



LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Pienyrityksen palvelinmigraatio

Tino Graubner

2018 Laurea



Laurea-ammattikorkeakoulu

Pienyrityksen palvelinmigraatio

Tino Graubner
Tradenomi
Opinnäytetyö
Toukokuu, 2018

Tino Graubner

Pienyrityksen palvelinmigraatio

Vuosi 2018 Sivumäärä 28

Opinnäytetyön tavoitteena oli selvittää tarvittavat toimenpiteet asiakasyrityksen palvelinmigraatiolle. Tarkoitus oli vaihtaa yrityksen vanha Windows Server 2008-käyttöjärjestelmää käyttävä palvelin uuteen Windows Server 2016 Essentials -palvelimeen. Migraation yhteydessä pyrittiin päivittämään yrityksen IT-infrastruktuuria vastaamaan parhaita käytäntöjä. Alkuperäisen palvelimen toiminnallisuuden kopioimisen lisäksi työ pyrittiin siten toteuttamaan alan standardeja noudattaen. Myös yrityksen olemassa olevaa infrastruktuuria on hyödynnetty mahdollisimman paljon työn helpottamiseksi.

Keskeiset tehtävät olivat siirtää Active Directory-hakemistopalvelu uudelle palvelimelle, asentaa Trend Micro Worry-Free Business Security-antiviruspalvelimen uusin versio, luoda uudelle palvelimelle verkkolevy ja siirtää sinne vanhan verkkolevyn sisältö. Lisäksi työasemat tuli siirtää uuden toimialueen piiriin ja niihin tuli asentaa Trend Micro Antiviruksen Security Agent-ohjelma. Infrastruktuuria on myös kehitetty automatisoimalla toimintoja ryhmäkäytännöillä ja ajastetuilla tehtävillä.

Työ toteutettiin iteratiivisena prosessina. Suunnittelua ja toteutusta tehtiin lyhyissä sykleissä. Tarvittavat ominaisuudet toteutettiin yrityksen toiminnan kannalta tärkeysjärjestyksessä. Prosessia vietiin eteenpäin saatujen tulosten ja asiakkaan palautteen perusteella. Tarvittaessa palattiin lisäämään tai hiomaan ominaisuuksia, kunnes työn tavoite saavutettiin. Tietoperustana on käytetty kokemusta Windows Server-palvelinympäristöistä sekä ohjelmistojen tuottajien ohjeita ja teknisiä foorumeita. Työn tuloksena yrityksen IT-infrastruktuuri on parantunut, ja esimerkiksi varmuuskopiointi on automatisoitu. Tätä opinnäytetyötä voi myös käyttää referenssinä pienen yrityksen tai organisaation Windows-palvelinympäristön luomisessa ja versiopäivityksessä.

Asiasanat: active directory, group policy, varmuuskopiointi

Tino Graubner

Server migration for a small company

Year	2018	Pages	28
------	------	-------	----

The goal of this thesis was to determine the actions required for the client company's server migration. The purpose was to swap the company's old server that utilized Windows Server 2008 as the operating system to a new one with Windows Server 2016 Essentials. During the migration the company wanted to update their infrastructure to be more in line with the best practices in IT. In addition to replicating the functionality of the original server efforts have been made to do so in accordance with modern standards. The company's existing infrastructure has been leveraged as much as possible to reduce the amount of work.

The main tasks were to migrate Active Directory to the new server, install the newest version of Trend Micro Worry-Free Business Security antivirus server, create a shared network folder and migrate all data from the old server. Additionally, all of the company's workstations had to be migrated to the new domain, and have Trend Micro's Security Agent software installed on them. The company's infrastructure has also been upgraded by automating work with group policies and scheduled tasks.

The work was done as an iterative project. Planning and implementation was done in short cycles. Features were implemented in the order of their importance for the client company. The initial results and feedback from the client were used to refine and add to the project as necessary, until the project was completed. The knowledge base used in the project is based on experience with Windows Server-environments as well as manuals from the software vendors and technical forums. As a result of the project the client company's IT-infrastructure is on a better foundation, and for example back-ups are automated. This thesis can also be used as a reference for creating and updating a small company's or organizations Windows-server environment.

Keywords: active directory, group policy, back-up

Sisällys

1	Johdanto	6
1.1	Suunnittelu	7
1.2	Työskentelymenetelmä	7
2	Asennus.....	8
3	Ominaisuuksien asennus.....	9
4	Active Directory	10
5	Verkkolevy	11
6	Trend Micro Worry-Free	14
6.1	Worry-Free palvelimen asennus	15
6.2	Asetusten määrittäminen	15
7	Ryhmäkäytännöt.....	16
7.1	Verkkolevy	17
7.2	HP LaserJet 2055x	17
7.3	Trend Micro Security Agent Install	18
8	Verkko	21
8.1	DHCP	22
8.2	DNS	23
9	Yhteenveto	24
9.1	Kehitysehdotukset	25
9.2	Oma arviointi	25

1 Johdanto

Lähes jokainen yritys nykypäivänä tarvitsee jonkinlaisen IT-infrastruktuurin työnteon tueksi. Useimmissa yrityksissä työntekijöillä on käytössä Windows-työasemia, jotka ovat liitetty yrityksen toimialueeseen. Toimialueella tarkoitetaan tässä yhteydessä Windows-käyttöjärjestelmällä toimivia työasemia, tai muita IT-infrastruktuurin osia kuten nettisivuja tai verkkolevypalvelimia, joita hallitaan keskitetysti yhden tai useamman Windows-palvelimen Active Directory Domain Services -palvelun kautta.

Asiakasyrityksen IT-infrastruktuuri käsittää työasemien, printterin, reitittimen ja kytkimen lisäksi palvelimen, joka mahdollistaa työasemien ja käyttäjätunnusten keskitetyn hallinnan, virustorjunnan sekä tiedostojen jakamisen ja varmuuskopioinnin verkkolevyllä. Palvelinta tullaan tässä työssä selkeyden vuoksi kutsumaan myös sen isäntanimellä (hostname), joka on SRV2016.

Asiakasyrityksen IT-infrastruktuuriin kuului yksi Windows 2008-palvelin, jonka vaihto oli tämän työn pääsääntöinen tehtävä. Tämän lisäksi yrityksen verkkoon on liitettynä 6 Windows-työasemaa, yksi printteri, Zyxelin palomuuuri/reititin, sekä Buffalo LinkStation verkkokovalevy. Palvelimen vaihto tuli yritykselle ajankohtaiseksi, koska vanhalla palvelimella oli vain 156 gigabittiä käytettävää tilaa, joka oli jaettu kahteen eri osioon, toinen käyttöjärjestelmälle ja toinen verkkolevyille. Osioinnissa oli kuitenkin aliarvioitu käyttöjärjestelmän tarvitsema tallennustila, jonka vuoksi sille ei lopulta tilanpuutteen takia saanut enää asennettua päivityksiä. Yritys oli myös joutunut luopumaan ostamansa Trend Micro Worry-Free Business -antiviruksen käytöstä, koska sen palvelinkomponenttia ei ollut mahdollista päivittää tilanpuutteen vuoksi. Tämän lisäksi Microsoftin tuki Windows Server 2008 -käyttöjärjestelmälle päättyy vuonna 2020.

Alun perin vanhan palvelimen Active Directory -tietokanta oli tarkoitus siirtää uudelle palvelimelle, niin että kaikki vanhat tunnukset toimisivat myös uuden palvelimen käyttöönoton jälkeen. Valitettavasti ennen kuin työ ehdittiin siltä osalta aloittaa, vanhan palvelimen kovalevyllä tapahtui virhe, jonka seurauksena Active Directoryn tietokanta korruptoitui. Tämä tarkoitti käytännössä, että keskitetty tunnistus yrityksen koneille ei enää toiminut, ja niille oli mahdollista kirjautua vain jo koneen muistissa olevilla tunnuksilla. Tästä syystä toimialue piti luoda kokonaan uudestaan uudelle palvelimelle, ja suorittaa työasemien ja niillä olevien käyttäjäprofiilien migraatio uuteen toimialueeseen.

Yrityksen uudeksi palvelimeksi päädyttiin hankkimaan Lenovon Thinkserver TS140 70A4-koonpanolla, ja käyttöjärjestelmäksi Windows Server 2016 Essentials. Nämä tuotteet valittiin,

koska ne sopivat hyvin hinnaltaan ja ominaisuuksiltaan yrityksen tarpeisiin. Tässä työssä kuvataan yksityiskohtaisesti uuden palvelimen ja sen ohjelmistojen asennus- ja asetusten määrittämisprosessit.

1.1 Suunnittelu

Suunnittelutyö aloitettiin kartoittamalla asiakasyrityksen tarpeet IT-infrastruktuurilta. Alun perin suurin tarve uudelle palvelimelle tuli vanhan palvelimen levytilan loppumisesta, jonka takia käyttöjärjestelmää ja Trend Micron Worry-Free-antiviruspalvelinta ei saanut enää päivitettyä. Tämän lisäksi asiakasyritys halusi uudelle SRV2016-palvelimelle automaattisen varmuuskopioinnin jaetulta verkkolevytä Buffalon verkkolevyasemalle.

Uudeksi palvelimeksi valittiin Lenovo Thinkserver TS140, 70A4-kokoonpanolla. Palvelimessa on Xeon E3-1226V3 -prosessori, 16 gigabittiä 1600 megahertsin DDR3 ECC välimuistia, RAID-ohjainkortti, sekä kaksi yhden teratavun kovalevyä. Kovalevyt ovat asetettu ns. peilaavaan, eli RAID1-tilaan. Tämä tarkoittaa, että molemmat kovalevyt sisältävät identtiset tiedot, mikä nopeuttaa tiedon lukua sekä mahdollistaa järjestelmän toimimisen yhden levyn hajotessa. (ThinkServer TS140 User Guide 2013, 32) Kyseisen palvelinmallin hankkimisesta sovittiin yhdessä asiakkaan kanssa, ja siihen päädyttiin, koska se oli hinnaltaan ja ominaisuuksiltaan tarpeita vastaava. Asiakasyritykselle oli tärkeää, että palvelimessa on riittävästi tehoa, ja että siinä on RAID1-ominaisuus kovalevyn hajoamisen varalta. Käyttöjärjestelmäksi valittiin Windows Server 2016 Essentials. Essentials on Windows Server 2016 -versioista kaikista halvin, mutta sisältää kuitenkin kaikki asiakasyrityksen tarvitsemat ominaisuudet, joten se sopi hyvin tähän tarkoitukseen.

