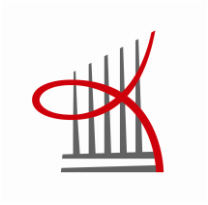


Windows Server 2008 R2-verkkoympäristön ylläpito

Lasse Kivelä

Opinnäytetyö
Toukokuu 2012
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma, Tietoliikennetekniikka ja tietoverkot

Tekijä	Lasse Kivelä
Työn nimi	Windows Server 2008 R2- verkkoympäristön ylläpito
Sivumäärä	31
Työn ohjaaja	Ilkka Tervaoja
Työn tilaaja	Cybercom Finland Oy

TIIVISTELMÄ

Tässä opinnäytetyössä käydään läpi Windows Server 2008 R2- verkkoympäristössä tapahtuvaa toimintaa sekä kuvataan verkkoympäristön rakennetta ja mitä toimivan ympäristön tulisi sisältää. Opinnäytetyö pureutuu myös tarkemmin ympäristön keskitettyyn ylläpitämiseen ja mitä asioita täytyy ottaa huomioon keskittämistä toteutettaessa.

Työn tarkoituksena on antaa kattava paketti tietoa Windows Server 2008 R2- ympäristöstä sekä siihen liittyvistä eri osa-alueista. Toimeksiantaja tähän työhön oli tietopalveluyritys Cybercom Finland Oy. Yritys halusi kartoittaa omaa Windows- ympäristöään sekä tehdä siitä päivitetyn dokumentaation. Tässä opinnäytetyössä käsitellään asioita kuitenkin vain yleisellä tasolla.

Tiedonlähteinä työssä on käytetty kirjallisuutta, Internetiä sekä yrityksen työntekijöitä. Valmiin työn on tarkoitus tarjota laaja-alainen katsaus Windows Server 2008 R2- verkkoympäristöstä sekä auttaa lukijaansa ymmärtämään ympäristön rakennetta, verkkoympäristössä toimivia laitteita sekä ns. best practice- ratkaisuja.

Avainsanat keskitetty ylläpito, kartoitus, best practice, dokumentaatio

TAMK University of Applied Sciences
Degree Programme in Information Technology, Telecommunication and networks

Writer	Lasse Kivelä
Thesis	Management of Windows Server 2008 R2- network environment
Pages	31
Thesis Supervisor	Ilkka Tervaoja
Co-operating Company	Cybercom Finland Oy

ABSTRACT

This thesis covers information about Windows Server 2008 R2- network environment and describes what it needs to include so it can work properly. Thesis also digs into centralized management of these network environments and what needs to be considered when implementing centralization.

The goal for this thesis is to offer a comprehensive package of information about the different sectors and fields of Windows Server 2008 R2- network environments. The co-operating company for this thesis is an information service firm named Cybercom Finland Oy. Company wanted to map their existing Windows- environment and make an updated documentation of it. However this thesis discusses topics in a more general level.

Information for this thesis was obtained through literature, Internet and by consulting Cybercom employees. Finished thesis should offer a widespread look into Windows Server 2008 R2- environments and help its reader to understand the structure of these network environments as well as devices and solutions used in the network.

Keywords centralized management, mapping, solution, documentation

Sisällys

Lyhenteet ja termit

Lyhenne	Merkitys	Selite
AD	Active Directory	Toimialueen tietojen hallintajärjestelmä
DC	Domain Controller	Ohjauspalvelin
DMZ	Demilitarized zone	Verkkoalue turvattoman ja turvallisen verkon välissä.
DNS	Domain Name System	Nimipalvelujärjestelmä
DHCP	Dynamic Host Configuration Protocol	Verkkoasetukset automaattisesti määrittävä protokolla.
GPO	Group Policy Object	Ryhmäkäytäntöobjekti
HPC	High Performance Computing	Korkealaatuinen tiedonkäsittely
HTML	Hyper Text Mark-up Language	Verkkosivujen ohjelmointikieli
IIS	Internet Information Services	WWW-palvelinohjelmisto
IMAP	Internet Message Access Protocol	Sähköpostin lukemiseen tarkoitettu protokolla
IP	Internet Protocol	Internetpakettien välitykseen käytetty protokolla
LAN	Local Area Network	Paikallisella rajatulla alueella toimiva lähiverkko
MBSA	Microsoft Baseline Security Analyzer	Windows-analysointityökalu
NTFS	New Technology File System	Uuden teknologian tiedostojärjestelmä
OU	Organizational Unit	Kansio, joka sisältää AD-objekteja.
POP3	Post Office Protocol, version 3	Sähköpostin lukemiseen tarkoitettu protokolla
PE	Preinstallation Environment	Ennen Windowsia käynnistyvä asennusympäristö
PXE	Pre-Boot Execution Environment	Verkkolaitteen yli asennustilan käynnistävä ympäristö.

SMTP	Simple Mail Transfer Protocol	Lähtevän sähköpostin protokolla
VLAN	Virtual Local Area Network	Tekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin osiin
WDS	Windows Deployment Services	Verkkopohjainen asennusteknologia
WIM	Windows Imaging Format	Levykuvaformaatti

Termi	**Selite**
Active Directory Schema	Active Directoryn objektien ja ominaisuuksien määrittävä kaavio
Administrator	Järjestelmän ylläpitäjä
Allokointi	Resurssien sijoittaminen tietyn laitteen käyttöön
Global Catalog	Pelkistetty versio AD:n objekteista, jota mainostetaan muille toimialueille.
Häiriöaika (Downtime)	Aika, jolloin laitteet eivät ole tavoitettavissa.
Juuritoimialue (Root domain)	Verkkoinfrastruktuurin ensimmäinen toimialue.
Klusteri (Cluster)	Joukko laitteita yhdistettynä suorittamaan samaa tehtävää.
Kryptaus (Encrypting)	Tiedostojen salakirjoittamista ja suojaamista ulkopuolisilta.
Noodi (Node)	Klusterin yksi laite
Oletusyhdyskäytävä (Gateway)	Osoite, johon laite lähettää ulospäin liikkuvan datan.
Skripti (Script)	Useita yksittäisiä komentoja koottuna yhteen pakettiin tiettyä käyttötarkoitusta varten.
Toimialue (Domain)	Alue jonka laitteet sijaitsevat samassa nimiavaruudessa ja samassa AD:n tietokannassa.
Verkkomaski (Mask)	Määrittelee IP-osoitteesta verkko-osoitteen ja laiteosoitteen pituudet.

1 Johdanto

Nykypäivänä verkkoympäristön toteutuksella voi olla suuri merkitys yrityksen toiminnassa. Jos ympäristö on huonosti suunniteltu, se voi aiheuttaa ongelmia koko organisaatiossa. Mikäli haluttuihin resursseihin ei päästä käsiksi silloin kun pitäisi, saattaa se johtaa siihen, että vaadittuja asioita ei pystytä hoitamaan ajallaan. Se taas saattaa johtaa lopputulokseen, että yrityksen asiakkaat hermostuvat ja pahimmassa tapauksessa siirtävät liiketoimintansa muualle. Myös työntekijöiden kärsivällisyys ja motivaatio saattavat olla koetuksella, jos verkkoympäristö toimii puutteellisesti.

Windowsin Server – tuoteperheen uusin palvelinjakelu, toukokuussa 2012, on Windows Server 2008 R2, jonka toimintaan tämä opinnäytetyö pääasiallisesti keskittyy. Windows Server 2008 R2- ympäristön rakennetta tullaan kuvaamaan vaihe kerrallaan kuvia hyväksikäyttäen aloittaen perusasioista ja työn edetessä siirtyen yksityiskohtaisempiin asioihin. Laitteiden elinkaareen tullaan erityisesti syventymään myöhemmissä kappaleissa.

