukaisesti edustavat korkeampaa turvallisuustasoa. Ryhmässä voi olla alana (scope) paikallinen toimialue (domain local), globaali (global) tai universaali (Universal). Ryhmän ala vaikuttaa sen toimialaan ja jäsenyyksiin. [9.]



Kuva 10. Global Security -ryhmän luominen

4.5.5 Ryhmien luominen ja hallinta

Ryhmiä voidaan luoda useisiin eri tarkoituksiin ja aloihin, myös toisten ryhmien sisään. Ryhmien tyyppejä ja aloja voi vaihdella tarpeen vaatiessa. Seuraava taulukko listaa ryhmän alan ja käyttötarkoituksen. [9]

Group Scope	Members from the same domain	Members from another domain in the same forest	Members from a trusted external domain
Local	Users Computers Global groups Universal groups Domain local groups Local users defined on the same computer as the local group	Users Computers Global groups Universal groups	Users Computers Global groups
Domain Local	Users Computers Global groups Domain local groups Universal groups	Users Computers Global groups Universal groups	Users Computers Global groups
Universal	Users Computers Global groups Universal groups	Users Computers Global groups Universal groups.	N/A
Global	Users Computers Global groups	N/A	N/A

Taulukko 1. Ryhmät ja scopet. [9]

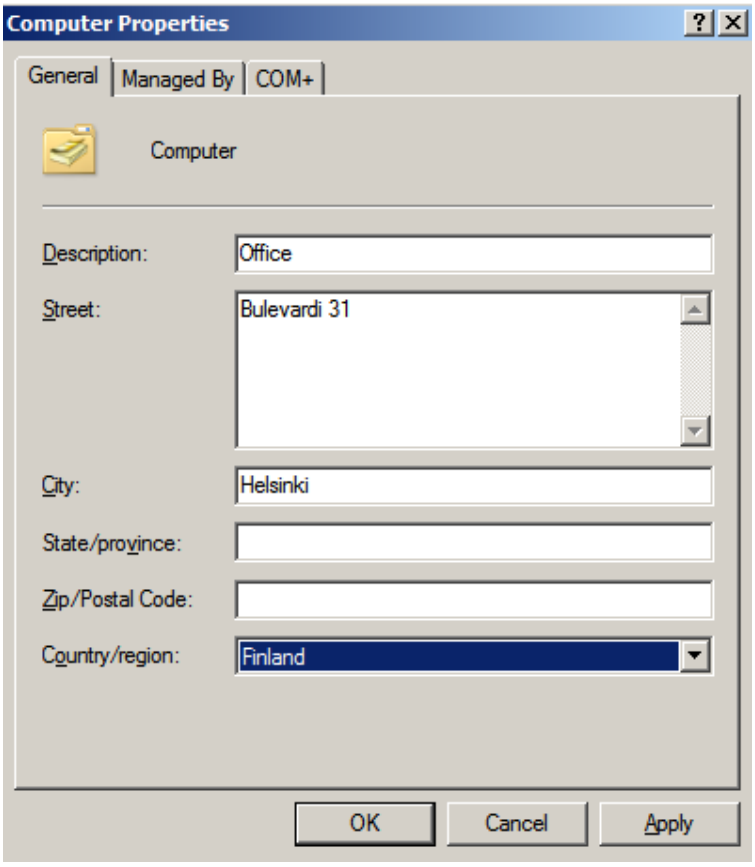
Active Directoryyn ryhmiä voidaan luoda samoin keinoin kuin käyttäjiä. Harjoituksissa ryhmiä luotiin Users And Computers snap-in-työkalulla, Windows Powershellillä, VBScriptillä, komentoriviltä sekä CSVDE- ja LDIFDE–kansioista. Komennot ja skriptit ryhmien luomiseen ovat samoja kuin luodessa käyttäjiä. Mukana on kuitenkin joitain eroavaisuuksia koskien ryhmien muokkaamista. [9.]

4.6 Tietokoneet

Tietokoneet objekteina toimialueessa ovat samankaltaisia kuin käyttäjät. Niitä varten on käyttäjätili ja salasana. Tietokoneet autentikoivat toimialueen kanssa, ne voivat kuulua ryhmiin, niillä voi olla pääsy resursseihin ja niille voidaan konfiguroida lupia ja oikeuksia. Tietokoneiden haasteellisuus tulee esille niiden ollessa osa Active Directory Domain Serviceä, mutta myös ollen fyysisiä laitteita. Tietokoneissa on toisinaan vikoja kun niitä korjataan tai niihin vaihdetaan osia, tulee niiden tulee olla offline–tilassa. Tämä tulee huomioida halllitessa Active Directoryä. Valitettavasti kaikki verkkoadministraattorit ja Active Directoryn ylläpitäjät eivät huomio tarpeeksi tietokoneiden ylläpitoa. Materiaalin harjoituksissa keskityttiin nimenomaan tietokoneiden riittävään tukeen ja ongelmien ennaltaehkäisyyn. [9.]

4.6.1 Tietokoneiden luominen ja toimialueeseen liittäminen

Ennen kuin tietokoneobjekteja voidaan luoda, täytyy niitä varten luoda OU. Yleensä OU:ta luodaan toimenkuvan mukaan kaksi kappaletta. Yksi OU-isäntäkoneille, joka pitää sisällään desktopin, laptopin ja muut käyttäjäkoneet. Toinen OU on tarkoitettu servereille. Harjoituksissa luotiin yksi OU tietokoneille ja toinen servereille Users And Computers snap-in-työkalun avulla. [9.]

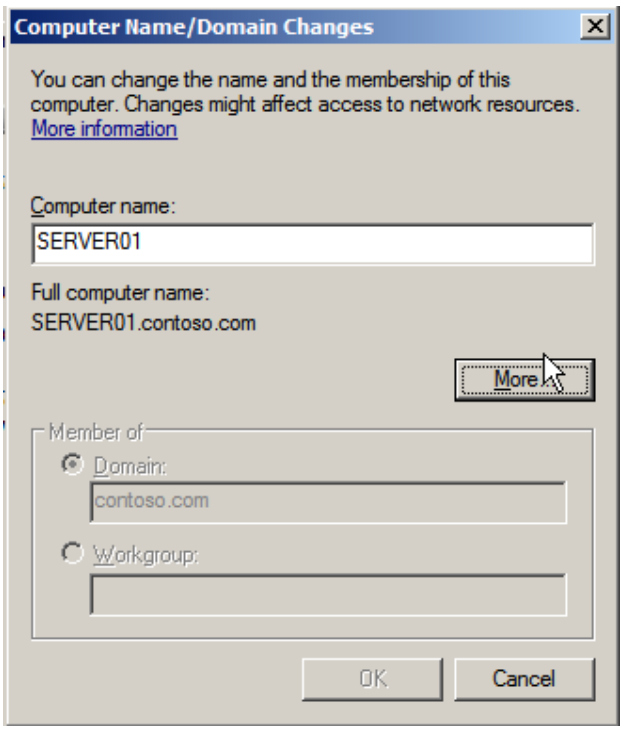


Kuva 11. Computer OU:n tietojen täyttäminen

Server 2008:n oletusasetukset sallivat vain hallintoryhmien luovan tietokoneobjekteja. Ryhmät voivat kuitenkin delegoida lupia luomaan tietokoneobjekteja muille ryhmille. Esimerkiksi tietyn ryhmän jäsenet voidaan sallia luomaan objekteja tietyn OU:n ryhmiin. [9]

