Haaga-Helia
ammattikorkeakoulu Oy

Oppilaitoksen aktiivihakemiston päivitysprojekti -testiympäristö ja testaaminen

Jani Ljungberg

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2018

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Jani Ljungberg

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Oppilaitoksen aktiivihakemiston päivitysprojekti –testiympäristö ja testaaminen

Sivu- ja liitesivumäärä
67 + 38

Tässä opinnäytetyössä rakennetaan testiympäristö Microsoftin aktiivihakemiston päivitysprojektille ja toteutetaan päivityksessä tarvittavat työvaiheet. Opinnäytetyö on tehty Haaga-Helia ammattikorkeakoulun tietohallinnon toimeksiantona. Haaga-Helia on Helsingissä toimiva ammattikorkeakoulu ja sen tietojärjestelmä palvelee yli kymmentä tuhatta opiskelijaa ja henkilökunnan jäsentä.

Haaga-Helian toimialueen ohjaustietokoneisiin on asennettu Windows Server –käyttöjärjestelmä. Käyttöjärjestelmäversio määrittelee toimialueen ja toimialuemetsän toiminnallisuustason. Kun toiminnallisuustasoa nostetaan, saadaan käyttöön uusia ominaisuuksia. Nämä ominaisuudet parantavat tietojärjestelmän hallittavuutta ja tietoturvaa.

Opinnäytetyö on jaettu kahteen osioon. Teoriaosuus kuvaa järjestelmäpäivityksen läpivientiin tarvittavia teknisiä ratkaisuja ja käytännön osuudessa kuvaillaan Haaga-Helian palvelinympäristön arkkitehtuuria, projektin kulkua ja menetelmiä. Opinnäytetyön tuloksena toivottiin syntyvän ohjeistus, jota seuraamalla päivityksen työvaiheet ovat helposti toistettavissa.

Projektissa virtuaaliseen testiympäristöön tuodaan kopiot Haaga-Helian kahdesta ohjauspalvelimesta, sekä aktiivihakemiston sisällöstä. Ympäristöön lisätään kolmas ohjauspalvelin. Toiminnallisuustason nostoa simuloidaan testiympäristössä dokumentoiden prosessi. Tuloksia hyödynnetään tuotantoympäristössä tapahtuvassa varsinaisessa päivitysprojektissa.

Asiasanat
Aktiivihakemisto, toiminnallisuustaso, Windows Server, päivittäminen, virtualisointi.

Sisällys

1 Johdanto

Haaga-Helia ammattikorkeakoulun tietojärjestelmän ytimessä on Microsoft Windows-palvelimissa toimiva aktiivihakemisto. Palvelinkäyttöjärjestelmä päivittyy ajoittain, kun siihen lisätään uusia ominaisuuksia ja vanhoja parannellaan. Palvelinympäristön toiminnallisuustaso kertoo, millaisia käyttöjärjestelmäversioita ja ohjelmistoja palvelimissa käytetään. Haaga-Helian palvelimissa on käytössä ominaisuuksia, jotka perustuvat yli kymmenen vuotta vanhaan teknologiaan. Tähän on kuitenkin tulossa muutos ja palvelimien päivittämistä suunnitellaan vuodelle 2019. Tässä opinnäytetyössä tehdään valmisteluja päivitystä varten ja testataan päivityksen aikana tarvittavia komentoja ja tekniikoita.

Opinnäytetyössä toteutettavat työvaiheet vaativat tarkkaa suunnittelua etukäteen. Päivittäminen on monivaiheinen prosessi, joka täytyy suorittaa oikeassa järjestyksessä ja testata etukäteen. Ennen tuotantopalvelimilla tapahtuvaa päivittämistä on selvitettävä lähtötilanne ja ymmärrettävä palvelinympäristön toiminta ja käytössä olevat ominaisuudet. Tämän jälkeen voidaan päivitystä alkaa suunnitella. Haaga-Heliassa tämä on tehty yhteistyössä Microsoftin asiantuntijoiden kanssa. Opinnäytetyön tekijänä olen ollut mukana projektin suunnittelussa alusta asti ja olen työskennellyt Haaga-Heliassa harjoittelijana vuoden ajan. Opinnäytetyö on toteutettu Haaga-Helian tietohallinnon toimeksiantona.

Opinnäytetyö on jaettu kahteen osaan. Teoriaosuus kuvaa Windows-palvelinympäristön toimintaperiaatteita yleisellä tasolla. Toisessa osassa kuvataan Haaga-Helian palvelinympäristö ja virtualisointiratkaisut, sekä toteutetaan toiminnallisuustason nostoon tarvittavat toimenpiteet. Haaga-Helian pyynnöstä työvaiheet on kuvattu yksityiskohtaisesti ja mukana on paljon asennuskuvia ja esimerkkejä eri työvaiheista. Samalla on testattu koulun palvelinten palauttamista varmuuskopioista. Työn tuloksena on syntynyt yksityiskohtainen ohjeistus eri työvaiheiden läpiviennistä kuvineen.

Päivityksen aikana kaikki aktiivihakemiston toiminnasta vastaavat ohjaustietokoneet päivitetään käyttämään Windows Server 2016 –käyttöjärjestelmää. Kun kaikki toimialueen ohjauskoneet on päivitetty, voidaan palvelinympäristön toiminnallisuustasoa nostaa, jolloin uudet ominaisuudet saadaan käyttöön. Vaikka palvelimet voidaankin periaatteessa päivittää suoraan uudempaan versioon, on parempi käytäntö rinnakkaispäivitys, jossa toimialueelle liitetään uudella käyttöjärjestelmällä varustettuja ohjauskoneita, joille tehtävät siirretään, ja lopuksi vanhat koneet poistetaan käytöstä (Warren 2018, 33).

Opinnäytetyössä käytettävät termit ja niiden selitykset ovat mukana liitteessä (Liite 1).

2 Haaga-Helian aktiivihakemiston komponentit

Haaga-Helia ammattikorkeakoulu Oy on pääkaupunkiseudulla ja sen ympäristössä toimiva ammattikorkeakoulu, joka kouluttaa asiantuntijoita liike-elämän ja palveluelinkeinojen tarpeisiin, sekä kehittää näihin aloihin liittyvää osaamista.

Haaga-Helia tarjoaa koulutusta neljällä kampuksella, jotka sijaitsevat Pasilassa, Haagassa, Vierumäellä ja Porvoossa. Koulutusaloja ovat liiketalous, tietotekniikka, johdon assistenttityö, hotelli-, ravintola- ja matkailuala, toimittajakoulutus, liikunta-ala sekä ammatillinen opettajakoulutus. (Haaga-Helia 2017, 3.)

Lähtökohtaisesti Haaga-Helia pyrkii vastaamaan liike- ja yrityselämän tarpeisiin käytännönläheisellä ja korkeakoulutasoisella opetuksella. Koulussa voi suorittaa ammattikorkeakoulututkintojen lisäksi ylempiä korkeakoulututkintoja, MBA-tutkinnon (Master of Business Administration), sekä ammatillisen opettajatutkinnon (Haaga-Helia 2017, 3).

Oppilaita on amk-tutkintoon johtavassa koulutuksessa noin 9000, ylempään amk-tutkintoon johtavassa koulutuksessa noin 900 ja ammatillisessa opettajakorkeakoulussa noin 500. Kun mukaan lasketaan ei-aktiiviset opiskelijat, löytyy koulun tietojärjestelmistä noin 12 000 oppilaan käyttäjätilit. Henkilökuntaa oli vuoden 2017 lopussa 626 henkilöä, joista päätoimisia opettajia oli 381. (Haaga-Helia 2017, 18.)

Haaga-Helian tietojärjestelmä palvelee koko organisaation tarpeita ja sitä ylläpitää tietohallinto, joka koostuu asiakas- ja järjestelmäpalveluista. Tietohallintopalvelut vastaavat Haaga-Helian tietotekniikkaresurssien ylläpidosta ja kehittämisestä arkkitehtuurilinjausten mukaisesti (Haaga-Helia 2017, 20).

Haaga-Helia on aloittanut toimintansa vuonna 2007, kun kaksi yhdeksänkymmentäluvun alussa perustettua ammattikorkeaa, Haaga instituutin amk ja Helsingin liiketalouden amk yhdistettiin. Tällöin Haaga instituutin tietojärjestelmien tiedot siirrettiin Helian (Helsingin liiketalouden ammattikorkeakoulu) tietojärjestelmän toimialueelle (engl. Domain). Samalla toimialue nimettiin uudelleen. (Silfver 2018.)

Kuluneen kymmenen vuoden aikana Haaga-Helian aktiivihakemistosta on ollut vastuussa monia henkilöitä, joiden osaamistaso on vaihdellut suuresti. Ajan myötä hakemistoon on kerääntynyt myös paljon vanhentunutta tietoa. (Silfver 2018.)

2.1 Haaga-Helian aktiivihakemisto

Toimialueen aktiivihakemisto (AD DS, Active Directory Domain Services) vastaa identiteettitietojen hallinnasta Windows Server –ympäristössä. Se asennetaan toimialueen ohjaustietokoneille (Domain Controller, DC) palvelinroolina ja se käsittelee käyttäjien todentamiseen ja oikeuksien tarkistamiseen liittyviä tehtäviä. (Warren 2017, 2.)

Toimialueen aktiivihakemisto sisältää käyttäjätilit, käyttäjäryhmät ja toimialueelle liitetyt tietokoneet, palvelut, sekä verkkoresurssit. Se rakentuu useasta komponentista, joista osa on fyysisiä laitteita ja osa loogisia kokonaisuuksia, jotka toimivat vuorovaikutuksessa.

Hakemistorakenne on usein jaettu organisaatioyksiköihin, jotka vastaavat organisaation rakennetta. Lisäksi se toimii pohjana, kun määritellään ryhmäkäytäntöjä (Group Policy Objects, GPO). Ryhmäkäytäntöjen avulla määritellään millaisia käyttöoikeuksia käyttäjät saavat toimialueella oleviin resursseihin.

Kun käyttäjä kirjautuu Haaga-Helian toimialueelle työasemalla, on aktiivihakemisto kirjautumistoimintojen tärkein komponentti. Se on kuitenkin vain osa paljon laajempaa kokonaisuutta. Kuvasta 1 näemme, että monet tekijät vaikuttavat siihen, millaiset asetukset käyttäjän työasemalla tulevat voimaan.

Kuva 1. Kirjautuessa koneelle voimaan tulevat asetukset

2.2 Aktiivihakemiston ohjaustietokoneet

Domain Controller (DC) on toimialueen ohjaustietokone. Toimialueella koneita voi olla yksi tai useampia. Niiden toiminta ja palveluiden päivittäminen ovat kriittisiä toimintoja koko Haaga-Helian järjestelmäkokonaisuuden kannalta. Haaga-Helian fyysiset palvelimet on uusittu viisi vuotta sitten ja samalla käyttöjärjestelmä päivitettiin Windows Server 2008:sta uudempaan Windows Server 2012 -versioon (Silfver 2018). Kun puhutaan siitä, mitä Windows Server –käyttöjärjestelmän ominaisuuksia on otettu käyttöön, puhutaan toiminnallisuustasoista (Active Directory Domain Services Functional Level). (Rouse 2017.)

Haaga-Helian toimialueella on kaksi ohjaustietokonetta, joiden nimet ovat DC12 ja DC7. DC12 on virtualisoitu ja se sijaitsee Haagassa, siinä missä DC7 on fyysinen palvelin, joka on sijoitettu Pasilan kampuksen palvelinhuoneeseen.

2.3 Aktiivihakemiston osat

Fyysisten palvelinkoneiden lisäksi aktiivihakemisto sisältää useita komponentteja, joiden toiminnan ymmärtäminen on välttämätöntä aktiivihakemiston päivitysprojektin aikana.

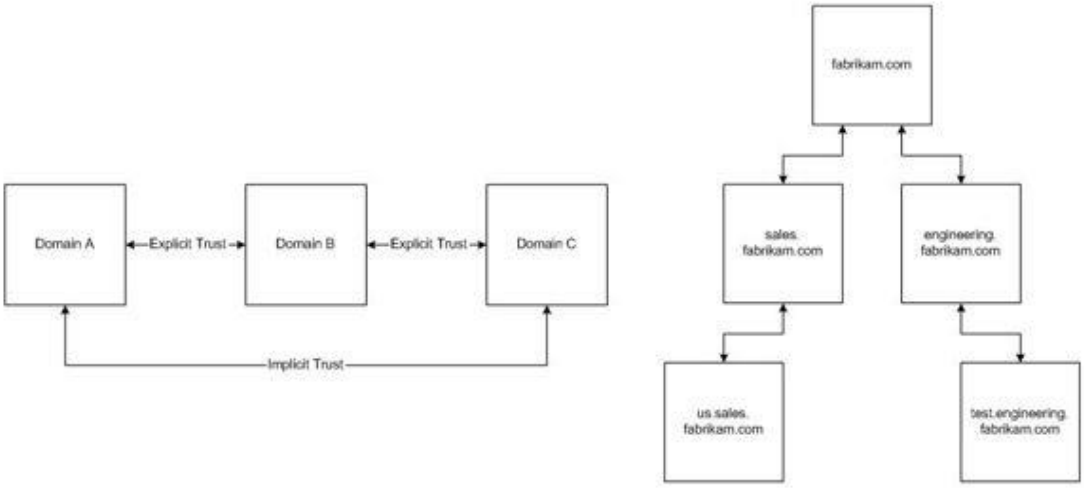
2.3.1 Toimialue (Domain)

Toimialue, eli Domain, tarkoittaa Windows palvelinympäristössä loogista hallinnollista kokonaisuutta, joka sisältää esimerkiksi käyttäjät, käyttäjäryhmät, tietokoneet ja muut objektit. Toimialueen tietokoneet käyttävät samaa aktiivihakemistoa (Warren 2018, 2). Jotta tietokone saa käyttöönsä oikeat asetukset ja resurssit, on se ensin lisättävä toimialueelle. Tällöin aktiivihakemistoon lisätään tietokoneelle tietue. Haaga-Helian organisaatio toimii yhden toimialueen alaisuudessa, jonka nimi on ”haagahelia.amk”.

2.3.2 Metsä (Forest) ja Puu (Tree)

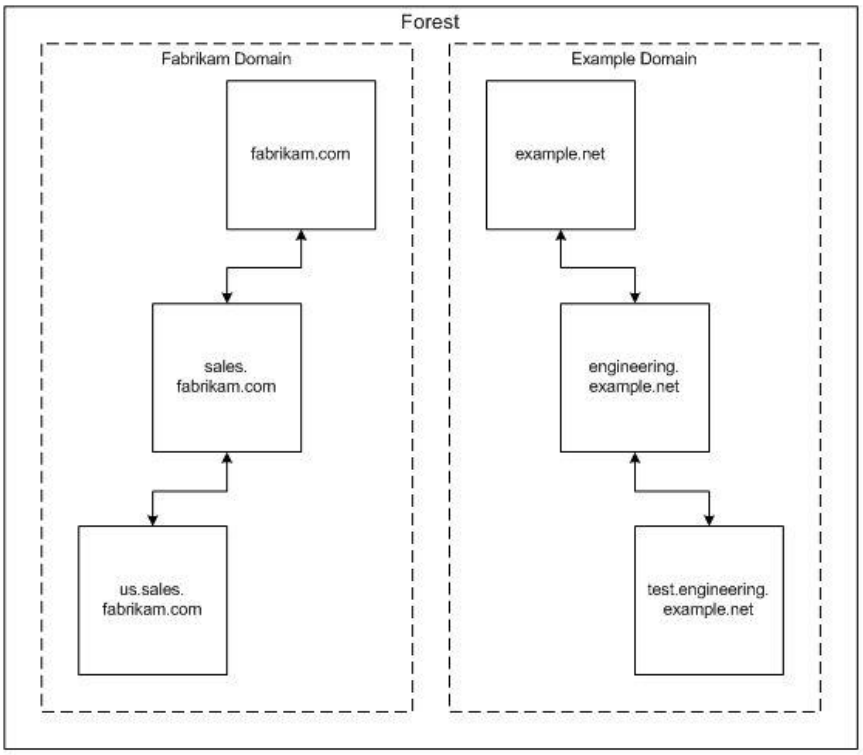
Puu (Tree) on kokoelma AD DS toimialueita, joilla on yhteinen periytyvä nimiavaruus. Samaan puuhun kuuluvat toimialueet jakavat yhteisen kaavan (schema), määritykset ja aktiivihakemiston yleisen luettelon (global catalog). (Microsoft 2018a.)

Toimialuepuuta voidaan tarkastella kahdella tavalla. Saman puun toimialueiden välillä on luottamussuhde, toisaalta ne jakavat saman hierarkkisen nimiavaruuden (kuva 2).



Kuva 2. Toimialuepuun luottamussuhteet ja yhteinen nimiavaruus (Microsoft 2018a)

Toimialuepuut yhdistyvät metsäksi (Forest). Metsässä olevien toimialueiden nimiavaruus ei ole yhtenäinen (kuva 3), mutta samassa metsässä olevilla toimialueilla on yhteinen kaava ja global catalog. Saman metsän toimialueet jakavat kirjautumistietoja luottamussuhteiden ja yhtenäisen hierarkkisen kirjautumisprotokollan, Kerberoksen avulla. (Microsoft 2018b.)



Kuva 3. Metsän epäyhtenäinen nimiavaruus (Microsoft 2018b)

2.4 Windows-palvelinten toiminnallisuustasot

Palvelinten toiminnallisuustasot määritellään erikseen domain- ja forest-tasoille. Kun toiminnallisuustasoa nostetaan, saadaan käyttöön uusia AD DS ominaisuuksia. Tällä hetkellä Haaga-Helian metsä on toiminnallisuustasolla 2008 R2 ja tässä testiprojektissa on tarkoitus nostaa se tasolle Windows Server 2016. Edellinen toimintatason nosto tehtiin Haaga-Heliassa vuonna 2015, kun käyttöön otettiin Active Directory recycle bin –ominaisuus, jonka avulla voidaan poistettuja aktiivihakemiston objekteja palauttaa nopeammin verrattuna perinteiseen varmuuskopiopalautukseen. Tällöin palautettavia objekteja voidaan käsitellä Active Directory Administrative Center -työkalulla 180 päivän ajan poistamisesta (Laakso 2017).

Toimialueelle liitetyissä työasemissa ja jäsenpalvelimilla (member server) voidaan käyttää mitä tahansa käyttöjärjestelmäversioita. Toiminnallisuustasot kuitenkin määräävät mitä käyttöjärjestelmiä toimialueen ohjaustietokoneilla voidaan käyttää. Kun AD DS –roolia asennetaan, kannattaa metsän toiminnallisuustaso (Forest Functional Level) aina määrittää korkeimmaksi mahdolliseksi, sillä näin saadaan käyttöön eniten käyttöjärjestelmän tukemia ominaisuuksia (Microsoft 2014a).

Windows Server 2016 käyttöjärjestelmän toiminnallisuustasot ovat:

- Windows Server 2008
- Windows Server 2008 R2 (Haaga-Helian Forest/Domain Level)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Metsän lisäksi jokaiselle toimialueelle määritellään erikseen toiminnallisuustaso (Domain Functional Level). Toimialueen toiminnallisuustaso ei koskaan voi olla matalampi kuin sen metsän toiminnallisuustaso, missä toimialue sijaitsee. Jos esimerkiksi metsä on toiminnallisuustasolla Windows Server 2008, täytyy kaikkien siihen kuuluvien toimialueiden olla vähintään samalla tasolla. Toimialueet voivat kuitenkin toimia ylemmällä tasolla, kuin metsä mihin ne kuuluvat.

Jokaisen uuden palvelinversion ja niiden mukana syntyneiden toiminnallisuustasojen mukana on saatu uusia käyttöominaisuuksia. Seuraavissa taulukoissa (taulukot 1 & 2) on

esitelty käyttöjärjestelmäversiot ja toimialueen toiminnallisuustasoon kuuluvat uudet ominaisuudet.

Taulukkoon on sisällytetty vain ne toiminnallisuustasot, jotka ovat merkittäviä Haaga-Helian päivystysprojektin aikana. Täydellinen taulukko, jossa on mukana kaikki toiminnallisuustasot, löytyy opinnäytetyön lopusta liitteestä 2.

Taulukko 1. Toimialueen toiminnallisuustasojen ominaisuudet (Microsoft 2014a & Microsoft 2018c)

Windows Server 2008 R2 (Haaga-Helia Domain level)	-User logon method authentication. -Automated SPN update. -Windows PowerShell cmdlets for AD.	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2
Windows Server 2012	-The KDC support for claims, compound authentication, and Kerberos armoring. -Dynamic Access Control.	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012
Windows Server 2012 R2	-DC-side protections for Protected Users. -Authentication Policies. -Authentication policy Silos.	Windows Server 2016 Windows Server 2012 R2
Windows Server 2016	-New Kerberos and NTLM features.	Windows Server 2016

Kuten toimialueella, myös metsälle asetettu toiminnallisuustaso tuo mukanaan uusia ominaisuuksia. Seuraavassa taulukossa on luetteloitu edellisen taulukon tapaan uudet, metsän toiminnallisuustasoon liittyvät ominaisuudet.

Taulukko 2. Metsän toiminnallisuustasojen ominaisuudet (Microsoft 2014a & Microsoft 2018c)

Windows Server 2008 R2 (Haaga-Helia Forest Level)	-**Active Directory Recycle Bin**, which provides the ability to restore deleted objects in their entirety while AD DS is running.	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2

Windows Server 2012	-No new features.	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012
Windows Server 2012 R2	-No new features.	Windows Server 2012 R2
Windows Server 2016	-Privileged access management (PAM) using Microsoft Identity Manager (MIM).	Windows Server 2016

Tuki Windows Server 2003 –käyttöjärjestelmälle on loppunut, joten kaikki Domain Controllerit nykyaikana täytyisi päivittää vähintäänkin toiminnallisuustasolle 2008.

2.5 Kaava (Schema)

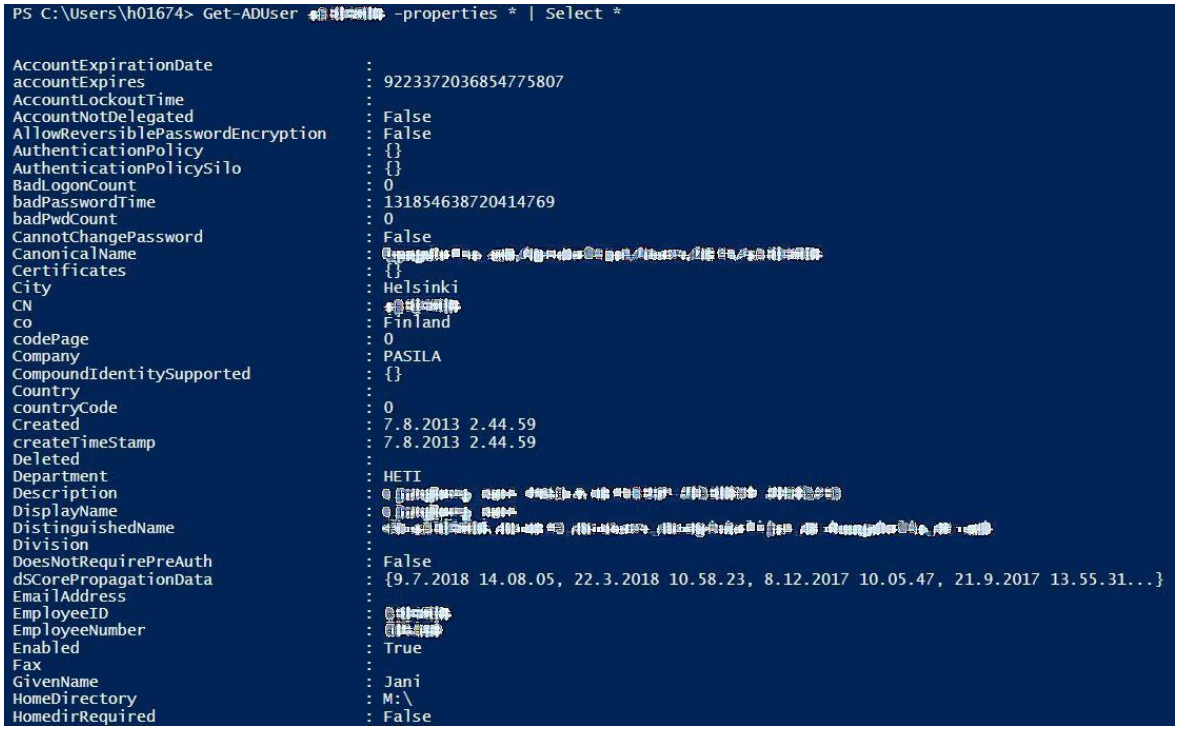
Aktiivihakemisto on rakenteeltaan tyypillinen hakemistopalvelu (Directory Service). Perinteisen hakemistopalvelun tehtävänä on tallentaa tietoverkon resursseja hakemistoon ja tarjota työkalut objektien lisäämiseen, poistamiseen, muokkaamiseen ja hakemiseen.

1980-luvulla syntyi tarve yhtenäisten hakemistopalvelustandardien käyttämiseen, kun eri kehittäjät loivat omia, yhteen sopimattomia järjestelmiään. Syntyi X.500-standardi, jonka pohjalta kehitettiin myöhemmin Lightweight Directory Access Protocol, eli LDAP. Aktiivihakemisto on Microsoftin kehittämä hakemistopalvelu, joka tukee LDAP-protokollaa. (Talvivaara s.a.)

AD DS on tietokanta, joka muodostuu erilaisista objekteista ja niiden ominaisuuksista, eli attribuuteista. Objektityypit ja niiden attribuutit määrittävät, millaisia tietoja aktiivihakemistoon voidaan tallettaa ja millaisessa muodossa. Tyypillinen aktiivihakemiston tietokantaobjekti on esimerkiksi käyttäjätili, jolla on lukuisia ominaisuuksia, kuten nimi, osasto ja salasana. Microsoft aktiivihakemiston kaava, eli schema, sisältää tarkat kuvaukset objektityypeistä ja niiden ominaisuuksista, joita metsän aktiivihakemistoon voidaan tallentaa. Jokaisella Domain Controllerilla on oma kopionsa kaavasta. (Warren 2018, 3.)

Yksittäisiä aktiivihakemiston objekteja kerätään luokkien (class) alle. Tyypillisiä luokkia ovat esimerkiksi käyttäjä, käyttäjäryhmä ja printterijono (User, Group, Print-Queue). Kun aktiivihakemistoon luodaan uusi käyttäjä, syntyy käytännössä uusi käyttäjä-luokan ilmentymä (instance).

Objektien attribuutit luodaan ja määritellään erillään luokista. Näin yksittäistä attribuuttia voidaan käyttää monen eri luokan osana. Windows PowerShell–työkalun avulla on helppo listata kaikki käyttäjätiliin liittyvät ominaisuudet. Seuraavassa kuvassa 4 on Haaga-Helian aktiivihakemiston user-luokan objekti ja sen attribuutteja.



Kuva 4. User-luokan objekti ja sen attribuutteja

2.6 Replikointi

Jokaisella metsän Domain Controllerilla on oma kopio aktiivihakemistosta. Kun muutoksia tehdään yhdelle koneelle, kopioituvat tiedot automaattisesti muiden koneiden aktiivihakemistoihin. Tätä prosessia kutsutaan replikoinniksi.

Tyypillisesti replikointi tapahtuu palvelimien välillä nopeimmalla mahdollisella tavalla. Tätä varten AD DS järjestelee palvelimet ryhmiksi, joita kutsutaan nimellä site. Koska replikointi halutaan suorittaa mahdollisimman nopeasti, kuuluvat paikalliset, nopeiden yhteyksien takana olevat koneet samalla samaan siteen (Intrasite replication). Nämä koneet saattavat sijaita maantieteellisesti lähekkäin vaikkapa samassa kaupungissa, tai nopeiden verkkoyhteyksien päässä samassa rakennuksessa. Tietoverkkoon kiinnitetyt laitteet käyttävät site-tietoa määritelläkseen lähimmän Domain Controllerin esimerkiksi silloin, kun ne hakevat sisäänkirjautumiseen tarvittavia tietoja. (Warren 2018, 3.)

Sitejen välinen (Intersite replication) toteutetaan niin, että nopeamman yhteyden yli kommunikoivat, samaan siteen kuuluvat koneet replikoivat keskenään ja yhteyden ulkopuolel-

le hoitaa erillinen välityspalvelin, eli site link bridgehead. Tällöin voidaan hitaamman yhteyden yli tapahtuva replikointi ajastaa tapahtumaan silloin, kun tietoverkossa on vähän liikennettä. (Morimoto, Shapiro, Yardeni, Noel, Abbate & Amaris 2017.)

Aktiivihakemiston tietokanta on jaettu kolmeen osioon, jotka ovat schema, configuration ja domain. Schema on metsän tasolla oleva osio, johon harvoin tehdään muutoksia. Samoin configuration, joka sisältää tiedot metsän asetuksista. Domain-osioon sen sijaan tehdään muutoksia usein ja valtaosa aktiivihakemiston replikointi-tiedosta onkin muutoksia tähän osioon. Domain-osioon kuuluvat esimerkiksi uudet käyttäjätilit ja vaihtuvat salasanat, sekä toimialueelle liitettävät tietokoneet. (Warren 2018, 113.)