1.1 Windows Server 2008 R2- käyttöjärjestelmä

Windows Server- tuoteperhe tuli markkinoille ensimmäisen kerran vuonna 1994, kun Microsoft julkaisi Windows NT Advanced Server- käyttöjärjestelmän. Sen jälkeen Microsoft on julkaissut tasaisin välein uusia ja kehittyneempiä versioita. Uusin 2008 R2 versio julkaistiin elokuussa 2009 ja se toi mukanaan jälleen paranneltuja ominaisuuksia aikaisempiin versioihin nähden. (10)

Windows Server 2008 R2 on työkalu, jolla yrityksen IT-infrastruktuurin luonti onnistuu sujuvasti ja luotettavasti. Siitä on olemassa kolme pääversiota Standard, Enterprise, Datacenter sekä neljä erikoisversiota, Web, Itanium-based systems, Foundation ja HPC, joita voidaan hyödyntää eri tarkoituksiin käyttökohteesta riippuen. Ne tarjoavat myös uusia virtuaalisointiominaisuuksia sekä paranneltua käytettävyyttä Active Directoryn kanssa. (11, 20)

Paras käyttöjärjestelmä työasemille verkkoympäristössä, jossa palvelimet käyttävät Windows Server 2008 R2:sta, on Windows 7. Yhdessä ne tarjoavat parhaan yhteensopi-

vuuden järjestelmien kesken ja mahdollistavat kaikkien uusimpien sovellusten ja teknologioiden käytön verkkoympäristössä. (29)

Yhtenä merkittävänä uudistuksena Windows Server 2008:ssa voidaan pitää uutta Hyper-V- ominaisuutta. Sen avulla pystytään luomaan ja ylläpitämään useita virtuaalipalvelimia ja/tai – työasemia yhdellä fyysisellä laitteella. Toinen huomioonottamisen arvoinen uudistus on Remote Desktop Services, jonka avulla pystytään tarjoamaan mahdollisuus käyttää sovelluksia ja työpöytiä etälaitteelta. Käyttäjien työasemilla ei tarvitse olla paikallista Windows-käyttöjärjestelmää asennettuna, koska työpöytä avataan erilliseltä laitteelta verkon välityksellä. Riittää, että työasemalla on yksinkertainen graafinen käyttöliittymä, joka mahdollistaa työpöydän avaamisen etälaitteelta. Kaikki tiedostot tallennetaan myös etälaitteelle, joten käyttäjän paikalliselle työasemalle ei muodostu suuria laitteistovaatimuksia. Positiivista on myös se, että pystytään valvomaan resursseja keskitetysti, koska etäkäyttäjät muodostavat yhteyden yhteen sijaintiin käyttäessään työpöytiään. (8, 9)

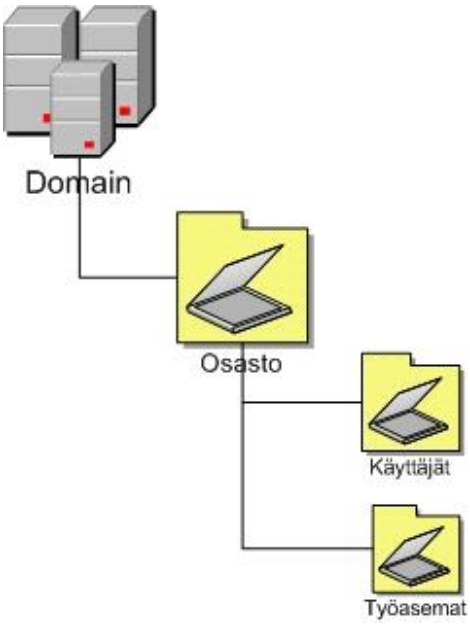
Yksi uudistus on Failover Clustering, joka mahdollistaa useiden palvelinlaitteiden yhdistämisen toisiinsa fyysisillä kaapeleilla, sekä sovellustasolla. Tällaisessa yhdistetyssä kokonaisuudessa yhtä palvelinlaitetta kutsutaan nimellä noodi. Failover Clusteringia on hyvä käyttää kohteissa, joissa palvelun saatavuus on korkein prioriteetti. Failover Clustering mahdollistaa palvelun toiminnan jatkumisen vaikka yhteen noodiin tulisi vikaa ja näin ollen palvelun häiriöaika pystytään pitämään mahdollisimman pienenä. (33)

Uutena ominaisuutena Windows Server 2008:aan tuli myös mahdollisuus asentaa käyttöjärjestelmästä karsittu Core- versio. Core toimii käytännössä pelkästään komentorivillä ja normaali graafinen käyttöliittymä on karsittu pois. Tämä tarjoaa Core- versiolle paremman tietoturvan, koska hyökkääjillä ei ole niin paljon vaihtoehtoja mistä yrittää murtautua järjestelmään. Core- versio ei kuitenkaan tue kaikkia samoja ominaisuuksia kuin normaali Windows Server asennus, joten on syytä suunnitella tarkkaan mihin laitteisiin haluaa asentaa Core- version ja mihin normaalin version. Koska Core- versiosta on karsittu normaali graafinen käyttöliittymä, voidaan sitä käyttää koneissa, joissa on heikompi laitteisto ja jotka eivät välttämättä pystyisi ajamaan normaalia Windows Server- asennusta. Core- asennus on mahdollista Windows Server 2008 R2 Standard, Enterprise ja Datacenter- versioissa. (34)

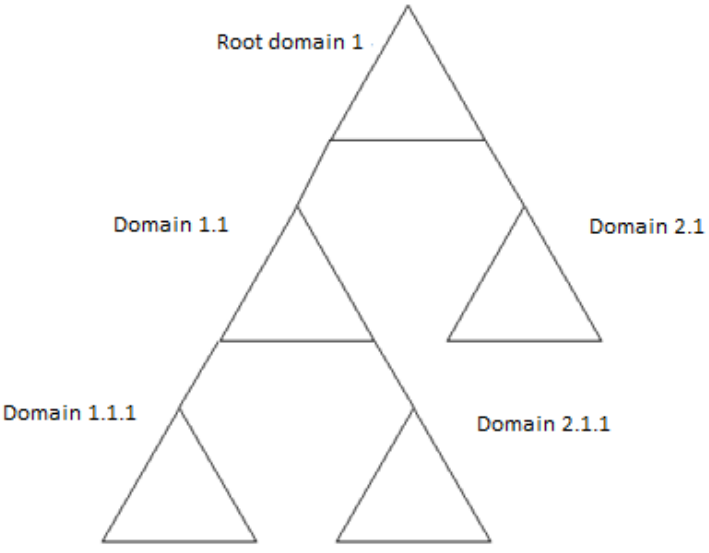
1.2 Active Directory

Active Directory on järjestelmä, jolla pystytään hallinnoimaan yrityksen ympäristön käyttäjätietoja, tiedonsuojaamista ja resursseja keskitetysti. Sillä pystytään luokittelemaan ympäristön käyttäjät omiin ryhmiinsä ja näille ryhmille pystytään määrittelemään halutut oikeudet käyttää ympäristön resursseja. Active Directoryssa käytetään hierarkista, puumaista rakennetta, jonka ansiosta tiedot pystytään sijoittelemaan loogisesti. Verkkoympäristössä voi olla myös useita toimialueita, jotka haarautuvat alkuperäisestä toimialueesta. Näitä rakenteita on esitetty kuvissa 1 ja 2. (12)

Active Directoryn avulla suoritetaan myös käyttäjien oikeaksi todentamista (authentication), kun he yrittävät kirjautua verkkoympäristössä sijaitseviin palveluihin. Käyttäjä kirjoittaa käyttäjätunnuksen ja salasanan palveluun, jonka jälkeen tarkistetaan vastaavatko kyseinen tunnus ja salasana tietokannassa olevia tietoja. Jos vastaavat, tarkistetaan vielä onko kyseisellä käyttäjätunnuksella oikeus päästä kirjautumaan palveluun. (34)



Kuva 1. AD:n tiedostorakenne (13)



Kuva 2. Toimialueiden haarautuminen

2 Palvelimet ja työasemat

Palvelimet ovat elintärkeä osa toimivaa IT-ympäristöä. Ne tarjoavat rooliensa mukaan palveluita verkon käyttäjälle, mikäli käyttäjälle on annettu oikeudet palvelun käyttöön. Palvelimille voidaan määrittää erinäisiä tehtäviä ja palvelimien Windows Server 2008 R2- versio ja laitteisto tulee valita käyttötarkoituksen ja tehtävän mukaan. Tärkeimmät palvelinten roolit ovat: ohjauspalvelin, nimipalvelin, WWW-palvelin, sähköpostipalvelin, tiedostopalvelin ja tulostuspalvelin. Yhdellä palvelimella voi olla useampia rooleja, mutta on otettava huomioon, että yhden palvelimen kuormitus ei kasva liian suureksi. Esimerkkinä ohjauspalvelimissa on usein samanaikaisesti nimipalvelinominaisuus käytössä. (3)

Työasemien ylläpito verkkoympäristössä ei vaadi aivan niin tarkkaa valvontaa kuin palvelinten, koska muiden laitteiden toiminta ei riipu yksittäisen työaseman tilasta. Työasemien käyttöönotto voi sen sijaan olla todella työllistävä tekijä, jos asennettavia laitteita on esimerkiksi kymmeniä kappaleita. Laitteiden asennuksesta ja käyttöönotosta lisää kappaleessa 2.2.1.1.