Oletusasetus Windows Server 2008:ssa on tietokoneen kuuluminen työryhmään (workgroup). Ennen kuin koneelle voi kirjautua sisään toimialueen käyttäjätilille, tulee koneen kuulua toimialueeseen. Liittyäkseen toimialuee-

seen koneella tulee siis olla tili toimialueessa. Koneen tilillä on kirjautumisnimi ja salasana, aivan kuin käyttäjätililläkin. Harjoituksissa liitettiin tässä vaiheessa toinen virtuaalikone contoso.com toimialueeseen. Tämä päätettiin kuitenkin jättää pois kurssilta Koulun opetusklusterin puutteellisen kovalevytilan vuoksi ei kaikille oppilaille tulisi olemaan käytössä kahta virtuaalikonetta. Kone liitettiin toimialueeseen systeemin ominasuudet -valikon kautta.

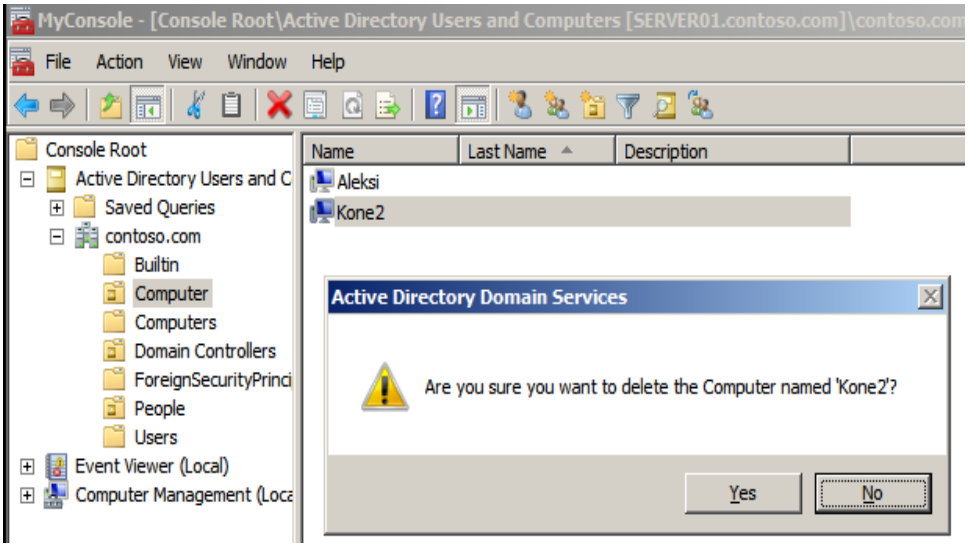


Kuva 12. Tietokoneen toimialueeseen liittäminen

4.6.2 Tietokoneiden konfigurointi ja tukeminen

Tietokoneobjekteja Active Directoryssä luodaan samoin keinoin kuin käyttäjiä ja ryhmiä. Käytössä on Users And Computers snap-in, komentorivi, komentoriviltä CSVDE ja LDIFDE –kansioilla, Windows Powershell ja VBScript. Koneiden atribuuttien konfiguroiminen onnistuu Users And Computers snap-in -työkalun kautta tai vaihtoehtoisesti samoilla työkaluilla, joilla se on luotu. Tietokoneen tilin resetoiminen on ajankohtaista, kun turvallisuusuhka on havaittavssa. Useimmiten käytetty tapa resetoida kone on siirtää se hetkellisesti toimialueesta työryhmään ja takaisin. Tässä on kuitenkin suuri uhka poistaa vahingossa koko tili. Helpoin ja turvallisin tapa resetointiin on Users and Computers snap-in, koneobjektin päällä hiiren oikeaa näppäintä painamalla saadaan esiin vaihtoehto *resetoi tili*. Kun tietokone taas tulee hetkeksi

sijoittaa offline–tilaan korjauksen ajaksi, samasta valikosta valitaan tilin *disabloiminen*. Disabloinnin merkiksi koneen päälle ilmestyy alaspäin osoittava nuolen kuva. Tilin pysyvä poistaminen tapahtuu myös samasta valikosta hiiren oikeaa painaen saadesta vaihtoehdosta *poista*.



Kuva 13. Tietokoneen poistaminen

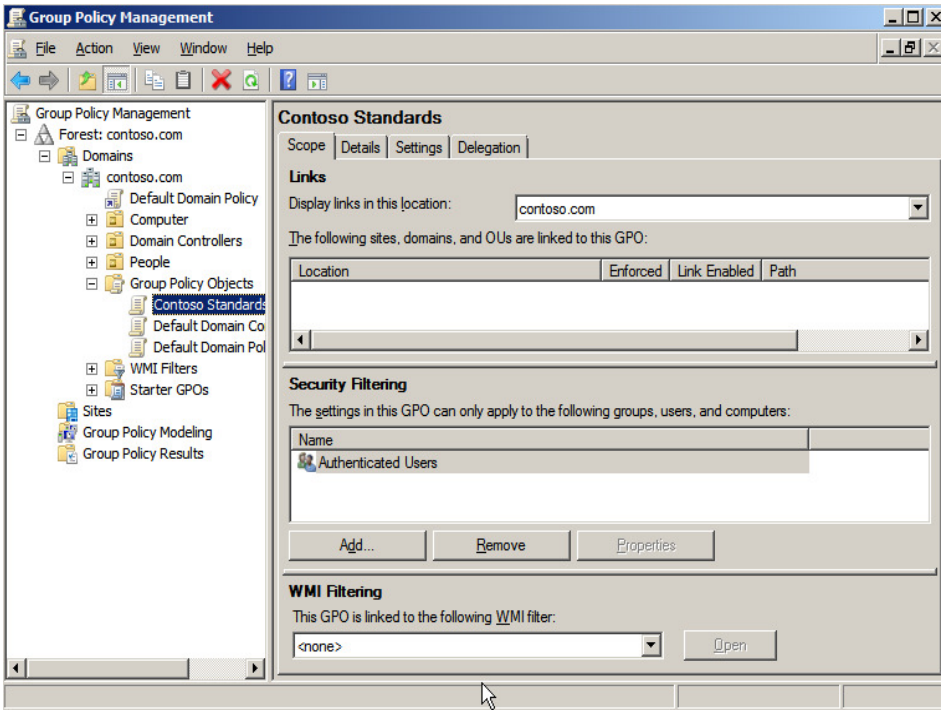
.