2.6.1 Replikoinnin yleiset periaatteet

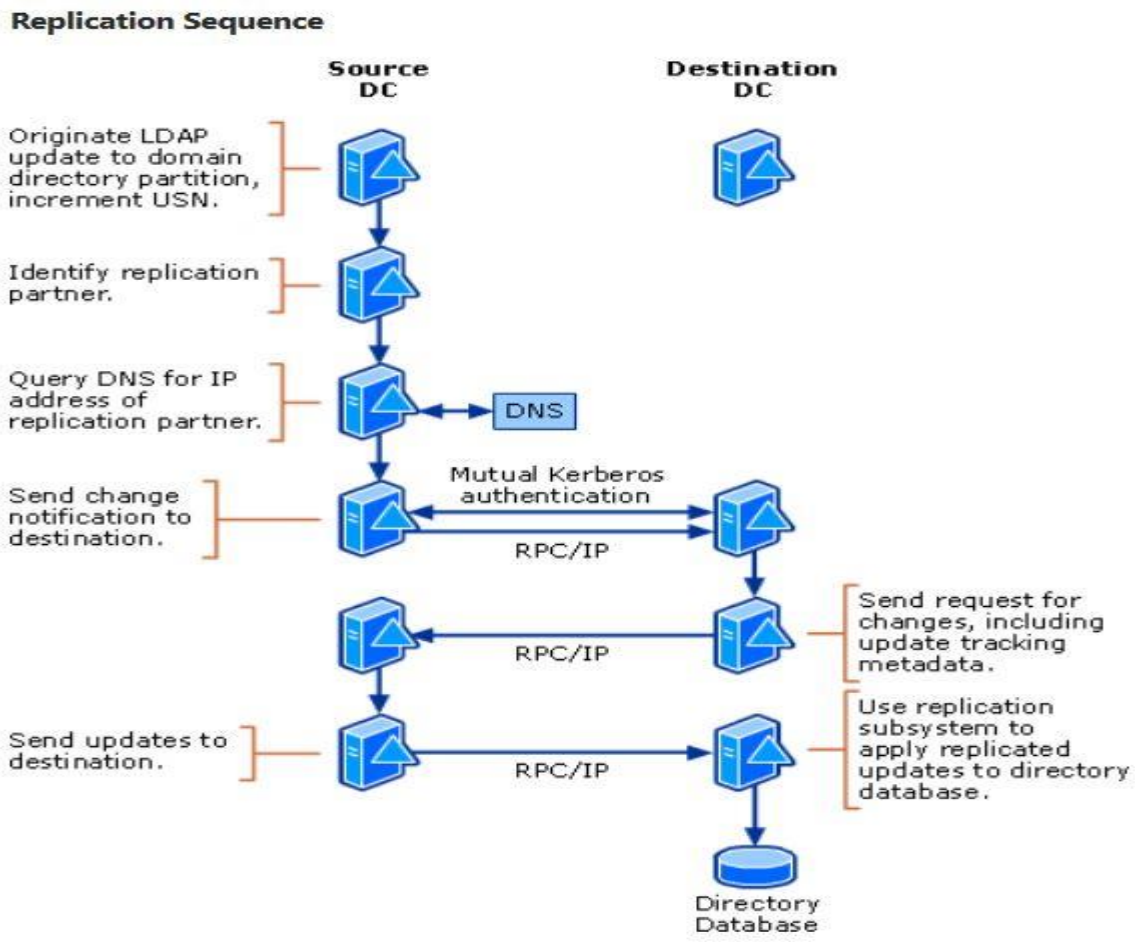
AD DS replikoinnin tarkoituksena on synkronisoida ohjaustietokoneille tallennetut aktiivihakemiston tiedot niin, että kaikkien ohjauskoneiden tiedot ovat identtiset. Muutoksia voidaan tehdä mille tahansa metsän Domain Controllerille ja ne ottavat vastaan LDAP-pyyntöjä attribuuttien muuttamiseksi. Kaikkien ohjauskoneiden tietokannat ovat sellaisia, että niille voidaan kirjoittaa dataa ja sitä voidaan muokata. Tämä multimaster-ominaisuus parantaa järjestelmän suorituskykyä ja vikasietoisuutta, kun muut ohjauskoneet voivat ottaa vaurioituneen yksikön tehtävät hoidettavakseen. (Warren 2018, 114.)

Käytännössä replikoivat Domain Controllerit eivät automaattisesti työnnä muutoksia muille ohjauskoneille, vaan replikoiva tietokone lataa muuttuneet tiedot itselleen (pulling). Kun ohjaustietokoneen aktiivihakemiston tiedot muuttuvat, se ilmoittaa verkon replikoiville koneille muutoksista ja nämä pyytävät muuttuneet tiedot itselleen, eli tekevät pull requestin. (Microsoft 2008a.)

Jotta replikoinnin aikana vältyttäisiin konflikteilta, kohdistuu replikointi kokonaisten objektien sijaan niiden attribuutteihin. Domain Controllerit tallentavat muuttuneet tiedot omaan tietokantaansa ja välittävät tiedot eteenpäin seuraaville kohdekoneille. Näin alkuperäistä ohjauskonetta ei tarvita tiedon levittämiseen kaikille palvelimille. Tätä kutsutaan Store and Forward –replikoinniksi. (Microsoft 2008a.)

Replikointi käynnistyy, kun paikallisen aktiivihakemistokopion tilassa (state) havaitaan eroja kohdekoneen ja lähettävän koneen välillä. Käytännössä tila pitää sisällään attribuuttiarvojen lisäksi metadataa, jota käytetään ristiriitatilanteiden selvittämiseen ja lähetettävän tiedon kohdentamiseen vain muuttuneisiin arvoihin. (Microsoft 2008a.)

Alla olevassa kuvassa 5 havainnoidaan kahden Domain Controllerin välillä tapahtuvaa replikointia. Source DC:n aktiivihakemistossa tehdään muutoksia ja se lähettää tiedon kohdekoneelle, joka pyytää itselleen muuttuneita tietoja, sekä niihin liittyvää metadataa. Lopuksi tiedot lähetetään kohdekoneelle ja sulautetaan sen tietokantaan.



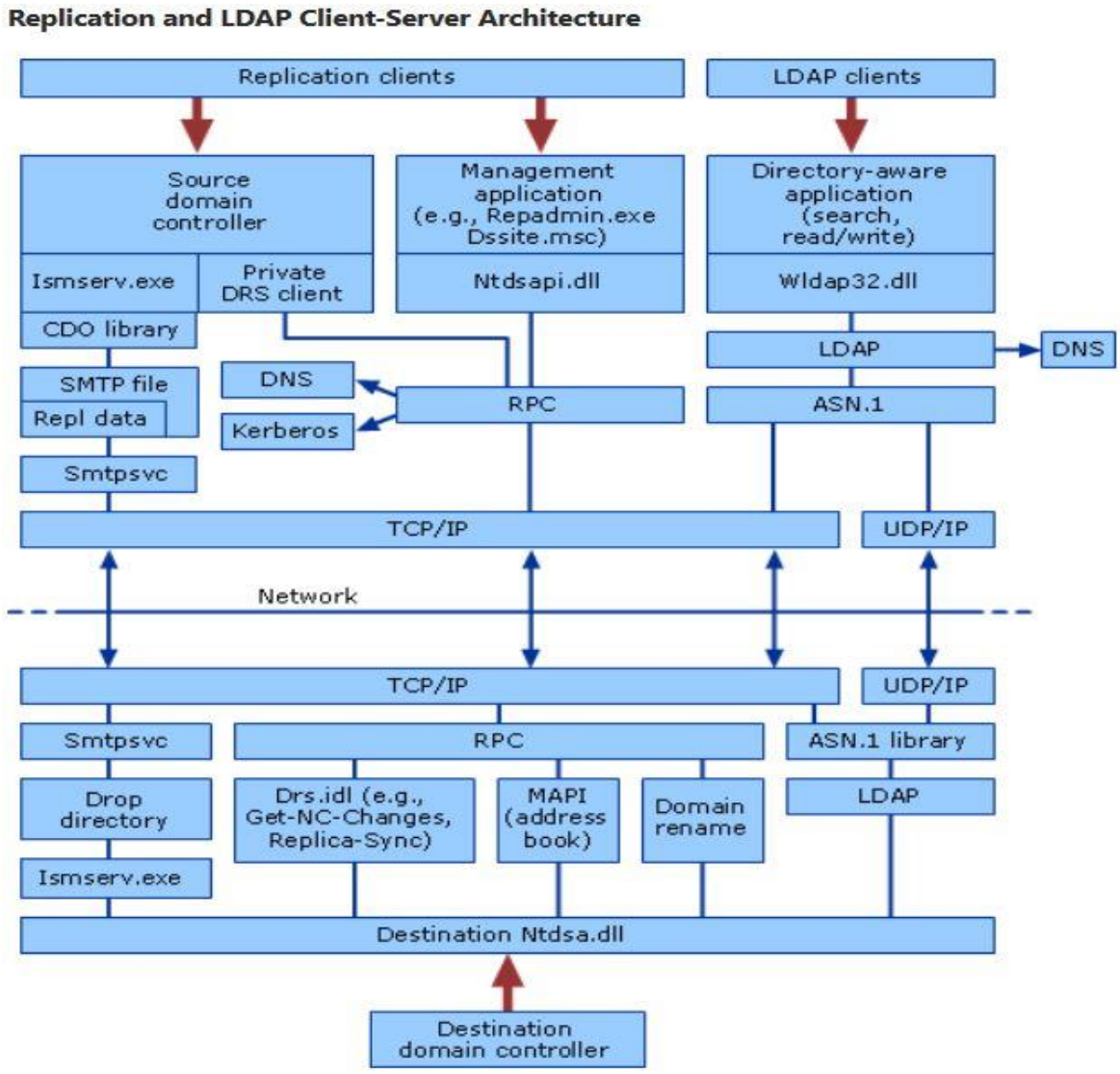
Kuva 5. Replikointi kahden Domain Controllerin välillä (Microsoft 2008a)

2.6.2 Aktiivihakemiston replikoinnin toteuttava arkkitehtuuri

Replikoinnin taustalla vaikuttaa monimutkaisempi arkkitehtuuri. Hakemistopalvelukomponenttiin, eli Ntdsa.dll-tiedostoon otetaan yhteyttä LDAP-protokollan ja LDAP C –ohjelmointirajapinnan avulla. Tämä rajapinta on nimeltään Wldap32.dll ja se sisältää hakemistopalvelun käyttöön vaadittavat kirjastot. Itse hakemistopalvelun muutokset siirretään Internet Protokollan (IP) välityksellä, kun ne on ensin paketoitu Remote Procedure Call (RPC) –protokollan avulla. Välissä toimii Ntdsapi.dll–tiedosto, tai vaihtoehtoisesti Private DRS client, jonka tehtävänä on hoitaa yhteyksiä RPC-protokollan ja hakemistopalvelun välillä. Joskus muita kuin domain-tason muutoksia voidaan valmistella Simple Mail Transfer –protokollan avulla ja siirtää TCP-protokollan avulla IP-verkon yli. (Microsoft 2008a.)

Kun tiedon siirtoon käytetään SMTP-protokollaa, luo Ismserv.exe lähdekoneella Collaborative Data Object (CDO) –kirjaston avulla SMTP-tiedoston, jossa replikoitava tieto on liitetty mukaan postitiedostona. Sitten sähköposti siirretään kohdekoneelle SMTP-palvelun avulla (Smtpsvc) TCP/IP –verkon yli ja Ismserv.exe ajaa muutokset kohdekoneelle. (Microsoft 2008a.)

Tietojen välittämisestä ja käyttöönotosta Domain Controllereiden välillä vastaa DRS, eli Directory Replication System, jolla on omat tehtävänsä palvelin- ja asiakaspuolella. Seuraavassa kuvassa 6 havainnollistetaan replikoinnin palvelin-asiakas –suhteita, sekä LDAP-clientin toimintaa.



Kuva 6. LDAP ja replikointi arkkitehtuuri (Microsoft 2008a)

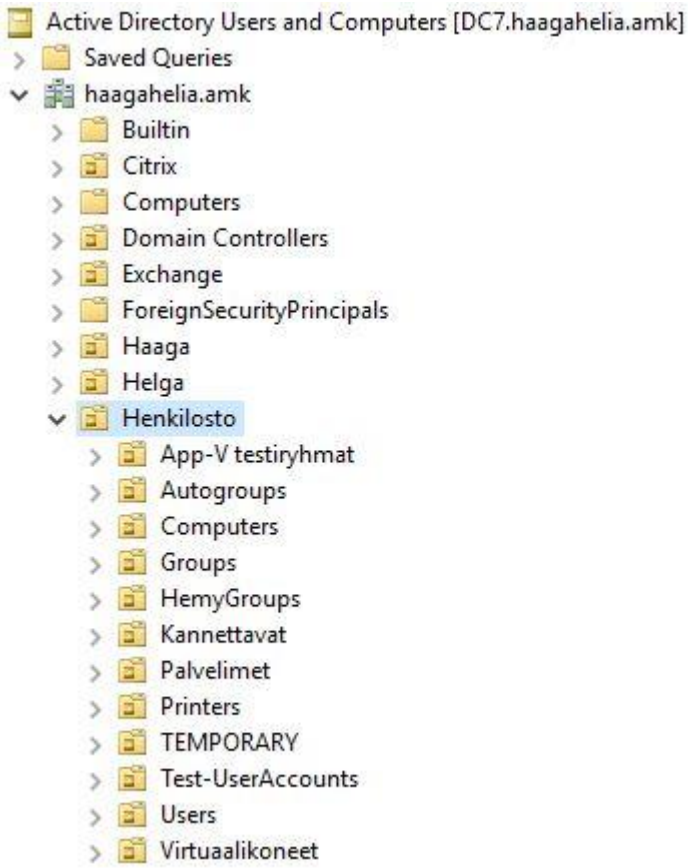
Replikoinnin yksityiskohdat pysyvät kuitenkin tavalliselta käyttäjältä melko hyvin piilossa. Microsoft on kehittänyt monia työkaluja replikoinnin seuraamiseen ja analysointiin.

2.7 SYSVOL

Käyttäjän kirjautuessa tietokoneelle, käyttöön tulevat tietyt asetukset. System Volume eli SYSVOL, on jaettu hakemisto, joka sijaitsee ohjauskoneilla ja sisältää kirjautumis-skriptit (Logon Scripts) ja ryhmäkäytännöt, eli Group Policy Objects (GPOs).

2.7.1 Group Policy Objects, eli ryhmäkäytännöt

Ryhmäkäytännöt mahdollistavat aktiivihakemiston toimialueelle liitettyjen resurssien keskitetyn hallinnan. Aktiivihakemistoon lisätyt objektit ryhmitellään organisaation rakenteen mukaan organisaatioyksiköihin (Organizational Unit, OU). Kun samassa organisaatioyksikössä oleville käyttäjä- tai konetileille halutaan voimaan yhteiset asetukset, luodaan Group Policy Object, ryhmäkäytäntö, ja linkitetään se organisaatioyksikköön. Näin saadaan helposti samat asetukset voimaan kaikille samassa organisaatioyksikössä oleville aktiivihakemiston objekteille. Alla olevassa kuvassa 7 on Haaga-Helian aktiivihakemiston Users and Computers –työkalun näkymässä organisaatioyksiköitä, joista avattuna näkyvissä Henkilöstö-organisaatioyksikkö.



Kuva 7. Haaga-Helian organisaatioyksiköitä

Ryhmäkäytäntöjen avulla voidaan aktiivihakemistossa antaa monenlaisia asetuksia. (Warren 2018, 156.)

- Windows-asetukset ja applikaatiot. Ryhmäkäytäntöjen avulla voidaan yhtenäistää koneiden Windows-käyttöjärjestelmäasetukset.
- Ohjelmisto asennukset. Ryhmäkäytäntö asentaa, konfiguroi ja päivittää työpöytä sovelluksia.
- Kansioiden uudelleenohjaus. Käyttäjät voivat kustomoida Windows-asetuksiaan muokkaamalla Start-valikkoa, työpöytää ja tiedostokansioitaan, jotka tallennetaan käyttäjän kotihakemistoon. Ryhmäkäytännön avulla kotihakemisto voidaan ohjata verkkoresurssiin, jolloin asetukset ovat käytettävissä kaikilla toimialueen koneilla.
- Tietoturvan asetukset. Ryhmäkäytännöt asettavat yhtenäiset tietoturva-asetukset toimialueen koneille.
- Infrastruktuuri. Ryhmäkäytäntöjen avulla annetaan koneille infraan liittyviä asetuksia. Näitä ovat esimerkiksi palomuurit ja langattomat verkot.

Käytännössä ryhmäkäytäntöjä muokataan Group Policy Management Editorin avulla. Tyypillisesti GPO rakentuu puumaisesti ja sisältää kansion ja alakansioita, jotka pitävät sisällään yksittäisiä asetustietoja. Päätasolla asetukset tehdään user configuration ja computer configuration jaon alle. Näiden alapuolella on joukko kansioita, jonne erilliset ryhmäkäytäntöön kuuluvat asetukset tehdään. Näitä ovat esimerkiksi Software Settings, Windows Settings (esimerkiksi skriptit ja turva-asetukset) ja Administrative Templates. (Warren 2018, 158.)

2.7.2 Ryhmäkäytäntöjen tallennus ja replikointi

Aktiivihakemistossa olevien ryhmäkäytäntöjen tallennus palvelimille tapahtuu kahteen komponenttiin.

Group Policy Container on säilö, joka on tallennettu aktiivihakemiston tietokantaan. Se sisältää ryhmäkäytäntöjen perustason attribuutit ja jokaiselle ryhmäkäytännölle on annettu oma, erillinen tunnisteensa, nimeltään Globally Unique Identity (GUID). Tätä komponenttia replikoidaan ohjaustietokoneiden välillä joko intersite- tai intrasite-replikointia käyttäen, kuten edellisessä kappaleessa on kuvattu. (Warren 2018, 156.)

Toinen ryhmäkäytäntökomponentti, Group Policy Template, koostuu tiedostoista ja kansioista, jotka on tallennettu SYSVOL-kansioon. Kansio löytyy jokaiselta toimialueen ohjaus-

koneelta ja sen sisältämistä tiedostoista löytyvät ryhmäkäytäntöjen sisältämät asetukset. SYSVOL-kansioon tallennetut GPO:t voidaan löytää hakemistopolun ”%Systemroot%\SYSVOL\Domain\Policies\{GUID}” takaa.

SYSVOL-hakemiston replikointi ohjauskoneiden välillä on toteutettu oman, muusta replikoinnista erotetun järjestelmänsä avulla. Windows Server 2008 ja sitä aikaisemmissa versioissa replikoinnissa käytössä oli File Replication Service (FRS). Uudemmat käyttöjärjestelmä versiot käyttävät Distributed File System Replication –järjestelmää (DFSR). Tällä hetkellä Haaga-Heliassa on käytössä vanhempi, Windows NT –pohjainen FRS, mutta päivityksen aikana käyttöön saadaan uudempi DFS-tiedostojakosysteemi.

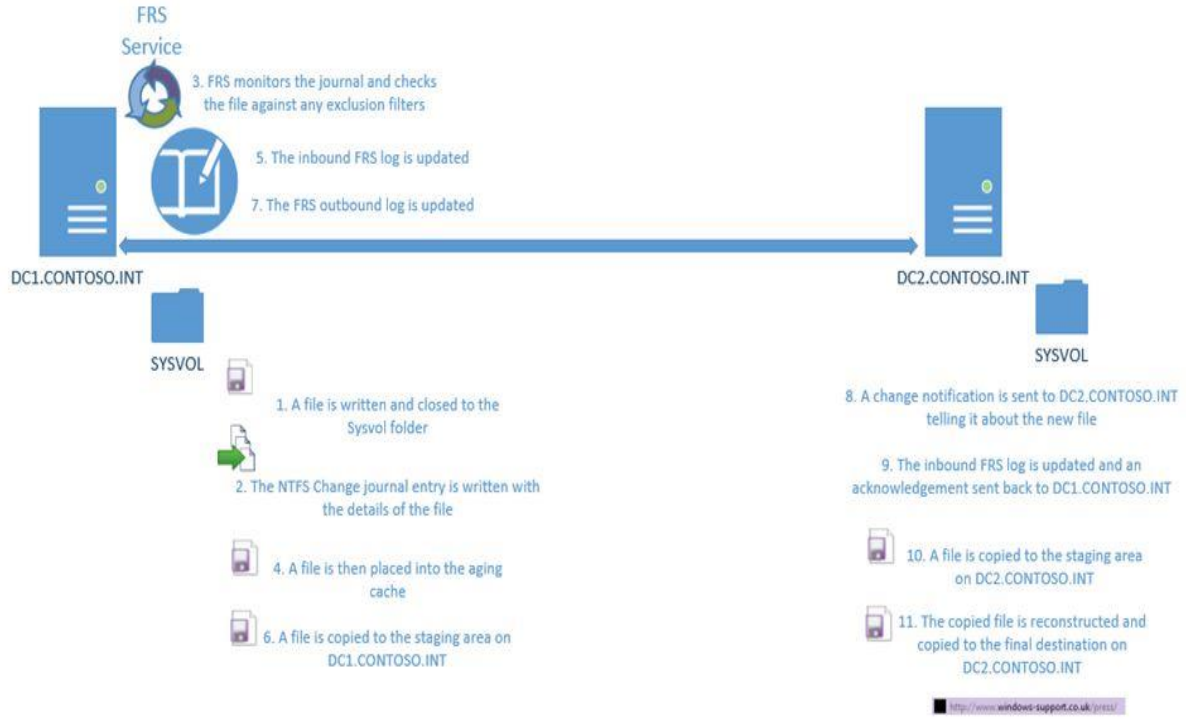
2.7.3 FRS

FRS (File Replication Service) on multimaster- ja multithread-ominaisuutta hyödyntävä replikointimetodi, mikä tarkoittaa, että jokainen palvelin voi tehdä muutoksia tiedostoihin. Replikoinnissa tarvittavat topologia ja aikataulutiedot haetaan aktiivihakemistosta. (Cooper 2014.)

Kun NTFS-levylle SYSVOL-kansioon tehdään muutoksia, NTFS Change journal, toiselta nimeltään USN journal, pitää kirjaa tiedostoihin tehdyistä muutoksista. FRS-palvelu seuraa USN-tietoja ja kolmen sekunnin odotuksen jälkeen käynnistää replikoinnin. Tämän tauon, niin sanotun aging cachen tarkoituksena on viivyttää replikoinnin aloitusta silloin, kun tiedostoa jatkuvasti päivitetään. Palvelin, jolla muutokset ovat tapahtuneet, kirjaa tiedot lokitiedostoihin. (Microsoft 2009.)

Sitten FRS kutsuu Backup API -ohjelmaa, joka luo VSS-teknologian avulla ”snapshotin” tiedostosta ja sen attribuuteista, sekä lisää tiedoston pakattuna palvelimen niin sanottuun staging-kansioon. Sitten palvelin lähettää ilmoituksen muuttuneista tiedoista muille palvelimille, ja replikoinnin kohdekoneet lataavat muuttuneet tiedot omiin staging-kansioihinsa. Lopuksi Backup API purkaa tiedostokuvan ja siihen paketoidut oikeudet (permissions) kohdekoneen SYSVOL–kansioon. (Microsoft 2009.)

Seuraavassa kuvassa 8 on kuvattu FRS-replikointia kahden ohjauskoneen, DC1:n ja DC2:n välillä. DC1 tekee muutoksia SYSVOL-kansioonsa ja ilmoittaa DC2:lle tästä. Muutokset kirjataan lokiin ja tiedostot kopioidaan staging-kansioiden välillä. Replikointiprosessia voi seurata numeroinnin avulla.



Kuva 8. FRS replikointi (Microsoft 2009)

2.7.4 DFS

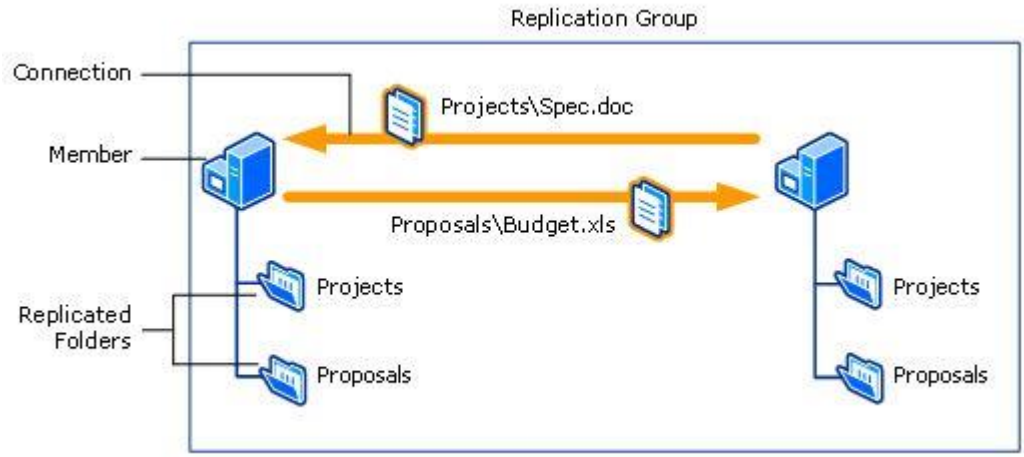
DFS on Microsoftin uudempi tiedostojen replikointiin tarkoitettu järjestelmä ja sen käyttö on mahdollista toimialueilla, joiden toiminnallisuustaso on vähintään Windows Server 2008. Tarkemmin DFS on kokoelma client-server palveluita, joiden avulla Microsoft Windows -ympäristössä SMB-tiedostojaot (Server Message Block) saadaan järjesteltyä yhden DFS root -kansion alle. DFS koostuu kahdesta komponentista, jotka ovat namespace component ja replication component. (Microsoft 2012.)

DFS Namespace on virtuaalinen näkymä organisaation jaettuihin tiedostoihin, jotka näkyvät saman namespacen, eli nimen alla, mutta voivat sijaita eri palvelimilla. Sen avulla hajallaan olevat tiedostojaot saadaan näkymään keskitetysti yhden kansion alla. Kun käyttäjä menee hakemistoon, ohjataan tämä käyttämään lähintä palvelinta, jolla on tarvittavat tiedot hakemistossaan. (Microsoft 2012.)

DFS-replikointi on multimaster-replikointia ja se käyttää Remote Differential Compression –nimistä pakkausalgoritmia (RDC), joka havainnoi muutoksia tiedostoissa ja käynnistää DFS-replikoinnin, joka siirtää kohdekoneelle vain tiedoston muuttuneet osat. Jotta DFS-

replikointi toimisi, on ensin palvelimista luotava Replication Group, jolle määritellään yhteiset jaettavat kansiot. (Microsoft 2012.)

Seuraavassa kuvassa 9 havainnoidaan palvelinten muodostaman replikointi-ryhmän rakennetta. Molemmilla palvelimilla on kansiot, joiden sisältö replikoidaan jäsenpalvelinten välillä. Kun uusia kansioita lisätään ryhmään, voidaan niille asettaa käyttöoikeuksia ja erilaisia ominaisuuksia, kuten filttereitä, käyttötarkoituksen mukaan.



Kuva 9. DFS-palvelinten replikointiryhmä (Microsoft 2012)

Kun SYSVOL-kansion replikointi siirretään käyttämään DFS-replikointia, saadaan monia etuja. Näistä kerrotaan myöhemmin lopputyön projektiosiossa.

2.8 Operations master roles

AD DS on ominaisuuksiltaan multimaster-ympäristö, jolloin mille tahansa ohjauskoneelle tehdyt muutokset replikoidaan muille palvelimille. Aina tämä lähestymistapa ei kuitenkaan ole paras tapa toimia -vaikkapa tiedon eheyden ja tietoturvan kannalta. Kun esimerkiksi salasanoihin liittyviä muutoksia tehdään, saattaa olla turvallisempaa käsitellä asia ensin yhdellä ohjauskoneella ja sitten vasta siirtää tiedot muille palvelimille. (Warren 2018, 36.)

Tällaisia tehtäviä varten palvelimille määritellään operations master –rooleja. Rooleja on viisi erilaista ja joskus niitä kutsutaan nimellä Flexible Single Master Operations (FSMO). Kaksi ensimmäistä rooleista toimii forest-tasolla ja loput kolme ovat domain-tason rooleja (Warren 2018, 36). Seuraavassa listassa on lueteltu master-roolit ja niiden merkitys tietojärjestelmässä.

1) Schema Master.
   Schema Master hallinnoi aktiivihakemiston kaavaa ja siihen liittyviä tietoja. Schema Master tekee päivitykset objekti – attribuuttitietoihin ja huolehtii muutosten välittämisestä muille ohjauskoneille. Koska kaavamuutokset ovat harvinaisia, voi järjestelmä säilyttää toimintakykynsä jonkin aikaa ilman Shema Master –konetta.

2) Domain Naming Master.
   Domain Naming Masterin tehtävänä on huolehtia AD DS -metsään liitettävistä toimialueista ja niiden hakemisto-osioista. Se myös valmistelee toimialueet uudelleen nimeämistä varten.

3) PDC emulator (Primary Domain Controller emulator).
   Tämän domain-tason roolin tehtävänä on vastata monesta toimialueen toiminnan kannalta tärkeästä toiminnosta. Palvelin vastaa toimialueen ajasta ja tekee salasanoihin työasemilta saapuvat muutokset. Se myös huolehtii ryhmäkäytännöistä silloin, kun niihin tehdään muutoksia.

4) Infrastructure Master.
   Palvelin ylläpitää verkkoinfrastruktuuriin liittyviä tietoja useasta toimialueesta koostuvassa metsässä. Se pitää kirjaa ja päivittää viittaukset objekteihin, joiden sijainnit ovat toisella toimialueella.

5) RID Master (Relative Identifier).
   Jokainen toimialueen objekti tarvitsee oman ID:n, eli tunnisteen. Tämä palvelinrooli jakaa jokaiselle ohjauskoneelle sarjan RID-tunnuksia. Samalla ohjauskone vastaa toimialueelle syntyvien uusien objektien nimeämisestä. Näitä objekteja ovat esimerkiksi käyttäjät, ryhmät ja tietokoneet. Kun toimialueelle lisätään uusia objekteja, niille muodostuu yksilöllinen Security Identifier (SID). Tämä on yhdistelmä toimialueen SID-tunnuksesta ja Relative ID:stä, joka haetaan ohjauskoneen RID tunnusvarastosta (pool).

   (Luettelon lähteet: Warren 2018, 36 – 37 & Microsoft 2008b.)

2.9 AD FS Extranet Lockout Policy

Tietoturvaan on tullut lisäominaisuuksia, joita voidaan päivityksen jälkeen ottaa Haaga-Heliassa käyttöön. AD FS (Active Directory Federation Services) on Microsoftin palvelu, jonka avulla voidaan jakaa identiteettitietoja luotettujen kumppaneiden kesken verkon välityksellä. Näistä kumppaneista käytetään nimitystä federation. Tällöin verkkosovelluksen käyttäjä tunnistetaan tämän omassa organisaatiossa ja tämän tiedot siirretään kohteelle claims-menetelmää käyttäen. Verkkopalvelua ylläpitävä taho sitten vertaa saapunutta tietoa omiin tietoihinsa (trust policy) ja tekee sen perusteella päätökset käyttäjän autentikoinnista (Microsoft 2018d). Haaga-Heliassa järjestelmä on käytössä esimerkiksi Office 365:ssä, Azure AD:ssa ja erinäisissä hallinnon järjestelmissä. (Silfver 2018).

AD FS Extranet Lockout Policy on tietoturvamekanismi, jonka tehtävänä on suojata aktiivihakemiston tilejä lukittumiselta, kun verkosta yritetään suorittaa brute force –hyökkäystä, jossa tunkeutuja yrittää arvailla käyttäjien salasanoja. Tällöin käynnistyy soft lockout, joka sulkee pääsyn käyttäjätilille verkon yli, mutta antaa kirjautua tilille sisäverkon luotettujen laitteiden kautta. Tämä ominaisuus vaatii kuitenkin usean DC:n käyttöä ja toiminnallisuustasoa 2012 R2. Tarkempi AD FS konfigurointi ei kuitenkaan kuulu tämän lopputyön aihepiiriin. (Windows IT Pro Center, 2018).