2.1 Palvelinroolit

Verkon palvelimille on tärkeää asettaa roolit, jotta ne voivat suorittaa oman tehtävänsä optimaalisesti. Windows Server 2008 R2 sisältää Server Manager- työkalun, jonka avulla kullekin palvelimelle pystytään asentamaan valitun roolin mukaan tiettyjä lisäominaisuuksia. Tässä kappaleessa on lueteltu ja kuvailtu tärkeimpiä palvelinrooleja sekä rooleihin liittyviä tehtäviä. Liitteestä 1 löytyy esimerkkikuvaus palvelinten sijainnista verkkoympäristössä. (3)

2.1.1 Ohjauspalvelin

Ohjauspalvelin on ensimmäinen laite, joka täytyy luoda uutta verkkoympäristöä rakennettaessa. Ohjauspalvelimia tehdään yleensä enemmän kuin yksi, jotta ympäristö olisi vikasietoisempi. Ohjauspalvelimia yhdessä voidaan kuvailla verkon ”aivoiksi”, koska ne toimivat Active Directory- toimialueen ylläpitäjinä. Jos toimialueella on enemmän

kuin yksi ohjauspalvelin, ne ylläpitävät keskenään identtisiä tietokantoja eli replikoituvat. Replikoituminen voidaan suorittaa verkon yli, joka on normaali käytäntö. Jos toimialue on valtavan suuri tai verkkoympäristössä on todella hitaat yhteydet, voidaan replikaatio suorittaa ulkoiselta medialta kuten DVD- levyltä. Tätä menetelmää ei kuitenkaan kannata käyttää ellei ole aivan pakko. Jos yhden ohjauspalvelimen tietokantaan tulee muutos, se ilmoittaa siitä kaikille muilla ohjauspalvelimille ja ne tekevät saman muutoksen omiin tietokantoihinsa. Tietokantojen täytyy olla identtisiä, jotta verkkoympäristö pystyy toimimaan käyttäjän näkökulmasta muuttumattomana vaikka yksi ohjauspalvelin vioittuisi. (3, 23)

2.1.2 Nimipalvelin

Nimipalvelimen tehtävä on hakea verkossa IP-osoitteita vastaavat laitteiden verkkotunnukset ja päinvastoin. Verkon laitteet kommunikoivat keskenään numeeristen IP-osoitteiden avulla. Nimipalvelin pystyy yhdistämään automaattisesti tietyn nimen tai tunnuksen ja tietyn IP-osoitteen toisiinsa. Jos nimipalvelimelta kysytään sellaista tietoa, jota ei löydy sen omasta tietokannasta, se voi pyytää tietoa muilta verkon nimipalvelimilta, aina Internetin juurinimipalvelimilta asti. Jos oikea tieto löytyy, se lähetetään takaisin alkuperäisen DNS-kyselyn lähettäjälle. (3)

2.1.3 Tiedostopalvelin

Tiedostopalvelimelle voidaan tallentaa esimerkiksi keskitetysti kaikkien käyttäjien henkilökohtaiset tiedostot. Palvelimelle voidaan myös tallentaa mitä tahansa muita tiedostoja, joita halutaan jakaa verkon välityksellä. Pääsynhallinta nousee merkittävään rooliin tiedostopalvelimessa, jos halutaan että vain tietyt käyttäjät pääsevät käsiksi tiettyihin tiedostoihin. Tämä on yleinen käytäntö ja sen takia verkon ylläpitäjän tulee määrittää jaetuille kansioille käyttöoikeudet. Käyttöoikeuksiin ja pääsynhallintaan pureudutaan tarkemmin tämän opinnäytetyön kappaleessa 2.2.3.1. Käytettävyyden kannalta on hyödyllistä kerätä kaikki tiedostot yhteen keskitettyyn sijaintiin. Jos verkkoympäristössä on useita tiedostopalvelimia, voidaan niiden tiedostot joko replikoida toistensa kanssa tai voidaan luoda yksi lista kaikista tiedostopalvelimilla sijaitsevista jaetuista kansioista, jonka kautta käyttäjät pääsevät käsiksi eri palvelimilla sijaitseviin tiedostoihin. (3, 23)

2.1.4 WWW-palvelin

WWW-palvelin on laite, joka sisältää HTML- kielellä kirjoitettuja verkkosivuja. Myös kaikki verkkosivuihin liittyvä data, kuten kuvat ja Flash-tiedostot sijaitsevat WWW-palvelimella. Selain, jolla verkkosivua yritetään näyttää, hakee verkkosivuun liittyvät komponentit yksi kerrallaan WWW-palvelimelta ja sovittaa käyttäjän näytölle. Verkkopalvelimen käyttöjärjestelmänä on järkevää käyttää Windows Server 2008 R2:n Web-versiota, koska versio on suunniteltu juuri siihen tarkoitukseen. Tämä versio sisältää myös IIS 7.5- teknologian, jonka avulla WWW-palveluja pystytään ylläpitämään turvallisesti sekä keskitetysti. WWW- palvelimella sijaitsee myös IIS:n tukemia dynaamisesti WWW- palvelimella luotuja Active Server Page- tiedostoja. Ne ovat käyttäjän pyynnön perusteella, skripteja käyttäen, sopiviksi muokattuja HTML- sivuja. (1, 3, 38)

2.1.5 Sähköpostipalvelin

Sähköpostipalvelin mahdollistaa sähköpostien lähettämisen ja vastaanottamisen sekä varastoi sähköpostitiedostot. Se prosessoi käyttäjiltä tulevat pyynnöt ja suorittaa niissä halutut toimenpiteet. Sähköpostipalvelin käyttää lähtevän postin käsittelemiseen SMTP-protokollaa ja tulevan postin käsittelemiseen joko POP3- tai IMAP- protokollaa. (2, 3)

2.1.6 Tulostuspalvelin

Tulostuspalvelin tarjoaa käyttäjille mahdollisuuden hyödyntää verkossa jaettuja tulostimia. Se kontrolloi tulostusjonoja ja pitää kirjaa tulostustapahtumista. Tulostuspalvelimen klusterointia kannattaa harkita, jos tulostuspalvelun saatavuus on korkea prioriteetti. Palvelimen käyttöönottajan on syytä tarkistaa, että palvelimella on tarpeeksi tilaa tulostusjonojen käsittelyyn ja, että tallennusmedia soveltuu nopeaan tiedonkäsittelyyn. (3)

2.1.7 Varmuuskopiopalvelin

Varmuuskopiopalvelimen rooli on luoda ja säilyttää varmuuskopioita tärkeistä tiedostoista ja kohteista. Sen tehtävä on myös palauttaa varmuuskopioidut tiedostot, jos alkuperäiset katoavat tai korruptoituvat. Varmuuskopioiden luominen on tärkeää, jotta vältetään datan menettäminen, kun tapahtuu laiterikkoja tai muita kriittisiä virheitä. Varmuuskopioiden tekijän täytyy suunnitella millä aikaväleillä varmuuskopioita kannattaa luoda. Liian lyhyt aikaväli kuormittaa verkkoa turhaan, kun taas liian pitkä aikaväli voi aiheuttaa sen, että suuri määrä viimeisen varmuuskopioinnin jälkeen lisättyjä tiedostoja menetetään, jos tapahtuu esimerkiksi laiterikko. (14)

2.1.8 DHCP-palvelin

DHCP-palvelimen tehtävä on jakaa verkkoympäristöön liittyville laitteille IP-osoitteet automaattisesti siihen ennalta määritetystä osoiteavaruudesta. DHCP:n avulla määritettyjä osoitteita kutsutaan dynaamisesti jaetuiksi osoitteiksi. On tärkeää määrittää osoiteavaruudet tarkasti, ettei laitteille tule päällekkäisiä osoitteita ja, että kaikki osoitteet tulee käytettyä mahdollisimman järkevästi. Jos liitettävä laite ei tue DHCP-protokollaa, täytyvät IP-asetukset määrittää siihen manuaalisesti. On syytä varmistaa, että asetettu IP-osoite on samassa aliverkossa kuin muu osoiteavaruus. IP-osoitteiksi luetaan pääsääntöisesti itse laitteen osoite, verkkomaski, oletusyhdyskäytävä ja yhden tai useamman nimipalvelimen osoite. Kullekin dynaamisesti määritetylle IP-osoitteelle annetaan niin sanottu vuokra-aika eli lease time. Puolessa välissä määritettyä lease timea DHCP-palvelin tarkistaa onko osoite vielä käytössä, ja jos on, käynnistää lease timen alusta. Jos osoite ei ole enää käytössä, palvelin vapauttaa sen, jolloin se voidaan antaa uudelle laitteelle. (3)

Yksi DHCP- palvelin voi olla vastuussa osoitteiden jakamisesta useisiin aliverkkoihin. Tällöin kuhunkin etäaliverkkoon täytyy määritellä niin sanottu ”DHCP- helper”- osoite, jonka kautta etäaliverkkojen laitteet pystyvät kommunikoimaan DHCP- palvelimen kanssa. DHCP- palvelin kannattaa myös kahdentaa vikasietoisuuden parantamiseksi.