4.7 Group Policy -infrastruktuuri

Ryhmät, käyttäjät ja koneet muodostavat yhdessä kokonaisuuden Active Directoryyn Tätä kokonaisuutta hallitaan tietyillä säännöillä ja asetuksilla. Tätä hallittavuutta kutsutaan Group Policyksi. Group Policyyn rakennetaan useista liikkuvista osista koostuva infrastruktuuri, jonka avulla Active Directoryä käytetään. [9.]

4.7.1 Group Policy -objektit

Group Policy -asetukset on määritelty Group Policy -objekteihin (GPO). GPO on objekti, joka sisältää yhden tai useamman asetuksen ja on tekemisissä yhden tai usemman käyttäjän tai tietokoneen kanssa. Harjoituksissa luotiin useampi GPO, linkitettiin niitä kohteisiin ja muokattiin asetuksia.



Kuva 14. GPO:n luominen

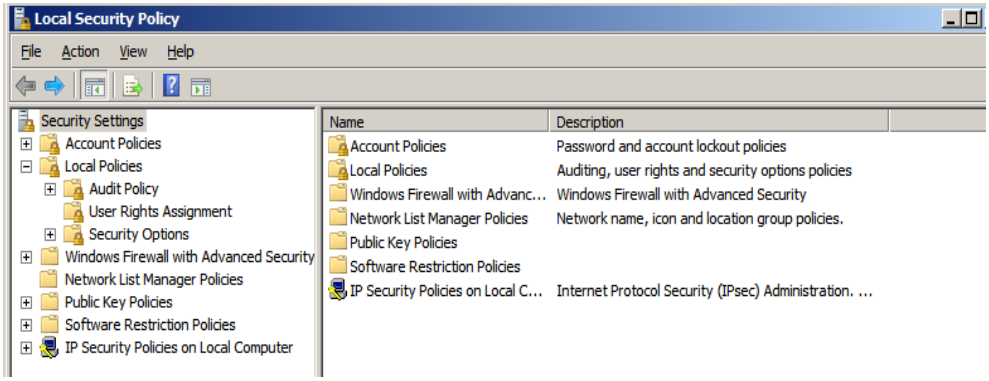
Windows Server 2008 tuo merkittävät Group Policy -lisäasetukset, jotka mahdollistavat yli 20 uutta ja parempaa keinoa hallita käyttäjien ja koneiden asetuksia. Tärkeimpinä ovat.

- sovellukset kuten Micrsoft Office 2003 ja 2007
- rekisteriasetukset
- kansioasetukset
- kartoitetut asemat
- alueelliset valinnat
- virta valinnat
- aikataulutetut tehtävät
- verkkoyhteydet.

4.7.2 Turvallisuus

Group Policyssä on lukematon määrä asetuksia Active Dirctoryn hallintaan. Yksi keskeisimmistä on turva-asetukset. Windows Server 2008 sisältää useita kaiken aikaa suojausta tarvitsevia palveluja hakemistoissaan. Osa porteista on aina auki sisään ja ulospäin lähtevälle dataliikenteelle. Myös luvat ja oikeudet käyttäjien keskuudessa tulee olla auditoinnin kohteena. Kaikki serverit, jotka pyörittävät Windows Server 2008 -käyttöjärjestelmää ylläpitävät

kokoelmaa turva-asetuksista. Turvasetuksia hallitaan paikallisella GPO:lla. Paikallista GPO:ta voidaan konfiguroida GPO Editor snap-in -työkalulla tai Local Security Policy -konsolia. [9.]



Kuva 15. Local Security Policy–konsolin aloitusnäkymä

Turvallisuus-template on toinen vahva mekanismi turvallisuusasetuksien konfigurointiin. Template on konfiguraatioasetuksia sisältävä tekstitiedosto .inf–päätteellä. Templaten etu on yksinkertaisuus: siihen voi kopioida, leikata ja liimata osia ilman monimutkaisia ohjelmia. Sen käyttö laukaistaan Security Configure And Analysis snap-in -työkalulla. Template sallii seuraavien asetusten konffiguroimisen.

- tilien Policy
- paikallinen Policy
- tapahtumalokin Policy
- uudelleenohjatut ryhmät
- systeemipalvelut
- rekisterien oikeudet
- systeemikansioiden oikeudet.

Harjoituksissa konfiguroitiin hallintotyökalujen kautta paikallista turvallisuuspolicya sallimalla etäkirjautuminen turvallisuusasetuksien oikeuksiin komennolla:

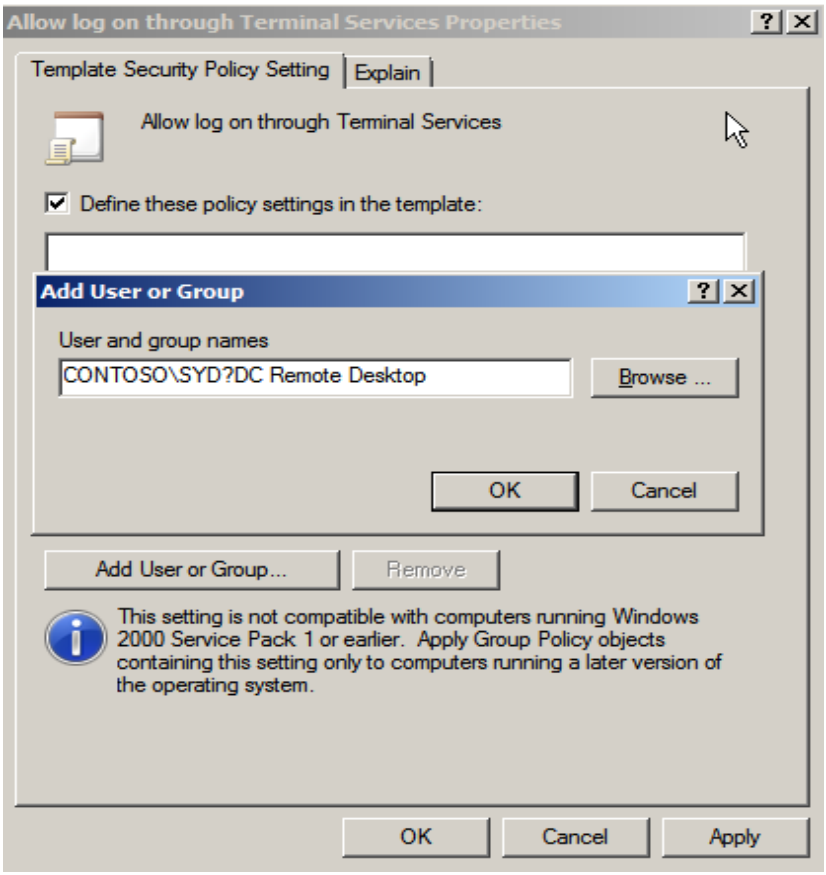
CONTOSO\SYS_DC Remote Desktop

Harjoituksissa sallittiin myös templaten kautta oikeuden antaminen etäkirjautumiseen. Template luotiin seuraavaa polkua seuraten.