Koska vanha palvelin oli toimialueen ainoa Active Directory-palvelin, ja sen tietokanta korruptoitui, oli tarve saada tämä ominaisuus heti uudella palvelimella käyttöön. Seuraava tehtävä oli saada yrityksen verkkolevy siirrettyä uudelle palvelimelle. Verkkolevy oli aikaisemmin toteutettu jaettuna kansioina vanhalla palvelimella, josta oli ajoittain manuaalisesti varmuuskopioitu tiedostot Buffalo-verkkolevyille. Infrastruktuurin päivityksen myötä varmuuskopiointi sovittiin toteutettavaksi ajastetulla tehtävällä, joka ajaa skriptin mikä varmuuskopioi verkkolevyjaon Buffalon varmuuskopiointi-verkkolevyasemalle.

1.2 Työskentelymenetelmä

Työ toteutettiin iteratiivisena prosessina, mikä tarkoittaa käytännössä, että palvelimelle asennettiin nopeasti asiakkaan haluamia ominaisuuksia ja ohjelmia, ja asennuksen jälkeen arvioitiin ominaisuuden/ohjelman toiminnan tarkoituksenmukaisuutta ja tehokkuutta, sekä pohdittiin ongelmakohtiin kehitysmahdollisuuksia. Työskentelyn kannalta tärkeät ominaisuudet asennettiin ja otettiin nopeasti käyttöön niiden yksinkertaisimmassa muodossa, jotta yrityksen päivittäinen toiminta ei häiriintyisi. Tämän jälkeen ohjelmia ja ominaisuuksia palattiin

hiomaan lopulliseen muotoonsa, keskeisenä tavoitteena manuaalisen ylläpidon tarpeen vähentäminen. Tietoperustana hyödynnettiin pitkälti käytännön kokemusta ja ymmärrystä Windows-toimialueista, ja yksityiskohtaiset asennusohjeet sekä ratkaisut ongelmiin haettiin ohjelmistojen valmistajien ohjeista ja teknisiltä foorumeilta.

2 Asennus

Asiakasyritys tilasi palvelimelle käytettäväksi Windows Server 2016 Essentials -käyttöjärjestelmän. Asennusmedia (CD-levy) toimitettiin palvelimen mukana ja sisälsi käyttöjärjestelmälle tarvittavan aktivointikoodin. Asennus aloitetaan käynnistämällä kone ja syöttämällä asennus-CD levyasemaan. Koneen käynnistyessä tulee painaa F9-näppäintä, jolla aukeaa BIOS-valikko. BIOS-valikosta on asetettu koneen kaksi kovalevyä RAID1- eli peilaavaan tilaan. Seuraavaksi valitaan ”Boot order”-valikko, josta määritellään miltä medioilta ja missä järjestyksessä kone yrittää ladata käyttöjärjestelmän. Tässä tapauksessa määriteltiin ensimmäiseksi koneelle luotu RAID-tallennustila, ja toiseksi CD-asema. Tämän jälkeen poistutaan BIOSista valitsemalla ”Save and exit”, jolloin muutokset tallentuvat ja kone käynnistyy uudelleen. Koska koneen sisäisestä tallennustilasta ei löydy vielä käyttöjärjestelmää, kone käynnistää Windowsin asennusvelhon käyttöjärjestelmän asennuslevyltä.

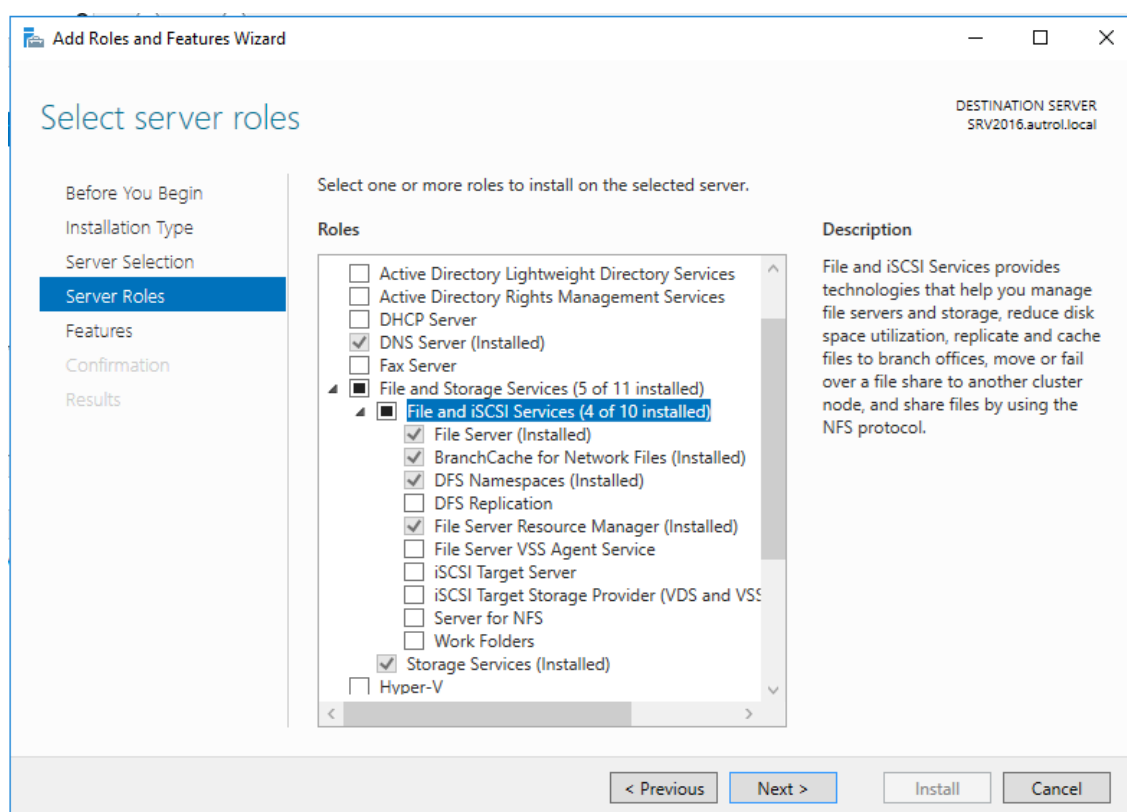
Asennusvelhon ensimmäisellä ruudulla valitaan käyttöjärjestelmän kieli, ajan ja valuutan formaatti sekä näppäimistöasettelu. Käyttöjärjestelmän kieleksi on valittu englanti, koska valtaosa internetistä löytyvästä käyttöjärjestelmän tukimateriaalista on englanniksi. Ajan ja valuutan formaatti sekä näppäimistöasettelu on asetettu suomeksi. Asennusvelhon seuraavassa vaiheessa syötetään käyttöjärjestelmän aktivointikoodi, jonka perusteella käyttöjärjestelmä pystyy todentamaan, että asennukseen on lisenssi. Mikäli aktivointikoodia ei syötä asennusvaiheessa, käyttöjärjestelmä toimii 180 päivää (ns. arviointi-aika) normaalisti jonka jälkeen se pysäyttää suurimman osan palveluista, ja siitä tulee pitkälti käyttökelvoton, ellei aktivointikoodia syötä.

Seuraavassa vaiheessa valitaan, halutaanko palvelimelle asentaa käyttöjärjestelmästä Server Core vai Desktop Experience -versio. Server Core -versiosta on riisuttu suurin osa graafisesta käyttöliittymästä, joka vähentää sen resurssijalanjälkeä, kun taas Desktop Experience -versio sisältää täyden käyttöliittymän, mutta vaatii enemmän resursseja. (Install Server with Desktop Experience 2017.) Tässä tapauksessa valitaan Desktop Experience -version, koska käytössä on runsaasti resursseja käyttöjärjestelmälle, ja graafinen käyttöliittymä on helppokäyttöisempi asiakkaalle, mikäli palvelimelle täytyy myöhemmin tehdä muutoksia.

Seuraavaksi valitaan levy, jolle käyttöjärjestelmä asennetaan. Tässä tapauksessa niitä on vain yksi -aikaisemmin luotu RAID1-peili. Tämän jälkeen luodaan salasanaa sisäänrakennetulle Administrator/Järjestelmänvalvoja -tilille. Näiden asetusten jälkeen asennusprosessi jatkuu loppuun ilman vuorovaikutusta.

3 Ominaisuuksien asennus

Käyttöjärjestelmän asennuksen jälkeen palvelimelle asennettiin tarvittavat roolit ja ominaisuudet ”Server Manager” -hallintapaneelin kautta. Rooleja ja ominaisuuksia lisätään avaamalla Server Managerista ”Manage”-valikko, ja sieltä ”Add roles or features”. Tässä tapauksessa palvelimelle asennettiin seuraavat roolit: Active Directory Domain Services, DNS Server, Storage Services, File Server, BranchCache for Network Files, DFS Namespaces, File Server Resource Manager, Print Server, Distributed Scan Server, DirectAccess and VPN, Web Server (IIS), sekä IIS Management Tools.