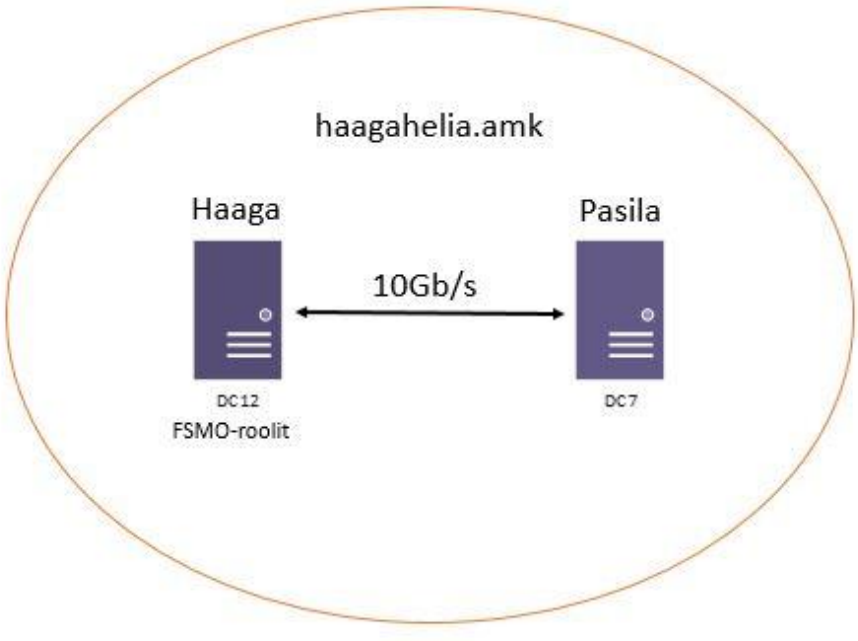
Opinnäytetyön seuraavassa osiossa rakennetaan testiympäristö Haaga-Helian aktiivihakemiston päivittämiseen, nostetaan järjestelmän toiminnallisuustasoja ja päivitetään SYSVOL-replikointi käyttämään DFS-järjestelmää.

3 Haaga-Helian aktiivihakemistopäivityksen testiprojekti

Haaga-Helian palvelinympäristön ja aktiivihakemiston päivitystä on suunniteltu vuodelle 2019. Ennen varsinaista tuotantopalvelimilla tapahtuvaa päivitystä on pystytettävä testiympäristö, jotta muutosten toimivuutta ja syntyviä ongelmatilanteita voidaan arvioida etukäteen. Tässä opinnäytetyön kolmannessa osiossa kuvataan Haaga-Helian palvelinympäristö ja kerrotaan päivitysprojektissa saatavista eduista ja ominaisuuksista. Lisäksi osiossa kuvataan projektin työvaiheet ja toteutetaan virtuaalinen testiympäristö, jossa päivitysten läpivientiä kokeillaan käytännössä.

3.1 Haaga-Helian palvelinympäristö

Haaga-Helian Windows-palvelinympäristössä on kaksi ohjaustietokonetta, Domain Controlleria. Toinen ohjauskoneista sijaitsee Haagan kampuksella ja on nimeltään DC12. Toinen ohjauskone, DC7, löytyy Pasilan kampuksen palvelinhuoneesta. Haaga-Helian aktiivihakemisto toimii yhden, haagahelia.amk-toimialueen alla (kuva 10). Vaikka ohjauskoneet fyysisesti sijaitsevat eri kampuksilla, kuuluvat ne samaan siteen ja replikoivat keskenään intrasite-replikointia käyttäen.



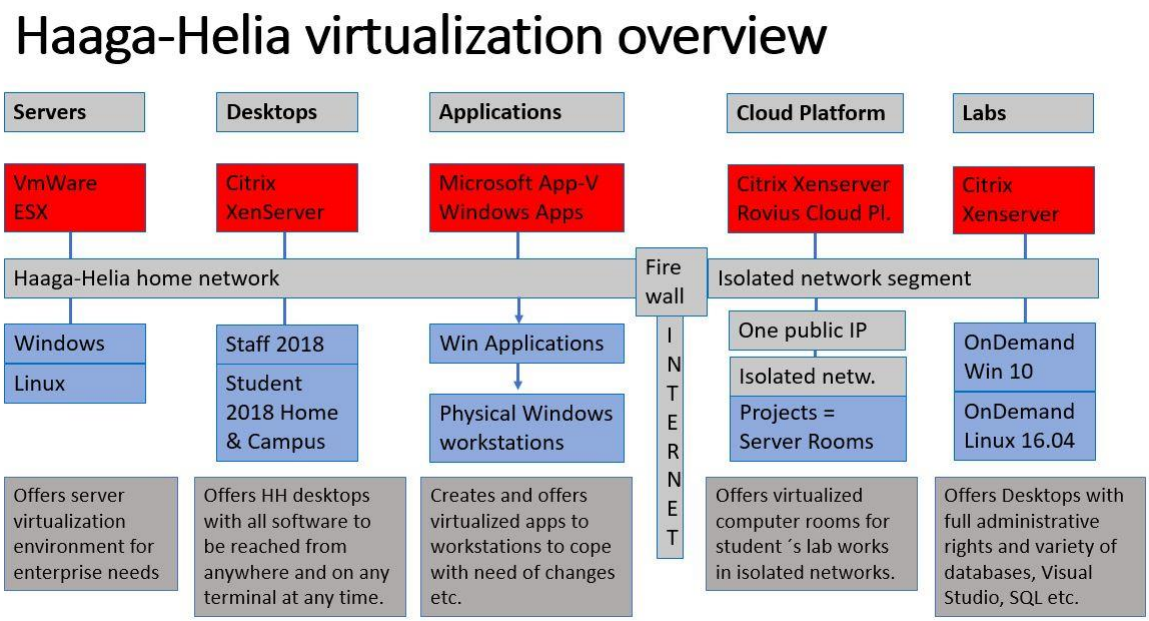
Kuva 10. Haaga-Helian toimialueen ohjaustietokoneet

Pasilassa sijaitseva ohjauskone DC7 on fyysinen laite ja se on Hewlett Packardin valmistama HP ProLiant –mallinen palvelin. Haagassa sijaitseva DC12 on sen sijaan virtualisoitu. Ohjauskoneet replikoivat tietojaan yhteyden yli, jonka nopeus on 10Gb/s.

3.2 Haaga-Helian virtualisointiratkaisut

Virtualisointi tarkoittaa tekniikkaa, jossa fyysisten laitteiden resursseja jaetaan käyttöön ohjelmallisesti. Tekniikan avulla voidaan luoda virtualisoituja työasemia, palvelimia, työpöytiä, tallennustiloja ja verkkolaitteita.

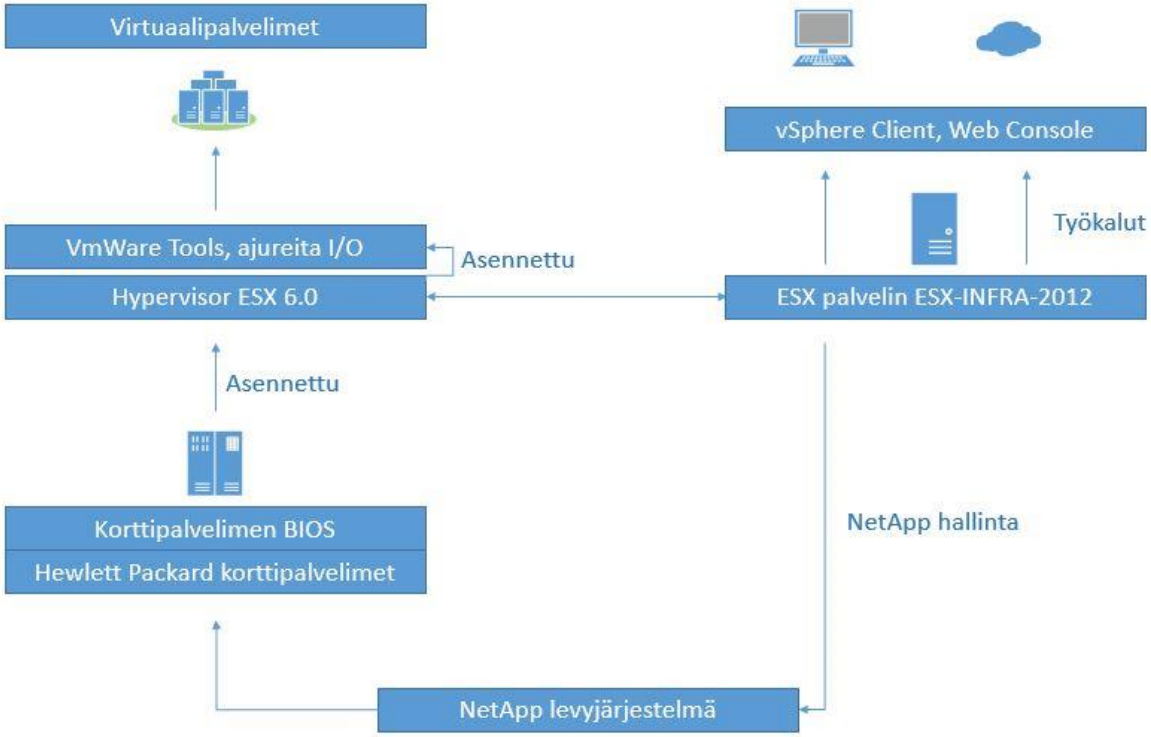
Kuten DC12, myös tässä projektissa käytettävä testiympäristö rakennetaan virtualisointialustan päälle. Haaga-Heliassa on käytössä monia virtualisointitekniikoita, joita voidaan nähdä kuvassa 11.



Kuva 11. Haaga-Helian virtualisointiteknologiat (Kalliomäki 2018)

Haaga-Helian virtuaalisessa palvelinympäristössä pyörii noin 200 palvelinta. Ne on rakennettu Hewlett Packardin valmistamien seitsemän korttipalvelimen ja kahden niin sanotun räkki-palvelimen päälle (blade, rack). Prosessoreja palvelimilla on 352 kappaletta ja muistia on käytössä 4,3Tb. (Kalliomäki 2018.)

Vuonna 1998 perustettu VMware on ensimmäinen virtualisointiratkaisuja tarjonnut yritys. Haaga-Helian palvelinvirtualisointi hyödyntää VMwaren kehittämää ESX-palvelinteknologiaa, joka taas kuuluu vSphere-nimiseen ohjelmistoon. Käytännössä ESX asennetaan suoraan fyysisten korttipalvelimien päälle ja on niin kutsuttu 1 tyypin hypervisor, jonka tehtävänä on jakaa fyysiset palvelinresurssit virtuaalikoneiksi, joilla on omat erilliset komponenttinsa, kuten prosessorit, muistikapasiteetti, verkkoyhteydet ja bios. Virtuaalipalvelinten levytila käyttää NetApp-levyjärjestelmää, joka on jaettu kahteen osaan (Haaga ja Pasila). Seuraavassa kuvassa 12 nähdään Haaga-Helian virtuaalipalvelinten arkkitehtuuri. (Kalliomäki 2018.)



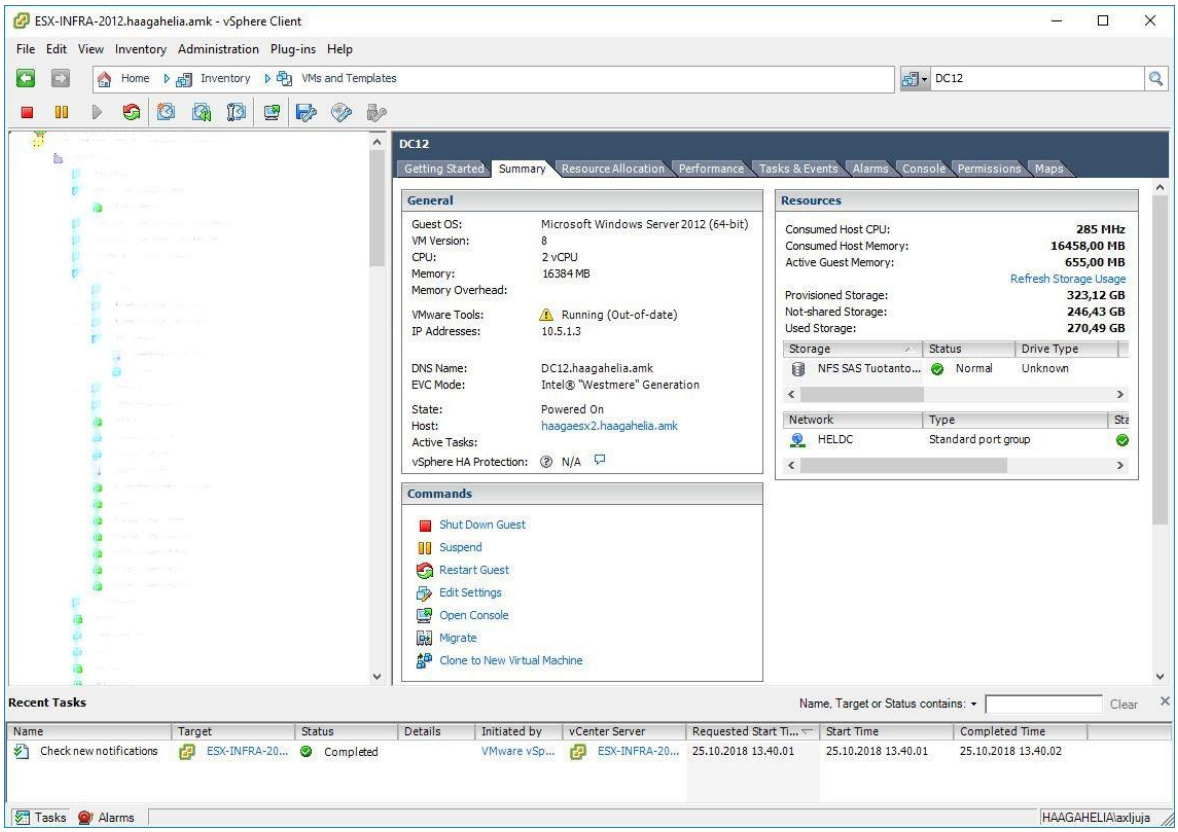
Kuva 12. Haaga-Helian virtuaalipalvelinympäristö

Virtuaalipalvelinten hallinta tapahtuu ESX-palvelimen kautta. Palvelimen nimi on ESX-INFRA-2012 ja se on luonteeltaan VMware vCenter Server. Virtuaaliympäristön hallintaan tarkoitetut työkalut ottavat yhteyttä tähän palvelimeen.

3.3 VMware vSphere Management Console

Virtuaalikoneiden hallintaan on olemassa vaihtoehtoja. Web-selaimella voidaan käyttää vSphere Web Client –portaalia, tai sitten koneelle voidaan asentaa vSphere Client. Toistaiseksi asennettavassa versiossa ei ole vielä mukana kaikkia hallintatyökaluja, mutta sen on tarkoitus vähitellen korvata Web Client kokonaan. (VMware 2018.)

Alla olevassa kuvassa 13 on esimerkki vSpheren käyttöliittymästä. Kuvassa on nähtävissä koulun toisen ohjaustietokoneen DC12:n tiedot vSphere Client –hallintapaneelissa. Vasemmalla olevassa listassa on virtuaalikoneita sisältäviä kansioita ja oikealla on nähtävissä summary-välilehti, jossa näytetään määritellyt resurssit, kuten prosessorit, muisti ja levytila. Lisäksi palvelimesta nähdään muita tietoja, kuten esimerkiksi IP-osoite.



Kuva 13. DC12-palvelimen tiedot vSphere-hallintapaneelissa

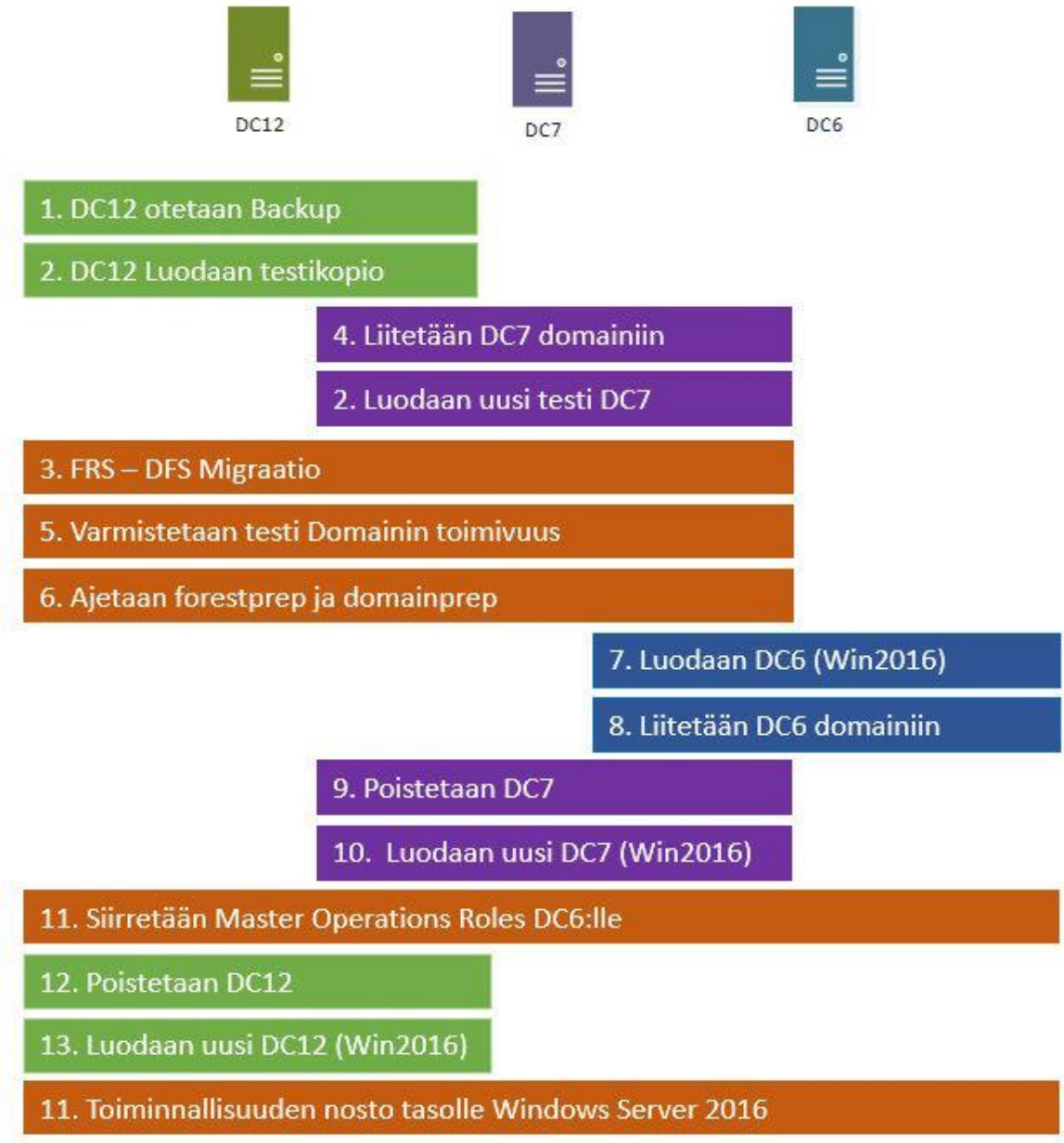
Voimme huomata, ettei yksittäinen palvelin tarvitse suuria resursseja. Sillä on käytössään 2 prosessoria, 16Gb muistia ja 200Gb levytilaa.

3.4 Aktiivihakemiston päivityksen kulku

Aktiivihakemiston päivitysprojektissa nostetaan Haaga-Helian metsän ja toimialueen toiminnallisuustasoa tasolle Windows Server 2016. Päivitys tapahtuu vaiheittain ja samalla toimialueelle lisätään uusi ohjauskone DC6.

Periaatteessa ohjauskoneet voidaan päivittää suoraan uudempaan versioon, eli tehdä niin sanottu in-place -päivitys. Tässä tulee kuitenkin helposti ongelmia. Parempi tapa onkin lisätä olemassa olevaan palvelinympäristöön Windows Server 2016 –käyttöjärjestelmällä varustettuja ohjauskoneita, sitten siirtää palvelinroolit niille ja lopuksi poistaa käytöstä vanhat Domain Controllerit. (Warren 2018, 33.)

Aktiivihakemiston päivitysprosessi kulkee kuvan 14 mukaisesti. Kuvan yläreunassa on värikoodattuina koulun ohjaustietokoneet ja oranssilla on kuvattu koko toimialueen ominaisuuksiin liittyvät tehtävät.



Kuva 14. Päivityksen prosessikaavio

Päivityksen aikana myös SYSVOL-replikointi siirretään käyttämään FRS-replikoinnin sijaan uudempaa DFS-replikointia. Kun päivitys on tehty, on toimialueella kolme Windows Server 2016 –käyttöjärjestelmällä varustettua ohjauskonetta. Lisäksi metsän ja toimialueen toiminnallisuustasot ovat tasolla Windows Server 2016.

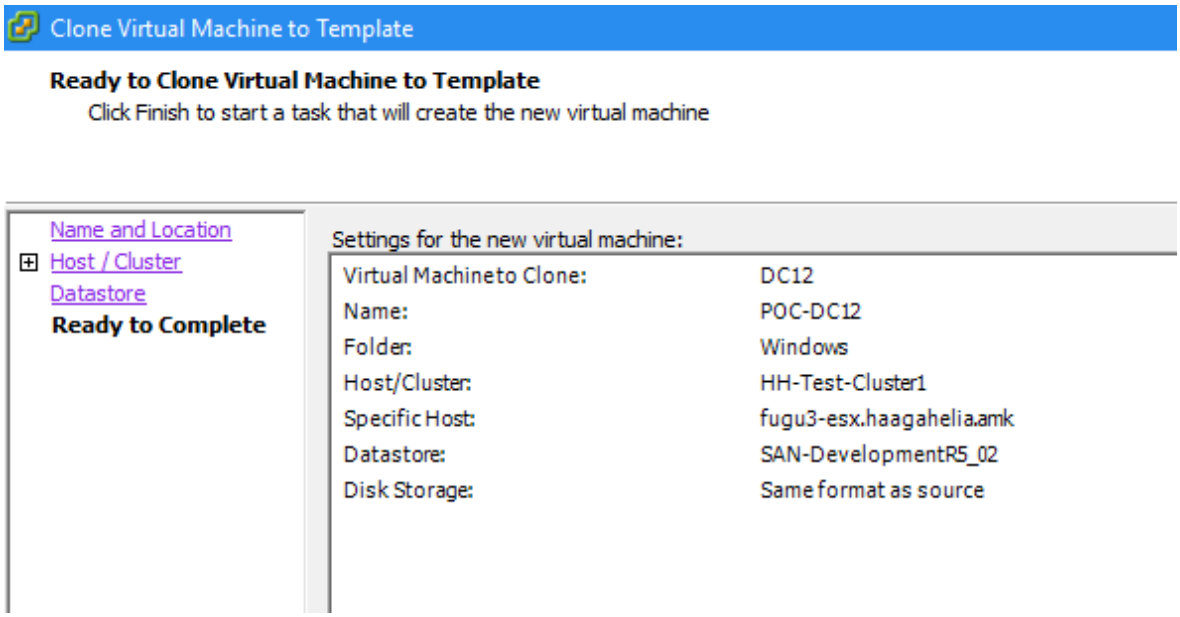
3.5 Ohjauskoneen DC12 kopiointi testiympäristöön

Päivitysprojekti aloitetaan niin, että tuotantoympäristössä olevasta palvelimesta DC12 luodaan kopio testiympäristöön. Aluksi DC12:sta luodaan pohja eli template, joka sitten muunnetaan takaisin virtuaalikoneeksi, mutta testiympäristöön. Näin syntyvälle kopiolle saadaan tarkalleen samat ominaisuudet kuin alkuperäisellä ohjauskoneella. Tämä ei kui-

tenkaan riitä, vaan käyttöjärjestelmä on vielä palautettava erikseen aikaisemmin luodun varmuuskopiotiedoston avulla. Tämä tehdään, jotta voisimme varmistaa olemassa olevien varmuuskopioiden toiminnan.

DC12 löytyy vSpheren Hosts and Clusters –lehdeltä hakutoiminnon avulla. Se on AD–nimisen resurssipoolin alla ja sitä voidaan käyttää pohjan luontiin valitsemalla valikosta ”Template -> Clone to Template”.

Käynnistyy asennusvelho, jossa asetukset annetaan kuvan 15 mukaisesti.



Kuva 15. DC12:n kopion luonnissa käytettävät palvelintiedot

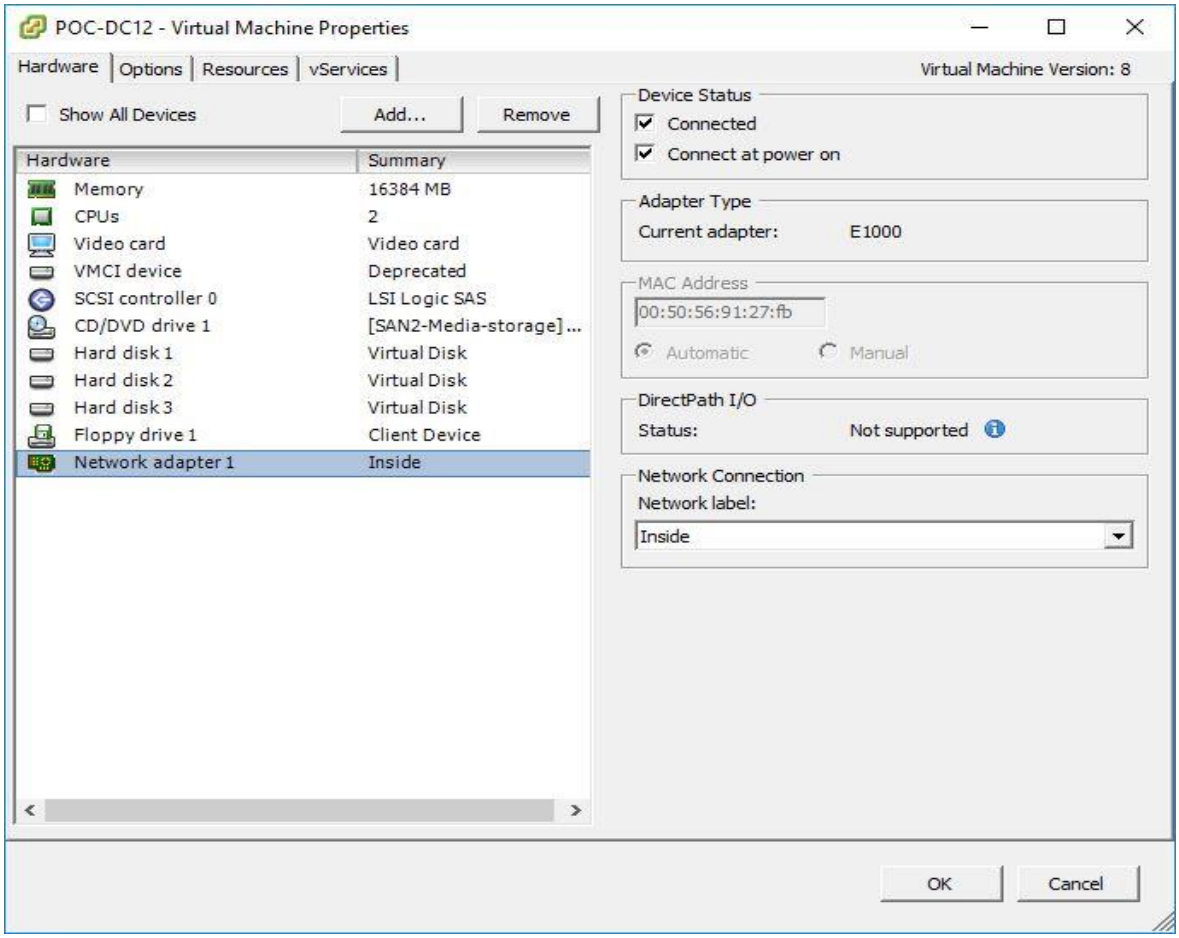
Ylläolevassa kuvassa 15 nähdään kloonattavan koneen nimi, sekä kansio minne se luodaan. Lisäksi määritellään mihin palvelinryhmään ja mille palvelimelle virtuaalikone asettuu. Lopuksi vielä kerrotaan Datastore, eli levytila, minne template-tiedosto sijoitetaan.

Syntynyt pohja löydetään VMs and Templates –sivun alta kohdekansiosta. Seuraavaksi template muunnetaan takaisin virtuaalikoneeksi valitsemalla ”Convert to Virtual Machine”. Näin syntyvä virtuaalikone siirretään vielä testiympäristön Resource Poolin alle. Resouce pool on yksikkö, jonka alle sijoitetuille koneille voidaan määritellä yhteisiä resursseja. Tässä tapauksessa sitä kuitenkin käytetään vain lajittelemaan virtuaalikoneita loogisiksi helpommin paikallistettaviksi kokonaisuuksiksi.

Haaga-Helian ohjaustietokoneet luovat automaattisesti varmuuskopioita itsestään kerran vuorokaudessa. Ohjauskoneilla on kolme levyosiota, joista e-levyä käytetään varmuusko-

pioiden tallentamiseen. Kokeilemme varmuuden vuoksi näiden varmuuskopioiden toimivuutta palauttamalla käyttöjärjestelmän Windows Backup –tiedostosta.

Tässä vaiheessa on erittäin tärkeää, ettei virtuaalikonetta käynnistetä, sillä se ei saa päästä kommunikoimaan (replikoimaan) oikeiden, tuotantokäytössä olevien palvelinten kanssa. Aloitamme ”Hardware -> Network adapter1” –välilehdeltä (kuva 16), missä valitsemme Network Connection –kohtaan verkoksi ”Inside”. Tämä tarkoittaa, että koneen verkko rajoittuu vain käytössä olevaan Host-palvelimen (fugu3-esx.haaga-helia.amk) sisälle. Näin koneella ei ole pääsyä esimerkiksi internettiin.



Kuva 16. DC12-verkkoasetukset

3.5.1 Palvelimen palauttaminen varmuuskopiosta

Kun palautamme Domain Controllerin varmuuskopiosta, olemme periaatteessa samanlaisessa tilanteessa kuin silloin, jos joutuisimme virhetilanteen jälkeen palauttamaan palvelimen toiminnan. Varmuuskopio on tehty käyttämällä Windows Server Backup –nimistä ohjelmaa, joka on erikseen lisättävä palvelimille Add features -toimintoa käyttäen. Van Keymeulen (2012) listaa verkkosivullaan varmuuskopion sisältämät tiedostot. Lista on englanniksi, sillä siinä on paljon vaikeasti suomennettavia termejä.

- Registry
- COM+ Class Registration database
- Boot files
- Active Directory Certificate Services (AD CS) database
- Active Directory database (Ntds.dit)
- SYSVOL directory
- Cluster service information
- Microsoft Internet Information Services (IIS) metadirectory
- System files that are under Windows Resource Protection
- Active Directory Federation Services

Käytännössä palautuksessa on monta työvaihetta. Ensin on palautettava palvelimen käyttöjärjestelmä ja aktiivihakemiston tietokanta, jonka jälkeen on tehtävä SYSVOL-kansion ”authoritative”-palautus.