2.2 Palvelimen elinkaari

2.2.1 Palvelinten käyttöönotto

Uuden palvelimen käyttöönotossa on mietittävä, mikä versio Windows Server 2008 R2:sta kannattaa valita ja kuinka tehokas laitteisto palvelimessa tarvitsee olla. Jos uuden palvelin rooli tulee olemaan ohjauspalvelin, käyttöjärjestelmäversioksi kannattaa valita joko Enterprise tai Datacenter. Myös palvelimen laitteistossa tulee ottaa huomioon verkkoympäristön laajuus sekä vaatimukset ja panostaa niiden mukaan. Jos ohjauspalvelimissa on liian heikko laitteisto siihen kohdistuneisiin vaatimuksiin nähden, voi se aiheuttaa ongelmia koko verkkoympäristöön. Jos palvelimen rooli on tiedostopalvelin tai tulostuspalvelin niin silloin kannatta harkita Standard- käyttöjärjestelmäversiota. Taulukossa 1 on esitetty eri versioiden käyttömahdollisuudet. Osa erikoisversioiden (Foundation ja HPC) käyttömahdollisuuksista sisältävät rajoituksia.

Palvelimen rooli	**Enter-prise**	**Data-center**	**Stan-dard**	**Itani-um**	**Web**	**Foun-dation**	**HPC**
Active Directory ohjaus-palvelin	√	√	√			√	√
DNS-palvelin	√	√	√		√	√	√
Tiedostopalvelin	√	√	√			√	√
Web Services (IIS)	√	√	√	√	√	√	√
Tulostuspalvelin	√	√	√			√	
DHCP-palvelin	√	√	√			√	√
Remote Desktop Services	√	√	√			√	√
Windows Deployment Services	√	√	√			√	√
Windows Server Update Services	√	√	√			√	√
Hyper-V	√	√	√				√

Taulukko 1. Käyttöjärjestelmäversioiden käyttömahdollisuudet (20)

2.2.1.1 Käyttöjärjestelmän asennus

Käyttöjärjestelmän asentaminen voidaan suorittaa joko normaalisti halutulla Windows käyttöjärjestelmän asennusmedialla tai automaattisesti käyttäen kahta yleistä asennusmenetelmää. Nämä automaattiset asennusmenetelmät ovat levykuvia hyväksikäyttävä asennus ja skripteja hyväksikäyttävä asennus. Jokaisen uuden palvelimen ja työaseman käyttöjärjestelmien asentaminen asennuslevyn avulla on työlästä ja aikaavievää. Sen takia paras tapa asentaa käyttöjärjestelmä on käyttää automatisoituja menetelmiä. Niiden avulla pystytään käyttöjärjestelmä asentamaan niin sanottu levykuvatiedoston avulla, joka avataan verkon välityksellä etäpalvelimelta. (23)

Windows Deployment Services -palvelua voidaan käyttää uusien koneiden käyttöönotossa. Jotta niin voidaan tehdä, täytyy yhdelle verkon palvelimelle asentaa Windows Server 2008 R2 asennuslevyn avulla ja sen jälkeen asentaa WDS- rooli. Verkon ylläpitäjä lisää asennettuun palveluun yhden tai useamman käynnistyslevykuvan sekä asennuslevykuvan. Käynnistyslevykuva tarvitaan siihen, että uusi laite pystyy käynnistyessään siirtymään asennustilaan. Tämä asennustila on Windowsiin sisäänrakennettu PE-ympäristö, jota voidaan käyttää ennen varsinaisen käyttöjärjestelmän käynnistymistä, asennusten suorittamiseen. Tämän jälkeen otetaan käyttöön asennuslevykuva, jolta itse käyttöjärjestelmä asennetaan. Levyasemalla, jolle levykuvatiedostot asennetaan, täytyy olla käytössä NTFS- tiedostojärjestelmä. Seuraavat asennuslevykuvat pystytään lisäämään WDS-palveluun, mikäli verkon ylläpitäjällä on niiden asennuslevyt käytössään: Windows Vista, Windows Server 2008, Windows Server 2008 R2 ja Windows 7. Jos halutaan ottaa käyttöön aiempia versioita Windowsista kuin Vista, täytyy luoda mukautettu asennuslevykuva. (26)

Kun levykuvatiedostot on luotu palvelimen WDS- palveluun, voidaan niiden avulla asentaminen aloittaa etäkoneilla. WDS:n käyttö edellyttää kuitenkin käyttöönotettavilta koneilta mahdollisuutta käynnistää järjestelmä verkkolaitteen, eli niin sanotun PXE-ympäristön avulla. Lisäksi koneen tulee täyttää asennettavan käyttöjärjestelmän laitevaatimukset ja, jotta WDS-palvelu toimisi, täytyy verkossa olla toimivat DHCP- ja DNS-palvelimet. Jos nämä kriteerit täyttyvät, voidaan mihin tahansa uuteen koneeseen asentaa WDS-palvelussa tarjolla olevat käyttöjärjestelmät verkon yli ilman minkäänlaista paikallista asennusmediaa. (26)

Jos halutaan luoda levykuvatiedosto, joka sisältää jo valmiiksi haluttuja asetuksia ja/tai sovelluksia, voidaan käyttää Windows Automated Installation Kit- pakettiin kuuluvaa ImageX- työkalua. Tällä työkalulla luotu levykuva voi sisältää käyttäjän valitsemia asetuksia ja sovelluksia, jotka asennetaan automaattisesti käyttöjärjestelmän yhteydessä. ImageX- työkalulla luotuja levykuvia pystytään käyttämään WDS- palvelussa samaan tapaan kuin normaaleja Windows- asennusmedialta asennettuja levykuvia. (23)

Skriptien käyttäminen käyttöjärjestelmän asennuksessa tarkoittaa sitä, että joko manuaalisen tai automaattisen perusasennuksen jälkeen käyttöjärjestelmään määritetään itseluodun skiptin avulla halutut asetukset. Tällä pystytään helpottamaan asioita, jos tarkoituksena on luoda monta laitetta, jotka sisältävät identtiset asetukset. Skriptien luomiseen tarvitaan aikaisemmin mainittua Windows Automated Installation Kit- pakettia ja siihen kuuluvaa Windows System Image Manager- työkalua. (23)

Käyttöjärjestelmän asennus voidaan suorittaa myös virtuaalialustalle, joka tarkoittaa, että asennettava laite on virtuaalinen ja sille allokoidaan haluttu määrä laitteistoresursseja, kuten keskusmuistia ja prosessoritehoa. Jotta virtuaalijärjestelmä voidaan asentaa, tarvitsee luoda virtuaalikovalevy, jolle haluttu käyttöjärjestelmä asennetaan. Tämä luotu virtuaalikovalevy ja siihen asennettu käyttöjärjestelmä toimivat erillään sen laitteen järjestelmästä, jolle virtuaalikovalevy on luotu. Tämä mahdollistaa useiden virtuaalijärjestelmien luomisen yhdelle fyysiselle kovalevylle. Tämä on toisaalta myös ongelma, sillä jos yhdelle fyysiselle kovalevylle on asennettu useita virtuaalijärjestelmiä ja fyysinen kovalevy rikkoutuu, muuttuvat myös virtuaalijärjestelmät käyttökelvottomiksi. (31)

2.2.2 Palvelimien ylläpito

2.2.2.1 Päivitykset

Palvelimet vaativat jatkuvaa tarkkailua ja ylläpitoa, jotta verkkoympäristö toimisi ongelmitta ja palvelut pysyvät saatavilla. Järjestelmät ja sovellukset täytyy päivittää säännöllisesti, jotta pystytään pitämään tietoturva mahdollisimman hyvällä tasolla ja, että ohjelmat saadaan toimimaan optimaalisesti. Päivitykset voivat kuitenkin aiheuttaa ongelmia verkossa, koska niiden asentaminen saattaa vaatia päivitettävän järjestelmän hetkellistä sammuttamista ja se voi suurissa verkkoinfrastruktuureissa esim. sairaaloissa

tai pankeissa aiheuttaa vakavia konflikteja. Joissakin tilanteissa on myös mahdollista, että päivitysten asentaminen aiheuttaa palvelun kaatumisen kokonaan.