C:\Users\Administrator\Documents\Security\Templates

Valittiin oikealla hiiren näppäimellä vaihtoehto *Uusi template*.

Uusi template tallennettiin nimellä DC Remote Desktop, jonka jälkeen sallittiin etäoikeus oletusasetukseksi. Template otettiin käyttöön Security And Configure snap-in -työkalun avulla.



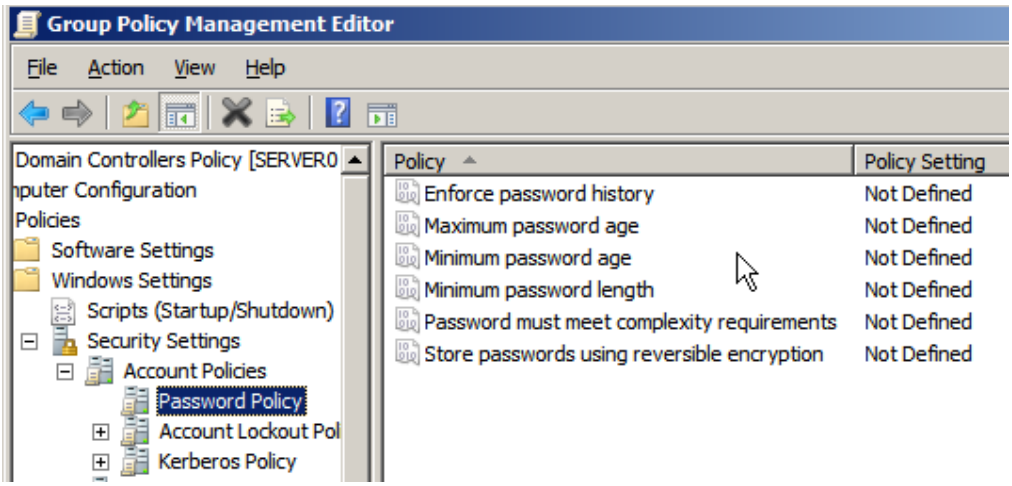
Kuva 16. Security Templaten luominen

4.8 Autentikointi

Käyttäjä syöttää käyttäjätunnuksen ja salasanan sisäänkirjautuessaan Active Directory Domain Serviceen. Systeemi käyttää näitä tietoja tunnistaakseen käyttäjän ja tietojen voimassaolevuuden. Systeemi siis autentikoi käyttäjän. Autentikoitintiin liittyy komponentteja ja monipuolisia policy–ohjeita, joita harjoituksissa käytiin läpi. Harjoituksissa luotiin myös Read-only Domain Controller (RODC). [9.]

4.8.1 Salasanat ja auditoinnin autentikointi

Windows Server 2008 -oletusasetus vaatii käyttäjiä vaihtamaan salasanan 42 päivän välein. Salasana–policyn seuraavaat askeleet määrittävät salasanan vähintään seitsemän merkkiä pitkäksi, sekä sisältämään numeroita ja isoja kirjaimia. Salasana–policyyn voi konfiguroida lukuisia ominaisuuksia parantamaan turvallisuusastetta. Toimialueen salasana–policy on skopattu GPO:sta. Toimialueeseen voidaan määritellä vain yhden tyyppinen salasana–policy. Policy koskee kaikkia käyttäjiä. Harjoituksissa konfiguroitiin salasanan ikääntyminen 90 päivän pituiseksi. Minimipituus salasanalle on 10 merkkiä ja tilin lukkeutuminen viiden epäonnistuneen sisäänkirjautumisyrityksen jälkeen. [9.]



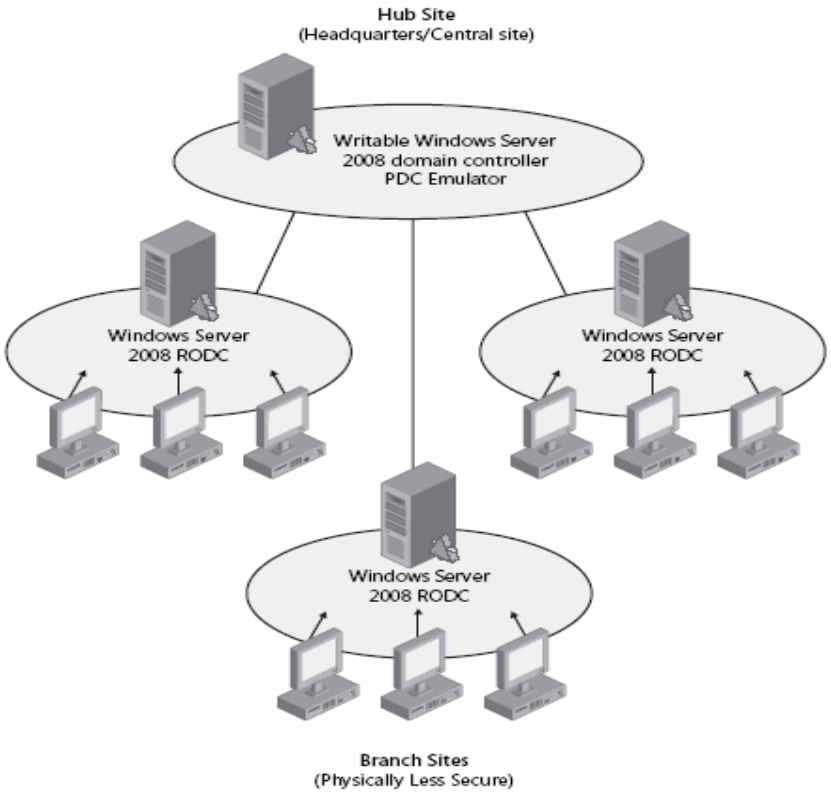
Kuva 17. Salasana-policyn määrittäminen

Seuraavaksi harjoituksissa luotiin Passwor Settings Object (PSO), joka on GPO:n tyylinen kokoelma asetuksista. PSO on GPO:sta irrallaan oleva kokokoelma asetuksia, niin sanottu fine-grained salasana–policy. PSO:lla voidaan määritellä seuraavia asetuksia. [9.]