Ohjauskoneen palauttamisessa tarvittavat työvaiheet olivat seuraavat:

1) Käyttöjärjestelmän palauttaminen backup -tiedostosta
2) Domain Administrator -salasanan haltuunotto
3) Windows Directory Services Restore Mode Administrator -salasanan vaihtaminen
4) Käytössä olevan SYSVOL-replikointitavan selvittäminen
5) System State Recovery (palauttaa aktiivihakemiston tietokannan)
6) Domain Administrator -salasanan haltuunotto uudestaan
7) SYSVOL Authorative Restore

3.5.2 Käyttöjärjestelmän palauttaminen

Aloitin palauttamalla käyttöjärjestelmän Windows Server Backup –ohjelmalla tehdystä varmuuskopiosta. Tämä tapahtui käynnistyslevyn avulla, joka sijoitettiin virtuaalikoneen DVD-asemaan. Kone käynnistettiin käynnistyslevyltä Windows Setup –ohjelmaan, jonka System Image Recovery –toiminnolla palautettiin käyttöjärjestelmä aikaisemmin luodun levykuvan avulla. Palautuksen asennuskuvat löytyvät liitteestä 3.

3.5.3 Domain Administrator -salasanan kaappaaminen

Seuraavaksi tarvitaan Domain Administrator –tasoinen salasana, jolla pääsemme muuttamaan seuraavissa vaiheissa tarvittavaa Directory Services Restore Mode Administrator

-salasanaa. Koska minulla ei ollut itselläni toimialueen administrator-oikeuksia, kun levykuva tehtiin, täytyi asiassa hieman improvisoida.

Kuka tahansa, joka saa laitettua Windows-asennuslevyn palvelimen levyasemaan voi ”hakkeroida” itselleen koko toimialueen administrator-salasanan varsin helposti. Tämä tapahtuu käynnistämällä kone asennuslevyltä ja seuraavaksi komentokonsoli painamalla ”shift+F10”. Tämän jälkeen voidaan helppokäyttötyökalujen päälle kopioida komentokonsoli. Kun kone käynnistetään, voidaan kirjautumisruudussa painaa helppokäyttötyökalujen kuvaketta, mikä käynnistääkin komentokonsolin, jota voidaan käyttää administrator-salasanan vaihtamiseen. (Pietroforte 2014.)

Salasanan vaihtoon liittyvät ruutukaappaukset selitteineen voidaan löytää liitteestä 4.

3.5.4 Windows Directory Services Restore Mode Administrator Password

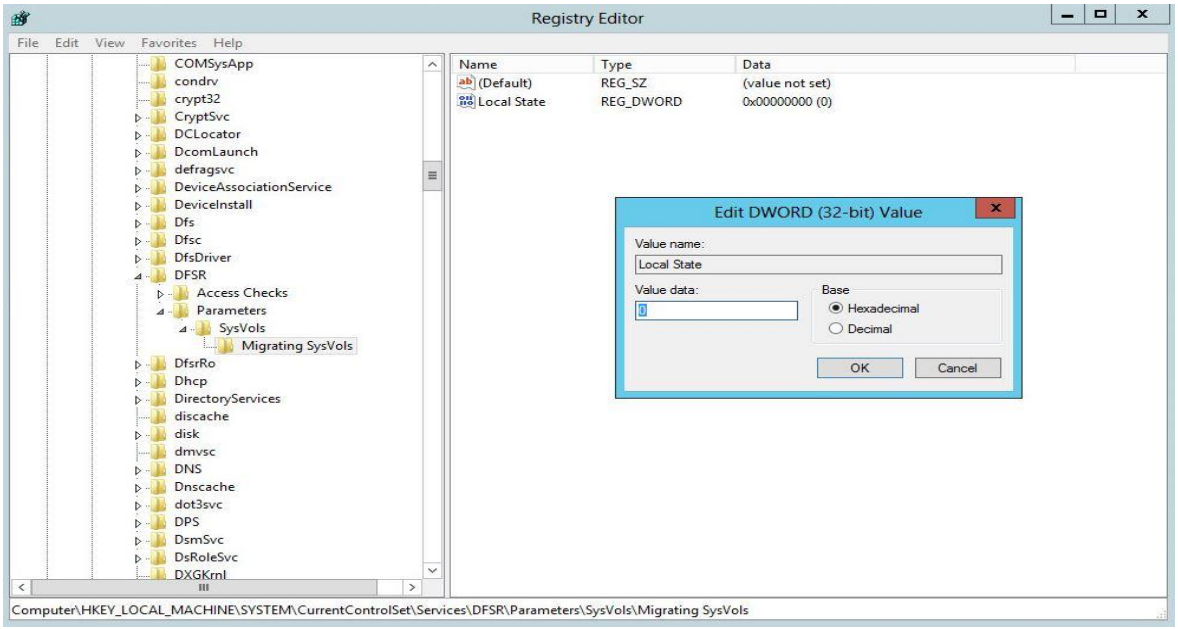
Jotta Windows voidaan käynnistää erityisessä Windows Services Restore Mode –tilassa, tarvitaan erillinen salasana, joka on määritelty alun perin silloin, kun palvelin on perustettu. Directory Services Restore Mode (DSRM) on Windows-käyttöjärjestelmän safe-mode -käynnistystapa, jonka avulla ylläpitäjä voi korjata tai palauttaa aktiivihakemiston tietokannan häiriötilanteessa. (Rouse 2012.)

Nyt kun meillä on administrator-tason tunnus palvelimelle, voimme vaihtaa DSRM-salasanan. Tämä tapahtuu Ntdsutil-työkalun avulla. Seuraavassa kuvassa 17 on esitetty komentosarja, jolla Restore-mode -salasanan vaihtaminen onnistuu. Kun salasana uudelleen asetetaan palvelimella, jonka arvona on ”null”, se tarkoittaa palvelinta, jolla komentokehotetta suoritetaan.

Kuva 17. DSMR-salasanan vaihtaminen palvelimella Ntdsutil-komennon avulla

3.5.5 FRS –tiedostojaon varmistaminen

Seuraavat askeleet eroavat toisistaan riippuen siitä, mikä tiedostojako menetelmä on käytössä. Tämän voimme selvittää tutkimalla rekisteriä alla olevassa kuvassa 18 näkyvässä osoitteessa. Jos Local State -muuttuja on 3, käytössä on DFSR, mutta kuten näemme, meillä käytössä on vielä vanhempi FRS (arvona on 0). (Microsoft 2018e.)



Kuva 18. SYSVOL-replikoinnin metodin selvittäminen rekisterin avulla

3.5.6 System State Recovery

Aluksi palautimme käyttöjärjestelmän levykuvan avulla. Levykuva ei kuitenkaan palauttanut kaikkia tarvitsemiamme tietoja, sillä palautus olisi pitänyt tehdä Windows Directory Services Restore Mode –tilassa, jonka salasanaa meillä ei vielä ollut tiedossamme. Nyt kuitenkin vaihdoimme salasanan ja voimme palauttaa aktiivihakemiston ja SYSVOL-kansion tiedot ennalleen. Tätä varten on suoritettava System State Recovery. System State -varmuuskopio on tehty erikseen Windows Backup –ohjelmalla ja se sisältää palvelimelle asennetut roolit ja aktiivihakemiston tietokannan. (Warren 2018, 106).

Ensin tietokone on käynnistettävä Windows DSRM Administrator –salasanan avulla Active Directory repair –tilaan. Kun kone on käynnistynyt uudestaan, voidaan komentotulkin avulla etsiä tallennetut varmuuskopiotiedostot ja käynnistää System State Recovery. Tähän liittyvät kuvaruutukaappaukset löytyvät liitteestä 5.

Palautuksen jälkeen voimme käynnistää koneen jälleen normaaliin tilaan ja havaita, että SYSVOL-kansioon ovat ilmestyneet ryhmäkäytännöt ja kirjautumis-skriptit (Logon scripts). Koska päivitys palautti aktiivihakemiston käyttäjätilit tilaan ennen varmuuskopion ottamista, aiheuttaa tämä meille lisäharmia. Administrator-salasana on otettava uudelleen haltuun käynnistyslevyn avulla. Kaikki tämä olisi tietysti vältettävissä, jos olisimme olleet toimialueen administrator-tunnuksen haltijoita alusta asti.

3.5.7 SYSVOL authoritative restore

Aktiivihakemiston toiminnan palauttaminen vaihtelee tilanteen mukaan. Jos ympäristössä on muita ohjauskoneita, helpointa saattaa olla poistaa viallinen ohjauskone ja lisätä sen tilalle uusi, minne tiedot sitten replikoituvat. Joskus palvelimella saattaa kuitenkin olla ohjelmia tai palveluita, joiden uudelleen asentaminen on hankalaa. Tällöin voidaan suorittaa AD DS –palautus. (Warren 2018, 110.)

Kun palautusta suunnitellaan, on tärkeää ottaa huomioon olosuhteet multimaster-ympäristössä, missä palautusta suunnitellaan. Jos toimialueella on muitakin ohjauskoneita samaan aikaan, voidaan niille tehdä muutoksia, jotka replikoituvat palautettavalle koneelle heti palautusoperaation jälkeen. Joissakin tilanteissa tämä on toivottavaa, sillä tietojen halutaan olevan ajan tasalla. Jos kuitenkin palautat esimerkiksi vahingossa poistamiasi aktiivihakemiston tietoja, et kuitenkaan halua, että replikointi pyyhkii uudelleen pois vasta palauttamasi tiedot. (Warren 2018, 110.)

Silloin, kun muut ohjauskoneet voivat kirjoittaa muutoksia palautettaviin tiedostoihin puhutaan nonauthoritative-palautuksesta. Meidän tapauksessamme palautimme aktiivihakemiston tietokannan juuri näin. SYSVOL-kansion osalta tämä ei kuitenkaan ole toimiva ratkaisu.

Palautetun palvelimen aktiivihakemisto ei käynnisty. Syynä on SYSVOL-kansion FRS-replikointi, jolle täytyy suorittaa authoritative restore. Olemme jo palauttaneet kansion paikoilleen ja se sisältää oikeat tiedostot. Koska kyseessä on ensimmäinen ohjauskone toimialueella, on SYSVOL-kansion replikointi asetettava niin, että muutokset jäävät voimaan. Tämä tapahtuu muuttamalla rekisterissä Burflags-rekisteritietoa, joka tekee omasta SYSVOL-kansiostamme ”authoritatiivisen”, jolloin sen tiedot replikoidaan myöhemmin eteenpäin toisille palvelimille, eikä toisinpäin.

Oikea rekisteri löytyy osoitteesta
”HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Back

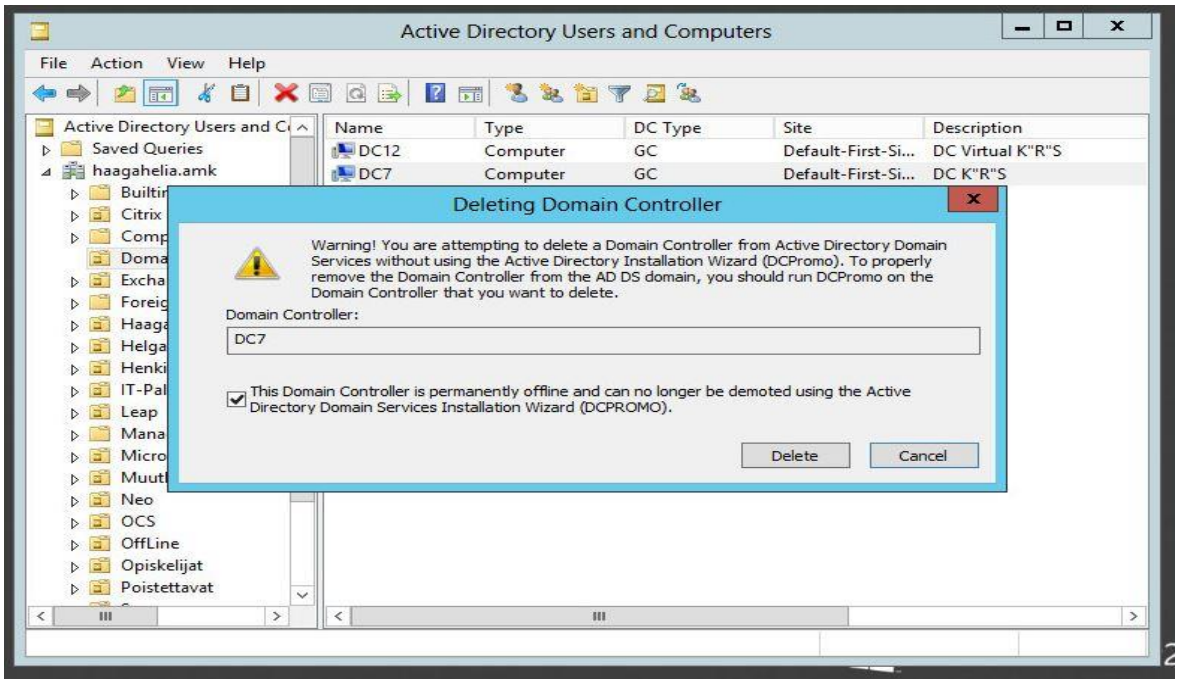
up/Restore\Process at Startup” ja sen arvoksi on annettava ”D4”, jonka merkitys on ”Authoritative mode restore”. Tätä ennen RFS-palvelu on pysäytettävä ja lopuksi se on käynnistettävä uudelleen. SYSVOL-kansion palautuksen kuvat ovat mukana liitteessä 6.

3.5.8 Lopputoimet palvelimen palautuksessa

Lopuksi tehdään vielä loppusiivouksia ja asetuksia DC12:lle. Aluksi varmistamme, että kaikki operations master –roolit todella ovat palvelimella. Alla olevassa kuvassa 19 nähtävän ”netdom query fsmo”-komennon avulla voimme huomata näin olevan.

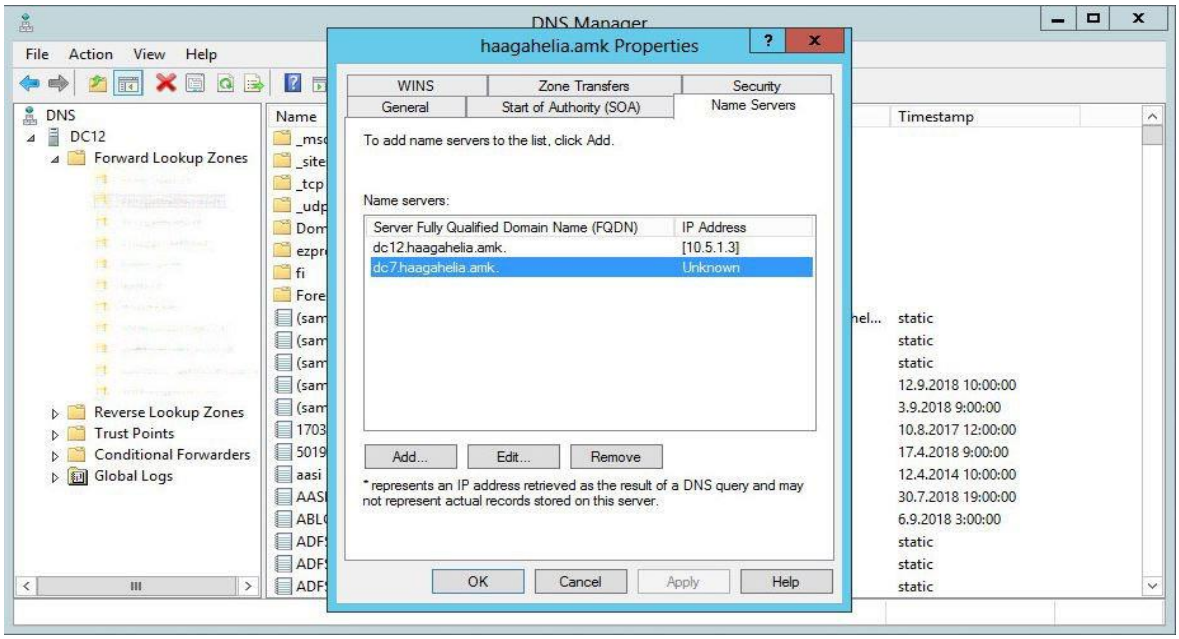
Kuva 19. Palvelinten FSMO-roolien selvittäminen komentokehotteen avulla

Tämän jälkeen poistetaan kaikki tiedot toisesta Domain Controllerista, sillä rakennamme pian uuden vastaavan tyhjästä. Onneksi Windows Server 2012 tekee tämän automaattisesti, kun Domain Controller poistetaan Active Directory Users and Computers –työkalun avulla, kuten kuvassa 20.



Kuva 20. DC7:n poistaminen aktiivihakemiston Users and Computers -näkymässä

Domain Name System (DNS), eli nimipalvelin vastaa toimialueella käytössä olevien IP-osoitteiden ja niitä vastaavien selkokielisten nimien yhdistämisestä. Windows Server 2012 asentaa DNS-palvelimen palvelinroolina. Meidän on kuitenkin poistettava kaikki DC7:ään liittyvät DNS-tietueet. Tämä tapahtuu DNS Manager -ohjelman avulla, missä avaamme haagahelia.amk–toimialueen ominaisuudet ja poistamme nimipalvelinten listalta DC7:n (kuva 21).



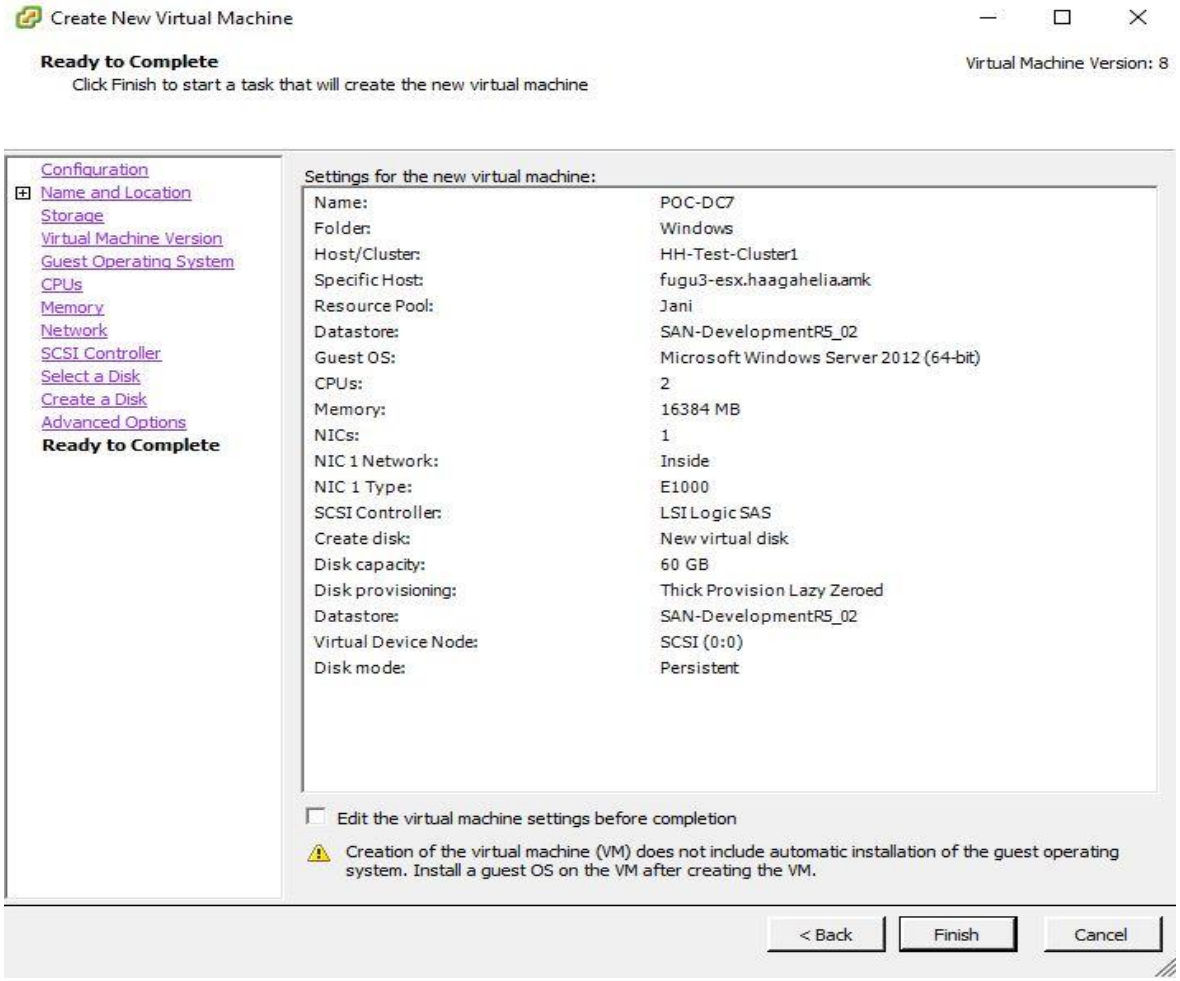
Kuva 21. DC7:n poistaminen nimipalvelinten listalta DNS Managerilla

Jos palvelin olisi palautettu ympäristöön, jossa olisi muita ohjauskoneita ja replikointia, myös muita asennustoimia täytyisi suorittaa. Tulemme nyt kuitenkin toimeen näillä asetuksilla ja jatkamme lisäämällä ympäristöön toisen ohjauskoneen, jotta testiympäristömme vastaisi Haaga-Helian järjestelmää.

3.6 DC7:n lisääminen toimialueelle

Seuraavaksi toimialueelle lisätään toinen ohjaustietokone DC7. Tämä tapahtuu luomalla kokonaan uusi Domain Controller virtuaaliympäristöön ja lisäämällä sille tarvittavat roolit, jolloin aktiivihakemisto voidaan replikoida. Näin saamme aikaan ympäristön, joka ominaisuuksiltaan vastaa Haaga-Helian tuotantopalvelimia.

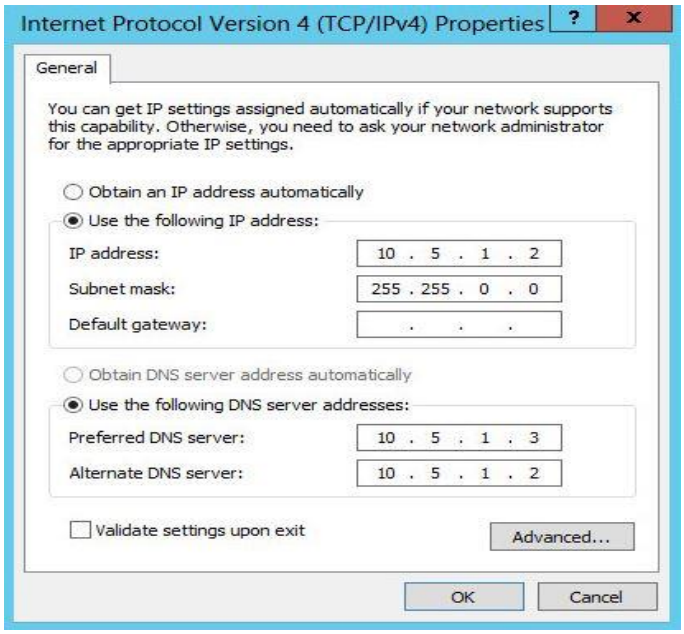
Uuden ohjauskoneen lisääminen on suoraviivainen toimenpide. Aluksi on luotava vSphere-ympäristöön uusi virtuaalikone, jolla on samat ominaisuudet, kuin toisellakin ohjauskoneella. Ohjauskoneet ovat ominaisuuksiltaan samanlaisia, jotta ongelmatilanteessa niitä voidaan palauttaa backup-tiedostoista ongelmitta (kuva 22).



Kuva 22. DC7-virtuaalikoneen asetukset vSphere-ympäristössä

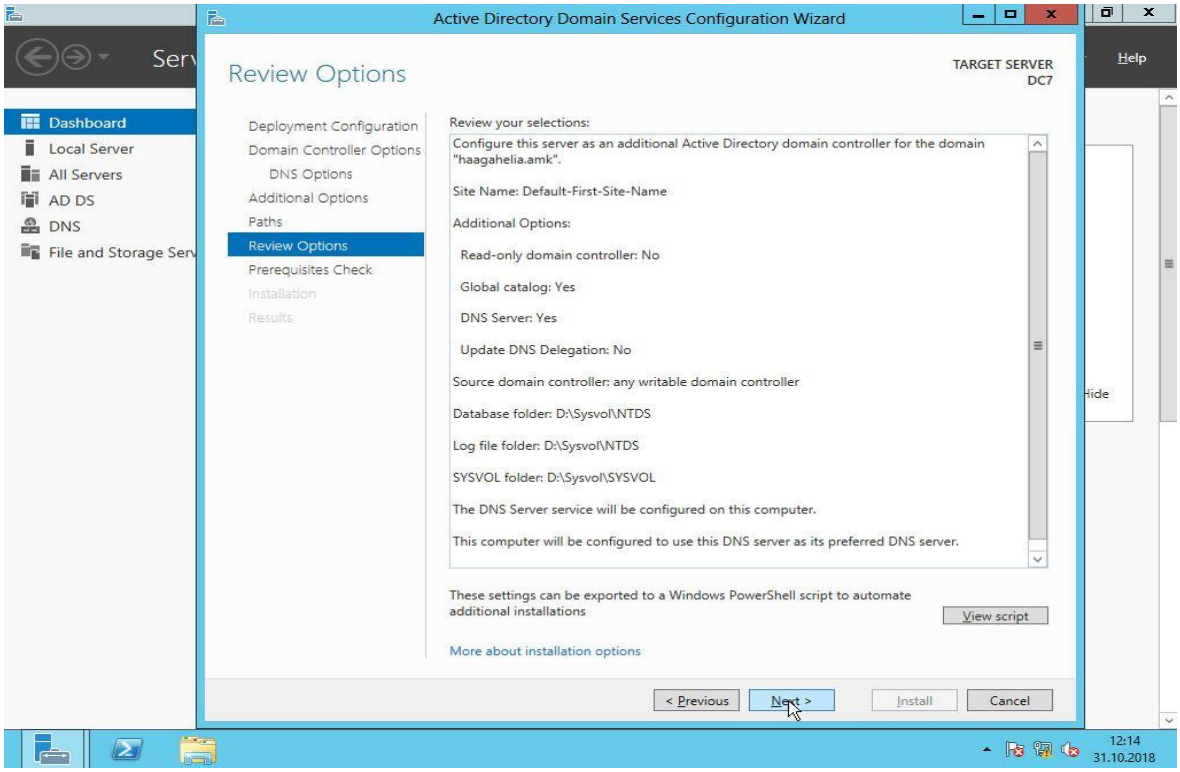
Kun virtuaalikone on luotu, asennetaan käyttöjärjestelmä normaalisti Windows Setup –ohjelmalla ja seuraamalla ruudun ohjeita. Käyttöjärjestelmälle valitaan kieliasetukset ja levyosio, jonka jälkeen kone käynnistyy uudelleen.

Ennen kuin kone voidaan ylentää ohjauskoneeksi, on joitakin asetuksia laitettava kuntoon. Koneen verkkoasetuksiin täytyy määritellä staattiset IP-osoitteet ja levyasemat täytyy alustaa. Lisäksi kello on laitettava oikeaan aikaan. Kone nimetään oikein DC7:ksi. Kuvassa 23 näkyy palvelimelle annettavat staattiset IP-osoitteet. Staattisilla IP-osoitteilla tarkoitetaan käsin asetettuja, muuttumattomia reititysosoitteita. IP-osoitteet kuuluvat yksityisille verkoille varattuun 10.5.0.0/16 –aliverkkoon.



Kuva 23. DC7-palvelimen staattiset IP-osoitteet

Kun asetukset on saatu kuntoon, voidaan kone nostaa ohjauspalvelimeksi. Tämä Tapahtuu asentamalla sille palvelinrooleja. Tarvittavat roolit ovat Active Directory Domain Services ja DNS. Seuraavassa kuvassa 24 on nähtävissä palvelinroolin asennuksessa käytettävät asetukset, mutta yksityiskohtaisemmat asennuskuvat löytyvät liitteenä 7.



Kuva 24. AD DS -asennuksen asetukset

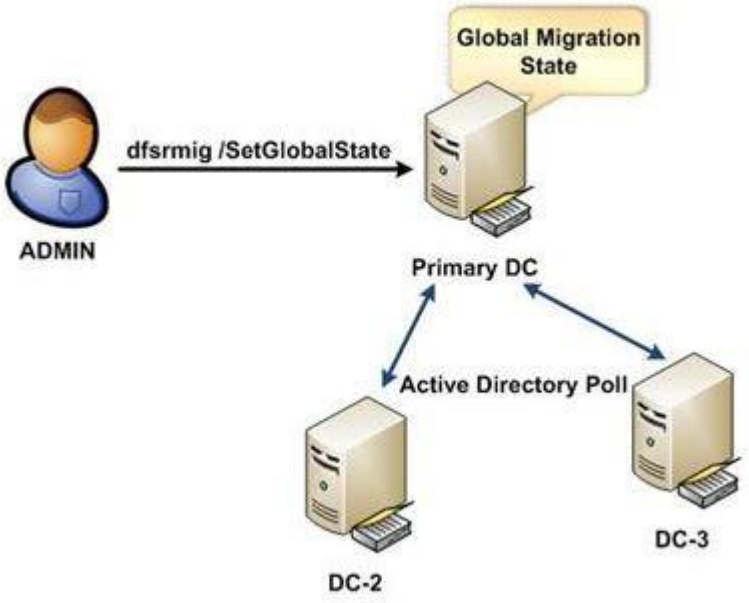
Asennuksen jälkeen meillä on toimiva kopio Haaga-Helian palvelinympäristöstä.

3.7 SYSVOL-kansion replikoinnin migraatio

Kuten jo aikaisemmin tarkistimme, meillä on käytössämme SYSVOL-kansion jaossa FRS-replikointi. Nyt kun virtuaaliympäristömme on kunnossa, voimme siirtää replikoinnin käyttämään uudempaa DFS-replikointia. Siirto on monivaiheinen prosessi, jonka tarkoituksena on varmistaa, että siirtyminen tapahtuu turvallisesti. DFSR sisältää monia parannuksia verrattuna vanhempaan järjestelmään.

Microsoft suosittelee, että SYSVOL-replikointi siirretään käyttämään DFS-replikointia. Se on tehokkaampi, paremmin skaalautuva ja luotettavampi kuin vanha järjestelmä. Se käyttää Remote Differential Compression –algoritmia muuttuneiden tiedostojen replikointiin. DFS-järjestelmässä voidaan laatia aikatauluja replikoinnille ja hallita sen käyttämää kapasiteettia tietoverkossa. Lisäksi siinä on automaattisia korjaustoimintoja ja sitä voidaan hallita Microsoft Management Consolen avulla. (Microsoft 2008c.)

Replikoinnin siirtämisessä käytetään ”dfsrmig.exe”-nimistä työkalua, jonka avulla järjestelmän ylläpitäjä voi hallita siirtymäprosessia. Kun muutoksia tehdään yhdelle ohjauskoneelle, huomaavat muut muutokset automaattisesti ja seuraavat perässä. Tätä havainnollistetaan kuvassa 25.