MBSA- työkaluun kuuluvan Security Hotfix Checker- toiminnon avulla pystytään tarkistamaan ovatko verkkoympäristön koneiden päivitykset ajan tasalla. MBSA:n avulla voidaan myös analysoida verkkoympäristön tietoturvan haavoittuvuuksia sekä virhekonfiguraatioita. (16)

Päivitysten automaattiseen asentamiseen voidaan käyttää useita eri teknologioita, kuten Windows Update, Automatic Updates, Software Update Services ja System Management Server. Päivitykset voidaan myös asentaa manuaalisesti verkkolevyltä tai erilliseltä medialta, mutta se ei ole suositeltavaa ainakaan isoissa verkkoinfrastruktuureissa. Manuaalisen asennuksen lisäksi suuriin verkkoympäristöihin ei sovellu Automatic Updates, koska sillä voidaan toteuttaa päivitykset vain yksittäisiin koneisiin tai pieniin ryhmiin koneita. Jos halutaan toteuttaa päivitykset suuressa yrityksessä, jossa on paljon koneita, kannattaa valita System Management Server tai Software Update Services. (16)

System Management Server on palvelin, jonka avulla pystytään suorittamaan identtisen päivityksen tai sovelluksen asennus suuressa määrässä koneita. Tämä voi olla hyödyllinen menettelytapa, jos yrityksessä halutaan pitää tarkkaan kirjaa mitkä identtiset päivitykset ovat asennettu kaikille verkkoympäristön koneille. Software Update Services-palvelin taas jakaa yhdestä keskitetystä sijainnista päivitykset muille verkon laitteille. Software Update Services ensin lataa päivitykset Windows Update- sivustolta ja lähettää halutuista päivityksistä ilmoitukset valituille laitteille. Tämän jälkeen työasemat lataavat päivitykset Software Update Services- palvelimelta. Tämä on tehokas menettelytapa, jos halutaan suodattaa mitä päivityksiä verkkoympäristön laitteille halutaan mainostaa ja asentaa, sekä optimoida yrityksen sisäverkon päivitysten asentamista. (15, 16)

2.2.2.2 Tietoturva

Tietoturva ja ehkä tarkemmin tietoturvamurrot ovat nykypäivänä yhä useammin esillä uutisissa ja julkisissa medioissa. Sen takia onkin yrityksen kannalta elintärkeää pitää sellainen tieto turvassa, jonka ei haluta pääsevän ulkopuolisten käsiin. Palvelinten osalta tietoturva täytyy ottaa huomioon niin fyysisen sijainnin kannalta kuin sovellustasolla. Palvelimet tulee sijoittaa lukittuun tilaan, johon on vain valituilla henkilöillä lupa kulkea. Jos kyseessä on todella arkaluontoista tietoa sisältäviä laitteita, voi turvatoimia vielä parantaa erillisillä lukitusmekanismeilla ja suojauksilla. (16)

Sovelluspuolella tietoturvaan on syytä panostaa myös kattavasti. Pahimmat tietomurrot tehdään verkon välityksellä eikä niinkään fyysisten laitteiden kanssa samassa paikassa. Tietoverkon ylläpitäjän tulee vaatia verkon käyttäjiltä vahvoja salasanoja, joiden murtamiseen menee kauemmin kuin pari sekuntia. Vahva salasana sisältää vähintään kahdeksan merkkiä, isoja kirjaimia ja pieniä kirjaimia sekä numeroita ja symboleja. Salasanan ei tulisi sisältää käyttäjänimeä, oikeaa nimeä tai yrityksen nimeä eikä kokonaista sanaa. (7)

Verkon ylläpitäjän tulee myös tarkistaa, ettei palvelimissa ole käynnissä ylimääräisiä käyttöjärjestelmän aloittamia palveluita, koska ne voivat heikentää tietoturvaa. Parhaassa tapauksessa kullakin käyttäjäryhmällä olisi käytössään vain ja ainoastaan ne palvelut ja resurssit, joita kukin ryhmä tarvitsee. Palvelimelle asennettujen roolien kasvava määrä myös kasvattaa haavoittuvuuksien määrää. Eli mitä vähemmän rooleja on käytössä, sitä vaikeampi palvelimelle on murtautua. (16)

Tärkeää tietoturvan kannalta on myös pitää verkkoympäristön tietokannat ajan tasalla. Jos verkkoympäristöstä poistetaan laite tai käyttäjä, tulee se myös poistaa tietokannasta, tässä tapauksessa Active Directorysta. Paikallisille koneille on syytä asettaa todella vahvat administrator- salasanat, koska on yleisessä tiedossa, että administrator-tunnuksilla kirjautuessa pääsee käsiksi vähintään kaikkiin paikallisen laitteen tiedostoihin ja pahimmassa tapauksessa myös muihin verkon tiedostoihin. Hyvä käytäntö on luoda verkon ylläpitäjille oma ryhmä Active Directoryyn, jonka jäsenet pystyvät kirjautumaan kaikille verkon koneille administrator-oikeuksilla. Näin oikeudet pystytään helposti ottamaan pois tarvittaessa. Active Directoryn ryhmistä ja oikeuksista kerrotaan lisää kappaleessa 2.2.3.1. (16)

2.2.3 Pääsynhallinta

Active Directoryn avulla pystytään hallitsemaan käyttäjien pääsyä käsiksi toimialueen jaettuihin resursseihin. Tämä on tärkeä ominaisuus varsinkin isoissa yrityksissä, joissa tiedostoja ja resursseja täytyy jakaa verkon välityksellä, mutta ei haluta kaikkien pääsevän käsiksi kaikkeen. Jotta Active Directoryllä pystytään toteuttamaan pääsynhallintaa, täytyy verkon tiedot olla asetettu huolellisesti. Tässä tapauksessa tiedoilla tarkoitetaan verkon käyttäjien, työasemien, ryhmien ja muiden resurssien lisäämistä ja määrittämistä Active Directoryyn.

Yrityksissä on usein tilanne, että kullekin työntekijälle halutaan luoda omat tunnukset, joilla pystyy kirjautumaan yrityksen verkkoon. Tämä pystytään toteuttamaan Active Directoryn avulla siten, että luodaan jokaiselle käyttäjälle oma objekti Active Directoryn tietokantaan. Kun halutaan rajata näiden käyttäjien pääsyä jaettuihin tiedostoihin ja resursseihin, puhutaan sellaisista käsitteistä kuin ryhmistä, ryhmäkäytännöistä ja käyttöoikeuksista. Näihin on syvennytty tarkemmin seuraavissa kappaleissa.

2.2.3.1 Käyttöoikeudet

Käyttöoikeuksilla tarkoitetaan sääntöjä, jotka asetetaan jokaiselle verkossa jaettavalle kansiolle tai resurssille. Nämä säännöt voidaan asettaa voimaan esim. yksittäiselle käyttäjälle, luodulle ryhmälle tai kaikille käyttäjille. Kaikki kohteet, joille käyttöoikeuksia asetetaan voimaan, on löydyttävä Active Directorysta. Ryhmiä luomalla voi helposti rajata pääsyä tietyiltä käyttäjiltä tai vastaavasti tarjota pääsyn tiettyyn kansioon tai resurssiin. Esimerkiksi, jos luodaan kaksi ryhmää nimeltä myynti ja hallinto, voidaan halutessaan antaa myynti-ryhmälle oikeus päästä lukemaan jaettavan kansion tietoja ja hallinto-ryhmältä estää pääsy kansioon kokonaan. Active Directoryssa pystytään määrittämään mitkä käyttäjät kuuluvat mihinkin ryhmään. (24)