- salasanan talletus kryptattuna
- salasanahistoria
- salasanan kompleksisuus
- salasanan pituus
- väärin syötetyn salasanan aiheuttaman lukkeutumisen kesto.

4.8.2 Read-Only Domain Controller

RODC on Windows Server 2008 tuoma uudistus. Read-only-tyyppinen Domain Controller, joka sisältää kopion Active Directoryn tietokannasta, on suunniteltu, että se sijoitetaan turvallisuutta kohentamaan haarakonttoreihin. RODC replikoi päivitykset toimialueesta. RODC:n luominen vaatii toisen fyysisen systeemin. RODC ei myöskään voi olla toimialueen ensimmäinen Domain Controller, jolloin sen asentaminen jo voimassa olevan systeemin päälle ei onnistu. Näistä syistä RODC:n luominen päätettiin jättää pois kurssilta. Harjoitusten testauskäytössä oli kuitenkin myös toinen virtuaalikone, jonka avulla RODC:n luominen testattiin. [9.]



Kuva 18. Read-only Domain Controllerin sijainti. [9]

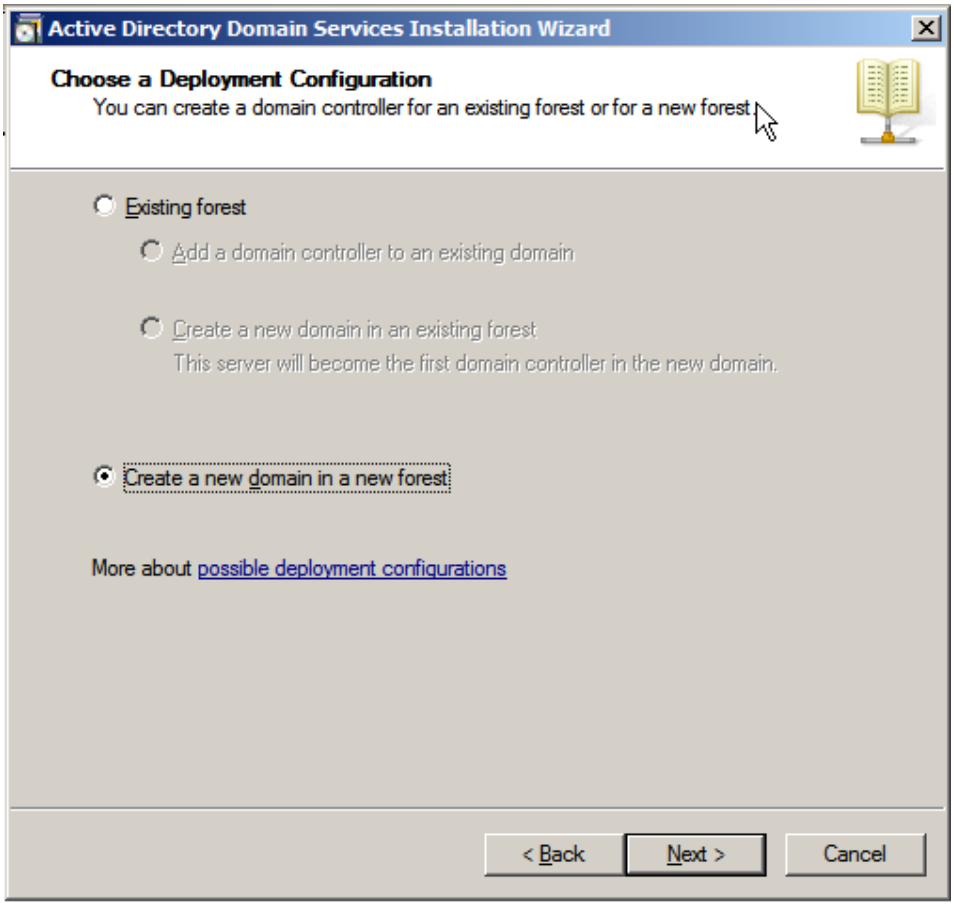
4.9 Ohjauskoneet

Domain Controller on Active Directoryn aivot isännöiden sen koko toimintaa. Microsoftin materiaalin harjoituksissa asennettiin jo aiemmin Domain Controller ja konfiguroitiin sen asetuksia. Materiaali piti sisällään useamman virtuaalikoneen tarvitsevan syventävän kappaleen Domain Controllereista.

Kappaleen harjoitukset jouduttiin jättämään kuitenkin pois kurssilta levytilan vähyyden vuoksi. Testausympäristössä oli käytössä toinen virtuaalikone ja osa harjoituksista testattiin. Tämä työ kuitenkin esittelee kevyemmin kappaleen asian, koska sen harjoitukset eivät kurssin kannalta olleet merkittäviä. [9.]

4.9.1 Ohjauskoneen asennus

Domain Controllerin asennus aloitetaan aina komentoriviltä komennolla *Dcpromo.exe*. Ensimmäin Domain Controller on aina tyyppiä Global Catalog. Domain Controllerin asennuksen yhteydessä määritellään metsän toimintataso, materiaalin harjoituksissa kaikki harjoitukset tehtiin Windos Server 2008 toimintatasolla. Dcpromo antaa mahdollisuuden valita toimintatasoksi myös Windows Server 2000 tai Server 2003. Toimintatasoa voidaan alentaa tai nostaa tarpeen mukaan. Toimintatason tulee toimialueessa olla alimman Domain Controllerin tasolla. [9.]



Kuva 19. Domain Controllerin luominen uuteen metsään

Domain Controlleriksi voidaan asentaa myös RODC-tyyppinen Domain Controller. RODC on haarakonttoreita ja haastavia sijainteja varten suunniteltu Domain Controller. Dcpromon kautta voidaan asentaa child–toimialue tai toimialuepuu. Domain Controlleriin voidaan konfiguroida Operational Master rooleja hallittavuuden parantamiseksi. Rooleja on viisi. [9.]

- Schema
- Toimialueen nimeäminen
- PDC Emulator
- RID
- Infrastructure

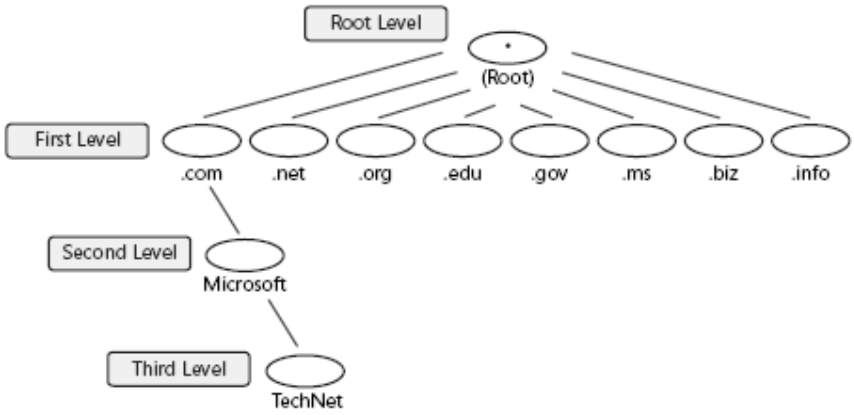
Windowsin System Volume (SYSVOL) on jaettu hakemisto, joka tallentaa serverin toimialueen julkisesti jaettavia kansioita. SYSVOL voidaan konfiguroida replikoimaan uudella multi-master DFS-R (The Distributed File System Replication) ominaisuudella, jos kaikki toimintatasot ovat Server 2008:n tasolla. [10.]