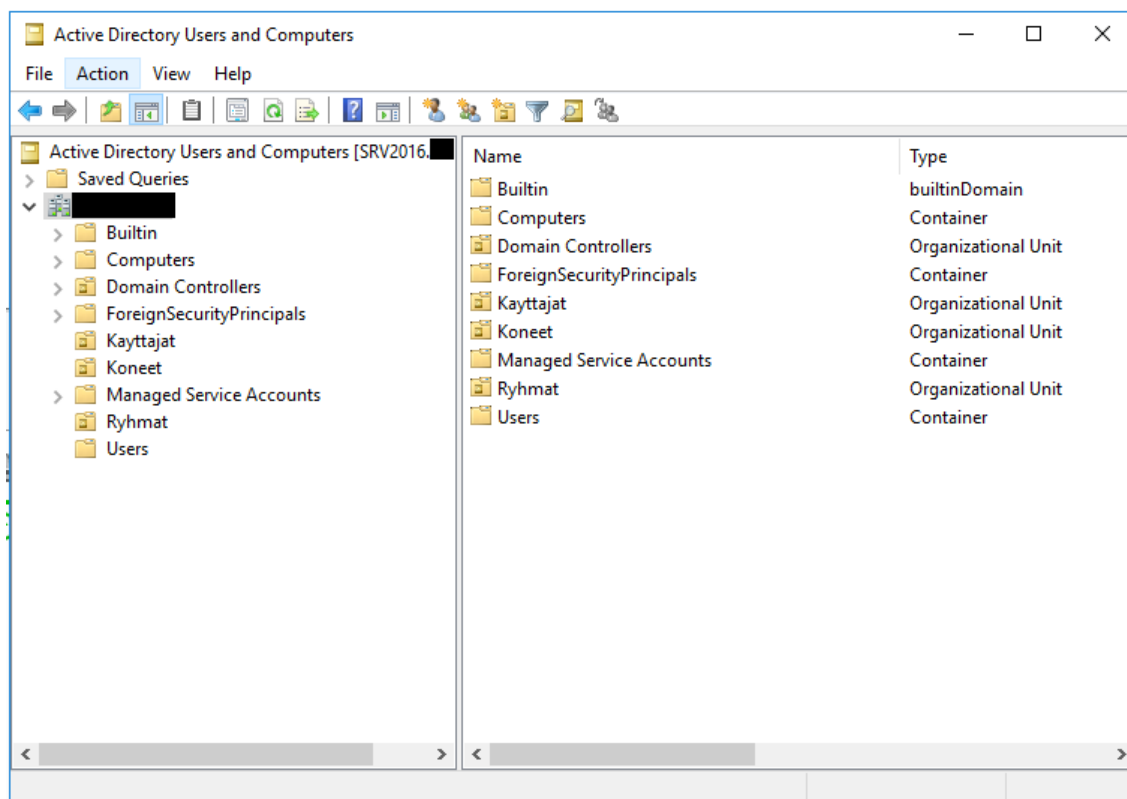
Kuvio 1 Roolien ja ominaisuuksien asennusvelho

Asennetut ominaisuudet ovat: .NET Framework 3.5, .NET Framework 4.6, ASP.NET 4.6, WCF Services (HTTP Activation, TCP Port Sharing), BranchCache, Group Policy Management, RAS Connection Manager Administration Kit, SMTP Server Tools, Active Directory module for Windows PowerShell, AD DS Tools, Certificate Authority Management Tools, DNS Server Tools, DFS Management Tools, File Server Resource Manager Tools, Print and Document Services Tools, Remote Access Management Tools, SMB 1.0/CIFS File Sharing Support, SMTP Server, Windows Defender Features, Windows Internal Database, Windows PowerShell 5.1, 2.0, ja ISE, Process

Model, Configuration APIs, Windows Search Service, Windows Server Backup, Windows Server Migration Tools, sekä WoW64 Support.

4 Active Directory

Active Directory -hakemistopalvelu on yleisesti Windows-toimialueissa käytettävä tietokanta, joka sisältää tiedot mm. toimialueen käyttäjätunnuksista ja koneista sekä niiden oikeuksista ja ryhmistä. Active Directory siis mahdollistaa keskitetyn hallinnan toimialueen käyttäjätunnuksille ja koneille. (Active Directory Domain Services Overview 2017.) Käytännössä tämä tarkoittaa, että kun kone on lisätty toimialueeseen, on sille mahdollista kirjautua toimialueen käyttäjätunnuksilla. Käyttäjätunnusten oikeuksia voi rajoittaa tarpeen mukaan. Active Directoryn rakennetta voi ja kannattaa muokata tarpeiden mukaan mm. tekemällä organisaatioyksiköitä, jotka toimivat AD:ssa kansion tapaan ja mahdollistavat ryhmäkäytäntöjen helpon rajauksen.



Kuvio 2 Active Directoryn hallintapaneeli

Koska vanhan palvelimen Active Directory -tietokantaa ei saanut palautettua kovalevyn hajoamisen jälkeen, oli kaikki yrityksen käyttäjätunnukset luotava uudestaan. Käyttäjille tehtiin oma organisaatioyksikkö Active Directoryyn, jotta käyttäjätileihin voi helpommin kohdistaa ryhmäkäytäntöjä. Oletuksena käyttäjätilit ovat "Users" -kansiossa, mutta koska tämä kansio

ei ole organisaatioyksikkö siihen ei ole mahdollista kohdistaa ryhmäkäytäntöjä. Oletuskäyttäjätunnukset, joita mm. erinäiset palvelut vaativat toimiakseen, ovat jätetty alkuperäiseen "Users" -kansioon.

Yrityksellä on käytössään kuusi Windows-työasemaa. Työasemille on Active Directoryssä luotu oma organisaatioyksikkö, sillä Active Directoryn oletuskansioihin ei voi kohdistaa ryhmäkäytäntöjä. (Sivarajan 2012.) Kaikille koneille on asennettu Windows 10 -käyttöjärjestelmä. Koska yrityksen toimialue jouduttiin siirtämään uuteen Active Directory -tietokantaan, vanhat käyttäjäprofiilit eivät enää toimineet, kun koneet liitettiin uuteen toimialueeseen. Vanhojen profiilien migraatioon käytettiin ForensIT -yrityksen Profile Wizard -ohjelmaa, joka siirtää vanhasta profiilista kaikki tiedostot sekä asetukset uuden toimialueen profiiliin. Ohjelman käyttö tapahtuu siten, että kone liitetään uuteen toimialueeseen, ohjelma käynnistetään, valitaan vanha profiili, josta tiedostot ja asetukset kopioidaan, sekä uusi profiili jonne ne kopioidaan. Tämän toimenpiteen jälkeen käyttäjiä pyydettiin varmistamaan, että kaikki heidän tiedostot olivat siirtyneet onnistuneesti, jonka jälkeen vanhat profiilit poistettiin koneilta.

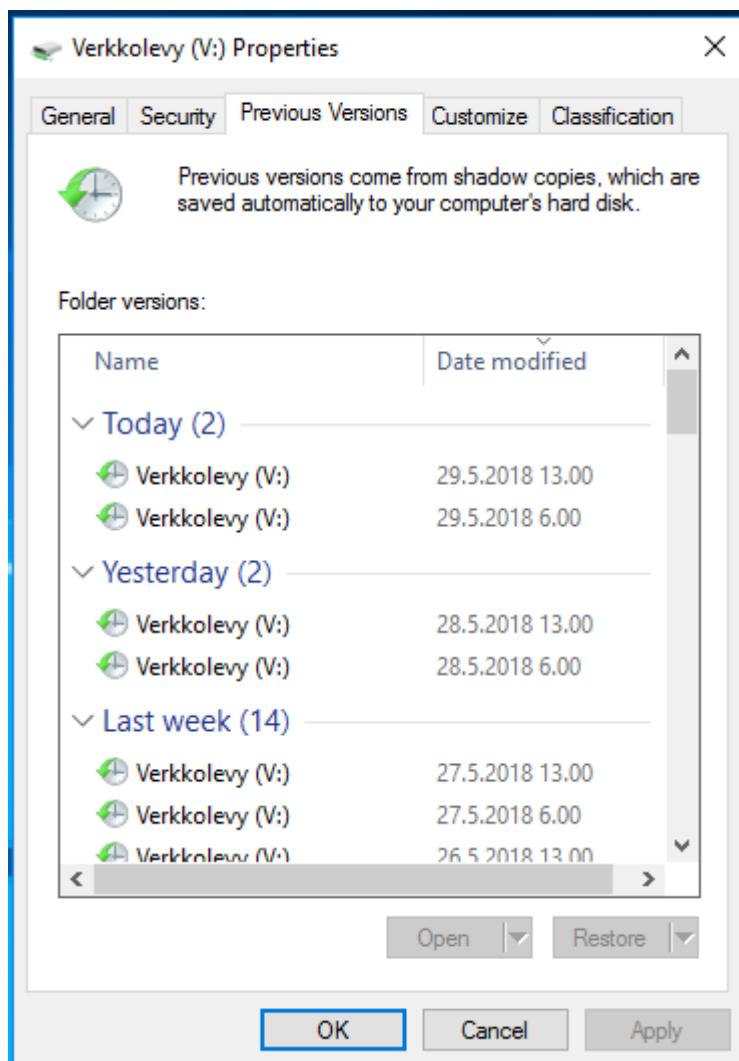
5 Verkkolevy

Nykyajan yritysverkkoihin kuuluu luonnollisesti verkkotallennusmahdollisuudet. Tietokoneiden ja mobiililaitteiden omaan tallennustilaan luottaminen ei ole turvallista, sillä ne voivat hajota tai laitteet voivat kadota tai tulla varastetuiksi. Tämän lisäksi verkkotallennustila tarjoaa mahdollisuuden tiedostojen versiointiin, jolloin virheelliset poistot tai muokkaukset voidaan poistaa palauttamalla tiedosto aikaisempaan versioon. Asiakasyrityksen kanssa sovittiin, että verkkotallennustila toteutetaan jakamalla palvelimelta kansio verkkoon, ja verkkolevyn sisältö varmuuskopioidaan päivittäin turvallisuus- sekä vakuutusyryistä toisessa huoneessa sijaitsevalle Buffalo Linkstation-verkkolevylle.

Verkkolevy on jaettu normaalisti Windowsin sisäänrakennetun verkkojako-ominaisuuden avulla. Yrityksen pienen koon takia kaikille toimialueen autentikoiduille käyttäjille on annettu "Modify" -oikeudet levylle. "Full control" -oikeudet on annettu "domain admins" -käyttäjäryhmälle. "Modify" -oikeudet sallivat käyttäjän lukea, muokata, luoda, ja poistaa tiedostoja. "Full control" -oikeudet sallivat lisäksi tiedoston oikeuksien muokkaukset. Tällä hetkellä kaikki käyttäjät pystyvät normaalisti hyödyntämään verkkolevyä ja kaikkia sinne tallennettuja tiedostoja. Tulevaisuudessa yrityksellä on mahdollisuus tehdä järjestelmänvalvojan tilillä kansioita tai tiedostoja, joihin vain tietyillä käyttäjillä tai ryhmillä on oikeudet.