Käyttöoikeudet tarjoavat kattavan määrän vaihtoehtoja, miten pääsyä voidaan rajoittaa. Jaettavan kansion luoja voi tarvittaessa antaa valituille käyttäjille tai ryhmille vain lukuoikeudet kansion sisältöön, jolloin käyttäjät pystyvät näkemään kansion sisällön, mutta eivät pysty muokkaamaan sitä millään tavalla. Taulukossa 2 on esitetty lista tärkeimmistä vaihtoehdoista, joita voidaan asettaa jaettavalle kansiolle tai tiedostolle. Jos yri-

tyksessä on tarve määritellä erittäin tarkasti pääsyoikeudet, on tarjolla myös lista erityisoikeuksia, joilla pystytään määrittämään yksityiskohtaisemmin kunkin kansion tai tiedoston käyttöoikeuksista. Pääsääntöisesti kuitenkin riittää seuraavassa listassa esitettyjen oikeuksien määrittäminen. (18)

Käyttöoikeudet	**Merkitys**
Full Control	Täydet hallintaoikeudet
Modify	Muokkausoikeudet
Read & Execute	Luku- ja suoritusoikeudet
List Folder Contents	Kansion sisällön listausoikeudet
Write	Kirjoitusoikeudet

Taulukko 2. Jaettavan kansion tai tiedoston käyttöoikeudet (18)

Näitä sääntöjä järkevästi yhdistelemällä saadaan luotua verkkoympäristöön sopivat käyttöoikeudet kansioille ja tiedostoille. Hyvin asetetut oikeudet edesauttavat verkkoympäristön tietoturvallisuutta ja helpottavat ylläpitoa. Oikeuksia asettaessa on otettava huomioon, että on mahdollista myös varta vasten estää tiettyjä oikeuksia. Paras menettelytapa onkin asettaa mahdollisimman tiukat rajoitteet kuitenkin mahdollistaen tarvittavat pääsyoikeudet halutuille käyttäjille. Myös viisas menettelytapa on asettaa käyttöoikeudet ryhmille ennemmin kuin yksittäisille käyttäjille. (25)

Verkkoympäristössä jaetuille tulostimille pystytään asettamaan käyttöoikeudet samaan tapaan kuin kansioille ja tiedostoillekin ryhmä tai käyttäjäkohtaisesti. Tulostimien osalta valittavana olevat oikeudet ovat kuitenkin hieman erilaiset. Nämä vaihtoehdot ovat esitetty taulukossa 3.

Käyttöoikeudet	**Merkitys**
Print	Tulostusoikeudet
Manage Documents	Tulostusjonojen hallintaoikeudet
Manage Printers	Tulostimien hallintaoikeudet

Taulukko 3. Jaettavan tulostimen käyttöoikeudet (17)

Kun käyttöoikeudet ovat asetettu halutulla tavalla, tulee ottaa huomioon oikeuksien periytyminen. Tämä tarkoittaa sitä että, jos kansioon johon on asetettu käyttöoikeudet, luodaan uusia tiedostoja tai kansioita, ne perivät samat oikeudet jotka ovat asetettu alkuperäiselle kansiolle. Uusille kansioille tai tiedostoille voidaan toki asettaa uudet oikeudet tarvittaessa. Periytymisen voi myös halutessaan ottaa pois käytöstä, jolloin uusille kansioille tai tiedostoille ei tule alkuperäisen kansion käyttöoikeuksia automaattisesti. (19)

2.2.3.2 Ryhmäkäytäntö

Ryhmäkäytännöllä tarkoitetaan kokoelmaa sääntöjä, jotka ovat kerätty yhteen pakettiin. Tätä pakettia kutsutaan nimellä Group Policy Object. Group Policy Objektit luodaan Active Directoryyn, jossa niitä voidaan linkittää eri käyttäjäryhmille tai työasemille. Yksi Group Policy Object voi sisältää sääntöjä esim. sovellusten asennukseen ja käyttöön, työasemien tiedostojen hallintaan, työasemilla ajettavien skriptien hallintaan tai tietoturvaan liittyen. Ryhmäkäytäntöihin määritettäviä asetuksia on satoja, ellei tuhansia. Tässä kappaleessa kerrotaan lyhyesti mihin ryhmäkäytäntöjä voidaan yleisesti käyttää yritysmaailmassa. (21)

Monissa yrityksissä halutaan rajoittaa käyttäjien työasemien käyttöä. Ryhmäkäytännöillä voidaan esimerkiksi estää käyttäjiä tekemästä muutoksia käyttöjärjestelmän asetuksiin, joka voi olla erittäin hyvä idea varsinkin, jos on kysymys käyttäjistä, jotka eivät tarkkaan tiedä mitä ovat tekemässä. Tämä helpottaa verkkoympäristön ylläpitäjän tehtäviä, kun käyttäjät eivät voi tahallaan tai vahingossa sekoittaa omia työasemiaan.

Ryhmäkäytännöillä voidaan myös määrittää sääntöjä esimerkiksi siitä, mihin kellonaikaan työasemalla voidaan olla kirjautuneena tai mitä sovelluksia työasemilla voidaan käyttää. Tietoturvallisuuden kannalta voidaan määritellä esimerkiksi se kuinka monta kertaa käyttäjä voi yrittää kirjautua sisään väärällä salasanalla ennen kuin käyttäjätili menee lukkoon. (21)

2.2.4 Palvelimen poisto

Jossain vaiheessa palvelimen elinkaarta tulee vastaan tilanne, kun palvelin tarvitsee ottaa pois tuotantokäytöstä. Syitä siihen voi olla esimerkiksi liian vanha ja heikko laitteisto, jota ei kannata enää päivittää, tai laitteiston vakava rikkoutuminen. Kun laitteiden virhetiheys rupeaa kasvamaan liian suureksi, se tulee ottaa pois käytöstä liian riskialttiuden takia.

Microsoft tarjoaa jatkettua tukea Windows Server 2003- versioille vuoteen 2015 ja Windows Server 2008 R2:lle perustukea vuoteen 2013 ja jatkettua tukea vuoteen 2018 saakka. Perustuen päättyminen tarkoittaa sitä, että käyttöjärjestelmään ei tarjota enää muita parannuksia ja korjauksia kuin tietoturvaan liittyen. Tuen päättyminen kokonaan on yksi tekijä minkä takia palvelin poistetaan tuotantokäytöstä, koska tietoturvariskit kasvavat liian suureksi. (36, 37)

Jos päädytään ratkaisuun että palvelin poistetaan kokonaan tuotantokäytöstä, tarvitsee myös varmistua että kaikki siihen liittyvät tiedot poistetaan verkkoympäristön tietokannoista. Poistettava palvelin tulee poistaa esimerkiksi WSUS- päivityslistalta, jotta WSUS- palvelin ei turhaan yritä lähettää sille uusia päivityksiä ja anna virheilmoituksia päivitysten epäonnistumisesta. Ylimääräinen ja turha tieto on aina hyvä poistaa tietokannoista, koska ne ovat potentiaalisia turvallisuusriskejä ja saattavat myös aiheuttaa muita ongelmia verkkoympäristössä.

3 Best practices

3.1 Active Directoryn suunnittelu

Kun lähdetään rakentamaan uutta Windows- verkkoympäristöä, yksi tärkeä osa on Active Directoryn suunnittelu. Hyvällä Active Directory- suunnittelulla voidaan ennaltaehkäistä käyttöönoton jälkeen muodostuvia ongelmia. Suunnittelussa on otettava huomioon asioita ylläpidon kannalta kuin myös käyttäjien näkökulmasta. On tärkeää ottaa huomioon, että resurssit ovat tavoitettavissa vaikka ne sijaitsevat eri toimialueilla. Paras tapa resurssien saatavuuden kannalta on luoda vain yksi toimialue, mutta suurissa verkkoympäristöissä se on vähintäänkin vaikeaa ylläpitää. Jos on tarpeellista luoda useita toimialueita, kannattaa ne eritellä maantieteellisen sijainnin mukaan. (23)

Kaikkia Active Directoryyn luotavia työasemia, käyttäjiä, ryhmiä jne. kutsutaan objekteiksi. Kun halutaan jaotella Active Directoryssa yhden toimialueen objekteja omiin lohkoihinsa, puhutaan Organizational Unit- yksiköistä. Yhden OU- yksikön sisään voidaan sijoittaa mitä tahansa Active Directory- objekteja. Active Directoryn suunnittelijan tulee miettiä millä perusteella jaotella objektit OU- yksiköihin. Kun OU- yksiköt ovat luotu, niiden muokkaaminen myöhemmin usein sekoittaa koko Active Directoryn ja siihen sidotut ryhmäkäytännöt. OU- yksiköiden jaottelussa kannatta miettiä mitä yksiköillä pyritään saavuttamaan. Esimerkiksi, jos pyritään saamaan organisaation kullekin toimipisteelle oma OU- yksikkö, kannattaa jaottelu tehdä maantieteellisen sijainnin mukaan. Hyvä tapa on myös sijoittaa työasema- ja käyttäjäobjektit eri OU- yksiköihin, koska tämä helpottaa ryhmäkäytäntöjen luomista. Paras menettely on kuitenkin luoda vain niin monta OU- yksikköä kuin oikeasti on tarpeellista. Usein yksinkertaisin tapa on paras tapa. (23)