4.10 Teoriatasolla esitetyt ominaisuudet

Tämän työn viimeinen kappale kertoo Microsoft Windows Server 2008 -ominaisuuksista teoriatasolla. Materiaalissa loppukappaleiden harjoitukset vaativat useampia virtuaalikoneita,mitä kurssilla oli mahdollista toteuttaa. Joitain yksittäisiä harjoituksia testauksessa kokeiltiin ja ne saatiin toimimaan, mutta kurssin kannalta ne eivät ole oleellisia. Kappale esittelee Windows Server 2008:n ominaisuuksia ja mahdollisuuksia.

4.10.1 Nimipalvelimen integrointi

Nimipalvelujärjestelmä eli DNS (Domain Name System) toimii hierarkisena nimeämisrakenteena kartoittaessa IP–osoitteita FQDN (fully qualified domain name)-tyyppisten osoitteiden parissa. Nimipalvelin myös tukee IP–verkkoa ja reitittää sähköpostia. Verkkoa on miltei mahdoton hallita ilman nimipalvelinta. Nimipalvelinta voi kutsua automaattisesti toimivaksi internetin puhelinluetteloksi joka kääntää konekielen IP–osoitteet nimiksi. Esimerkki, *www.example.com* kääntyy muotoon *208.77.188.166.* [12.]



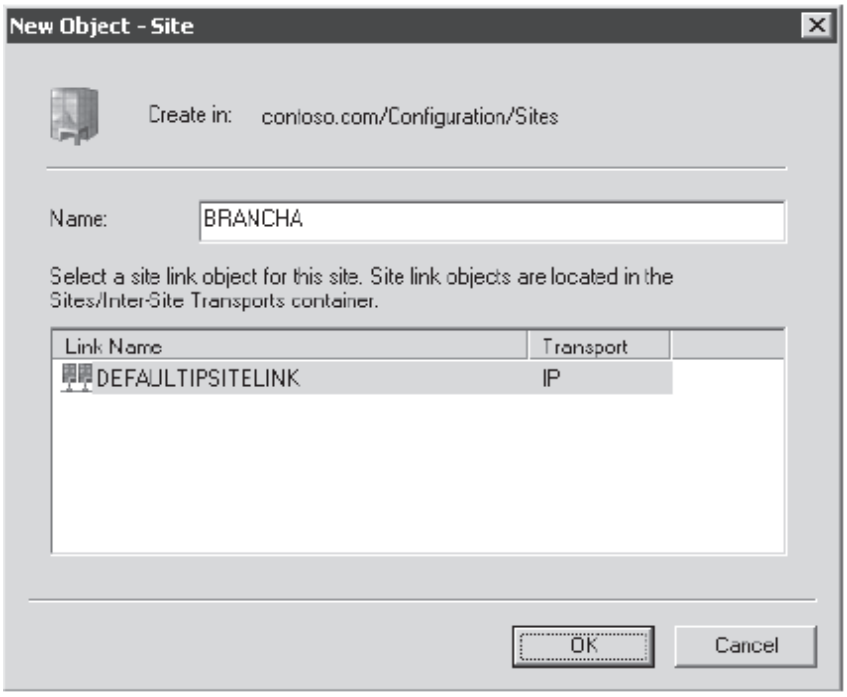
Kuva 20. Nimipalvelimen hierarkia internetissä

Active Directory Domain Servicen metsärakenne perustuu täysin samaan hierarkiseen rakenteeseen kuin nimipalvelin. Nimipalvelin tukee palvelusijaintien tunnistamista, esimerkikisi Active Directory Domain Servicen sisäänkirjautumisprosessia. Ilman nimipalvelinta ei AD DS toimi moitteettomasti. Kun AD DS asennetaan, on nimipalvelin tämän vuoksi integroitu asentumaan samassa prosessissa. [9.]

Windows Server 2008:n tärkeimpänä nimipalvelin uudistuksena on päivitys tukea myös IPv6–protokollaa. IPv6 mahdollistaa 128–bittisen osoiteformaatin käytön IPv4:n 32–bittisen osoiteformaatin rinnalle.

4.10.2 Site–replikointi

Domain Controllerit toimivat ohjauskoneina Active Directoryn toiminnassa. Toinen tärkeä osa toimivuutta on Active Directory Domain Services sitet. Sitet ovat hakemistopalvelun ydinkomponentteja, jotka tukevat paikallistamista ja replikointia. Site on fyysinen sijainti, joka voidaan määritellä esimerkiksi toimistona tai kaupunkina, jota Domain Controller ohjaa. Sitet linkitetään toisiinsa perinteiseen tapaan, kuten soittoyhteyksillä tai kuidulla. Yhdessä sitet fyysisillä sijainneillaan muodostavat verkko–infrastruktuurin. [9.]



Kuva 21. Site-objektin luominen

Siten konfigurointiin luodaan site-objekti, joka assosioi aliverkko-objektin kanssa. Sitella voi olla useita aliverkkoja, mutta aliverkko voi kuulua vain yhteen siteen. Sitet autentikoidaan Kerberos -todennusprotokollalla. Kerberos on suunniteltu internetin kaltaisiin verkkoihin, joissa käyttäjien henkilöllisyys todistetaan myös verkon yli. Kerberos tunnistaa, jos viestiä on matkalla muokattu. [13.]

4.10.3 Yritys jatkuvuus

Yritysjatkuvuuden varmistaminen on maailmanlaajuisesti viimeaikaisten luonnonkatastrofien myötä ollut vahvassa kehityksessä. Hurrikaanit, hyökyaallot ja maanjäristykset aiheuttavat suurta tuhoa myös yrityksille. Peräti 40 % pienten ja keskisuurten yritysten toiminnasta katkeaa suureen katastrofiin. Active Directory tarjoaa ratkaisun suurten tuhojen varalta. Objekteista luodaan tallettaessa eräänlainen varasto, josta vahinkopoiston tai luonnonkatastrofin jälkeen voidaan hakea replikoitua tietoa. Varastoitu objekti tallentuu kaikkine atribuutteineen, jotka ovat yhä voimassa objektin palautuksen jälkeen. [9.]