Kuva 25. FRS-DFS migraatio (Microsoft 2008c)

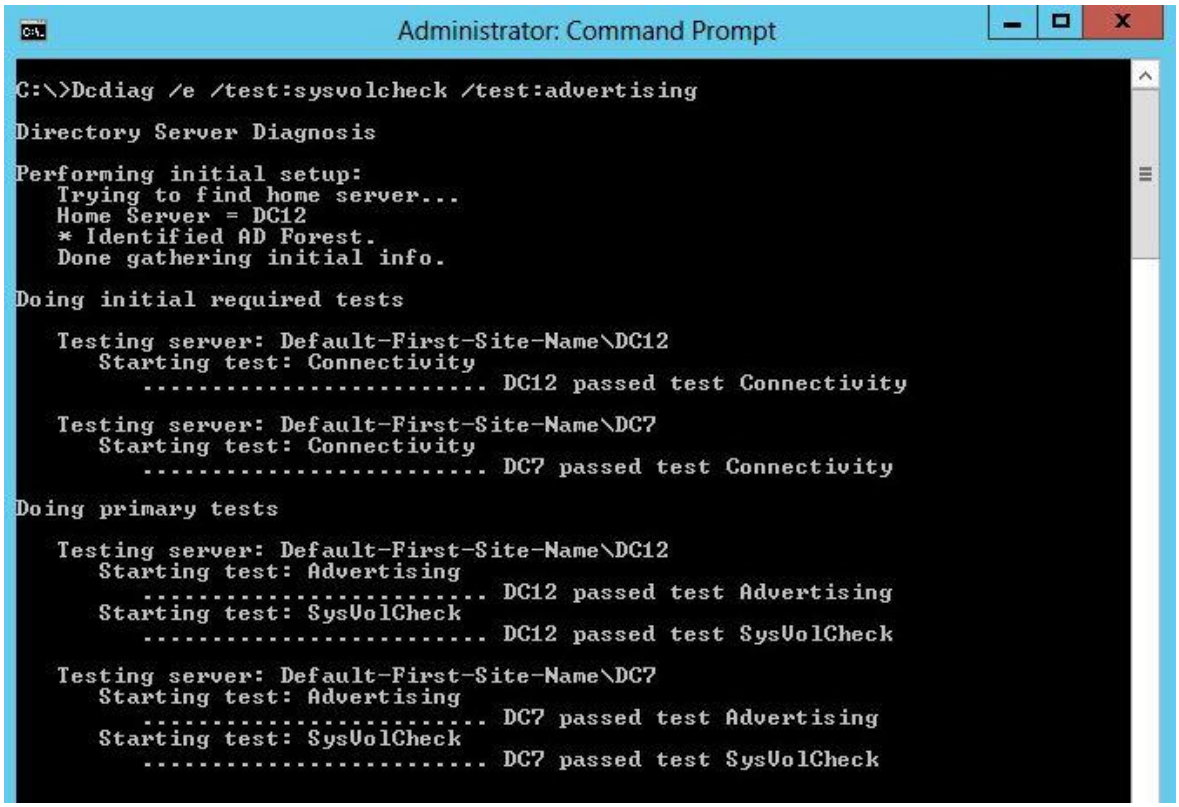
Siirrossa on neljä vaihetta, jotka kuvaavat replikoinnin vaiheittaista siirtymistä järjestelmästä toiseen. Näin pystytään varmistamaan, että siirto suoritetaan niin, että tiedon eheys voidaan varmistaa. Lisäksi vältetään tuotantoympäristössä pitkät käyttökatkokset ja palvelinten sulkeminen. Lisäksi seuraavaan tasoon voidaan siirtyä vasta, kun on varmistettu,

että kaikki todella toimii kuten pitää. Muutokset on mahdollista peruuttaa, kunnes päästään viimeiseen askeleeseen, jonka jälkeen muutokset ovat pysyviä. (Microsoft 2008c.)

Warrenin (2018, 119) mukaan Migraation vaiheet ovat:

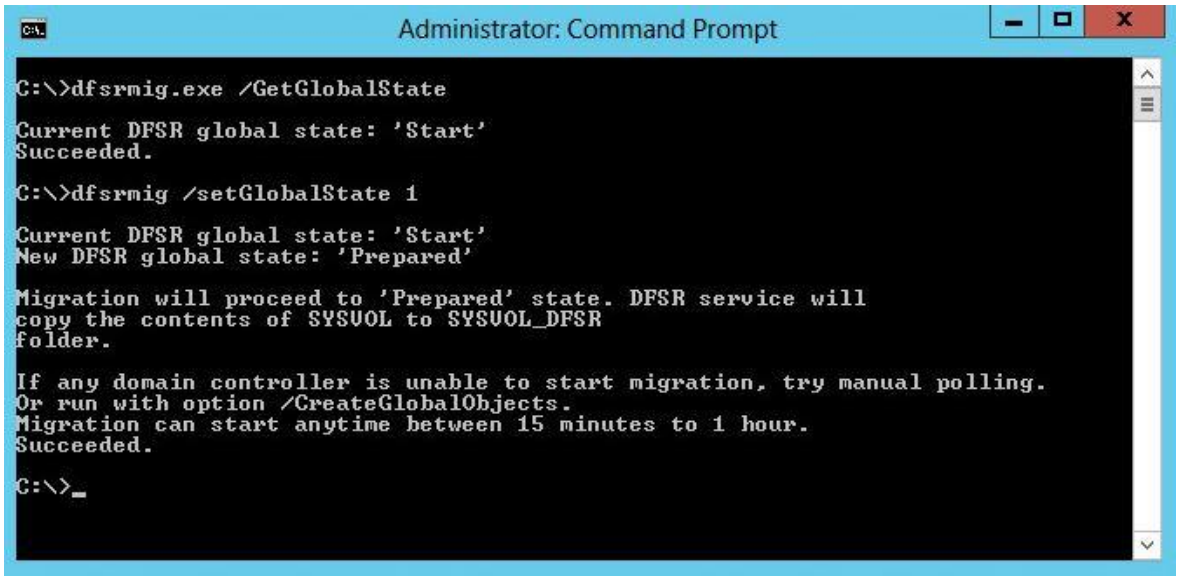
1) State 0, start: Aloitus taso, jolloin SYSVOL replikoi vain käyttäen FRS-järjestelmää.
2) State 1, prepared: Replikoinnissa yhä käytössä FRS, mutta DFSR luo replikoidun kopion SYSVOL-kansiosta.
3) State 2, redirected: DFSR aloittaa SYSVOL-replikoinnin. FRS kuitenkin säilyttää oman kopionsa SYSVOL-kansiosta.
4) State 3, eliminated: FRS ei enää ole käytössä ja SYSVOL-replikointia hoitaa DFSR.

Ennen päivittämisen aloitusta voimme tarkistaa, että SYSVOL-kansio on todella löydettävissä ja se ilmoittaa ohjauskoneille muutoksistaan. Voimme ajaa testejä asian selvittämiseksi, kuten seuraavassa kuvassa 26. Lisäksi on syytä varmistaa, että AD-replikointi toimii kunnolla.



Kuva 26. SYSVOL-kansion testaaminen Dcdiag-komennon avulla

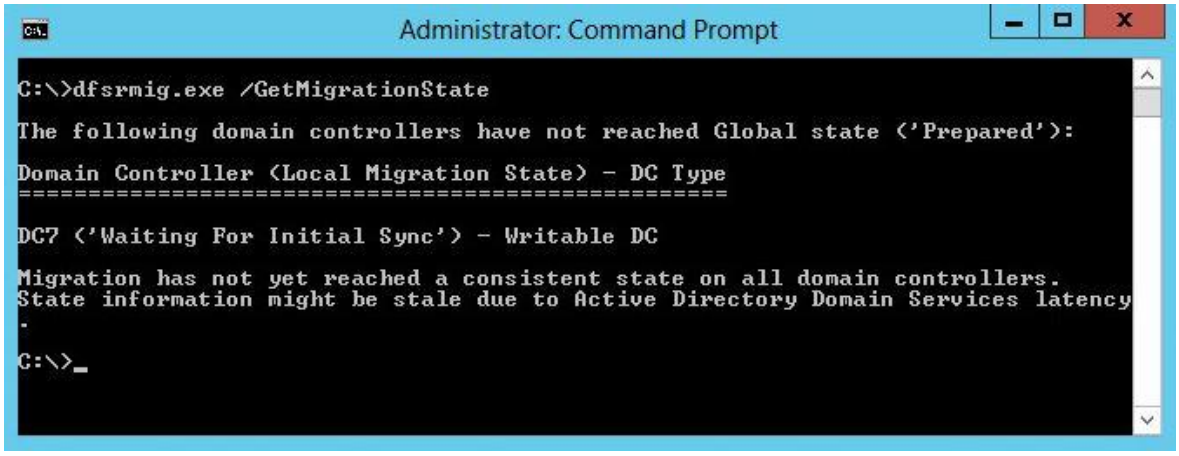
Aloitamme SYSVOL-migraation selvittämällä missä tilassa SYSVOL-replikointi on Haaga-Helian toimialueella. Toimiakseen dfsrmig.exe tarvitsee toimialueen, jonka toiminnallisuustaso (Domain Functional Level) on vähintään Windows Server 2008. Alla olevassa kuvassa 27 tarkastamme ensin, että olemme varmasti ”start”-tasolla, jonka jälkeen nousemme tilaan ”prepared”. Tämä tapahtuu ”dfsrmig.exe /SetGlobalState”-komennon avulla.



Kuva 27. Siirtyminen ”prepared”-tilaan

Kuten kuvasta näkyy, olemme nyt siirtyneet ”prepared”-tilaan, missä DFSR luo SYSVOL-tiedoista kopion SYSVOL_DFSR-kansioon. Tiedostojen jakamista hoitaa kuitenkin yhä FRS.

Voimme tarkistaa missä tilassa järjestelmä on ”dfsrmig.exe /GetMigrationState”-komennon avulla. Kuten alla olevasta kuvasta 28 havaitsemme, eivät muutokset ole vielä ehtineet replikoituneet DC7:lle.

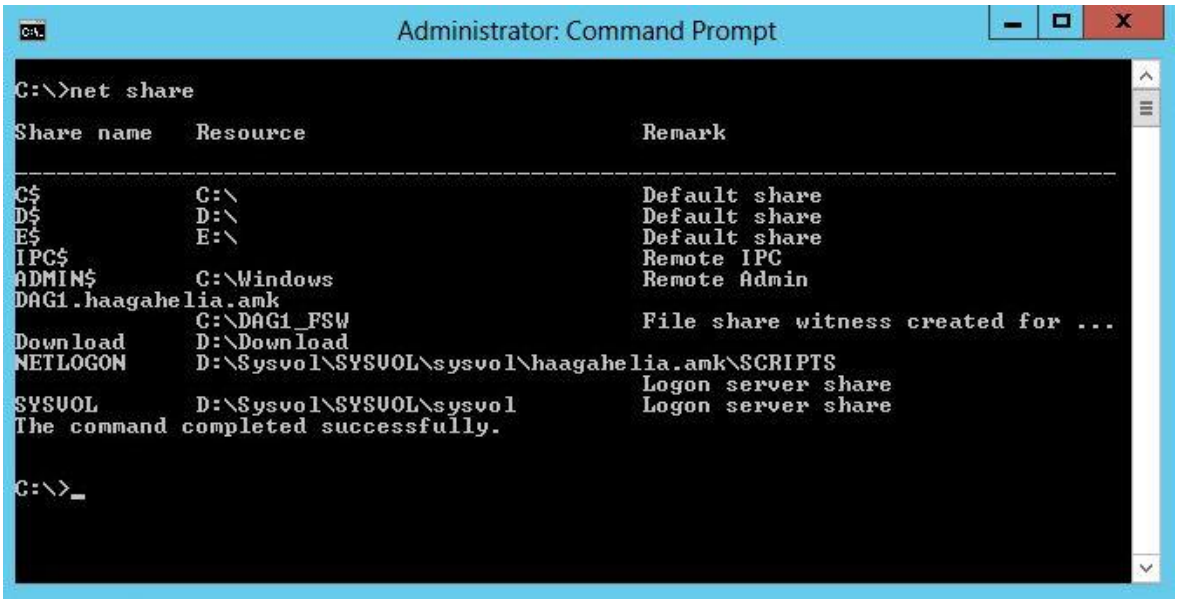


Kuva 28. GetMigrationState-komennon käyttö siirtymätilan selvittämiseksi

Odotettuamme vähän aikaa huomaamme kuvan 29 mukaisesti, että kaikki ohjauskoneet ovat nyt tilassa ”prepared”.

Kuva 29. Kaikki ohjauskoneet ovat siirtyneet tilaan ”prepared”

Lisäksi voimme tarkistaa ”net share”-komennon avulla, että jaetut kansiot SYSVOL ja NETLOGON ovat yhä samat kuin aloittaessamme (kuva 30).

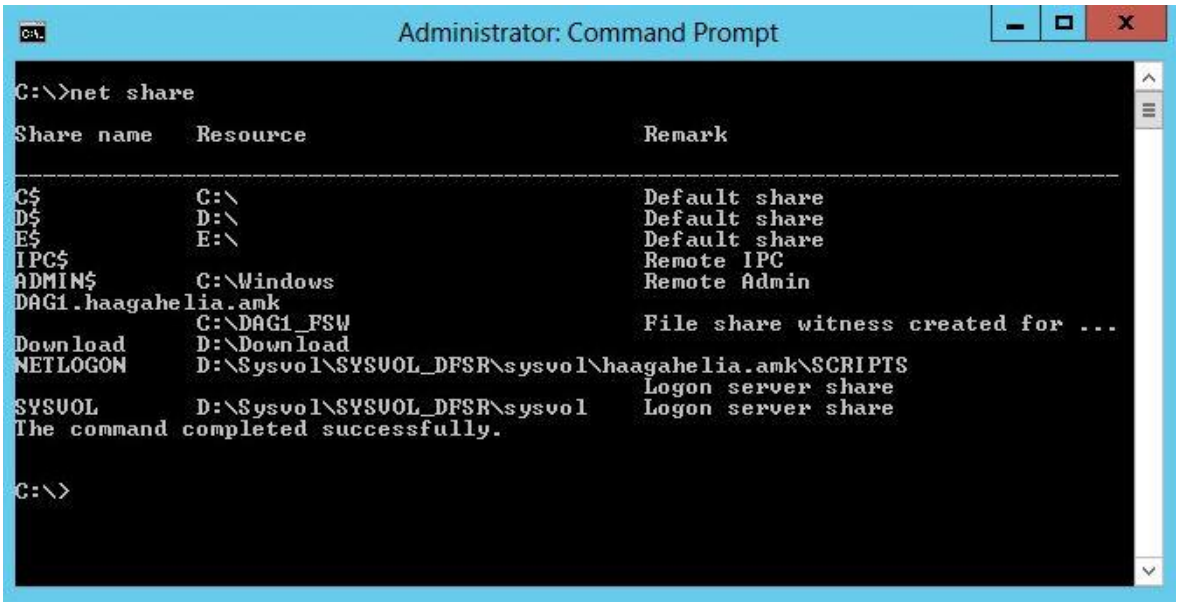


Kuva 30. Jaettujen kansioiden selvittäminen ”net share”-komennon avulla

Seuraavaksi siirrymme ”redirected”-tilaan, missä FRS ja DFSR säilyttävät omat versionsa SYSVOL-kansiosta, mutta DFSR ottaa haltuunsa SYSVOL ja NETLOGON -jaot. Komento täytyy ajaa koneella, jolla on PDC emulator –rooli. Meidän tapauksessamme kaikki roolit ovat DC12:lla. Kuvassa 31 siirrymme tilaan ”redirected” ja tarkastamme, että kaikki muutokset ovat menneet läpi ilman ongelmia. (Pyle 2014.)

Kuva 31. Siirtyminen ”redirected”-tilaan ja sen tarkistaminen palvelimilta

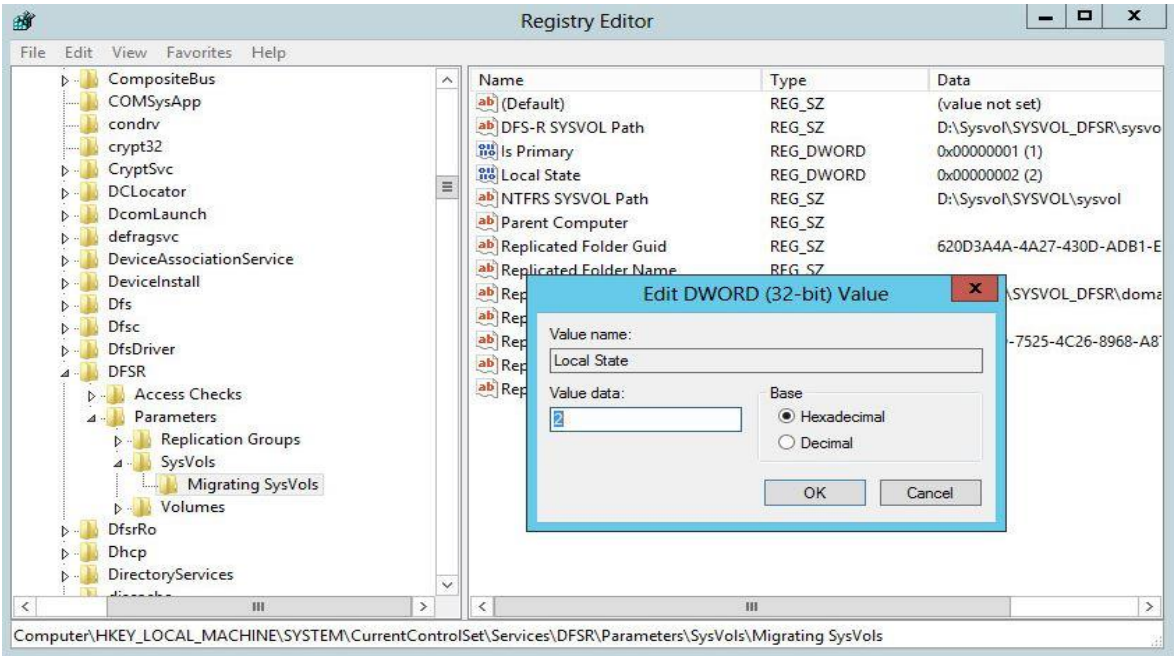
Jos nyt tarkistamme jaetut kansiot uudelleen, huomaamme, että olemme siirtyneet käyttämään SYSVOL_DFSR-kansiota (kuva 32). SYSVOL-kansion nimi on vaihtunut.



Kuva 32. System Volume on nyt nimeltään SYSVOL_DFRS

Olemme yhden askeleen päässä tavoitteestamme. Kaikki tähän asti tehdyt vaiheet voidaan peruuttaa yksinkertaisesti asettamalla jokin aikaisemmista tiloista voimaan. Seuraavaa ”eliminated”-tilaa ei voida kuitenkaan peruuttaa, joten meidän kannattaa varmistaa, että jaot toimivat kunnolla ennen viimeistä tilan siirtoa. Vaiheittaisen prosessin tarkoituksena onkin nimenomaan seurata replikointia ja jos ongelmia tulee, voidaan työvaiheet peruuttaa.

Tässä vaiheessa voimme tarkistaa rekisteristä, että kaikki ohjauskoneet ovat siirtyneet tilaan ”redirected”. Lisäksi rekisteri viittaa oikeaan SYSVOL_DFSR-kansioon (kuva 33).



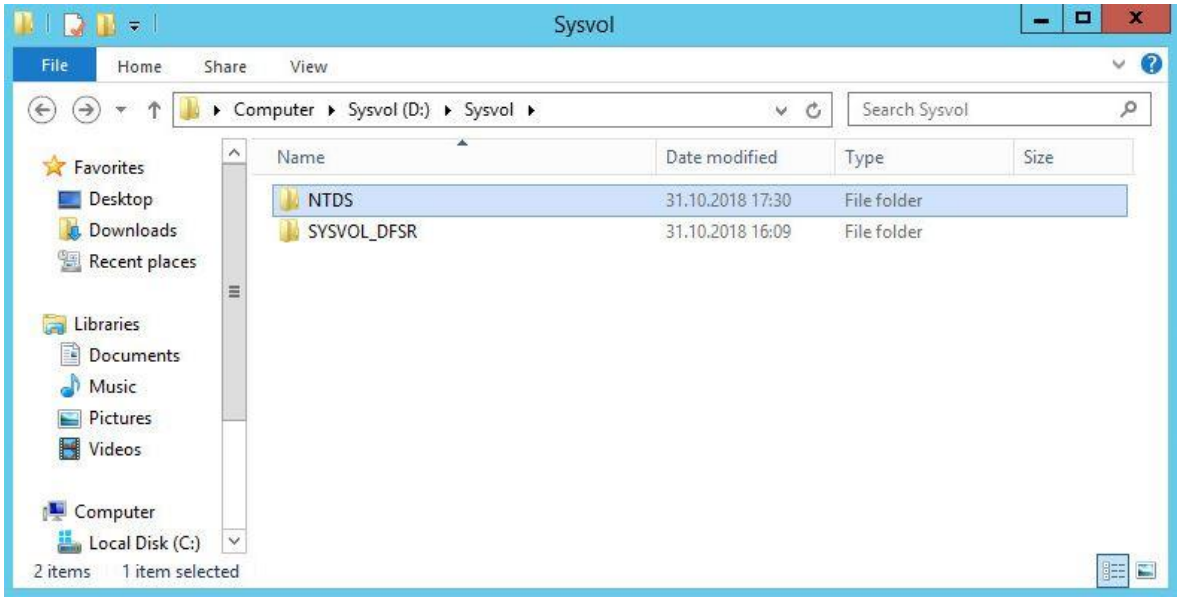
Kuva 33. Rekisterissä arvo 2, eli ”redirected”

Koska kaikki näyttää olevan kunnossa siirrymme lopullisesti käyttämään DFS-tiedostojakoa. Tämä tapahtuu edellisten tasojen tapaan komennolla ”dfrsmig /setGlobalState 3”.

Olemme siirtyneet ”eliminated”-tilaan. Kuvassa 34 tarkistamme tilanteen vielä samojen komentojen avulla, kuin aikaisemmin (”net share” ja ”GetMigrationState”).

Kuva 34. Järjestelmä käyttää DFS-tiedostojakoa

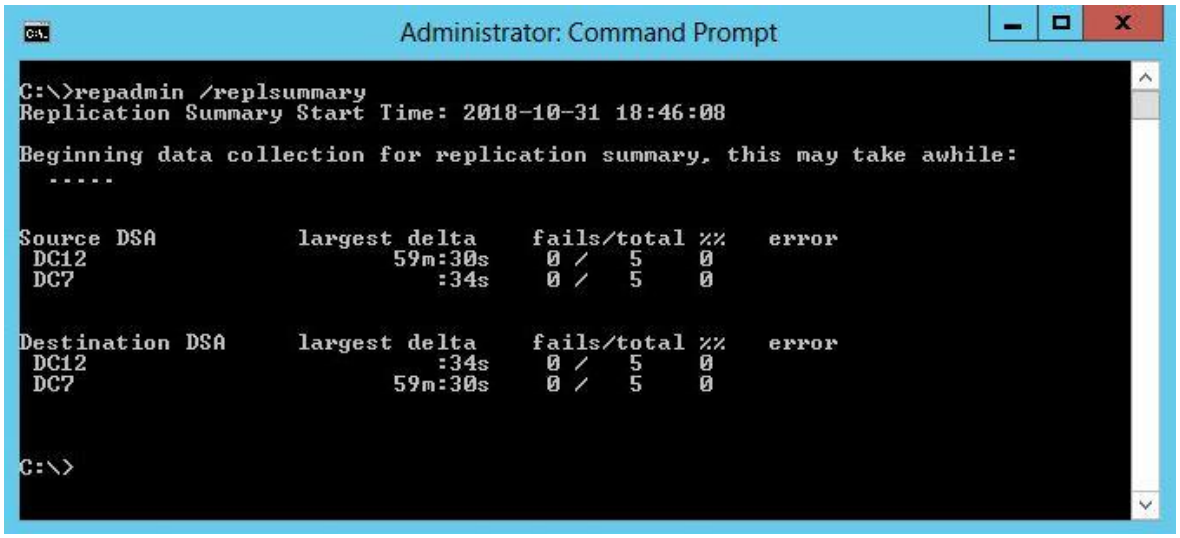
Kun SYSVOL-replikointi käyttää DFS-jakoa, emme voi palata vanhaan Replicated File System –menetelmään takaisin. Myöhemmin toimialueelle lisätyt koneet ottavat myös automaattisesti käyttöönsä DFS-jaon. Tämä tulee viimeistään selväksi, kun huomaamme vanhan SYSVOL-kansion kadonneen kokonaan ohjauskoneilta (kuva35).



Kuva 35. Sysvol-kansion sisältö ohjauskoneella DC12 (vanha SYSVOL puuttuu kokonaan)

3.8 Palvelinten replikoinnin testaaminen

Olemme siirtyneet käyttämään DFS-replikointia ja haluamme varmistua, että kaikki toimii oikein. Aloitamme ajamalla ”Repadmin /replsummary”-komennon, joka laatii yhteenvedon tämänhetkisestä replikointi tilanteesta (kuva 36).

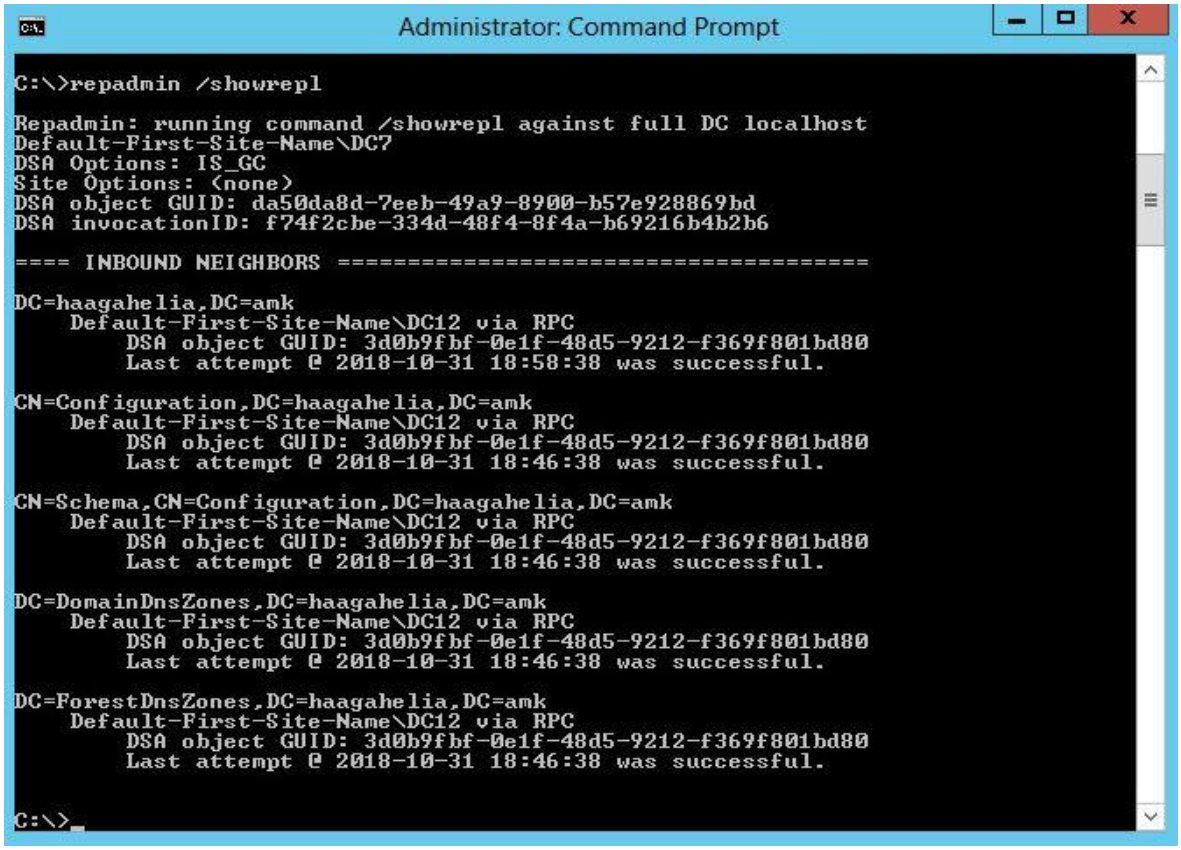


Kuva 36. Ohjauskoneiden replikointitiedot, jotka ovat kunnossa

Seuraavaksi tarkistamme DC7-koneelta, onko replikointijonossa siirtymättömiä tietoja. Tämä tapahtuu komennolla ”Repadmin /Queue” (kuva 37).

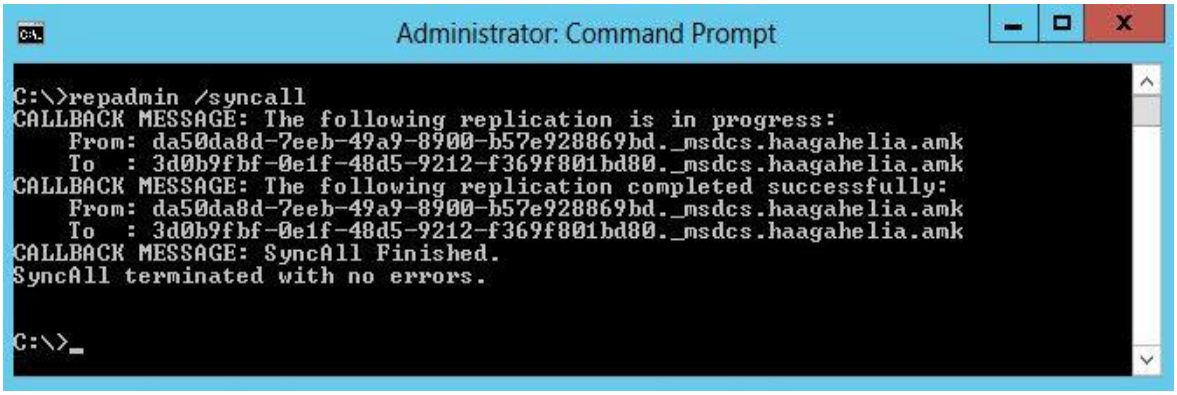
Kuva 37. Jonossa olevien replikointiobjektien selvittäminen

Jatkamme tarkistamalla viimeiseen tiedostojen lataamiseen liittyvät tapahtumat molemmilla ohjauskoneilla ”Repadmin /Showrepl”-komentoa käyttäen (kuva 38).