Niin kuin on mainittu kappaleessa 3.1.1.1, on syytä suunnitella vähintään kaksi ohjauspalvelinta jokaiseen toimialueeseen. Mikäli verkkoinfrastruktuuri sisältää useita toimialueita, kannattaa yksi ohjauspalvelin jokaiselta toimialueelta määrittää toimimaan Global Catalogina. Jos rakentaa verkkoympäristönsä niin, että sijoittaa vain yhden ohjauspalvelimen jokaiselle toimialueelle, tulee ympäristöstä todella riskialtis. Jos toimialueen ainoa ohjauspalvelin vioittuu, aiheuttaa se koko toimialueen ”lamaantumisen”, ja suuri osa kyseisen toimialueen palveluista on saavuttamattomissa. (23)

3.2 Päivittäminen Windows Server 2003- versiosta Windows Server 2008- versioon

Paras tapa uudistaa toimialueen käyttöjärjestelmä uuteen Windows Server 2008 versioon on tehdä niin sanotusti puhdas asennus ennemmin kuin vain päivitys vanhasta Windows Server 2003- versiosta. Kun palvelimet ovat olleet kauan tuotantokäytössä, kertyy niihin ylimääräistä dataa, joka ajan mittaan saattaa ruveta hidastamaan prosesseja. Saman käyttöjärjestelmän puhdasta asentamista ei usein viitsitä suorittaa sen työläyden ja hankaluuden takia. Jos kuitenkin halutaan päivittää käyttöjärjestelmät uuteen versioon, voidaan samalla suorittaa puhdas asennus. (23)

Ensimmäinen vaihe uutta käyttöjärjestelmäversiota käyttöönotettaessa on Active Directory Scheman päivittäminen Windows Server 2008:aa varten. Tämä Schema pitää sisällään viralliset määritykset kaikista objektiluokista, joita voidaan luoda Active Directoryyn. Scheman fyysinen rakenne koostuu näistä määrityksistä ja Schema itsessään on tallennettu Active Directoryyn. Scheman päivittäminen on vaikein osa käyttöjärjestelmän päivitysprosessia. Scheman päivittäminen voi mahdollisesti aiheuttaa vakavia ongelmia, joten järjestelmien varmuuskopiointi ennen aloittamista on enemmän kuin suositeltavaa. (23, 28)

Kun lähdetään tekemään puhdasta asennusta, vaaditaan sitä, että palvelin jota päivitetään, täytyy ottaa pois tuotantokäytöstä päivityksen ajaksi. Jotta verkkoympäristö pysyisi muuttumattomana asennusprosessin ajan, täytyy toimialueeseen lisätä yksi ohjauspalvelin, jolle replikoidaan olemassa oleva tietokanta. Tätä uutta palvelinta käytetään sen ajan, kun yhdelle ohjauspalvelimelle tehdään asennusta. Koska tämä uusi palvelin on väliaikainen ratkaisu, kannattaa harkita sen toteuttamista virtuaalisena. (23)

Harkinnan arvoinen vaihtoehto on myös se, että sammutetaan yksi toimialueen ohjauspalvelimista päivityksen ajaksi. Jos päivityksen aikana ilmenee ongelmia eikä varmuuskopioiden avulla palauttaminen jostain syystä onnistu, voidaan sammutetun palvelimen tietokannasta palauttaa alkuperäiset konfiguraatiot. Tämä palvelin voidaan päivittää viimeisenä, kun muut palvelimet ovat saatu onnistuneesti päivitettyä uuteen versioon. (23)

Kun kaikki toimialueen ohjauspalvelimet ovat saatu päivitettyä uuteen versioon, voidaan toimialueen toiminta-aste (Function Level) nostaa uudelle Windows Server 2008-tasolle. Tämä avaa uusia ominaisuuksia verkkoympäristön ylläpitäjän käyttöön. (23)

3.3 Windows Server 2008 R2- ympäristön tietoturvan vahvistaminen

Ensimmäinen asia mikä kannattaa suorittaa, kun lähtee vahvistamaan tietoturvaa, on asentaa Security Configuration Wizard. Se tarkistaa portteja ja palveluita heikkouksien varalta, ottaen huomioon palvelimelle asennetun roolin. Kaikki turhat avoimet portit ja palvelut on syytä sulkea, sillä ne tarjoavat mahdollisuuksia hyökkäyksille. Palvelimelle asennettavien sovellusten määrä on syytä pitää minimissään ja, jos joku sovellus jää ylimääräiseksi, se on syytä poistaa. Jotkut sovellukset saattavat avata takaportteja joita hyökkääjät käyttävät hyväkseen. (30)

Jokaiselle palvelimelle on syytä asettaa käyttöön palomuuri. Windows Serveriin on sisäänrakennettu Windows Firewall with Advanced Security, jota voi käyttää mikäli ei halua asentaa kolmannen osapuolen palomuuria. Windowsin oma palomuuri on kehittynyt vuosien saatossa merkittävästi ja on varteenotettava vaihtoehto yrityksen palomuurisovellukseksi. (30)

Windows Server 2008 R2:ssa Active Directoryn tietojen auditointi on kehittynyt Windows Server 2003- versiosta. Uudessa auditoinnissa pystytään tarkistamaan muutetun atribuutin vanha ja uusi tieto sekä pystytään katsomaan kuka on tehnyt muutoksen. Tämä auttaa ongelmien paikantamisessa ja ratkaisussa. (30)

Palvelimille tallennettava tärkeä data on todella suositeltavaa kryptata siihen soveltuvalla ohjelmistolla. Windows Server 2008 R2 tarjoaa oman tiedon kryptaustyökalun nimeltä Bitlocker Drive Encryption. Tämän avulla pystytään salakirjoittamaan kokonaisia levyasemia. (30)

Verkkoympäristön ylläpitäjän tulee pitää palvelimien ja niissä pyörivien sovellusten päivitykset ajan tasalla, koska ne sisältävät tietoturvaparannuksia ja korjauksia. Jokaisella palvelimella tulisi olla käytössä myös antivirus- ohjelmisto, jonka tietokanta tulee myös pitää ajan tasalla. (30)

3.4 Hyper V- palvelinrooli

Kun palvelimelle otetaan käyttöön Hyper V- palvelinrooli, tarvitsee ottaa huomioon useita asioita parhaan toimintakyvyn saavuttamiseksi. Ensimmäinen asia mitä tulee miettiä, on palvelimen kuormitusaste. Ennen palvelimen käyttöönottoa on syytä suunnitella, kuinka monta virtuaalijärjestelmää palvelimella aiotaan ylläpitää. Paras käyttöjärjestelmäversio Windows Server 2008 R2:sta useiden virtuaalijärjestelmien ylläpitämiseen on Datacenter x64, joka tukee 64:ää prosessoria sekä kahta teratavua keskusmuistia ja tukee teoriassa ääretöntä määrää virtuaalijärjestelmiä. (32)

Toinen asia mitä kannattaa miettiä, on palvelimella käytettävien kovalevyjen tyyppi. Jos palvelimella pyörii useita virtuaalijärjestelmiä, jotka kaikki hyödyntävät samaa fyysistä kovalevymuistia, on syytä käyttää ns. highspeed- kovalevyjä, jotka tarjoavat mahdollisimman nopean datan käsittelyn. (32)

Hyper V- roolissa toimivalle palvelimelle on myös viisasta kytkeä useampia verkkokortteja. Yksi verkkokortti kannattaa allokoida pelkästään palvelimen ylläpitoa varten ja vähintään kaksi verkkokorttia virtuaalijärjestelmien liikennettä varten, vikasietoisuuden parantamiseksi. Hyper V- palvelimen suorituskykyä on syytä valvoa kokoajan erinäisillä valvontatyökaluilla, jotta pystytään tunnistamaan, jos esimerkiksi johonkin järjestelmään pitää allokoida enemmän resursseja tai johonkin järjestelmään on allokoitu liikaa. Myös verkkoliikennettä tulee valvoa ja määritellä kuormanjako järkevästi. Resurssien ja kaistan optimaalinen jakaminen mahdollistaa parhaan suorituskyvyn kaikille virtuaalijärjestelmille. (32)

Jos Hyper V- palvelimella on käytössä antivirus- ohjelmisto, kannattaa harkita Hyper V- prosessien (Vmms.exe ja Vmswp.exe) jättämistä antivirus- ohjelmiston aktiivisen valvonnan ulkopuolelle. Myös virtuaalijärjestelmien määritykset sisältävät kansiot, kannattaa jättää aktiivisen valvonnan ulkopuolelle. Lisäksi levyasemille, joihin virtuaalijärjestelmien tiedostot on sijoitettu, ei kannata tallentaa mitään muuta dataa. (32)

4 Pohdinta

Tähän opinnäytetyöhön on kerätty kompakti paketti tietoa aiheista, joista olisi mahdollista kirjoittaa monta kirjaa. Opinnäytetyö pyrkii tarjoamaan lukijalleen yhteenvedon/ tiivistelmän verkkoympäristön osa-alueista ja pyrkii kiinnittämään lukijan huomion tärkeisiin seikkoihin, joita tarvitsee harkita ollessaan Windows- verkkoympäristöjen kanssa tekemisissä.