Windows Server 2008 on tuonut myös hallintaan ja monitorointiin vahvoja parannuksia Active Directoryn toiminnan kannalta. Työkalut kuten Task Ma-

nager, Event Logs, Reliability Monitor ja Performance Monitor takaavat tarkemman policy-konfiguroinnin ongelmatilanteiden varalle. [9.]

4.10.4 Active Directoryn Lightweight Directory Services

Active Directory Lightweight Directory Service (AD LDS) perustuu samaan koodiin kuin AD DS. AD LDS on kuitenkin nimensä mukaan kevyempi ja yksinkertaisempi versio. Jos on mahdollisuus, kannattaa AD LDS:ää käyttää AD DS:n sijaan. Mutta esimerkiksi Exchange Serverin käyttöön tarvitaan AD DS. AD LDS ei muuta serverin konfiguraatiota kuten AD DS, sillä AD LDS on vain sovellus. AD LDS tukee kaikkia AD DS:n ominaisuuksia verkko-operaatiosysteemiä lukuun ottamatta. AD LDS:n asennukseen tarvitaan Windows Server 2008, asennusvaihtoehto valitaan Wizardin avulla rooleista. Myös Core–asennus on mahdollinen. Roolin määrittelyn jälkeen luodaan instanssit serverin käyttöön. Eriarvoisia instansseja käytettäessä työskennellään myös serverien nimien ja porttinumeroiden kanssa. [9.]

4.10.5 Sertifikointipalvelut ja Public Key Infrastructre

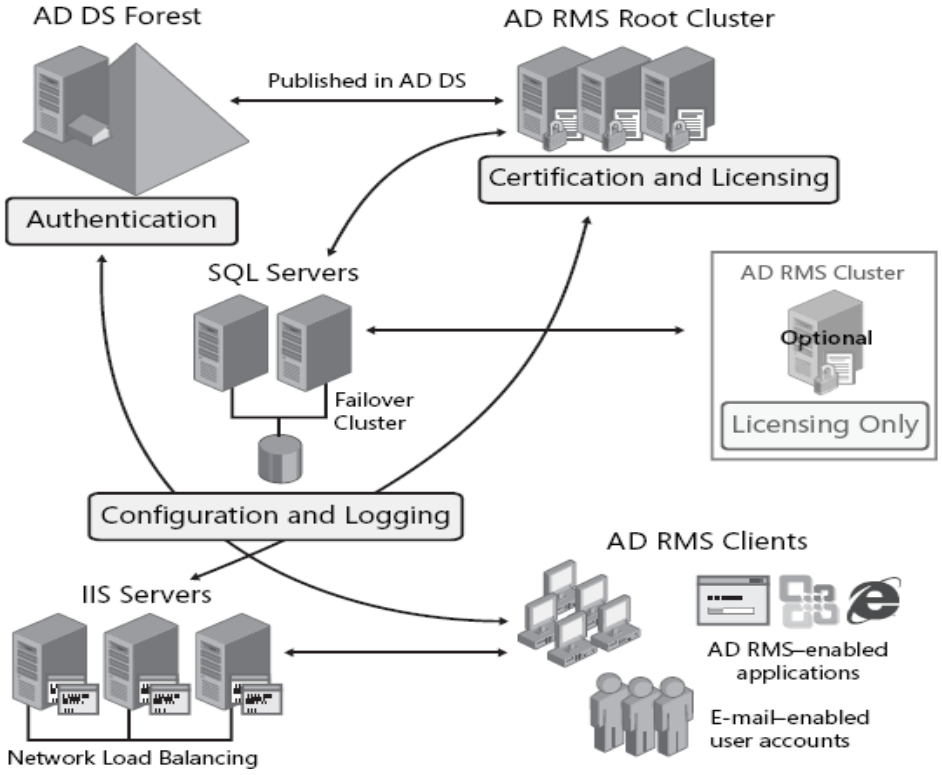
Windows Server 2008 esittelee Active Directory Certificate Services (AD CS)-ominaisuuden, joka mahdollistaa yritysten itsensä määritellä ja hallita infrastruktuuri. Public key infrastructures (PKIs) alkavat olla ydinkomponentteja modernissa verkkohallintaa vaativissa yrityksissä. PKI:t ovat käytössä joko turvaamassa langatonta kommunkointia, integroitu Seure Sockets Layeriin (SSL) virtuaalisissa verkoissa tai ihan vain todentamassa sähköposteja Web–ympäristössä. PKI-sertifikaattien mukana tulee itse infrastruktuuri, joka ensin kuitenkin luodaan. Microsoft on sisällyttänyt hiljattain käyttöjärjestelmäänsä mahdollisuuden luoda ja hallita PKI:tä. [9.]

Supported Components and Features	Web	Standard	Enterprise	Datacenter
Standalone certificate authority	☐	☑	☑	☑
Enterprise certificate authority	☐	☐	☑	☑
Network Device Enrollment Service (NDES)	☐	☐	☑	☑
Online responder service	☐	☐	☑	☑
Key archival	☐	☐	☑	☑
Role Separation	☐	☐	☑	☑
Certificate Manager restrictions	☐	☐	☑	☑
Delegated enrollment agent restrictions	☐	☐	☑	☑

Taulukko 2. AD CS -ominaisuudet versioittain. [9.]

4.10.6 Active Directory Rights Management Services

Active Directory Rights Management Services (AD RMS) eli oikeuksien hallintapalvelut on Windows Server 2008:n mukana tullut päivitys Windows Server 2003:ssa olleeseen Rights Management Serviceen. AD RMS server on nyt rooli ja suurin muutos edeltäjäänsä nähden. AD RMS on suunniteltu laajentamaan sisäinen verkko turvallisesti digitaalisten oikeuksien avulla ulkomaailmaan palomuurin yli. Rooli takaa sertifikoinnin ja lisenssien hallittavuudet. AD RMS -roolia hallinnoidaan Microsoft Management Consolen kautta. AD RMS:ää asentaessa luo se itsestään Server Licensor Certificaten (SLC), joka antaa serverille oikeuden liittyä AD RMS -rakenteeseen. AD RMS tuo mukanaan myös useita uusia administraatiotason rooleja. Käyttäjällä tulee olla sallittu sähköpostitili AD DS -toimialueella, jotta AD RMS toimii. [9.]