Kuva 38. Edelliset koneelle suuntautuneet replikointitapahtumat ovat onnistuneet

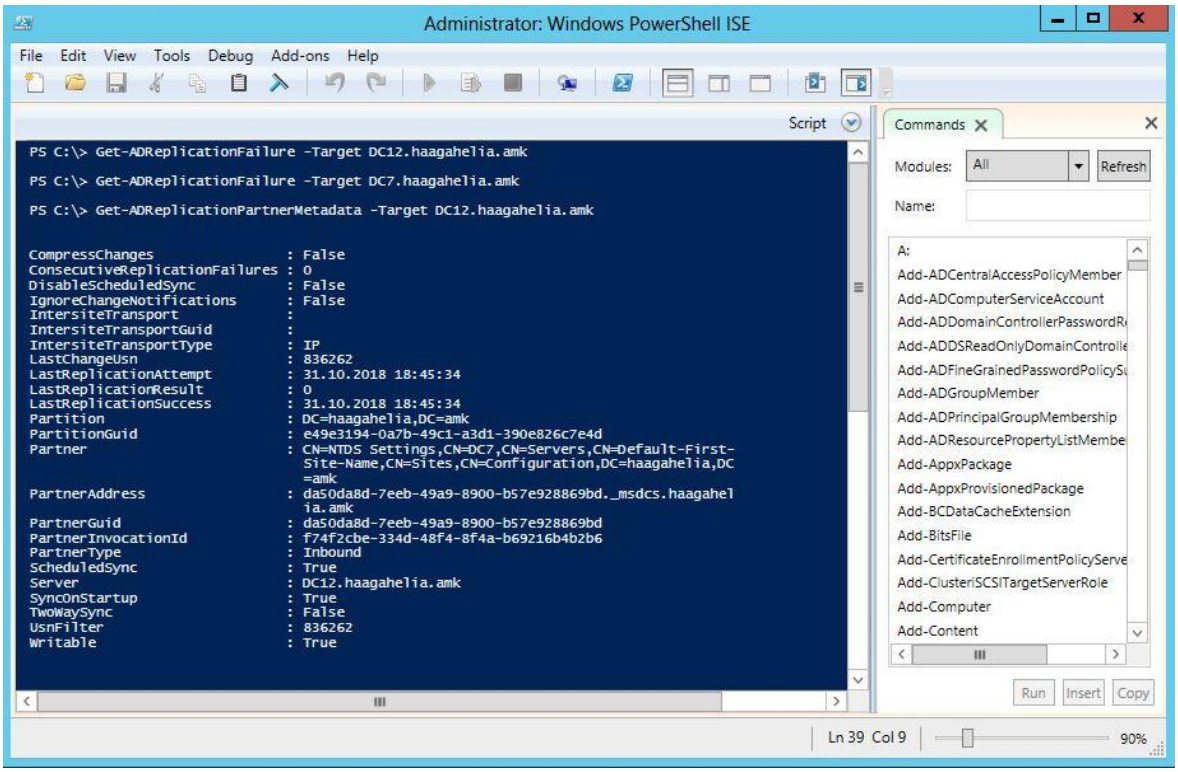
Lopuksi kokeillaan replikoida koko aktiivihakemisto kohdekoneelle, jotta löydämme mahdollisia virhetilanteita (kuva 39). Tätä ei kuitenkaan suositella suurissa tuotantoverkoissa, sillä se syö paljon resursseja. Testiympäristössä voimme kokeilla mitä tapahtuu ”repadmin /syncall”-komennolla. (Kapoor, 2016).



Kuva 39. Ohjauskoneen pakotettu replikointi muiden ohjauskoneiden kanssa

Kaikki edelliset testit näyttivät onnistuvan ja replikointi näyttää toimivan normaalisti. Muita hyödyllisiä komentoja ovat esimerkiksi ”Repadmin /KCC”, joka etsii verkosta uusia tietokoneita, joiden kanssa replikoida ja laatii uuden topologian, joka ottaa huomioon uudet lisätyt ohjauskoneet, sekä ”Repadmin /replicate”, jolla voidaan aloittaa jonkin hakemistoosan välitön replikointi muille ohjauskoneille. (Kapoor, 2016.)

Myös Windows PowerShell käy hyvin joidenkin replikointitietojen etsintään. Seuraavassa kuvassa 40 on molemmilta ohjauskoneilta etsitty replikointivirheitä ja sitten vielä haettu DC12:en tiedot erikseen.



Kuva 40. PowerShell näyttää tietoa replikoinnista

Koska kaikki näyttää toimivan kuten pitää, siirrymme lisäämään toimialueelle uuden Windows Server 2016 –käyttöjärjestelmällä varustetun ohjaustietokoneen.

3.9 Toimialueen valmistelu Windows Server 2016 –käyttöjärjestelmää varten

Ennen kuin aktiivihakemiston toimintaympäristöön voidaan lisätä uudella käyttöjärjestelmäversiolla (Windows Server 2016) toimivia ohjauskoneita, täytyy palvelinympäristö valmistella. Tämä tapahtuu Adprep.exe-komennon avulla. Erityisesti tällainen tilanne syntyy silloin, kun ohjauskone päivitetään uudempaan käyttöjärjestelmään niin, ettei sitä ensin poisteta käytöstä, asenneta uudelleen ja sitten palauteta toimialueelle. (Warren 2018, 35.)

3.9.1 Adprep.exe

Adprep.exe voidaan löytää käyttöjärjestelmän asennuslevyltä ja se voidaan ajaa joko automaattisesti silloin, kun palvelin nostetaan toimialueen ohjauskoneeksi, tai manuaalisesti, jolloin toimenpide on paremmin hallittavissa. Adprep on päivittynyt jokaisen palvelinversion myötä, mutta myöhemmin tulevat versiot korvaavat aikaisemmat niin, että riittää kun ohjelmasta ajetaan viimeisin käyttöjärjestelmän mukana tuleva versio. (Microsoft 2014b.)

Adprep valmistelee ympäristön uutta käyttöjärjestelmää varten. Vaikka jokainen versio ohjelmasta eroaakin hieman edellisistä, suorittavat kaikki käytännössä samankaltaisia toimintoja ohjauskoneilla. Komento tekee päivityksiä aktiivihakemiston kaavaan, mihin se lisää tarvittavia uusia objekteja ja säiliöitä. Lisäksi se tekee muutoksia turvallisuusasetuksiin, joita ovat Security Descriptors, sekä näiden sisältämät Access Control –listat. Käytännössä nämä ovat objekteihin liittyviä käyttö- ja pääsyoikeuksia (access rights, permissions). (Microsoft 2014b.)

Ennen kuin kaavapäivityksiä ryhdytään ajamaan tuotantopalvelimilla, on syytä tehdä System State –varmuuskopio Schema Master –ohjaustietokoneesta ja ainakin yhdestä toisesta toimialueen ohjauskoneesta. Koska asioita voi mennä pieleen, on päivitystä syytä kokeilla ensin testiympäristössä, kuten olemme juuri tekemässä. Jotta päivitykseen tarvittavat komennot voidaan ajaa, on käyttäjän kuuluttava Schema Admin, Enterprice Admin ja Domain Admin –ryhmiin. (Microsoft 2014b.)

Microsoft on rakentanut päivitykseen ominaisuuksia, jotka pyrkivät korjaamaan mahdollisia virhetilanteita jo ohjelman ajon aikana. Ohjelma osaa itsenäisesti selvittää mahdollisia konfliktitilanteita esimerkiksi liittyen objektien tunnisteisiin (Microsoft 2014b). Tämän vuoksi Microsoft ei välttämättä enää suosittele ohjauskoneen replikoinnin pysäyttämistä päivi-

tyksen ajaksi. Meidän tapauksessamme kuitenkin teemme näin, jotta virheen sattuessa emme vahingoita muita palvelimia.

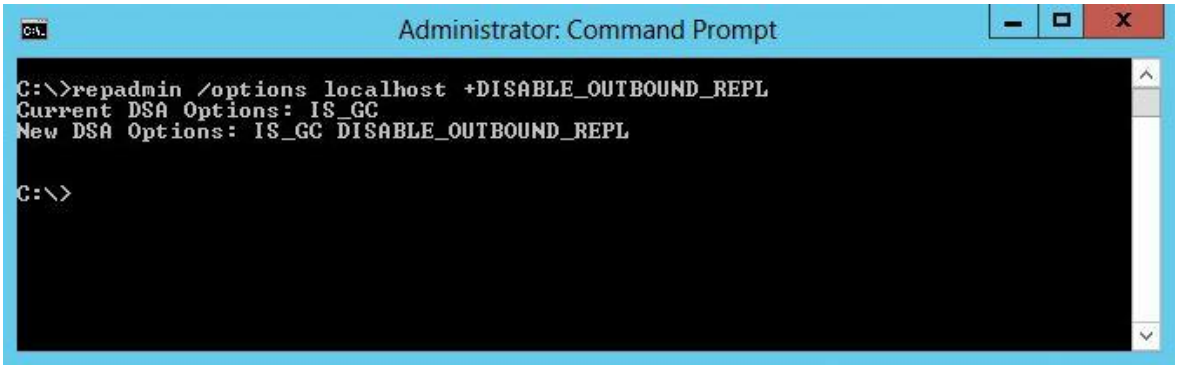
Alla olevaan taulukkoon 3 on kuvattu Adprep–komennon toiminta.

Taulukko 3. Adprep-komennon käyttöskenaariot (Lamppu 2018)

Command	Permission	Domain Controller	Runtime	Number of times to run command
adprep forestprep	Schema, Domain Enterprise Admins	Schema Master	5-10 mins	Once for the entire forest
adprep /domainprep	Domain Admins	Infrastructure Master	Seconds	Once in each domain where you plan to install an additional domain controller that runs a later version of Windows Server than the latest version that is running in the domain.
adprep /rodcprep	Enterprise Admins	Domain Naming Master	Seconds	Once for the entire forest
adprep /gpprep	Domain Admins	Infrastructure Master (If you already ran this command for Windows Server 2008, you do not have to run it again for Windows Server 2008 R2.)	Seconds	Once in each domain within the forest

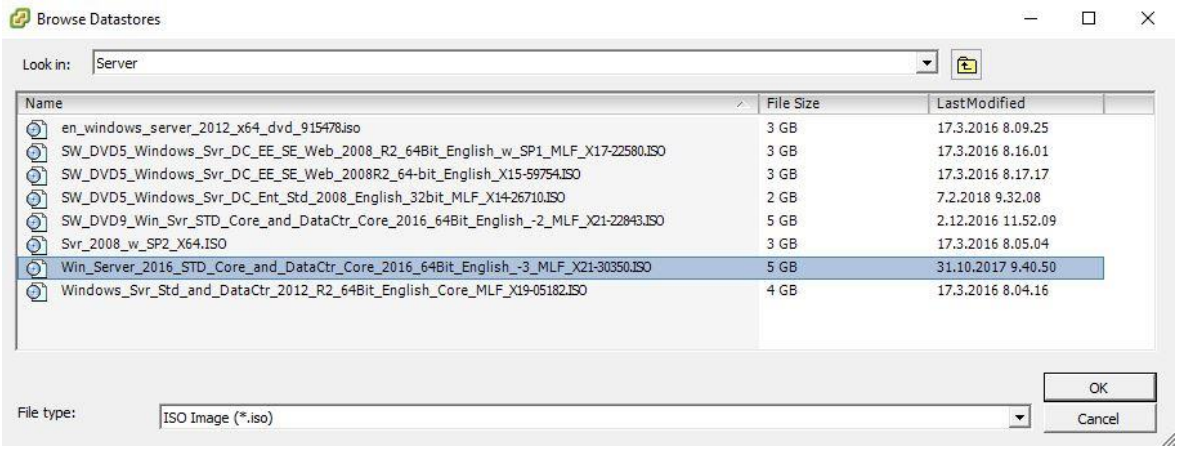
3.10 Kaavapäivitysten ajaminen

Aloitamme pysäyttämällä replikoinnin kohdekoneella. Tämä tapahtuu jo aikaisemmin käyttämämme repadmin-työkalun avulla alla olevan kuvan 41 mukaisesti. Kuvan komennossa nähtävä ”+”-merkki tarkoittaa siis aktivointia, mutta komennon kanssa kannattaa olla tarkkana.



Kuva 41. Ulospäin suuntautuvan replikoinnin pysäyttäminen

Seuraavaksi asetamme Window Server 2016 –asennuslevyn asemaan ja kopioimme support/adprep-kansion ohjauskoneelle. Kuvassa 42 näemme saatavilla olevat levykuvat.



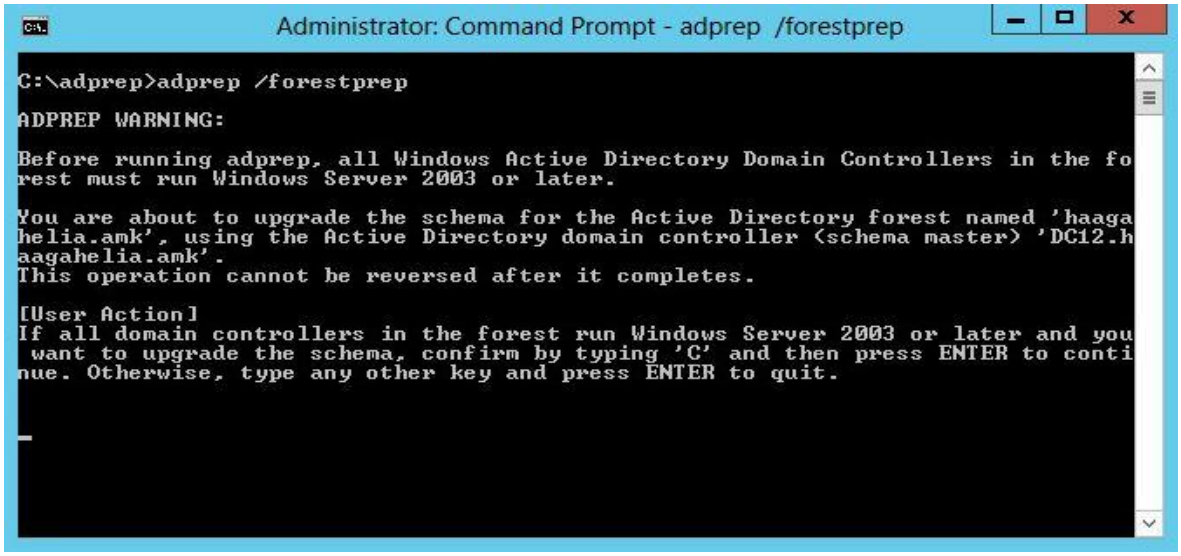
Kuva 42. Levykuvan haku levyvarastosta

Kun adprep ajetaan kohdekansiossa, saamme kuitenkin virheilmoituksen. Tämä johtuu siitä, että käyttäjä ei kuulu oikeisiin ryhmiin. Virheilmoitus näytetään kuvassa 43.

Kuva 43. Puutteelliset käyttöoikeudet adprep-komennon suorittamiseen

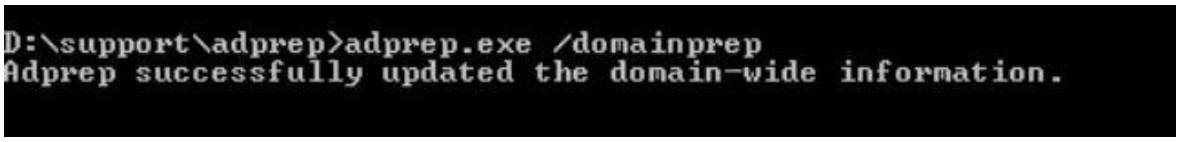
Kun lisäämme käyttäjän aktiivihakemistossa ryhmiin Domain Admins, Schema Admins ja Enterprice Admins, saamme tarvittavat oikeudet päivityksen tekemiseen. Tätä ennen on muistettava päivittää muutokset ”gpupdate /force”–komennolla, joka hakee aktiivihakemistoon tehdyt muutokset kohdekoneelle ilman odottelua.

Lopulta saamme päivityksen suoritettua (kuva 44).



Kuva 44. Forestprep-komennon suorittaminen onnistuneesti

Forestprep ajetaan vain kerran koko metsän alueella ja se riittää. Seuraavaksi on päivitettävä toimialue ja se tapahtuu domainprep-komennon avulla. Domainprep suoritetaan kerran jokaisella metsän toimialueella. Sen formaatti on sama kuin edellisen komennon ja ajamme sen tällä kertaa suoraan dvd-levyn kansiosta (kuva 45).



Kuva 45. Domainprep-komennon suorittaminen asennuslevyn adprep-kansiosta

Lopuksi meidän täytyy muistaa palauttaa replikointi takaisin päälle komennolla ”repadmin /options localhost –DISABLE_OUTBOUND_REPL”.

Windows Server 2012 ja sen jälkeen ilmestyneet käyttöjärjestelmät osaavat kuitenkin tehdä edellisen kappaleen valmistelut automaattisesti, kun ohjauskone lisätään toimialueelle. Tämän kappaleen valmistelut ovatkin tarpeen vain silloin, kun muutosprosessia halutaan kontrolloida tarkemmin, esimerkiksi vianselvitystä varten.

3.11 Uuden Windows Server 2016 –palvelimen lisääminen

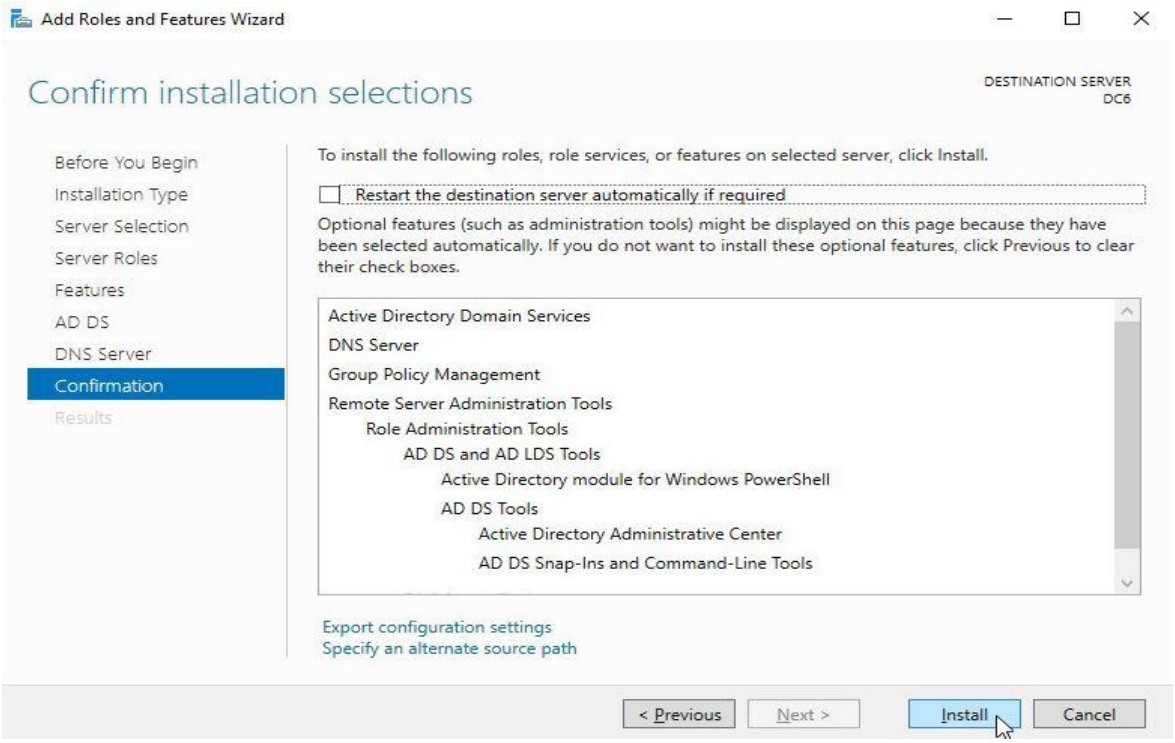
Lopullisena tavoitteenamme on nostaa ympäristön toiminnallisuutta tasolle Windows Server 2016. Ennen kuin tämä on mahdollista, on kaikkien toimialueen ohjauskoneiden oltava samalla tasolla. Teemme päivityksen niin sanottuna rinnakkaispäivityksenä, jolloin ympäristöön lisätään uudella käyttöjärjestelmällä varustettuja koneita, joille palvelut siirretään. Seuraavaksi lisäämme toimialueelle ensin uuden ohjauskoneen DC6:n ja sen jälkeen päivitämme DC7:n poistamalla käytöstä vanhan ja rakentamalla uuden. Kun molemmat koneet ovat valmiina, siirrämme FSMO-roolit DC12:lta DC6:lle ja päivitämme viimeisenkin kolmesta koneesta.

Hyödynnämme uuden virtuaalikoneen luonnissa valmista pohjaa (template), joskin voisimme luoda virtuaalikoneen myös täysin tyhjästä kuten DC7:n tapauksessa. Aikaisemmin tehty pohja voidaan löytää vSpheren VMs and Templates –välilehdeltä Mallipohjat-Windows-kansiosta ja ne saadaan käyttöön valitsemalla Deploy Virtual Machine from this Template. Nämä levykuvat on tehty Haaga-Helian järjestelmäpalveluiden toimesta aikaisemmin testikäyttöä varten. Virtuaalikonetta luotaessa käynnistyy asennusvelho, jolle annetaan tarvittavat tiedot, jotka löytyvät liitteestä 8.

Kun asennus päättyy, lisätään koneelle vielä tarvittavat laiteasetukset. Käytännössä tämä tarkoittaa kahden virtuaalisen kovalevyn lisäämistä ja verkon vaihtamista inside-verkkoon. Asetukset ovat samat kuin aikaisemmin koneella DC7. Kolmea kovalevyä tarvitsemme, koska haluamme SYSVOL-jaon ja varmuuskopiot omille levyilleen. Lopuksi nostamme muistin määrän 16 Gigatavuun.

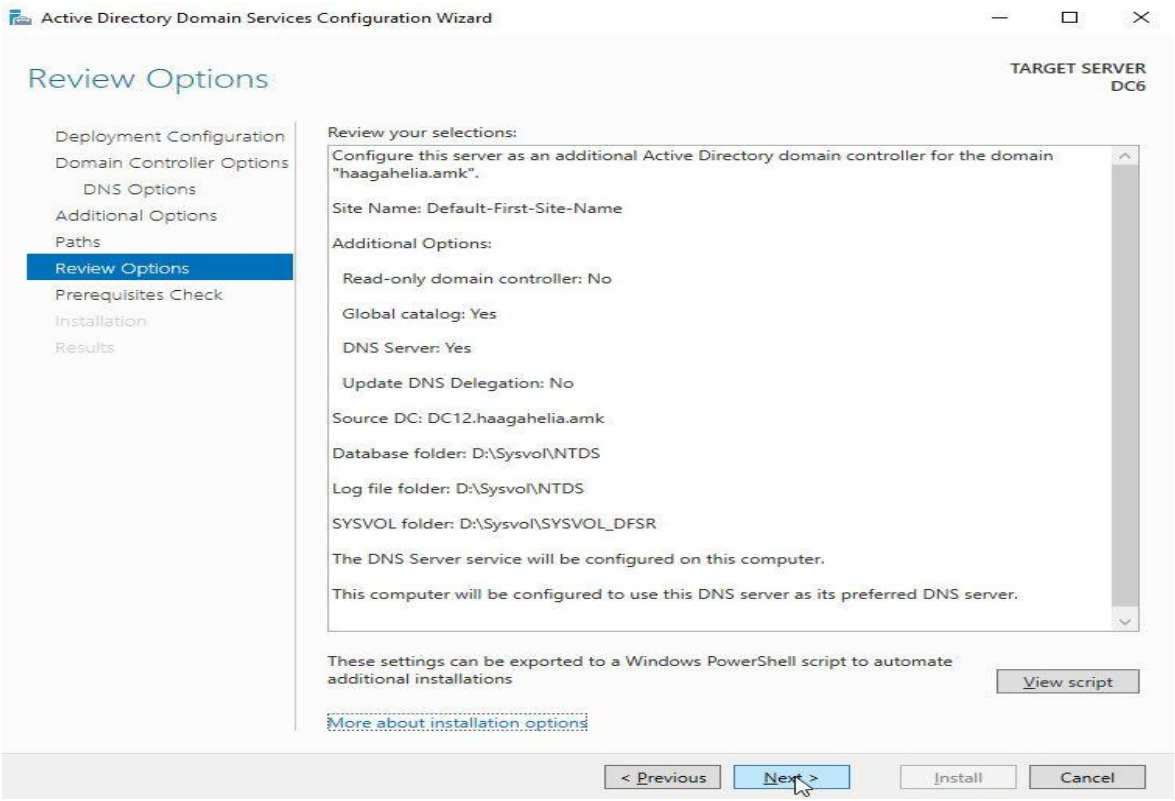
Lopuksi asennamme käyttöjärjestelmän Windows Server 2016 Datacenter -levyltä. Asennuksen jälkeen nimeämme koneen uudelleen DC6:ksi ja määrittelemme staattiset IP-osoitteet. Lisäksi alustamme levyosiot Computer Management –työkalun avulla.

Viimeisenä työvaiheena kone liitetään toimialueelle ohjauskoneeksi. Kuten viimeksi tämä tapahtuu lisäämällä koneelle aktiivihakemistopalvelut Add Roles and Features –toimintoa käyttäen. Askeleet ovat täysin samat kuin aikaisemmin, kun lisäsimme roolit DC7:lle. Seuraavassa kuvassa 46 on kuitenkin yhteenveto asennetuista AD DS ja DNS –rooleista.



Kuva 46. Asennettavat AD DS ja DNS –roolit DC6-koneella

Roolien jälkeen palvelin nostetaan ohjauskoneeksi valitsemalla Server Manager –näkymässä Promote to Domain Controller. Alla olevassa kuvassa 47 nähdään tulevan ohjauskoneen asetukset.

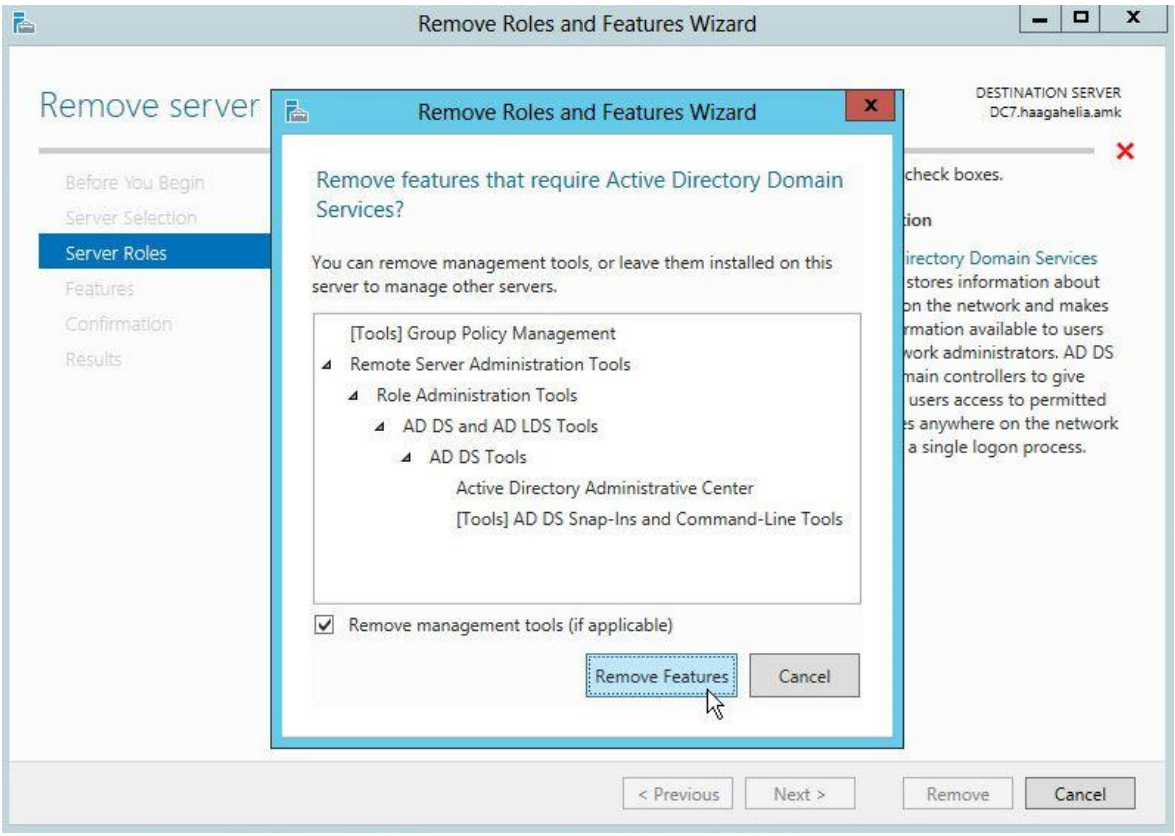


Kuva 47. Promote to Domain Controller -asetukset

3.12 DC7:n päivitys

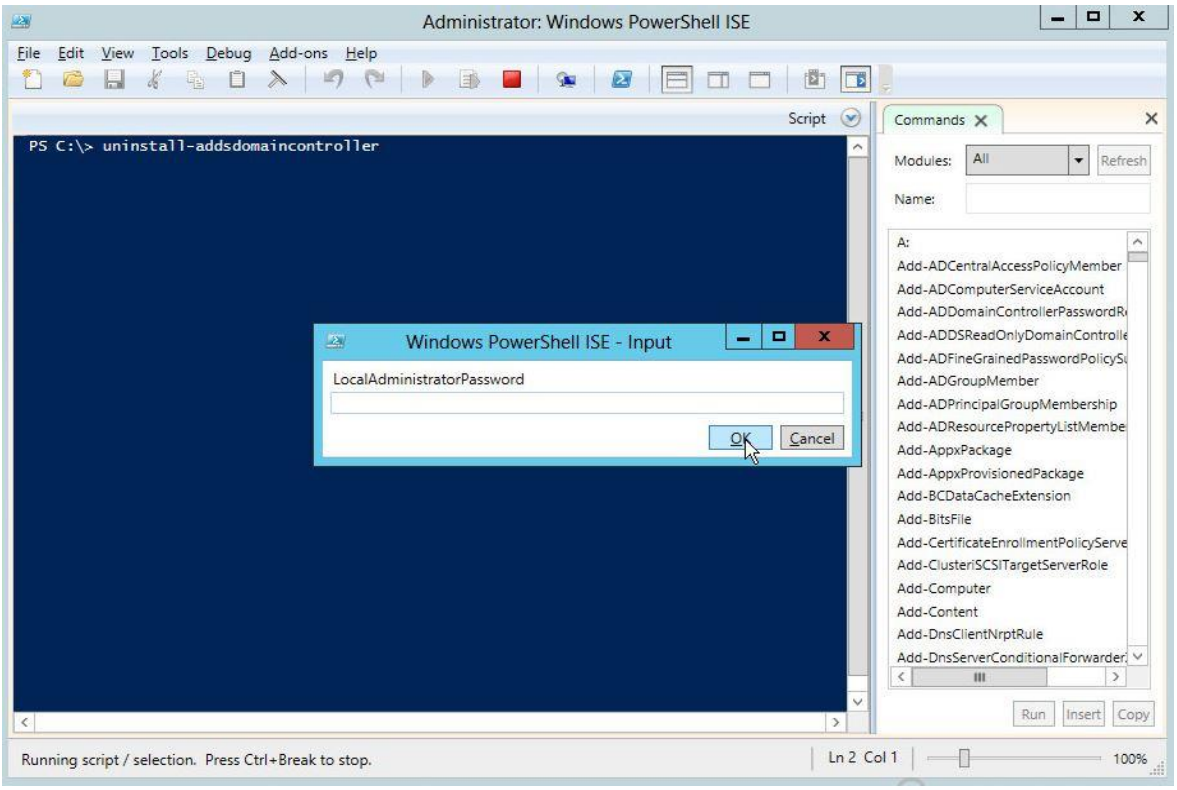
Siirrymme seuraavan ohjauskoneen pariin ja teemme DC7:lle käyttöjärjestelmäpäivityksen. Tämä tapahtuu poistamalla vanha ohjauskone ensin käytöstä ja lisäämällä sen tilalle uudella käyttöjärjestelmällä varustettu kone.