Tiedonhaku työhön tapahtui sujuvasti, sillä materiaalia tästä aiheesta löytyi runsaasti. Vaikeuksia tuotti se, kun yritti valita vain tämän työn puitteisiin tärkeitä asioita todella laajasta materiaalista. Suurin osa tiedoista löytyi Internetistä ja osa kirjallisuudesta. Myös Cybercomin Finland Oy:n työntekijöiden kanssa käytiin läpi opinnäytetyön sisältöä useita kertoja.

Työn kirjoittaminen oli haastava mutta samalla palkitseva projekti, jonka aikana oppi paljon uutta asiaa tietoverkoista yleisesti ja ennen kaikkea Windows- ympäristöistä. Yritykset käyttävät Windows- verkkoympäristöjä laajalti nyt ja varmasti tulevaisuudessakin, joten niiden osaaminen ja ymmärtäminen on selkeä etu työelämässä.

Lähteet

1. What is web server - a computer of a program? [online] [viitattu 26.3.2012] http://www.webdevelopersnotes.com/basics/what_is_web_server.php

2. What is a Mail Server? [online] [viitattu 26.3.2012] http://whatismyipaddress.com/mail-server

3. Understanding Server Roles [online] [viitattu 26.3.2012] http://www.tech-faq.com/understanding-server-roles.html

4. Windows Server 2008 R2 [online] [viitattu 19.3.2012] http://www.microsoft.com/en-us/server-cloud/windows-server/default.aspx

5. Windows Deployment Services Getting Started Guide [online] [viitattu 26.3.2012] http://technet.microsoft.com/en-us/library/cc771670%28v=ws.10%29.aspx

6. Roggen, Kurt 2007. Server Manager - Adding Roles & Features [online] [viitattu 27.3.2012] http://trycatch.be/blogs/roggenk/archive/2007/07/13/server-manager-adding-roles-amp-features.aspx

7. Vihjeitä vahvan salasanan luomiseen [online] [viitattu 2.4.2012] http://windows.microsoft.com/fi-FI/windows-vista/Tips-for-creating-a-strong-password

8. Implement a Centralized Desktop Strategy [online] [viitattu 5.4.2012] http://www.microsoft.com/en-us/server-cloud/windows-server/remote-desktop-services-overview.aspx

9. Windows Server 2008 R2 Hyper-V Overview [online] [viitattu 5.4.2012] http://www.microsoft.com/en-us/server-cloud/windows-server/hyper-v-overview.aspx

10. Rist, Oliver 2009. Windows Server 2008 R2 Reaches the RTM Milestone! [online] [viitattu19.3.2012] http://blogs.technet.com/b/windowsserver/archive/2009/07/22/windows-server-2008-r2-rtm.aspx

11. Microsoft Windows Server 2008 R2 [online] [viitattu 26.3.2012] http://www.moonsoft.fi/products/000562.aspx

12. Active Directory Overview [online] [viitattu 26.3.2012] http://www.microsoft.com/en-us/server-cloud/windows-server/active-directory-overview.aspx

13. [online] [viitattu 5.4.2012] http://www.grouppolicy.biz/wpcontent/uploads/2010/08/image_thumb3.png

14. What is a Backup Server? [online] [viitattu 10.4.2012] http://www.spamlaws.com/backupserver.html

15. Petri, Daniel 2009. Microsoft Software Update Service (SUS) [online] [viitattu 10.4.2012] http://www.petri.co.il/sus.htm

16. Identifying Security Issues Common to All Server Roles [online] [viitattu 10.4.2012] http://www.tech-faq.com/identifying-security-issues-common-to-all-server-roles.html

17. Assigning printer permissions[online] [viitattu 10.4.2012] http://technet.microsoft.com/en-us/library/cc773372%28v=ws.10%29.aspx

18. How to set, view, change, or remove special permissions for files and folders [online] [viitattu 10.4.2012] http://support.microsoft.com/kb/308419

19. How inheritance affects file and folder permissions [online] [viitattu 10.4.2012] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/acl_inherit_permissions.mspx?mfr=true

20. Windows Server 2008 R2 Editions [online] [viitattu 24.4.2012] http://www.microsoft.com/en-us/server-cloud/windows-server/2008-r2-editions.aspx

21. In Microsoft Active Directory, what are group policies? [online] [viitattu 10.4.2012] http://kb.iu.edu/data/ajgk.html

22. Deploy Windows Server 2008 R2 [online] [viitattu 10.4.2012] http://technet.microsoft.com/en-us/library/ee344846%28v=ws.10%29.aspx

23. Shields, Greg. 2008. The Definitive Guide to Building Windows Server 2008 Infrastructure. Realtime Publishers.

24.Melber, Derek 2005. Share Permissions [online] [viitattu 12.4.2012] http://www.windowsecurity.com/articles/share-permissions.html

25. Best practices for permissions and user rights [online] [viitattu 12.4.2012] http://technet.microsoft.com/en-us/library/cc779601%28v=ws.10%29.aspx

26. Windows Deployment Services Getting Started Guide [online] [viitattu 12.4.2012] http://technet.microsoft.com/en-us/library/cc771670%28v=ws.10%29.aspx

27. [online] [viitattu 12.4.2012] http://msdn.microsoft.com/enus/library/windows/desktop/ms675085%28v=vs.85%29.aspx

28. How the Active Directory Schema Works [online] [viitattu 12.4.2012] http://technet.microsoft.com/en-us/library/cc773309%28v=ws.10%29.aspx

29. Windows 7 and Windows Server 2008 R2 Application Quality Cookbook [online] [viitattu 16.4.2012] http://msdn.microsoft.com/en-us/library/dd371778%28v=vs.85%29.aspx

30. *De Carvalho, Daniel 2008. 10 steps to harden Windows Server 2008 [online] [viitattu 17.4.2012] http://blog.tevora.com/enterprise-applications/10-steps-to-harden-windows-server-2008-2/*

31. *Posey, Brian M. 2004 The Pros and Cons of Running Virtual Server [online] [viitattu 18.4.2012] http://www.windowsnetworking.com/articles_tutorials/pros-cons-virtual-server.html*

32. *7 Best Practices for Physical Servers Hosting Hyper-V Roles [online] [viitattu 18.4.2012] http://technet.microsoft.com/en-us/magazine/dd744830.aspx*

33. *Failover Clusters in Windows Server 2008 [online] [viitattu 18.4.2012] http://technet.microsoft.com/en-us/library/ff182326%28v=ws.10%29.aspx*

34. *What Is Server Core? [online] [viitattu 20.4.2012] http://technet.microsoft.com/en-us/library/dd184075.aspx*

35. *What is Active Directory? [online] [viitattu 20.4.2012] http://www.dekart.com/howto/howto_logon/howto_logon_active_directory/whatis_active_directory/*

36. *Microsoft-tuotetuen elinkaari [online] [viitattu 23.4.2012] http://support.microsoft.com/lifecycle/?LN=fi&x=16&y=14&p1=10394*

37. *Microsoft-tuotetuen elinkaari [online] [viitattu 23.4.2012] http://support.microsoft.com/lifecycle/?LN=fi&x=15&y=12&p1=14134*

38. *Active Server Page (ASP)[online] [viitattu 27.4.2012] http://searchwindowsserver.techtarget.com/definition/Active-Server-Page*

Liitteet

Liite 1. Esimerkkikuva palvelinten sijainnista verkkoympäristössä.