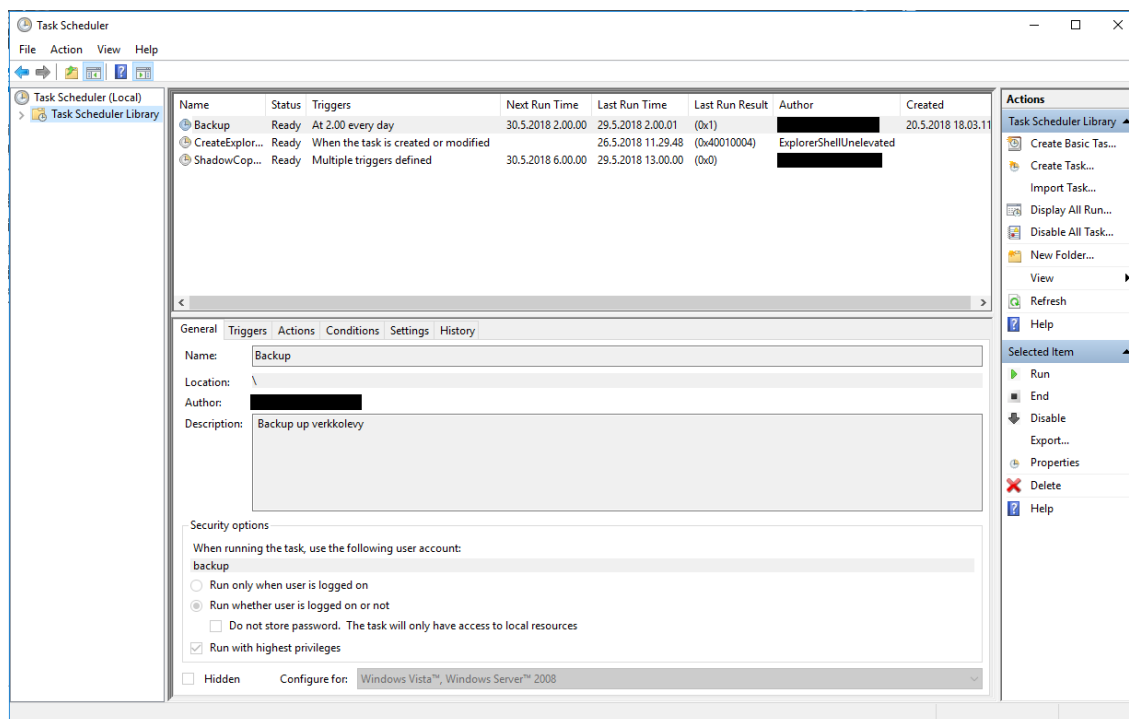
Palvelimella on myös käytössä kaikkien verkkojakojen versiointi, ns. "shadow copy", joka luo kaksi kertaa päivässä jaetuista kansioista palautuspisteitä. Tämän ominaisuuden avulla on siis mahdollista tarkastella verkkolevyjaon sisältöä sellaisena, kun se on ollut vaikka viikko sitten, ja tiedostoja on mahdollista palauttaa versiohistoriasta esim. vahingossa tapahtuneen poiston

jälkeen. (What is a shadow copy? 2005.) Versiointia voi hallita avaamalla ”Computer Management” -> ”Shared Folders” -> ”All Tasks” -> ”Configure Shadow Copies...”.



Kuvio 3 Verkkolevyn palautuspisteet

Verkkolevy varmuuskopioidaan päivittäin Buffalo Linkstation-verkkolevyasemalle ajastetulla tehtävällä, joka käynnistää varmuuskopiointi-komentosarjan. Komentosarja on luotu notepad-ohjelmalla ja tallennettu .bat -tiedostomuotoon. BAT-tiedostopäätte on tarkoitettu tiedostoille, jotka sisältävät MS-DOS -komentosarjoja. BAT-tiedosto ajetaan päivittäin kello 2:00 Windowsin sisäänrakennetulla ”task scheduler” -ohjelmalla. Ajastetun tehtävän ajoa varten on luotu oma käyttäjätunnus ”backup”. Tunnuksella on lukuoikeudet verkkolevyyn ja lisäksi sille on annettu kirjoitusoikeudet varmuuskopiointin lokitiedostoon polussa ”C:\Verkkolevy\admin\backup.log”.



Kuvio 4 ajastettujen tehtävien hallintapaneeli

Komentosarjalla ajettava komento on:

```
@echo off
```

Tällä komennolla estetään komentojen ja niiden tuottamien viestien näkyminen konsolissa.

```
net use B: /d /y
```

Tämä rivi varmistaa, ettei levykartoitus epäonnistu päällekkäisyyden vuoksi poistamalla B: - aseman mahdolliset olemassa olevat levykartoitukset. /d -parametri tarkoittaa "delete" (poista), ja /y kuittaa mahdolliset ilmoitukset vastauksella "yes" (kyllä).

```
net use B: \\10.0.0.1\backup /user:tunnus salasana
```

Tämä rivi kartoittaa B: -asemaan osoitteesta löytyvän hakemiston ja yhdistää käyttämällä määritettyä käyttäjätunnusta ja salasanaa.

```
robocopy "C:\Verkkolevy" "B:\verkkolevy" /MIR /R:5 /W:15 /MT:16 /V /NP /LOG:C:\Verkkolevy\admin\backup.log
```

Tämä rivi on itse varmuuskopiointikomento. Kopiointiohjelmana käytetään robocopya, ja sille annetaan polku, josta tiedostot kopioidaan, sekä polku johon ne kopioidaan. /MIR -parametri määrittää ohjelman toimimaan "Mirror" -moodissa, mikä tarkoittaa, että pelkän kopiointin

lisäksi ohjelma myös poistaa kohdekansioista tiedostot joita ei ole lähdekansioissa. Tämä varmistaa, ettei varmuuskopioasema säilö turhaan jo verkkolevyltä poistettuja tiedostoja. /R:5 ja /W:15 -parametrin määrittävät, että mikäli ohjelma kohtaa tiedoston jota se ei voi kopioida (esimerkiksi jos tiedosto on käytössä), ohjelma yrittää uudelleen viisi kertaa, ja odottaa 15 sekuntia yritysten välissä. /MT:16 -parametri käskee ohjelman toimimaan ”multithreaded”-moodissa, eli käyttämään useampaa prosessorisäiettä toiminnan nopeuttamiseksi. Oletusasetus ilman itse tehtyä määrittystä on 8 säiettä, tässä tapauksessa ohjelma on määritetty käyttämään kaikkia prosessorin säikeitä, joita on kuusitoista kappaletta. /V-parametriä käytettäessä ohjelma tuottaa runsassanaista diagnostiikkatietoa, ja kertoo kaikki ohitetut tiedostot. /NP määrittää ohjelman jättämään prosessin etenemistiedot näyttämättä. Varmuuskopiointia ei ole tarkoitettu tehtäväksi käsin, joten etenemisen näyttäminen on turhaa. /LOG-parametri määrittää ohjelman kirjoittamaan lokitiedoston määriteltyyn sijaintiin. (Robocopy 2018.)

6 Trend Micro Worry-Free

Trend Micron Worry-Free on erityisesti pienyrityksille suunnattu antivirus-ohjelmisto. Yrityksellä on käytössä Worry-Free Standard-versio, jossa infrastruktuuriin kuuluu keskitetyn hallinnan palvelin, jota käytetään web-käyttöliittymän avulla, sekä asiakaskoneet joilla on käytössä itse antivirus-ohjelma, jota kutsutaan nimellä ”Security Agent”. (Worry-Free Standard 2018.) Security Agent on asennettu yrityksen koneille ryhmäkäytännön kautta, ja siitä kerrotaan tarkemmin ryhmäkäytännöt-osiassa.

The screenshot displays the Trend Micro Worry-Free Business Security management console. At the top, the logo and navigation menu are visible. The main content area is titled 'Live Status' and includes a 'View Mode' dropdown set to 'All' and a 'Customize notifications' link. The 'Threat Status' section shows a list of security features with green checkmarks, including Ransomware, Outbreak Defense, Antivirus, Anti-spyware, Web Reputation, URL Filtering, Behavior Monitoring, Network Viruses, and Device Control. To the right, two large cards display 'Ransomware detections' and 'Affected devices', both showing a count of 0. Below this, a link to the Trend Micro Knowledge Base is provided. The 'System Status' section shows a 'Smart Scan' feature with a green checkmark and a message stating 'Status level is normal based on your specified event settings.' A table below shows 'Scan Service Disconnections' with a count of 0 for 'Desktops/Servers'.

Kuvio 5 Worry-Free palvelimen hallintapaneeli

Worry-Free Standard sisältää antivirus-toiminnallisuuden joka estää vakoilu- ja haitallisten ohjelmien toimimisen. Tämän lisäksi siihen sisältyy myös web-sivujen estomahdollisuus ja turvallisuusluokittelu, palomuurominaisuus, käyttäytymisen tarkkailu, WiFi-yhteyksien turvallisuustarkistus, usb-laitteiden käytön hallinnan, Exchange-sähköpostipalvelinten turvallisuusliitännäisen, sekä liitännäisen Outlook-sähköpostiohjelmaan spam-viestien ehkäisyyn.

6.1 Worry-Free palvelimen asennus

Palvelimen asennus aloitetaan lataamalla Trend Micron sivuilta Worry-Free Standardin asennuspaketti. Asennuspaketti käynnistetään järjestelmänvalvojan tunnuksilla. Ensimmäisellä ruudulla valitaan polku, johon asennuspaketti puretaan. Tämän jälkeen itse asennusohjelma käynnistyy automaattisesti. Seuraavaksi tulee hyväksyä ohjelman lisenssisopimus, jonka jälkeen valitaan asennuksen tyyppi (tyypillinen, minimaalinen, tai mukautettu). Tässä tapauksessa valittiin tyypillinen asennus, koska asennuksen oletusasetukset sopivat hyvin tarpeisiimme. Seuraavalla ruudulla tulee syöttää ohjelman lisenssiavain. Mikäli lisenssiavainta ei syötä, ohjelma toimii 30 päivää kokeiluversiona. Seuraavaksi valitaan kansio, johon ohjelma asennetaan. Tämän jälkeen asennuksessa määritellään salasanat web-hallintapaneeliin, sekä Security Agent-ohjelmalle. Security Agentin salasanaa tarvitsee, mikäli ohjelmaan haluaa tehdä muutoksia paikallisesti koneella, esimerkiksi mikäli Security Agent pitää syystä tai toisesta ottaa pois päältä. Seuraavassa kohdassa määritellään SMTP-palvelimen osoite ja portti, joita palvelin käyttää sähköposti-ilmoituksien lähettämiseen, sekä sähköpostiosoitteet joihin ilmoitukset lähetetään. Näillä viesteillä palvelin ilmoittaa uusista versiopäivityksistä ja muista ylläpitoon liittyvistä asioista. Viimeisellä ruudulla voi valita haluaako lähettää Trend Microlle diagnostiikkatietoa palvelun kehittämiseksi. Tässä tapauksessa asetus on otettu pois päältä. Tämän jälkeen on mahdollista vielä asentaa Messaging Security Agent, mikä on Microsoft Exchange -sähköpostipalvelimille tarkoitettu turvallisuusohjelma, mutta sitä ei tässä tapauksessa ole käytetty.