Vanhaa käyttöjärjestelmää käyttävän palvelimen poistaminen tapahtuu alentamalla (demote) se ohjauskoneen asemasta, jonka jälkeen siltä voidaan poistaa asennetut roolit. Lisäksi aktiivihakemistosta poistetaan koneeseen liittyvät tiedot DNS-palvelimen osalta, sekä viittaukset Sites and Services -näkymästä. AD DS voidaan poistaa Windows Serverin Remove Roles and Features –työkalun avulla, kuten seuraavassa kuvassa 48.



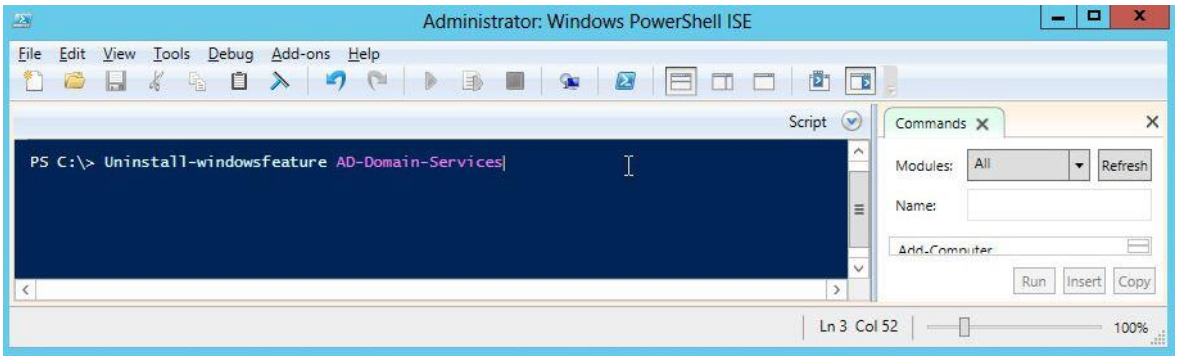
Kuva 48. AD DS -roolin poisto vanhalta DC7-koneelta

Meidän tapauksessamme käytämme kuitenkin Windows PowerShell–komentotulkkia. Edellisessä kohdassa nostimme palvelimen ohjauskoneeksi, mutta nyt alennamme palvelimen pois toimialueen ohjauskoneen tehtävistä. Se tapahtuu PowerShell-komennolla ’uninstall-addsdomaincontroller’ (kuva 49). Kun ohjauskone poistetaan näin, poistuu se aktiivihakemiston Domain Controllers –kansiosta, josta se siirtyy Computers-säilöön. Täältä kone on käytävä erikseen poistamassa.



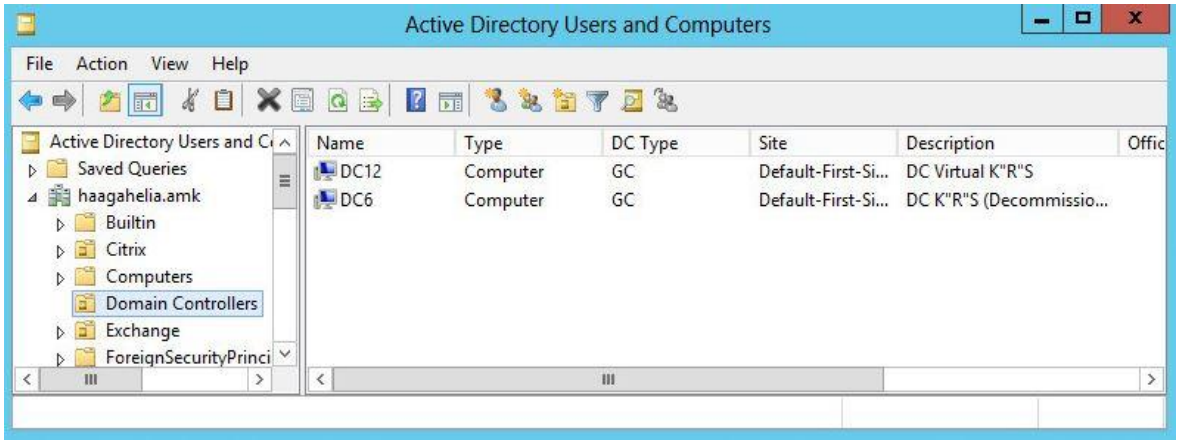
Kuva 49. Ohjauskoneen poistaminen PowerShellin avulla

Ohjauskoneelta voidaan vielä erikseen poistaa aktiivihakemistopalvelut (kuva 50).



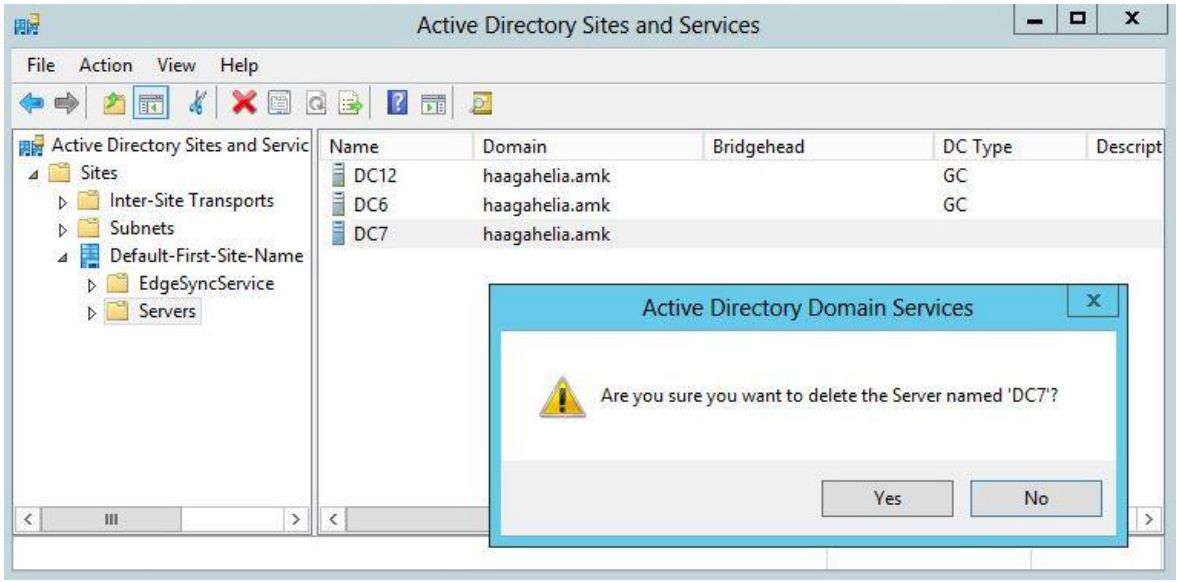
Kuva 50. AD DS -palveluiden poistaminen ohjauskoneelta

Kun nyt avaamme aktiivihakemiston, huomaamme, että DC7 on poistunut toimialueen ohjauskoneiden kansiosta (kuva 51).



Kuva 51. Ohjauskoneen poiston varmistaminen Domain Controllers -kansiosta

Käymme poistamassa site-merkinnät ohjauskoneesta Active Directory Sites and Services –työkalun avulla (kuva 52).



Kuva 52. Ohjauskoneen poisto Sites and Services -tiedoista

Lopuksi voimme poistaa ohjauskoneen Computers-säiliöstä Active Directory Users and Computers -näkymästä.

Kun vanha DC7 on poistettu, asennamme uuden ohjauskoneen ja liitämme sen toimialueelle. Tämä tapahtuu täsmälleen samalla tavalla, kuten edellisessä kappaleessa lisäsimme DC6:n palvelinympäristöön. Tämän jälkeen meillä on toimialue, jossa on kaksi Windows Server 2016 –käyttöjärjestelmällä varustettua ohjauskonetta ja vanha DC12, jolla on kaikki MFSO-roolit.

3.13 Operations Master –roolien siirtäminen

Ennen kuin viimeinen ohjauskone, DC12 voidaan päivittää, sen Operations Master –roolit on siirrettävä toisen palvelimen vastuulle. Kuten muistamme, kaksi rooleista toimivat metsän tasolla ja loput kolme ovat toimialuekohtaisia. Aloitamme siirtämällä metsän laajuudella toimivat kaksi roolia ja sen jälkeen loput kolme toimialueroolia.

3.13.1 Metsän Operations Master –roolit

Windows PowerShell-komennolla ”Get-ADForest” voimme ottaa selvää, mille ohjauskoneelle metsän Operations Master –roolit on asennettu (kuva 53).

```
PS C:\> get-adforest


ApplicationPartitions : {DC=DomainDnsZones,DC=haagahelia,DC=amk, DC=ForestDnsZones,DC=haagaheli
                        a,DC=amk}
CrossForestReferences : {}
DomainNamingMaster    : DC12.haagahelia.amk
Domains               : {haagahelia.amk}
ForestMode            : Windows2008R2Forest
GlobalCatalogs        : {DC12.haagahelia.amk, DC6.haagahelia.amk, DC7.haagahelia.amk}
Name                  : haagahelia.amk
PartitionsContainer   : CN=Partitions,CN=Configuration,DC=haagahelia,DC=amk
RootDomain            : haagahelia.amk
SchemaMaster          : DC12.haagahelia.amk
Sites                 : {Default-First-Site-Name}
SPNSuffixes           : {}
UPNSuffixes           : {haaga-helia.fi, myy.haaga-helia.fi}
```

Kuva 53. Metsän FSMO-roolien selvittäminen ”get-adforest”-komennolla

Metsän tasolla toimivat FSMO-roolit ovat Domain Naming Master ja Schema Master. Tarkemmin näiden tehtävistä kerrottiin jo teoria osuudessa. Kuten kuvasta 53 voidaan havaita, ovat molemmat palveluista DC12-koneella, jonka haluaisimme päivittää. Roolit on siis siirrettävä toiselle, Windows Server 2016 –käyttöjärjestelmään päivitetylle koneelle. Roolien siirto tapahtuu sillä koneella, jolle roolit siirretään. (Warren 2018, 38.)

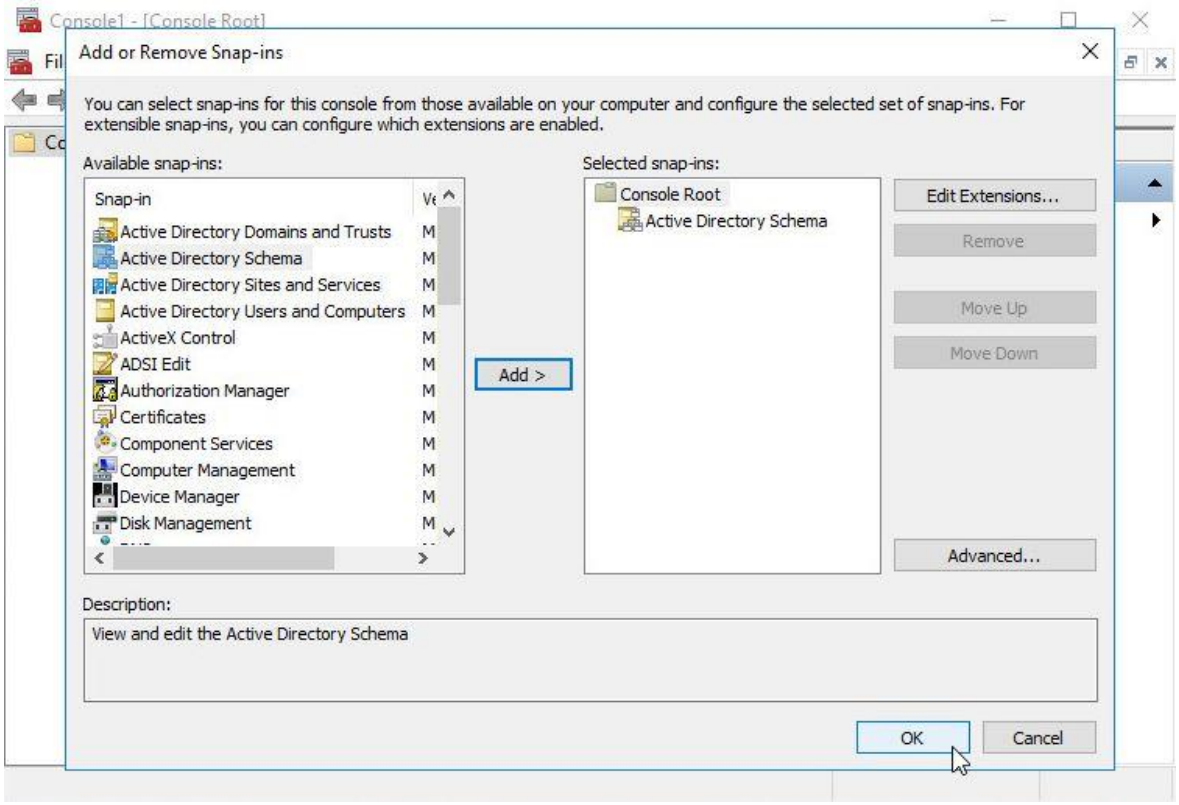
Ensimmäisessä siirrossa käytämme Microsoft Management Console –nimistä työkalua (MMC). Se on tarkoitettu Microsoftin järjestelmien ylläpitäjille ja se toimii niin sanottujen Component Object Model –osasten avulla, joita kutsutaan nimellä snap-in. Miltei kaikki tärkeimmät hallintatyökalut saa liitettyä konsoliin ja suuri osa esimerkiksi ohjauspaneelin hallintatyökaluista ovat todellisuudessa MMC-komponentteja. Paljon käytettyjä MMC-työkaluja ovat esimerkiksi Active Directory Users and Computers, Event Viewer ja Group Policy Management.

Aloitamme siirtämällä Schema Master –roolin ohjauskoneelle DC6. Tämä tapahtuu Microsoft Management Consolen avulla. Koska kaavaan tehtävien muutosten tekeminen on harvoin suositeltavaa, on kaavamuutoksiin tarvittava kirjasto ensin lisättävä rekisteriin.

Tämä tapahtuu alla olevan kuvan mukaisesti ”regsrv32 schmmgmt.dll”-komennolla (kuva 54).

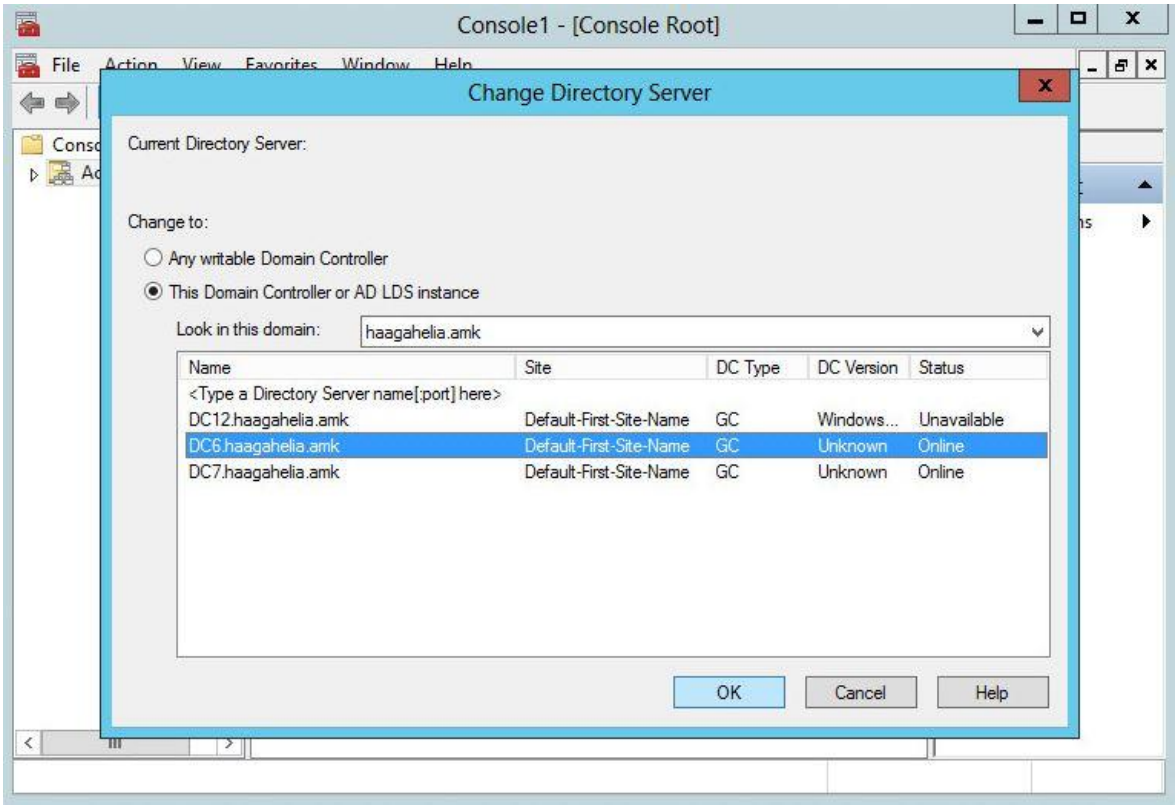
Kuva 54. Kaavamuutoksiin tarvittavan kirjaston rekisteröinti

Käynnistämme Microsoft Management Consolen ja nyt voimme lisätä tarvitsemamme Active Directory Schema snap-in –työkalun alla olevan kuvan 55 mukaisesti.



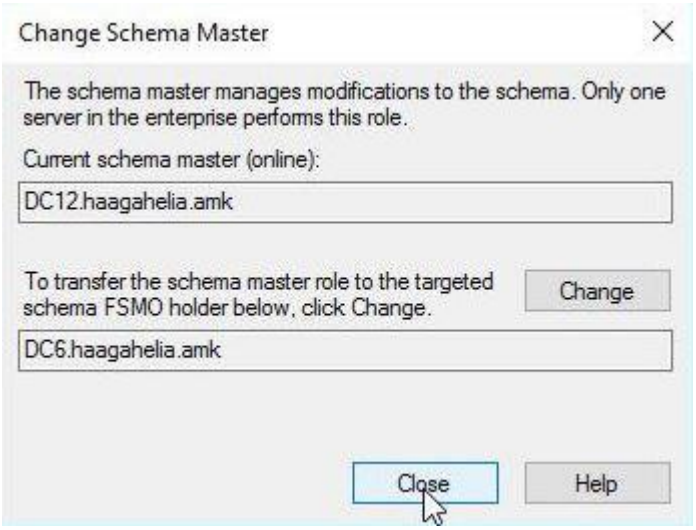
Kuva 55. Active Directory Schema –työkalun lisääminen

Avaamme oikealla hiirennapilla aktiivihakemiston schema-osion ja valitsemme avautuvasta valikosta ”Change Active Directory Domain Controller”. Valitsemme alla olevan kuvan 56 mukaisesti sen ohjauskoneen, jolle haluamme siirtää Schema Master –roolin.



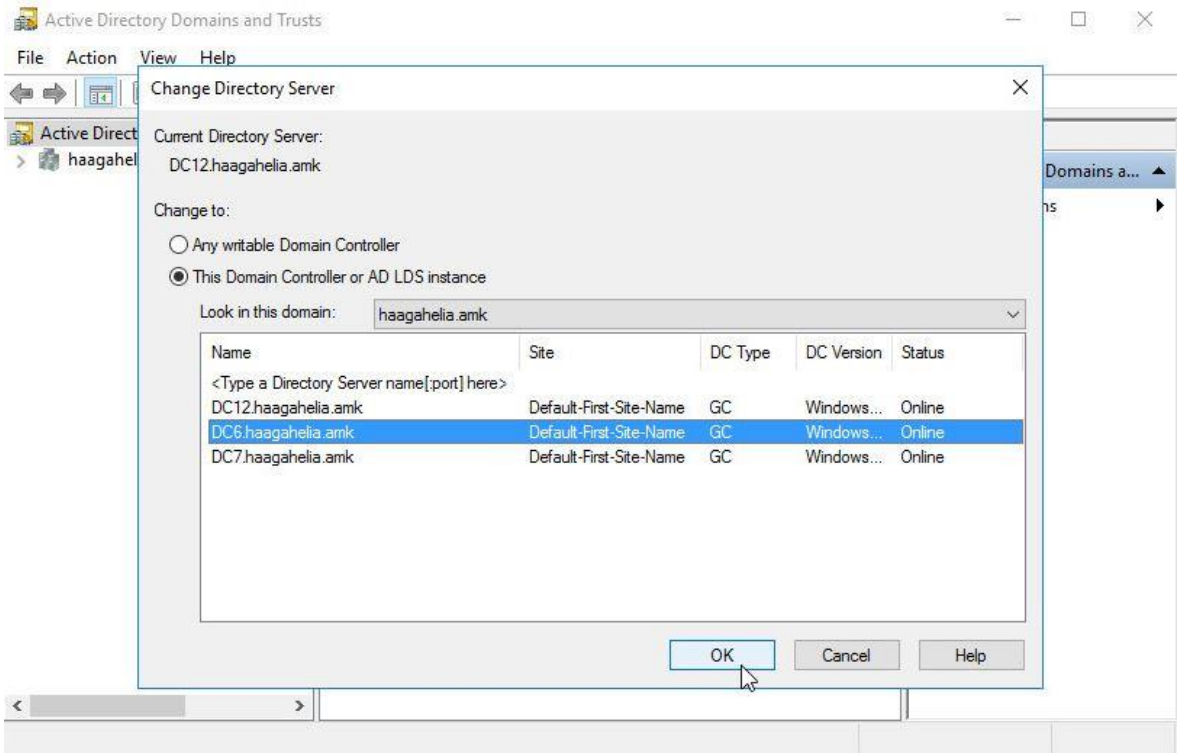
Kuva 56. Uuden Schema Master –koneen valinta

Kun oikea palvelin on valittu, voidaan avata oikealla hiirennapilla valikko samasta paikasta kuin äsken, josta valitaan ”Operations Master”. Avautuu ikkuna, jossa voimme vaihtaa roolin ohjauskoneelle DC6 (kuva 57).



Kuva 57. Roolin siirto koneelle DC6

Domain Naming Master –roolin siirto muistuttaa läheisesti edellä tehtyä Schema Master –siirtoa. Tällä kertaa siirrymme käyttämään Active Directory Domains and Trusts –näkymää. Täällä valitsemme vasemman laidan paneelista Active Directory Domains and Trusts ja avaamme valikon oikealla hiirennapilla. Edellisen kohdan tapaan valitsemme ensin palvelimen, jolle rooli halutaan siirtää (kuva 58).

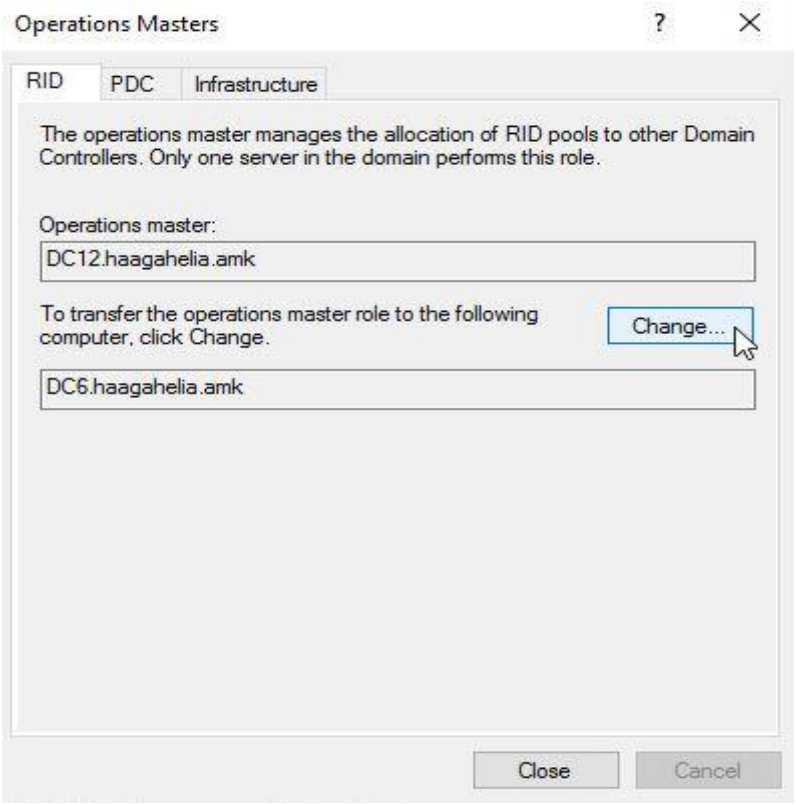


Kuva 58. Palvelimen valinta Active Directory Domains and Trusts –näkymässä

Palvelun siirto tapahtuu kuten edellisessä kohdassa valitsemalla valikosta ”Operations Master”.

3.13.2 Domain-tason roolien siirto

Loput kolme roolia voidaan siirtää Active Directory Users and Computers –työkalun avulla. Kun toimialueen nimeä klikkaamalla aukeaa valikko, jossa valitaan ”Operations Masters”. Aukeaa ikkuna (kuva59), jonka avulla voidaan vaihtaa kaikki kolme roolia toiselle ohjaus-koneelle.



Kuva 59. Domain-tason roolien siirto toiselle ohjauskoneelle

Kun kaikki roolit on siirretty, voimme tarkistaa samoin kuin aikaisemmin, että kaikki on kuten pitää ”netdom query FSMO”-komennon avulla (kuva 60).

```
C:\>netdom query FSMO
Schema master               DC6.haagahelia.amk
Domain naming master        DC6.haagahelia.amk
PDC                         DC6.haagahelia.amk
RID pool manager            DC6.haagahelia.amk
Infrastructure master       DC6.haagahelia.amk
The command completed successfully.
```

Kuva 60. Palvelut on siirretty DC6 -palvelimelle

Olisimme voineet siirtää roolit myös Windows PowerShellin avulla. Tällöin yksi komento olisi riittänyt jokaisen viiden roolin siirtämiseen. Tarvittava komento on:

Move-ADDirectoryServerOperationMasterRole -Identity DC6 -OperationMasterRole SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster, InfrastructureMaster

3.14 DC12-palvelimen päivittäminen

Koska olemme aikaisemmissa kappaleissa käsitelleet sekä ohjauskoneen poistamiseen, että uuden palvelimen lisäämiseen tarvittavat työvaiheet, emme käy kaikkia työvaiheita

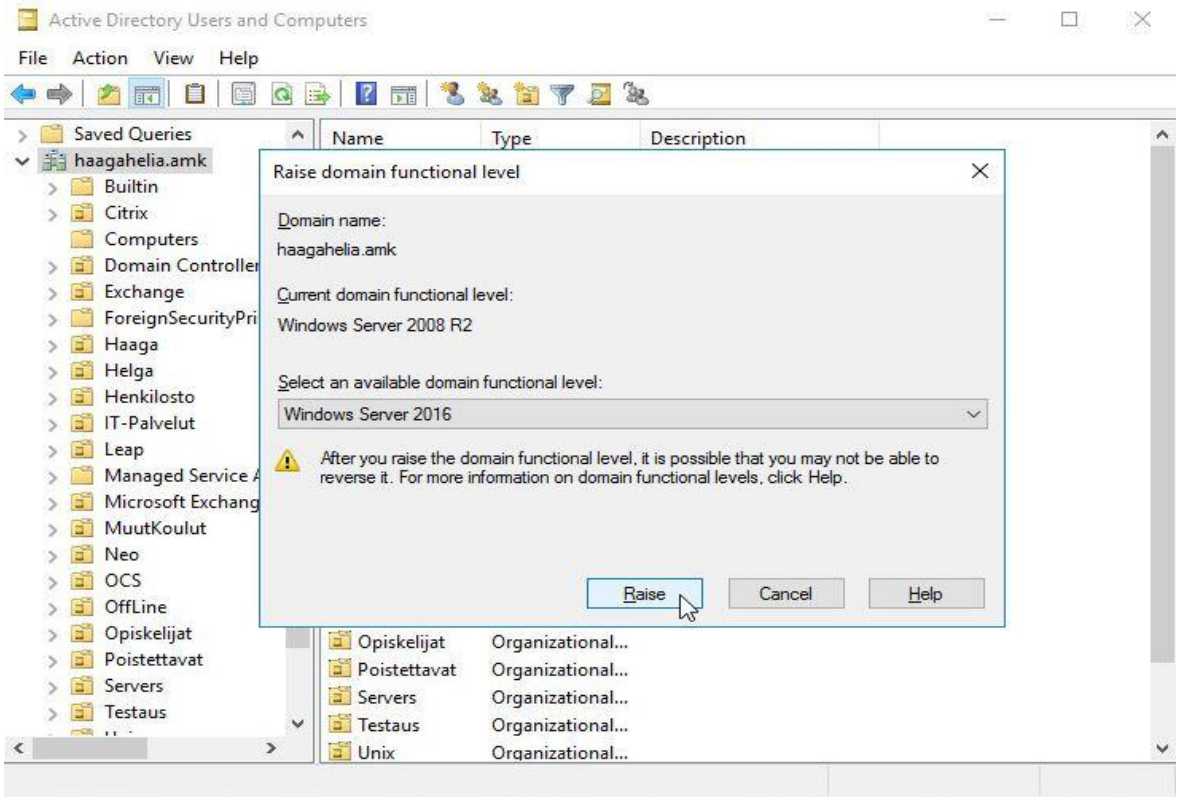
läpi uudestaan. Viimeisen palvelimen päivittäminen tapahtuu samalla tavalla, kuin aikaisemmin päivittämämme DC7:n kohdalla –vanha kone poistetaan tietoineen ja uusi pystytetään sen tilalle.

3.15 Palvelinympäristön toiminnallisuustasojen nosto

Olemme saaneet päivitettyä kaikki ohjauskoneet ja on aika nostaa sekä metsän, että toimialueen toiminnallisuus tasolle Windows Server 2016. Kuten muistamme, täytyy toimialueen kaikkien ohjauskoneiden käyttöjärjestelmien olla vähintään samalla tasolla, kuin toiminnallisuustaso, jolle aiomme noston tehdä. Kun toimialueen toiminnallisuustasoa on nostettu, teemme saman metsälle.

Toiminnallisuustason nostaminen onnistuu helposti Active Direcory Users and Computers –asetusten kautta. Tätä varten käyttäjällä on oltava Domain Admin tai Enterprice Admin –tasoiset käyttöoikeudet. Toiminnallisuustasoa on nostettava ohjauskoneella, jolle on annettu PDC Emulator operations master –rooli.