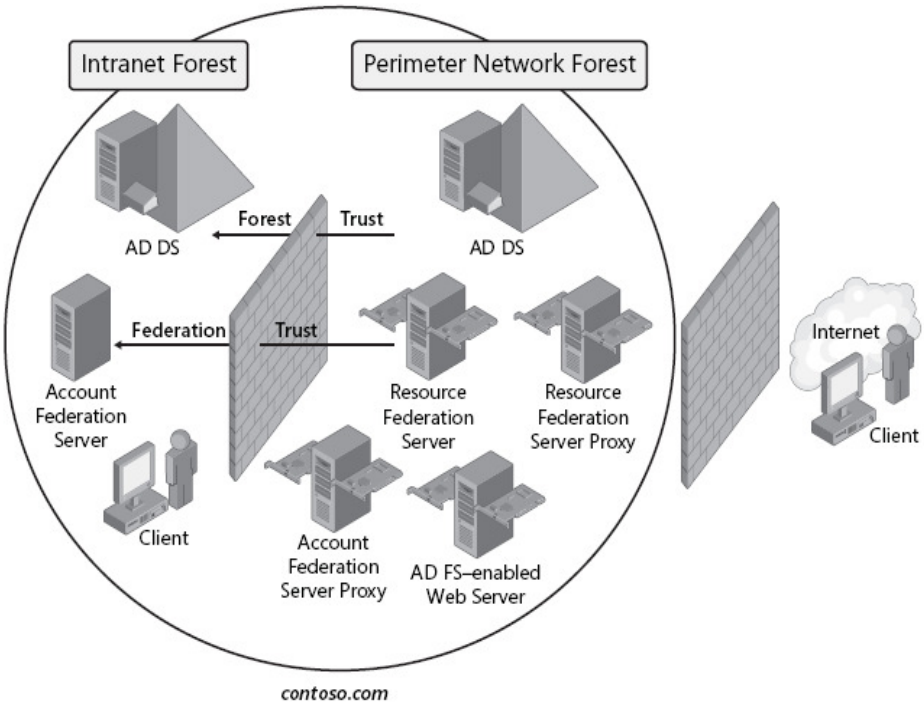


Kuva 22. AD RMS-rakenne.[9]

4.10.7 Active Directory Federation Services

Verkkojen ylläpitäjät ovat painineet turvallisuusongelmien kanssa siitä asti ku internet keksittiin. Windows Server 2008 esittelee Active Directory Federation Services (AD FS)-teknologian, joka laajentaa verkon toimivaltaa autenti-

koimisessa sisäisen verkon ulkopuolelle. AD FS luo yhteistyö–trustin ja tuo toiminnallisuutta metsän luotettavuuteen http-porttien eikä perinteisen TCP/IP-porttien kautta. AD FS:n kommunikointi on turvattu ja kryptattu. AD FS on standardipohjainen toteutus, joka mahdollistaa vuorovaikutuksen Windows- Unix- Linux- ja Mac-operaatiosysteemien kesken.



Kuva 23. AD FS -toimintamalli. [9]

4.11 Yhteenveto

Kun harjoitukset ja ympäristö oli testattu toimiviksi, päätettiin tarkalleen, mitkä harjoitukset kurssille otettaisiin mukaan. Harjoituksia silmällä pitäen oli luotu laboratoriomanuaali harjoituksissa ilmenneiden kirjoitusvirheiden ja epäkohtien varalle. Harjoituksia testatessa saatiin tarkka kuva, minkälaiset virtuaalikoneet olisivat kurssille ideaalisimmat. Ensin luotiin yksi virtuaalikone, johon asennettiin 32–bittinen versio Windows Server 2008. Koneelle määriteltiin muistia 1024 megatavua ja kiintolevylle tilaa 25 gigatavua. Virtuaalikoneelle kurssilla tarvittavat sovellukset ja kansiot siirrettiin serverin C-levylle, josta oppilaat harjoitusten edetessä niitä tarpeen mukaan voisivat hakea. Templatesta kopiotiin 24 kopiota. Koneet asennettiin samaan verkkoon ja määriteltiin osoitteet valmiiksi.

- IP–osoitteet: 10.95.251.135 - 10.95.251.158

- Aliverkon maski:255.255.254.0
- Oletus yhdyskäytävä:10.95.251.1.

Koneet nimettiin väliltä ADServer01 – 24. Koneisiin ei asennettu Active Directory Domain Serviceä. Sen asennus päätettiin jättää kurssin ensimmäiseksi tehtäväksi. Näillä asetuksilla koneet olivat käyttöönottokunnossa kurssia varten.

VIITELUETTELO

[1] Active Directory [verkkodokumentti]. [vitttattu 9.11.2009]. Saatavissa: http://fi.wikipedia.org/wiki/Active_Directory .

[2] Windows Server [verkkodokumentti]. [viitattu 10.11.2009]. Saatavissa: http://www.microsoft.com/finland/pr/press/windowsserver2008_27022008.mspx .

[3] Windows Server 2008 [verkkodokumentti]. [viitattu 12.11.2009]. Saatavissa: http://en.wikipedia.org/wiki/Windows_Server_2008 .

[4] Active Directory [verkkodokumentti]. [viitattu 11.11.2009]. Saatavissa: http://en.wikipedia.org/wiki/Active_Directory .

[5] Domain Controller [verkkodokumentti]. [viitattu 13.11.2009]. Saatavissa: http://technet.microsoft.com/en-us/library/cc786438(WS.10).aspx .

[6] Read-only Domain Controller [verkkodokumentti]. [viitattu 16.11.2009]. Saatavissa: http://technet.microsoft.com/en-us/library/cc732801(WS.10).aspx .

[7] WMvare ESX [verkkodokumentti]. [viitattu 15.11.2009]. Saatavissa: http://fi.wikipedia.org/wiki/VMware .

[8] Remote Desktop Connection [verkkodokumentti]. [viitattu 16.11.2009]. Saatavissa: http://en.wikipedia.org/wiki/Remote_Desktop_Connection#Remote_Desktop_Connection .

[9] Holme Dan; Ruest Nelson; Ruest Danielle, Configuring Microsoft Windows Server 2008 Active Directory Self Paced Training-Kit, Microsoft Press, 2008.

[10] SYSVOL [verkkodokumentti]. [viitattu 20.11.2009]. Saatavilla: http://www.webopedia.com/TERM/S/SYSVOL.html .

[11] Laboratorioinsinööri Tapio Wikström [sähköpostiviesti 31.3.2209]

[12] Nimipalvelin. [verkkodokmentti]. [viitattu 21.11.2009] Saatavilla: http://en.wikipedia.org/wiki/Domain_Name_System .

[13] Kerberos autentikointi. [verkkodokumentti]. [viitattu 22.11.2009] Saatavilla: http://fi.wikipedia.org/wiki/Kerberos_(tietotekniikka).

[14] Dell palvelinkehikko. [verkkodokumentti]. [viitattu 24.11.2009] Saatavilla: http://static.desktopnexus.com/wallpapers/8311-bigthumbnail.jpg .