6.2 Asetusten määrittäminen

Worry-Free -palvelimen asennus luo työpöydälle pikakuvakkeen, joka käynnistää nettiselaimessa palvelimen web-hallintapaneelin. Hallintapaneeliin kirjaututaan asennuksessa määritellyllä salasanalla. Hallintapaneelissa voi määrittää halutut asetukset ja ominaisuudet, jotka otetaan käyttöön, ja palvelin viestittää muutokset asetuksissa asiakaskoneiden Security Agent -ohjelmalle.

The screenshot displays the Trend Micro Worry-Free Business Security management console. At the top, the logo and product name are visible. The navigation bar includes 'Live Status', 'Security Settings', 'Outbreak Defense', 'Scans', 'Updates', 'Reports', 'Preferences', and 'Help'. The 'Security Settings > Servers (default)' path is shown. On the left, a sidebar lists settings: Scan Method, Antivirus/Anti-spyware, Firewall, Web Reputation, URL Filtering, Approved/Blocked URLs, Behavior Monitoring, Trusted Program, Device Control, Agent Privileges, and Quarantine. The 'Scan Method' section is expanded, showing a description for 'Conventional Scan' and 'Smart Scan'. The 'Smart Scan' option is selected with a radio button. A 'Save' button is located below the options.

Kuvio 6 Worry-Free palvelimen asetukset hallintapaneelissa

Asetuksien määrittäminen tehdään valitsemalla hallintapaneelista ”Security Settings”->”My Company”->”Servers” tai ”Desktops”, ja oikeaklikkaamalla valintaa, jolloin tulee näkyviin ”Configure Settings” -nappi. Valitsemalla ”Servers” tai ”Desktops” määritellään mihin laitteisiin kyseiset asennukset kohdistuvat. Asetuksia voi myös rajata tarkemmin esim. yksittäisille laitteille, jotka tulevat näkyviin ”Servers” tai ”Desktops” valikkojen alle riippuen laitteen tyy-
pistä.

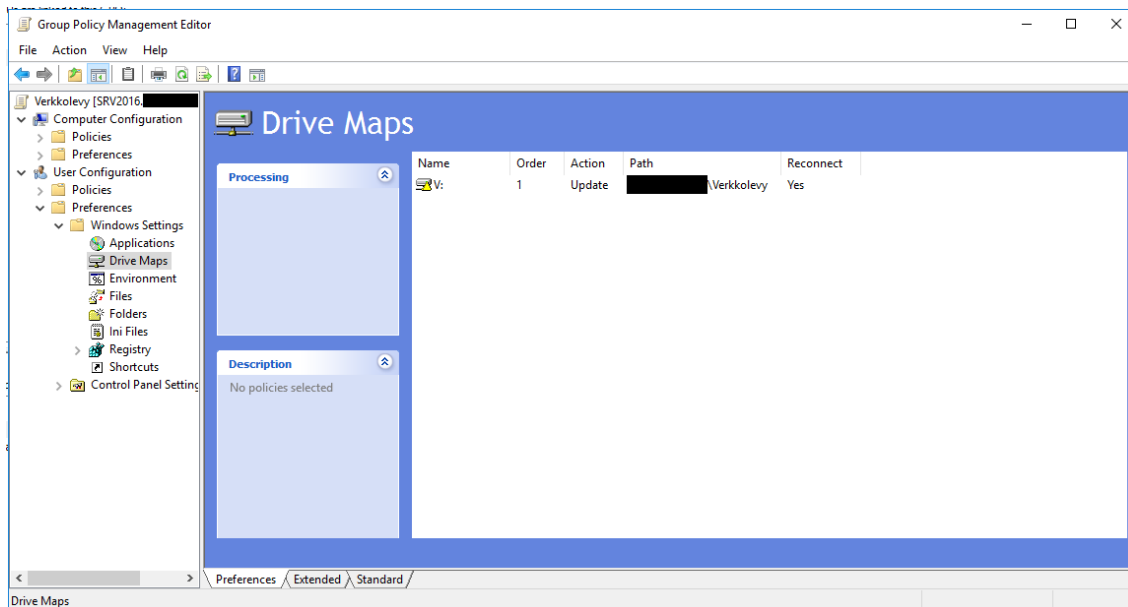
Tässä tapauksessa asetuksia on muutettu siten että haittaohjelmien skannaustyyppiksi on vaihdettu ”Smart Scan” oletusasetuksen (Conventional Scan) sijaan. Conventional Scan skannaa tiedostot koneella sijaitsevien tunnistustietojen avulla, kun taas Smart Scan käyttää ensin paikallisia tunnistetietoja, ja mikäli se ei pysty määrittelemään tiedoston turvallisuutta ohjelma siirtyy käyttämään palvelimen tunnistetietoja, ja lopuksi tarvittaessa Trend Micron pilvessä sijaitsevia tunnistetietoja. Tämä vähentää Security Agentin päivystystarvetta ja nopeuttaa sen toimintaa, koska paikallisten tunnistustietojen ei tarvitse olla yhtä kattavia ja ajantasa-
aisia. (Difference between the Conventional Scan and Smart Scan functions of Worry-Free Business Security 2017.) Tämän lisäksi kaikki muut oletuksena pois päältä olleet ominaisuudet ovat otettu käyttöön, mutta niiden asetuksia ei tietoturvasyistä tässä kerrota.

7 Ryhmäkäytännöt

Ryhmäkäytännöt eli ”Group policy” on Windows-toimialueiden tapa määrittää tietyille käyttäjille, ryhmille, tai koneille erilaisia käytäntöjä kuten verkkolevykartoituksia, verkkotulostimia, ajastettuja tehtäviä, automatisoituja ohjelmistoasennuksia ja lähes mitä tahansa muuta. (Group Policy Objects 2018.) Ryhmäkäytännöt mahdollistavat siis keskitetysti hallittavia toimenpiteitä, joka helpottaa IT-infrastruktuurin ylläpitoa, sillä toimenpiteitä ei tarvitse tehdä käsin jokaisella koneella ja/tai käyttäjätilillä, vaan ne voidaan määrittää palvelimella. Asiakasryitykselle määriteltiin käyttäjätileihin kohdistettu verkkolevyn ja tulostimen kartoitus, ja konetileille automatisoitu Trend Micro Security Agentin asennus.

7.1 Verkkolevy

Tämä ryhmäkäytäntö kartoittaa käyttäjälle palvelimen verkkolevyaseman, jolloin käyttäjä saa pikalinkin verkkolevylle tiedostojenhallinnassa.

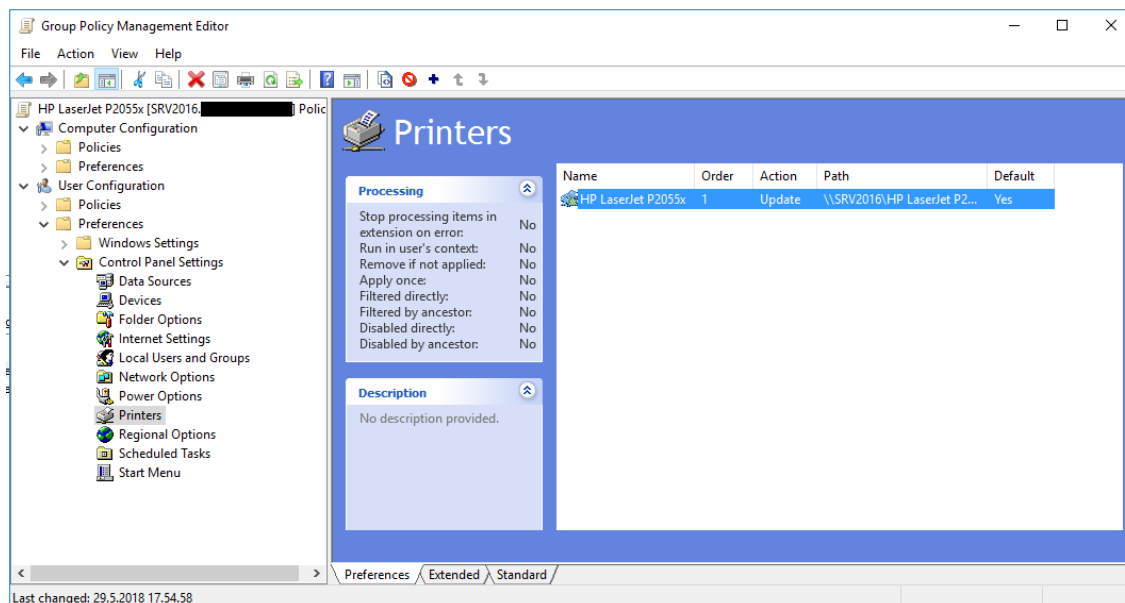


Kuvio 7 Verkkolevy-ryhmäkäytäntö

Tämä käytäntö on kohdistettu "Kayttajat" -organisaatioyksikköön, ja "Domain Users" -ryhmälle on annettu siihen "Delegation" -välilehdeltä "Apply" -oikeudet. Ryhmäkäytännössä on valittu "User configuration" -> "Windows settings" -> "Drive maps", jonne on lisätty verkkolevy antamalla sen osoite, ja valittu levyaseman kirjaimeksi "V:".

7.2 HP LaserJet 2055x

Tämä ryhmäkäytäntö lisää nimensä mukaisesti käyttäjän koneelle yrityksen HP LaserJet 2055x -printterin. Käytäntö on kohdistettu "Kayttajat" -organisaatioyksikköön, ja "Authenticated Users" -ryhmälle on annettu "Apply Group Policy" -oikeudet. Printteri on ensin lisätty palvelimelle tavanomaisesti ohjauspaneelistä, jonka jälkeen printterin kohdalta valitaan "manage" -> "properties" -> "sharing", ja valitaan "share this printer" ja "List in the directory", jolloin printteri tulee näkyviin Active Directoryssa.

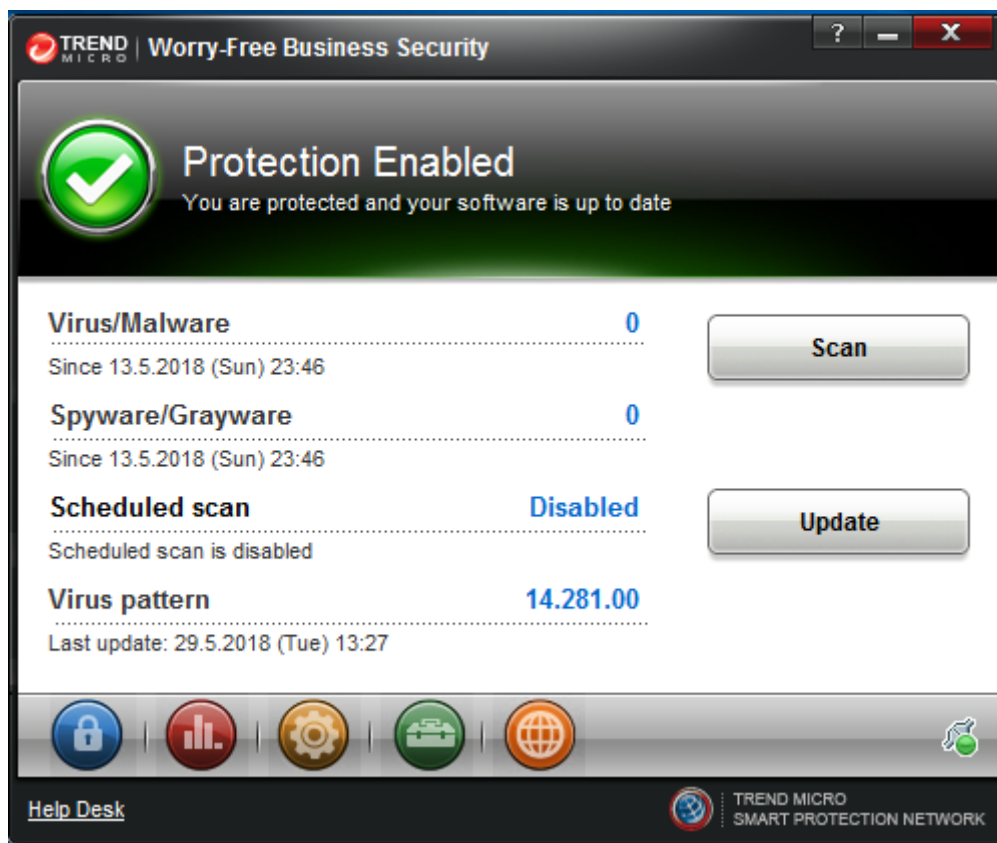


Kuvio 8 HP LaserJet 2055x-ryhmäkäytäntö

Tämän jälkeen SRV2016-palvelimelle tehtiin uusi ryhmäkäytäntö nimellä ”HP LaserJet 2055x”, jossa on valittu ”User configuration” -> ”Preferences” -> ”Control Panel Settings” -> ”Printers”, ja luotu tässä näkyvässä uusi printteri. Printterijaon osoite (share path) on haettu Active Directorystä, ja se määrittyy oletusprintteriksi, mikäli koneella ei ole valmiina oletusprintterinä paikallista printteriä.

7.3 Trend Micro Security Agent Install

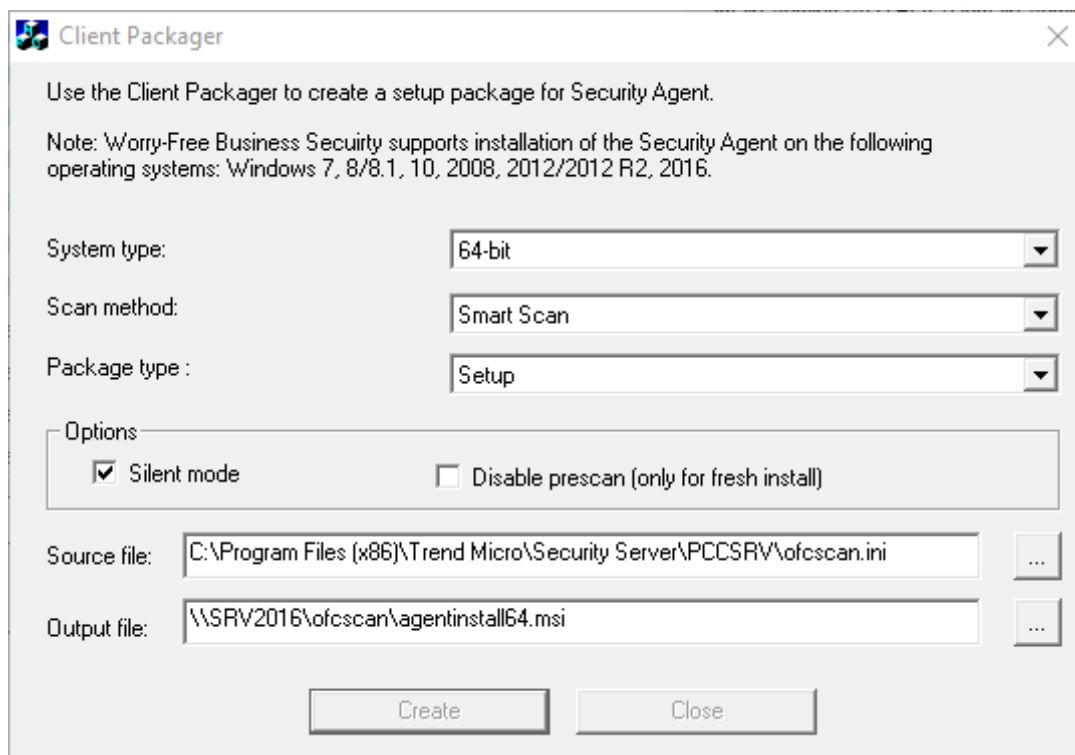
Tämä ryhmäkäytäntö asentaa yrityksen koneille Trend Micron Security Agent -antivirusohjelman. Käytäntö on kohdistettu ”Koneet” sekä ”Domain Controllers” -organisaatioyksiköihin, eli se asentuu kaikille yrityksen koneille ja toimialuepalvelimille.



Kuvio 9 Security Agent-ohjelman hallintapaneeli

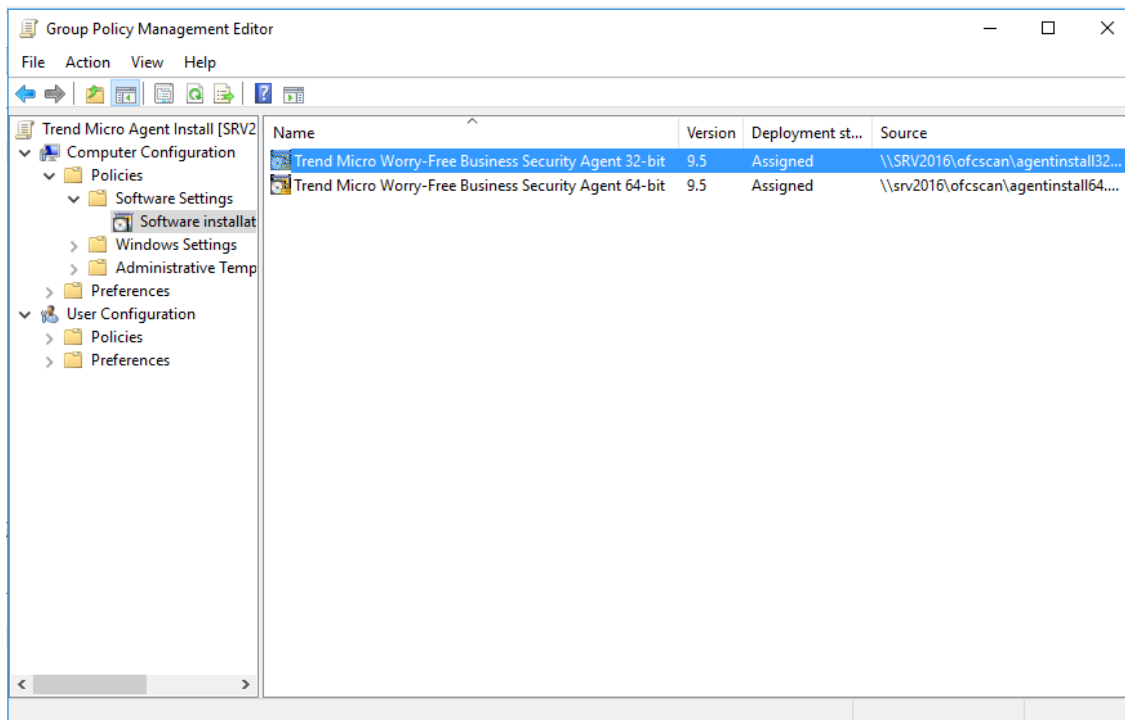
Security Agentista on tehty .msi -asennuspaketti Worry-Free -palvelimen Client Packager -työkalun avulla, joka sijaitsee oletuksena polussa "C:\Program Files (x86)\Trend Micro\Security Server\PCCSRV\Admin\Utility\ClientPackager\ClnPack.exe".

Työkalussa valitaan järjestelmän tyyppi (32 tai 64-bittinen), skannaustyyppi (Smart Scan tai Conventional Scan), paketin tyyppi (Setup tai Update), valinnaiset optiot (Silent mode ja Disable prescan), sekä lähdetiedosto ja kohdetiedosto. (OfficeScan Administrator's Guide 2013.)



Kuvio 10 Trend Micron Client Packager-ohjelma

Tässä tapauksessa palvelimelle on luotu sekä 32- että 64-bittiset asennuspaketit Smart Scanilla. Paketin tyyppi on Setup eli asennus, valinnaisista optioista on valittu Silent mode, joka ajaa asennuksen taustalla ilman että käyttäjä näkee sitä. Lähdetiedosto on jätetty oletukseksi ja kohdetiedostoksi on määritetty agentinstall32.msi 32-bittisen paketin kohdalla, ja agentinstall64.msi 64-bittisen kohdalla. Kohdetiedoston poluksi on määritelty Worry-Free -palvelimen automaattisesti verkkoon jaettu "ofscan"-kansio, josta se on luettavissa ryhmäkäytäntöä varten.



Kuvio 11 Trend Micro Security Agent Install -ryhmäkäytäntö

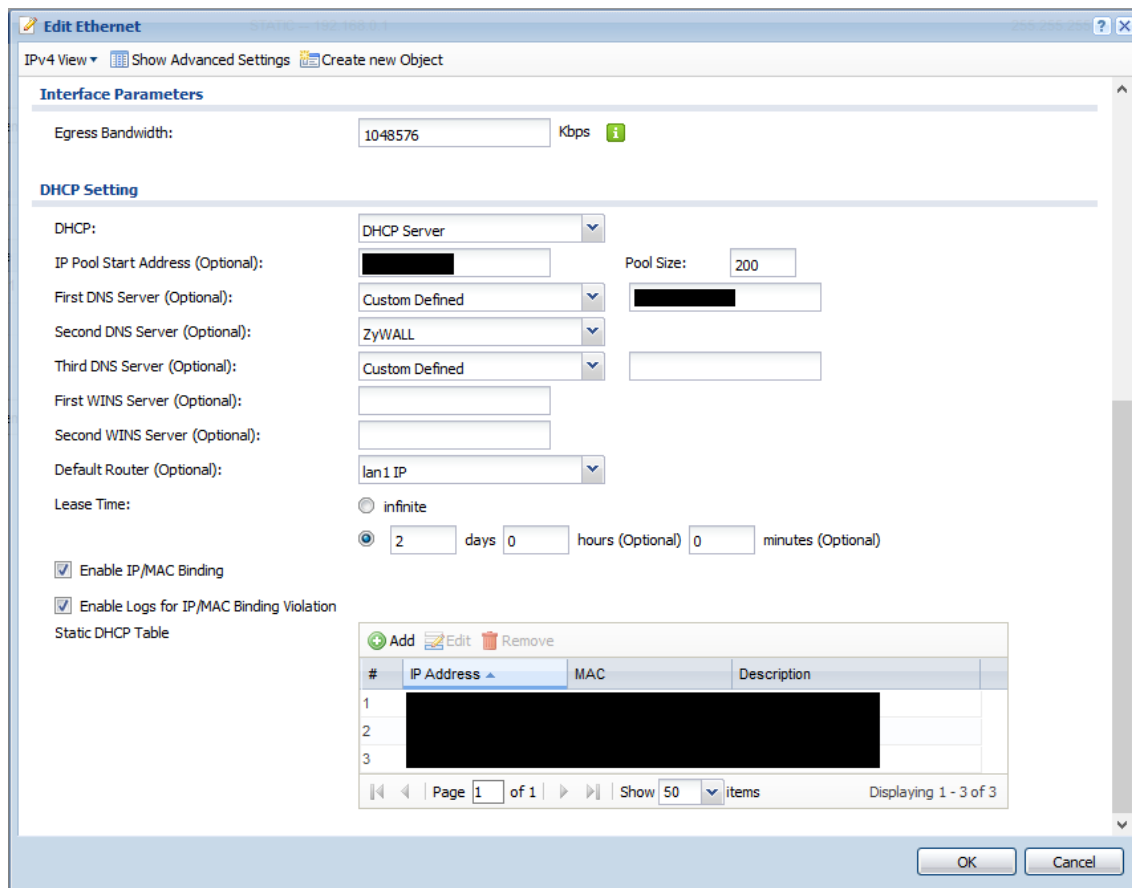
Ryhmäkäytäntö on luotu tekemällä ensin uusi ryhmäkäytäntöobjekti Group policy objects -organisaatioyksikköön. Tämän jälkeen editoidaan ryhmäkäytäntöä seuraavasti: ”Computer Configuration”->”Policies”->”Software Settings”->”Software installation”, ja hiiren oikeaklikkauksen kautta valitaan ”New”->”Package”, ja avautuvasta valikosta haetaan Security Agentin asennuspaketti. Tällä toimenpiteellä lisätään sekä 32- että 64-bittiset asennuspaketit. 32-bit-tisestä asennuksesta on määriteltävä, että se ei asennu 64-bittisille koneille oikeaklikkaamalla objektia ryhmäkäytäntöjen hallinnassa ja valitsemalla ”Properties”->”Deployment”->”Advanced”, ja ottamalla täppä pois ”Make this 32-bit x86 application available to Win64 machines”-kohdasta. Näin ryhmäkäytäntö kohdistaa paketit automaattisesti oikein koneen prosessoriarkkitehtuurista riippuen. (Burchill 2010.) Kun ryhmäkäytäntö on päivittynyt asiakaskoneille, Security Agent asentuu automaattisesti koneiden uudelleenkäynnistymisen yhteydessä.

8 Verkko

Yrityksen internet-yhteyden palveluntarjoajana toimii Nebula Oy. Internet-yhteys tulee Zyxelin palomuurin kautta, johon on määriteltävä DNS- ja DHCP-palvelin. Yrityksen pääsääntöinen DNS-palvelin on kuitenkin asennettu SRV2016-palvelimelle, koska käytännössä huomattiin, ettei Zyxelin palomuri osannut selvittää lähiverkossa sijaitsevien laitteiden isäntänimiä. Yrityksen työasemat ovat yhteydessä palomuriin erillisen hallitsemattoman kytkimen kautta.

8.1 DHCP

Dynamic Host Control Protocol on protokolla, joka toimii TCP/IP verkoissa ja jakaa verkossa oleville laitteille IP-osoitteet sekä muut konfiguraatiodiedot, jotta laitteet pystyvät kommunikoimaan verkossa ja saamaan internet-yhteyden. (Droms 1997.)



Kuvio 12 DHCP-asetukset Zyxelin palomuurissa

Yrityksen verkossa Zyxelin palomuri toimii DHCP-palvelimena. DHCP-palvelimen olisi voinut asentaa myös SRV2016-palvelimelle, mutta toiminto päätettiin pitää palomuurissa, jotta yrityksen internet-yhteys toimii myös, jos SRV2016 on syystä tai toisesta pois päältä.

DHCP-asetukset ovat seuraavat:

Osoitevaruuden alku: 10.0.0.2.

Osoitevaruuden koko: 200 osoitetta.

Ensisijainen DNS-palvelin: 10.0.0.224 (SRV2016).

Toissijainen DNS-palvelin: ZyWall-palomuuri.

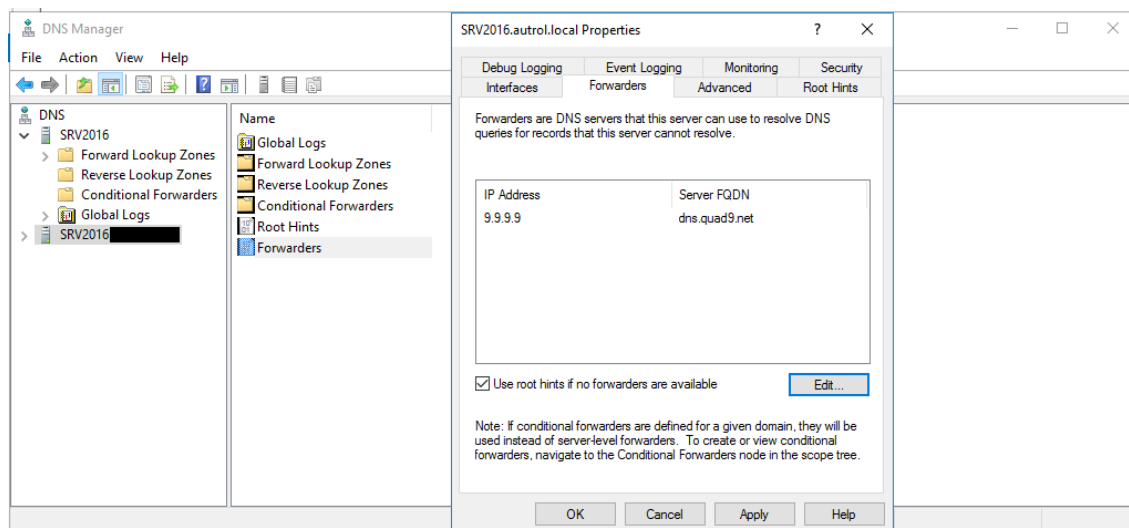
Oletusyhdykäytävä: Zywall-palomuuri.

IP-osoitelainan kesto: 2 päivää.

Lisäksi DHCP-palvelimella on määritelty SRV2016-palvelimelle, Buffalon verkkolevyasemalle, sekä monitoimilaitteelle staattiset IP-osoitteet niiden MAC-osoitteiden perusteella.

8.2 DNS

DNS eli Domain Name Service on palvelu, joka mahdollistaa URL-osoitteiden, esimerkiksi www.google.fi, selvittämisen IP-osoitteiksi, jotta kommunikointi osoitteessa sijaitsevan palvelimen tai muun resurssin kanssa on mahdollista. (Mockapetris 1987.) Asiakasyrityksen verkossa DNS-palvelu on määritelty sekä Zyxelin palomuriin että SRV2016-palvelimelle. DNS palvelu toimii siten että palvelin pitää omaa tietokantaa URL osoitteita vastaavista IP-osoitteista, ja mikäli osoite ei ole tiedossa, palvelin kysyy tietoa toiselta verkossa sijaitsevalta DNS-palvelimelta.



Kuvio 13 DNS-palvelimen hallintapaneeli SRV2016-palvelimella

SRV2016-palvelimella verkossa sijaitsevaksi DNS-palvelimeksi on valittu Quad9, jonka palvelu sijaitsee osoitteessa 9.9.9.9. Quad9 on IBM Securityn Packet Clearing Housen ja Global Cyber Alliancen perustama nimipalvelu, joka estää haitallisille sivuille pääsyn vertaamalla osoitetta IBM'n X-Force -uhkatietokantaan. Mikäli selvittävä sivusto on tietokannassa merkitty haitalliseksi, estetään sen IP-osoitteen selvitys, jolloin yhteys sivulle ei pääse muodostumaan. (FAQ 2018.)

Domain Zone Forwarder

#	Domain Zone	Type	DNS Server
1	██████████	User-Defined	██████████
2	██████████	User-Defined	9.9.9.9
-	*	Default	N/A

Page 1 of 1 | Show 50 items

Kuvio 14 DNS-asetukset Zyxelin palomuurissa

Zyxelin palomuriin on määritelty ensisijaiseksi DNS-palvelimeksi SRV2016, koska se tietää toimialueen Active Directoryssä olevien koneiden isäntänimet (hostname), ja toissijaiseksi DNS-palvelimeksi Quad9, jotta yrityksen internet-yhteys toimii myös, mikäli DNS-palvelu SRV2016-palvelimella ei syystä tai toisesta toimi, esimerkiksi jos palvelin on pois päältä.

9 Yhteenveto

Työn tuloksena yrityksellä on toimiva ja nykyaikainen IT-infrastruktuuri, joka vastaa tarpeita ja vähentää manuaalisia ylläpitotehtäviä. Työn päätarkoituksena oli vaihtaa toimialuepalvelin, jonka pääsääntöiset tehtävät olivat Active Directory -palvelu, Worry-Free antiviruspalvelin, sekä verkkolevy. Tämän lisäksi on kuitenkin kiinnitetty tarkempaa huomiota asetuksiin ja otettu käyttöön ominaisuuksia, jotka puuttuivat täysin vanhasta infrastruktuurista.

Uusi palvelin on osiensa puolesta huomattavasti tehokkaampi kuin vanha palvelin, ja RAD1-tilassa olevat kovalevyt ja ECC-välimuisti auttavat ehkäisemään tiedostojen korruptoitumista levyvirheiden takia. (What is ECC memory? 2017.) Windows Server 2016 on uusin versio Windows Server-tuoteperheessä, ja vanhaan palvelimeen verrattuna käyttöjärjestelmässä harpattiin kokonaisen generaation (Windows Server 2012) ohi. Kovalevytilan puutteen vuoksi vanhalla palvelimella ei ollut edes käyttöjärjestelmän viimeisintä versiopäivitystä asennettuna (Windows Server 2008 R2). Lisäksi Trend Micron Worry-Free Business antivirus oli yrityksessä täysin pois käytöstä, koska sen palvelinkomponenttia ei ollut mahdollista päivittää kovalevytilan puutteen vuoksi.

Vanhan palvelimen aikaiseen infrastruktuuriin verrattuna suurin yrityksen arjessa näkyvä muutos on ryhmäkäytäntöjen, ja verkkolevyn versioinnin sekä ajastetun varmuuskopiointin käyttöönotto. Ryhmäkäytäntöjen ansiosta kaikille yrityksen koneille asentuu automaattisesti uudelleenkäynnistyksen yhteydessä Trend Micron Security Agent, joka on yhteydessä keskitettyyn hallintapalvelimeen. Käyttäjien kirjautuessa koneille heille tulee automaattisesti näkyviin verkkolevy V: asemassa, ja toimiston tulostin määrittyy oletustulostimeksi. Täten kun yritys lisää uuden koneen toimialueeseen, se on heti yrityksen tietoturva-asetusten mukainen, ja tiedostoja pystyy jakamaan sekä tulostamaan toimistolla. Verkkolevyn tiedostojen versiointi ja automaattinen varmuuskopiointi varmistavat tietojen säilymiset inhimillisten virheiden ja

laitteiden hajoamisen varalta, ja poistaa manuaalisen varmuuskopioinnin tarpeen täysin. Automaattinen varmuuskopiointi on myös nopeampi kuin käsin suoritettu, sillä robocopy-ohjelma osaa kopioida vain sellaiset tiedostot jotka ovat uusia, tai uudempia kuin varmuuskopio-verkkolevyllä sijaitsevat versiot.

9.1 Kehitysehdotukset

Tulevaisuudessa asiakasyrityksen kannattaisi pohtia pilvipalveluun tapahtuvaa varmuuskopiointia. Nykyinen ratkaisu on riittävä pienemmissä ongelmatapauksissa, kuten jos palvelin tai sen levyt hajoavat syystä tai toisesta, mutta se ei ole riittävä suuremman onnettomuuden, kuten tulipalon tapauksessa, koska molemmat levyasemat sijaitsevat samassa toimistossa. Tämän takia olisi järkevää ostaa pilvitallennustilaa, jonne kaikki tiedostot voitaisiin varmuuskopioida. Työntekijät voisivat mahdollisesti käyttää tätä pilvitallennustilaa myös oman työnsä apuna, sillä tämän hetkiseen verkkolevyyn ei ole pääsyä toimiston ulkopuolelta.

Työssä oli alun perin tarkoitus myös tutkia VPN-palvelimen asennusta, mutta se päätettiin jättää pois ajanpuutteen vuoksi. VPN eli Virtual Private Network on teknologia, joka mahdollistaa salatun yhteyden verkkojen välillä. Tämä helpottaisi työntekijöiden työskentelyä etänä, mahdollistaen esimerkiksi pääsyn verkkolevyille ja etäyhteyden toimistolla sijaitsevaan koneeseen. Yrityksen kannattaa tutkia tätä mahdollisuutta tulevaisuudessa, mutta toimiston internet-yhteyden nopeus tulee huomioida, sillä VPN-yhteys vaatii kohtuullisen lähetyksenopeuden.

9.2 Oma arviointi

Toiminnallinen osuus opinnäytetyöstä onnistui erittäin hyvin, vaikka kehitettävää yrityksen IT-infrastruktuurista toki vielä löytyy. Asennusprosesseja olisi pitänyt dokumentoida tarkemmin, mikä olisi myös helpottanut raportin kirjoituksessa. Ajankäyttö ja aikataulutus olivat hieman haastavia, asennusprosessit suoritettiin nopeasti mutta niiden välissä oli pidempiä taukoja, joita olisi pitänyt välttää. Lisäksi raporttia olisi pitänyt kirjoittaa enemmän itse asennusprosessin aikana.

Työn teosta sai hyvää kokemusta erityisesti ryhmäkäytäntöjen osalta. Ryhmäkäytännöt ovat yleisesti hyvin laajassa käytössä yritysmaailmassa, joten niiden käytön opetteleminen on kannattavaa ammatillisen kehityksen kannalta. Työn lopputulos sopii tällä hetkellä hyvin kyseisen pienen yrityksen tarpeisiin, ja todennäköisesti jatkamme yhteistyötä kehittämisen ja päivittämisen puitteissa tulevaisuudessakin.

Lähteet

Painetut

Lenovo. 2013. ThinkServer TS140 User Guide.

Sähköiset

Microsoft. 2017. Active Directory Domain Services Overview. Viitattu 30.5.2018.

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

Trend Micro. 2017. Difference between the Conventional Scan and Smart Scan functions of Worry-Free Business Security. Viitattu 30.5.2018.

<https://success.trendmicro.com/solution/1053817>

Quad9. 2018. FAQ. Viitattu 30.5.2018

<https://www.quad9.net/faq/>

Microsoft. 2018. Group Policy Objects. Viitattu 30.5.2018.

[https://msdn.microsoft.com/en-us/library/aa374162\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa374162(v=vs.85).aspx)

Microsoft. 2017. Install Server with Desktop Experience. Viitattu 30.2.2018.

<https://docs.microsoft.com/en-us/windows-server/get-started/getting-started-with-server-with-desktop-experience>

Burchill, A. 2010. Software Deployment x86 and x64. Viitattu 30.5.2018.

<https://social.technet.microsoft.com/Forums/windowsserver/en-US/14f17fac-4521-418d-aac2-53017b219e84/software-deployment-x86-and-x64>

Trend Micro. 2013. OfficeScan Administrator's Guide. Viitattu 30.5.2018.

http://docs.trendmicro.com/all/ent/officescan/v10.6/en-us/osce_10.6_sp3_olh/ins_mth_client_create.html

Mockapetris, P. 1987. Request for Comments: 1034. Viitattu 30.5.2018.

<https://www.ietf.org/rfc/rfc1034.txt>

Droms, R. 1997. Request for Comments: 2131. Viitattu 30.5.2018.

<https://www.ietf.org/rfc/rfc1034.txt>

Microsoft. 2018. Robocopy. Viitattu 30.5.2018.

<https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/robocopy>

Microsoft. 2005. What is a shadow copy? Viitattu 30.5.2018.

<https://technet.microsoft.com/en-us/library/cc161481.aspx>

Crucial. 2017. What is ECC memory? Viitattu 30.5.2018.

<http://eu.crucial.com/eur/en/memory-server-ecc>

Sivarajan, S. 2012. What is the difference between Organizational Unit and Groups and container? Viitattu 30.5.2018.

<https://social.technet.microsoft.com/Forums/windowsserver/en-US/27e5b07b-15a5-4872-bf26-3e88073a3fa8/what-is-the-difference-between-organizational-unit-and-groups-and-container>

Trend Micro. 2018. Worry-Free Standard. Viitattu 30.5.2018.

https://www.trendmicro.com/en_fi/small-business/worry-free-standard.html

Kuviot

Kuvio 1 Roolien ja ominaisuuksien asennusvelho.....	9
Kuvio 2 Active Directoryn hallintapaneeli	10
Kuvio 3 Verkkolevyn palautuspisteet	12
Kuvio 4 ajastettujen tehtävien hallintapaneeli	13
Kuvio 5 Worry-Free palvelimen hallintapaneeli	14
Kuvio 6 Worry-Free palvelimen asetukset hallintapaneelissa.....	16
Kuvio 7 Verkkolevy-ryhmäkäytäntö	17
Kuvio 8 HP LaserJet 2055x-ryhmäkäytäntö.....	18
Kuvio 9 Security Agent-ohjelman hallintapaneeli	19
Kuvio 10 Trend Micron Client Packager-ohjelma.....	20
Kuvio 11 Trend Micro Security Agent Install -ryhmäkäytäntö	21
Kuvio 12 DHCP-asetukset Zyxelin palomuurissa	22
Kuvio 13 DNS-palvelimen hallintapaneeli SRV2016-palvelimella	23
Kuvio 14 DNS-asetukset Zyxelin palomuurissa	24