Toiminnallisuustasoa nostetaan valitsemalla paneelista haagahelia.amk–toimialue ja valitsemalla valikosta ”Raise Domain Fuctional Level”. Avautuvasta valikosta valitaan toiminnallisuustasoksi Windows Server 2016 (kuva 61).

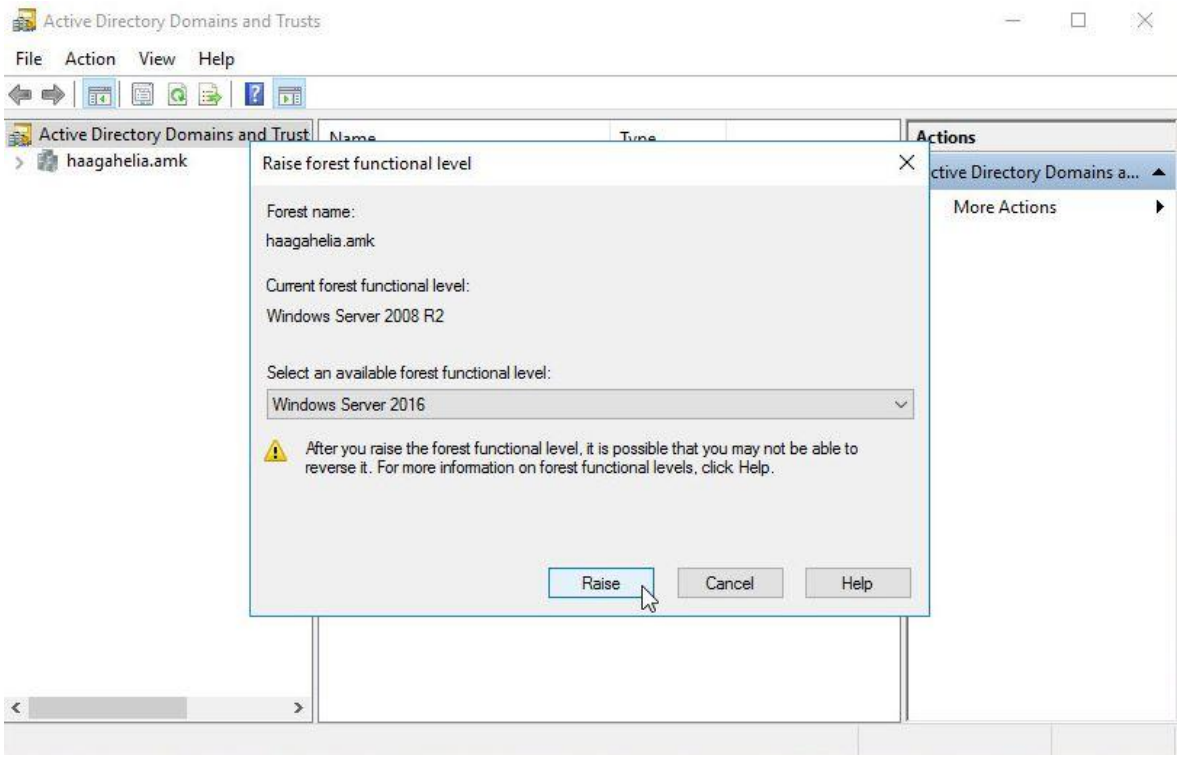


Kuva 61. Toimialueen toiminnallisuustason nostaminen tasolle Windows Server 2016

Toiminnallisuustason nostaminen on pysyvä ja sitä ei voida peruuttaa kuin tietyissä erikoistilanteissa. Peruuttaminen onnistuu vain Windows Server 2008:n jälkeisissä versioissa. (Microsoft 2014a.)

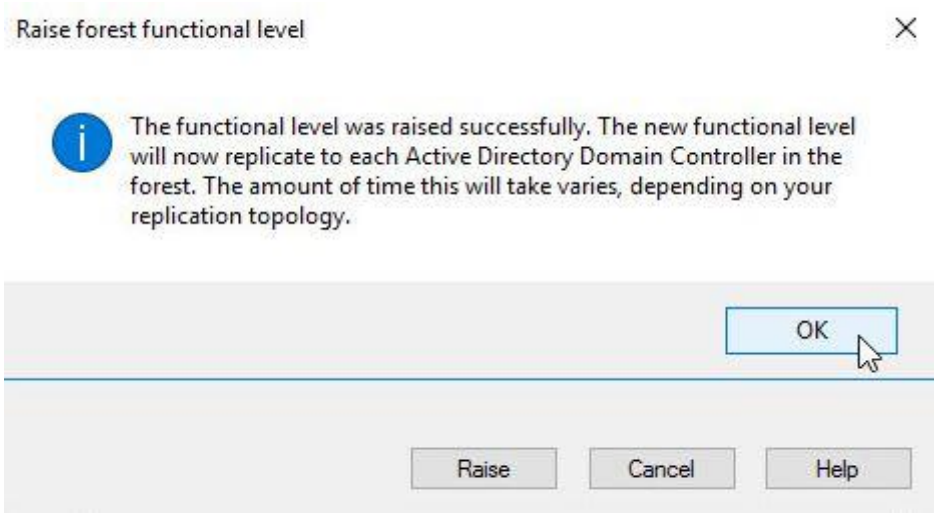
Metsän toiminnallisuustasoa nostetaan Schema Master –koneelta. Toimialueemme on tasolla Windows Server 2016, joten voimme lopuksi nostaa myös metsän toiminnallisuustasoa. Tähän tarvitsemme Active Directory Domains and Trusts –käyttöliittymää. Jos toiminnallisuustason nosto ei onnistu, tallennetaan prosessin aikana myös lokitiedosto, johon on listattu syyt, miksi toiminnallisuustason nosto epäonnistui. (Microsoft 2014c.)

Toiminnallisuustasoa nostetaan valitsemalla Active Domains and Trusts –sivupaneelista Raise Domain Functional Level (kuva 62).



Kuva 62. Metsän toiminnallisuustason nostaminen

Lopuksi saamme ilmoituksen, että toiminnallisuustason nosto on onnistunut (kuva 63). Saamme käyttöömme kaikki uusien toiminnallisuustasojen mukana tulevat ominaisuudet, joita on kuvattu tämän työn teoriaosuudessa.



Kuva 63. Ilmoitus onnistuneesta toiminnallisuustason nostosta

Toiminnallisuustason nostaminen on mahdollista myös Windows Powershellin avulla. Tällöin käytettävät komennot ovat ”Set-ADForestMode” ja ”Set-ADDomainMode”. Käskyille saadaan annettua lukuisia parametreja, mutta toiminnallisuustasojen nosto olisi tapahtunut komennoilla:

Set-ADDomainMode –Identity haagahelia.amk –DomainMode Windows2016Domain

Set-ADForestMode –Identity haagahelia.amk –ForestMode Windows2016Domain

Toiminnallisuustasot voidaan tarkastaa Windows PowerShellin avulla, kuten teemme kuvassa 64.

```
PS C:\> Get-ADDomain | fl Name,DomainMode


Name       : haagahelia
DomainMode : Windows2016Domain



PS C:\> Get-ADForest | fl Name,ForestMode


Name       : haagahelia.amk
ForestMode : Windows2016Forest
```

Kuva 64. Palvelinympäristön toiminnallisuustasot päivityksen jälkeen

Onnistuimme päivittämään Windows-palvelinten käyttöjärjestelmät, sekä nostimme toimialueen ja metsän toiminnallisuustasoja onnistuneesti. Toimialueelle lisätyllä Windows 10 –työasemalla kirjautumista kokeiltiin vielä erilaisilla käyttäjätunnuksilla.

4 Projektin tulokset

Testiympäristön rakennus sujui hyvin ja kaikki työvaiheet saatiin toteutettua onnistuneesti. Suunnittelun tärkeyttä tämänkaltaisessa projektissa ei kannata aliarvioida. Monet palvelimille tehdyt toimenpiteet ja asetukset ovat kertaluonteisia ja harvinaisia, sekä joissain tapauksissa peruuttamattomia. Juuri tästä syystä testiympäristön rakentaminen ja päivityksessä tehtävien työvaiheiden testaaminen etukäteen olikin välttämätöntä. Aktiivihakemiston keskeinen rooli palvelinympäristön resurssienhallinnassa tekee siitä tietojärjestelmän toiminnan kannalta keskeisen komponentin.

4.1 Selvitys ja suunnittelu

Sain idean tämän opinnäytetyön kirjoittamiseen ollessani Haaga-Heliassa työharjoittelussa kesällä 2018. Osallistuin kokoukseen, jossa Microsoftin konsultti selvitti järjestelmäpalveluiden asiantuntijoille päivittämisprojektin vaatimuksia ja siinä tarvittavia tekniikoita. Kokouksen jälkeen vaikutti siltä, että aihe sopisi hyvin opinnäytetyöhön ja päätin valita sen itselleni. Syksyllä harjoittelun jälkeen aloitin opinnäytetyön suunnitteluvaiheella.

Palvelinympäristön päivittämiseen löytyy kirjallisuudesta suositeltavia käytäntöjä. Ennen projektiin ryhtymistä on selvitettävä vanhan järjestelmän tila ja tukeeko palvelinympäristö uuden käyttöjärjestelmän vaatimuksia. Lisäksi on tärkeää huomioida, missä ja miten yrityksen toiminnan kannalta kriittistä dataa säilytetään ja miten sen turvallisuus pystytään takaamaan päivityksen aikana. (Morimoto, Shapiro, Yardeni, Noel, Abbate & Amaris 2018, 86.)

Projektin suunnittelu oli opinnäytetyön onnistumisen kannalta tärkeää. Työvaiheet oli suoritettava oikeassa järjestyksessä ja siten, ettei koulun tietojärjestelmän toiminta vaarannu. Esimerkiksi väärään verkkoon liitetty ohjauspalvelin olisi saattanut aiheuttaa koulun tietokoneille peruuttamatonta vahinkoa. Suunnittelun aikana tutustuin koulun fyysisiin palvelinlaitteisiin palvelinhuoneessa ja niiden arkkitehtuuriratkaisuihin haastattelemalla koulun järjestelmäpalveluiden työntekijöitä. Lisäksi sain heiltä paljon materiaalia ja ajateltavaa projektiin liittyen. Tässä vaiheessa yritin keskittyä ymmärtämään kokonaisuutta ja tunnistamaan päivitysprojektin kannalta tärkeimmät elementit. Samalla etsin tietoa kirjallisuudesta ja tietoverkoista.

Kun palvelinten lähtötilanne ja virtuaaliympäristön arkkitehtuuri oli selvillä, keskityin laatimaan suunnittelun kannalta tärkeää projektikaaviota, jossa eri palvelimille tehtävät toimenpiteet kuvataan. Kun tarvittavat työvaiheet olivat selvillä, aloin toteuttaa niitä yksitellen

käytännössä. Haaga-Helian toiveena oli ohjeistus, jota seuraamalla Windows-ympäristön toimintaan aikaisemmin perehtynyt henkilö voi suorittaa toimenpiteitä opinnäytetyön avulla. Tästä syystä opinnäytetyö kuvaa tarkasti työvaiheet ja esittelee niitä yksittäisten komentojen tasolla.

4.2 Projektin onnistuminen ja oman oppimisen arviointi

Kaikki opinnäytetyön prosessikaaviossa esitetyt työvaiheet suoritettiin onnistuneesti ja testiympäristön toiminnallisuus saatiin nostettua tasolle Windows Server 2016. Koska kysymys on tietoverkon toiminnan kannalta hyvin tärkeiden laitteiden päivittämisestä, on aiheesta löydettävissä paljon yksityiskohtaisia ohjeita ja päivittäminen on tehty niin yksinkertaiseksi, kuin mahdollista. Osittain tästä syystä, osittain etukäteen tehdyn suunnittelun ansiosta, en ajautunut opinnäytetyötä tehdessäni suuriin vaikeuksiin.

Opinnäytetyön kirjoittamisen aikana sain paljon tietoa Windows-palvelinympäristön arkkitehtuurista ja aktiivihakemiston toiminnasta. Opinnäytetyön laaja-alaisuus oli oppimisen kannalta parasta, sillä suunnitteluvaiheessa oli tärkeää ymmärtää miten asiat toimivat ja tarkastella järjestelmää kokonaisuutena.

Aktiivihakemiston tehtävien ja komponenttien lisäksi oli mielenkiintoista selvittää, millaiset laitteistot palvelinhuoneesta löytyy ja miten fyysisiä palvelinresursseja saadaan jaettua virtuaalikoneiden käyttöön. WMwaren palvelinympäristön arkkitehtuuri säiliöineen ja tietovarastoineen vaati hieman opettelua. Myös virtuaalikoneiden asentaminen ja konfigurointi veivät suhteellisen paljon aikaa, mutta olivat lopulta melko suoraviivaisia tehtäviä, kun ensin olin tutustunut vSphere-hallintakonsoliin ja sen työkaluihin.

Projektissa käytettyjä menetelmiä voidaan hyödyntää myös toisenlaisiin tilanteisiin. Esimerkiksi palvelinten palautus varmuuskopioista tehtiin juuri samalla tavalla kuin silloin, kun koulun tietojärjestelmät joudutaan palauttamaan epätodennäköisen, mutta halvauttavan ongelmatilanteen jälkeen. Palautimme koko toimialuemetsän varmuuskopioista samalla varmistaen niiden toimivuuden.

Yksittäisen palvelimen käyttöjärjestelmän lisäksi palautimme aktiivihakemiston ja SYSVOL-kansion, sekä saatoimme ne toimintakuntoon. Tämänkaltainen palautus saatetaan joutua tekemään esimerkiksi tilanteessa, jossa aktiivihakemiston objekteja vahingossa tuhoutuu. Tämän työvaiheen keskeinen asia oli ymmärtää palautuksen ja replikoinnin väliset suhteet ja vaikutukset koko toimialueen tasolla. Aktiivihakemiston palautuksessa on syytä miettiä, milloin palautus on ”authoratiivinen” ja milloin ei.

Päivityksen erikoisimmat vaiheet liittyivät suoraan koko toimialueen toimintaan. Näitä olivat aktiivihakemiston palauttamiseen ja salasanojen vaihtoon liittyvät asiat, SYSVOL-replikoinnin siirto DFS-jaon käyttöön, kaavapäivityksen ajaminen ja roolien siirto palvelimelta toiselle. Muutosten jälkeen replikointi tehostuu ja on paremmin hallittavissa. Lisäksi opin etsimään replikoinnissa tapahtuvia mahdollisia virheitä Windows Powershell –komentojen avulla.

Projektin aikana sain kokemusta käyttöjärjestelmien asentamiseen virtuaaliympäristössä ja palvelinten oikeaoppiseen poistamiseen. Nämä työvaiheet toistettiin useita kertoja, kun palvelimia ensin ajettiin alas ja sitten korvattiin uusilla. Samalla asensimme palvelinrooleja ja teimme nimipalvelimeen, sekä verkkoinfraan liittyviä perusasetuksia.

Suurin osa päivityksen ja toiminnallisuustason noston mukana tulevista ominaisuuksista vaikuttaa tietoturvaan. Tällainen ominaisuus on esimerkiksi teoriaosuudessa mainittu AD FS Extranet Lockout Policy, mutta myös muut toiminnallisuustason noston jälkeen käytettävissä olevat palvelut parantavat aktiivihakemiston tietoturvaa. Näistä voidaan mainita esimerkiksi Privileged Access Management (PAM), jonka avulla aktiivihakemiston käyttöoikeuksia voidaan myöntää vain tehtävien suorittamiseen tarvittavaksi ajaksi (Microsoft 2017).

4.3 Projektin jatko

Koska päivityksen aikana rakennettu testiympäristö vaikutti toimivan oikein ja toimialueelle kirjautuminen onnistui normaalisti, voidaan tuotantoympäristön päivittäminen aloittaa. Päivitysprojektia on suunniteltu vuoden 2019 alkuun ja sitä varten on valmiiksi hankittu Hewlett Packardin valmistama DL360p Generation 8 –palvelin. Päivityksen yhteydessä myös ohjauspalvelimen laitteisto uusitaan.

SYSVOL-replikoinnin siirto käyttämään DFS-replikointia aloitettiin samana päivänä, kun kirjoitan tätä viimeistä kappaletta. Opinnäytetyön kirjoittamisen aikana olen parantanut huomattavasti ymmärtämystäni Windows-palvelinympäristöstä ja päässyt kokeilemaan käytännössä järjestelmänhallintaan liittyviä toimenpiteitä, joita suoritetaan erittäin harvoin ja joiden harjoittelu kotioloissa olisi ollut vaikeasti toteutettavissa. Yhteistyö Haaga-Helian tietohallinnon kanssa on sujunut hyvin ja olen saanut opinnäytetyön aikana paljon hyviä neuvoja ja opastusta.

Lähteet

Cooper, D. 2014. Active Directory Back to Basics –Sysvol. Microsoft TechNet. Luettavissa: https://social.technet.microsoft.com/wiki/contents/articles/24160.active-directory-back-to-basics-sysvol.aspx. Luettu: 16.10.2018.

Haaga-Helia 2018. Vuosikertomus 2017. Haaga-Helia ammattikorkeakoulu Oy. Luettavissa: http://www.haaga-helia.fi/sites/default/files/Kuvat-ja-liitteet/Palvelut/Julkaisut/haagahelia_vuosikertomus_2017.pdf?userLang=fi. Luettu: 3.10.2018.

Kapoor, R. 2016. Repadmin –Active Directory Replication Tools. Itingredients.com. Luettavissa: http://www.itingredients.com/repadmin-active-directory-replication-tools/. Luettu: 31.10.2018.

Kalliomäki, A. 2018. Haaga-Helian asiantuntija. Haaga-Helia Server & Desktop Virtualization. Kalvosarja. Helsinki.

Kalliomäki, A. 23.10.2018. Haaga-Helian asiantuntija. Haaga-Helian virtualisointiratkaisut. Haastattelu. Helsinki.

Van Keymeulen, P. 2012. Windows Server 2012 AD Backup and Disaster Recovery Procedures. EDE Consulting. Luettavissa: https://www.edeconsulting.be/downloads/WindowsServer2012ADBackupandDisasterRecoveryProcedures_V1.2.pdf. Luettu: 7.11.2018.

Laakso Mika 2017. Microsoft-aktiivihakemisto moniasiakasympäristössä Case Calpro. Hämeen ammattikorkeakoulu. Luettavissa: https://www.theseus.fi/bitstream/handle/10024/136259/MICROSOFT-AKTIIVIHAKEMIS-TO%20MONIASIAKASYMPARISTOSSA%20CASE%20CALPRO.pdf?sequence=1. Luettu: 10.10.2018.

Lamppu, S. 2018. Upgrading AD DS Schema to Windows Server 2016. Sam’s Corner. Luettavissa: https://samilamppu.com/2016/11/06/upgrading-ad-ds-schema-to-windows-server-2016/. Luettu: 1.11.2018.

Microsoft 2008a. How the Active Directory Replication Model Works. Microsoft Docs. Luettavissa: https://technet.microsoft.com/pt-pt/library/cc772726(v=ws.10).aspx#w2k3tr_repup_how_gmzg. Luettu. 16.10.2018.

Microsoft 2008b. What are Operations Masters? Microsoft Docs. Luettavissa: https://technet.microsoft.com/pt-pt/library/cc779716(v=ws.10).aspx. Luettu: 18.10.2018.

Microsoft 2008c. SYSVOL Migration Series: Part 1 – Introduction to the SYSVOL migration process. Luettavissa: https://blogs.technet.microsoft.com/filecab/2008/02/08/sysvol-migration-series-part-1-introduction-to-the-sysvol-migration-process/. Luettu: 31.10.2018.

Microsoft 2009. How FRS Works. Microsoft Docs. Luettavissa: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758169(v=ws.10). Luettu: 17.10.2018.

Microsoft 2012. Overview of DFS Namespaces. Microsoft Docs. Luettavissa: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc730736%28v%3dws.10%29. Luettu: 17.10.2018.

Microsoft 2014a. Understanding Active Directory Domain Services (AD DS) Functional Levels. Microsoft Docs. Luettavissa: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754918(v=ws.10)#Features%20that%20are%20available%20at%20forest%20functional%20levels. Luettu: 12.10.2018.

Microsoft 2014b. Running adprep.exe. Microsoft Docs. Luettavissa: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd464018(v=ws.10). Luettu: 1.11.2018.

Microsoft 2014c. Raise the Domain Functional Level. Microsoft Docs. Luettavissa: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753104(v=ws.11). Luettu: 7.11.2018.

Microsoft 2017. Privileged Access Management for Active Directory Domain Services. Microsoft Docs. Luettavissa: https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services. Luettu: 15.11.2018

Microsoft 2018a. Domain Trees. Windows Dev Center. Luettavissa: https://docs.microsoft.com/en-us/windows/desktop/ad/domain-trees. Luettu: 10.10.2018.

Microsoft 2018b. Forests. Windows Dev Center. Luettavissa: https://docs.microsoft.com/en-us/windows/desktop/ad/forests. Luettu: 10.10.2018.

Microsoft 2018c. Forest and Domain Functional Levels. Windows IT Pro Center. Luettavissa: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels. Luettu: 12.10.2018.

Microsoft 2018d. Active Directory Federation Services. Microsoft Docs. Luettavissa: https://msdn.microsoft.com/en-us/library/bb897402.aspx. Luettu: 20.9.2018.

Microsoft 2018e. Backing Up and restoring an FRS-Replicated SYSVOL Folder. Windows Dev Center. Luettavissa: https://docs.microsoft.com/en-us/windows/desktop/VSS/backing-up-and-restoring-an-frs-replicated-sysvol-folder#determining-whether-a-domain-controllers-sysvol-folder-is-replicated-by-dfsr-or-frs. Luettu: 29.10.2018.

Morimoto, R. & Shapiro, J. & Yardeni, G. & Droubi, O. & Noel, M. & Abbate, A. & Amaris, C. 2017. Windows Server 2016 Unleashed. Pearson Education.

Pietroforte, M. 2014. Forgot the Domain Admin Password? 4sysops. Luettavissa: https://4sysops.com/archives/forgot-the-domain-admin-password/. Luettu: 26.10.2018.

Pyle, N. 2014. Streamlined Migration of FRS to DFSR SYSVOL. Storage at Microsoft. Luettavissa: https://blogs.technet.microsoft.com/filecab/2014/06/25/streamlined-migration-of-frs-to-dfsr-sysvol/. Luettu: 31.10.2018.

Rouse, M. 2012. Directory Services Restore Mode. TechTarget. Luettavissa: https://searchwindowsserver.techtarget.com/definition/Directory-Services-Restore-Mode-DSRM. Luettu: 17.11.2018.

Rouse, M. 2017. Active Directory functional levels. TechTarget. Luettavissa: https://searchwindowsserver.techtarget.com/definition/Active-Directory-functional-levels. Luettu: 7.11.2018.

Silfver, K. 19.9.2018. Haaga-Helian järjestelmäasiantuntija. Haastattelu. Helsinki.

Talvivaara, J. s.a. Verkon nimi- ja hakemistopalvelut. Virtuaali AMK. Luettavissa: http://www2.amk.fi/mater/tietotekniikka/nimipalvelut/8_activedirectory.html Luettu: 16.10.2018.

Uski, J. 20.9.2018. Haaga-Helian järjestelmäasiantuntija. Haastattelu. Helsinki.

VMware 2018. vSphere. Luettavissa: https://www.vmware.com/products/vsphere.html. Luettu: 5.11.2018.

Warren, A. 2017. Identity with Windows Server 2016. Pearson Education.

Liite 1. Lopputyössä käytetyt käsitteet ja niiden merkitykset

ACL	Acceess Control List. Tiedostojärjestelmän objektiin liittyvien käyttöoikeuksien lista.
Aktiivihakemisto	Active Directory, AD. Microsoftin hakemistopalvelu, johon on tallennettu tietoverkon resurssit. Sisältää työkaluja objektien hallintaan.
AD Administrative Center	ADAC. Aktiivihakemiston ylläpitoon käytettävä ohjelma.
AD Functional Level	Aktiivihakemiston toiminnallisuustaso. Määrittää mitä aktiivihakemiston ominaisuuksia voidaan ottaa käyttöön.
AD Recycle bin	Aktiivihakemiston ominaisuus, jolla poistettuja objekteja voidaan palauttaa 180 päivän ajan.
AD Users and Computers	Aktiivihakemiston hallintanäkymä, jonka avulla käsitellään toimialueen käyttäjä- ja tietokonetilejä.
AD DS	Active Directory Directory Services, sama kuin aktiivihakemisto.
Administrator	Tietoverkon ylläpitäjä.
Adprep.exe	Aktiivihakemiston kaavan valmisteluun käytettävä komento (ohjelma).
AD FS	AD FS (Active Directory Federation Services) on Microsoftin palvelu, jonka avulla voidaan jakaa identiteettitietoja luotettujen kumppaneiden kesken verkon välityksellä.
AMK	Ammattikorkeakoulu.
Authorative Restore	Aktiivihakemiston palautus, jossa palautuksen jälkeen muuttuneita tietoja ei päivitetä muilta palvelimilta.

Azure AD	Microsoftin pilvipohjainen hakemisto- ja identiteettitietojen hallintaan tarkoitettu sovellus.
BIOS	Basic Input-Output System. Tietokoneen käynnistyksessä ajettava ohjelma, jonka tehtävänä on ladata käyttöjärjestelmä ja tavallisimmat ajurit keskusmuistiin.
CDO	Collaborative Data Object –kirjasto, jota käytetään sähköpostin yhteydessä.
Clobal Catalog	Ohjauskoneilla sijaitseva tietovarasto, joka käsittää kaikki aktiivihakemistometsän objektit.
Datastore	Palvelin ympäristön tietovarasto. VMwaren virtuaaliympäristössä tiedosto, joka sisältää virtuaalikoneen.
DC	Domain Controller. Toimialueen ohjaustietokone.
DFS	Distributed File System. Microsoft-palvelinten tiedostojakopalvelu. Käytetään replikoinnissa.
Dfsrmig.exe	Tiedostojakojärjestelmän siirrossa käytettävä ohjelma (FRS – DFS migraatio).
DSRM, Directory Services Restore Mode	Aktiivihakemiston palauttamisen yhteydessä käytettävä käynnistystila.
DNS	Domain Name System. Nimipalvelu, jonka tehtävänä on yhdistää IP-osoitteita ja verkkotunnuksia.
Domain	Microsoft-palvelinympäristössä toimialue, jonka koneilla on yhteinen aktiivihakemisto ja nimiavaruus.
Domain Administrator	Toimialueen ylläpitäjä ja aktiivihakemiston ylläpitoon käytettävä ryhmä.

Domain Functional Level	Toimialueen toiminnallisuustaso. Kaikkien toimialueen ohjauskoneiden käyttöjärjestelmien täytyy olla samalla tasolla.
DRS-client	Directory Replication System. Replikoinnissa käytettävä ohjelmistokomponentti.
ESX	VMware ESXi. Suoraan palvelinten päälle asentuva hypervisor, jonka tehtävänä on jakaa resursseja virtuaalikoneiden käyttöön.
Forest Functional Level	Toimialuemetsän toiminnallisuustaso. Kaikkien metsän toimialueiden täytyy olla samalla tai ylemmällä toiminnallisuustasolla.
FRS	File Replication System. Microsoftin tiedostojakomenetelmä, jota käytetään jaettujen kansioiden ja ryhmäkäytäntöjen siirtämiseen.
FSMO	Flexible Single Master Operations –rooli. Aktiivihakemiston ohjauskoneelle asennettavia rooleja. Käytetään silloin, kun tavanomainen multimaster-replikointi ei riitä.
GPO	Group Policy Object. Ryhmäkäytäntö, jonka avulla käyttäjä- ja tietokonetileille saadaan voimaan tietyt ennalta määrätyt asetukset.
GUID	Globally Unique Identity. 128-bittinen tunnusluku, jota käytetään objektien tunnistamiseen Windows-palvelinympäristössä. Voidaan antaa esimerkiksi komponentille, käyttäjälle, ohjelmalle tai tiedostolle.
Hypervisor	Ohjelmisto tai laite, joka luo ja ajaa virtuaalikoneita.
Intersite-replikointi	Replikointi eri ”siteen” sijoitettujen ohjauskoneiden välillä. Tapahtuu yleensä hitaamman yhteyden yli. Voidaan ajastaa tapahtumaan silloin, kun verkon tietoliikenne on vähäistä.

Intrasite-replikointi	Nopeaa replikointia samaan ”siteen” kuuluvien ohjauskoneiden välillä.
IP	Internet Protocol. Huolehtii IP-tietoliikenteen välittämisestä tietoverkossa.
Kerberos	Windows-palvelimilla käytössä oleva todennusprotokolla.
LDAP	Lightweight Directory Access Protocol. Hakemistopalvelujen käsittelyyn tarkoitettu protokolla.
Logon Script	Käynnistämisen yhteydessä ajettava komentoketju.
MMC	Microsoft Management Console. Käyttöjärjestelmän työkalu, jolla hallitaan Windows-tietoverkon ja päätelaitteiden asetuksia. Käyttää ”snap-in”-komponentteja, joita voidaan lisätä tarpeen mukaan.
Multimaster-ympäristö	Palvelinympäristö, jossa muutoksia voidaan tehdä kaikille ohjauspalvelimille, jotka replikoivat tiedot toisilleen.
NetApp	Tiedostojen pilvitallentamisen menetelmiä kehittävä yritys, jonka levyjärjestelmä on käytössä Haaga-Heliassa.
NETLOGON	Käyttäjien ja palveluiden autentikointiin tarkoitettu taustalla ajettava Windows-palvelu.
NTFRS	File Replication System. Sama kuin FRS.
NTFS	New Technology File System. Microsoftin levyjärjestelmä.
Operations Master –roolit	Sama kuin FSMO-roolit. Aktiivihakemiston ohjauskoneelle asennettavia rooleja.
OU	Organization Unit. Aktiivihakemiston organisaatioyksikkö, jonka avulla objekteja voidaan luokitella loogisiksi kokonaisuuksiksi ja

	jolle voidaan määritellä yhteisiä asetuksia esimerkiksi ryhmäkäytäntöjen avulla.
PDC Emulator	Primary Domain Controller Emulator. FSMO-rooli, joka vastaa toimialueen ajasta ja tekee salasanoihin työasemilta saapuvat muutokset. Se myös huolehtii ryhmäkäytännöistä silloin, kun niihin tehdään muutoksia.
Privileged Access Management (PAM)	Aktiivihakemiston ominaisuus, jonka avulla käyttöoikeuksia voidaan myöntää vain tehtävien suorittamiseen tarvittavaksi ajaksi.
RDC	Remote Differential Compression. Palvelinten tiedostojen jaossa käytettävä replikointi-algoritmi, joka välittää tiedostoista eteenpäin vain osat, joissa on tapahtunut muutoksia.
Replikointi	Menetelmä, jonka avulla ohjauskoneet päivittävät muutokset aktiivihakemistoon kopioimalla muuttuneet tiedot toisilleen.
Resource Pool	Resouce pool on yksikkö, jonka alle sijoitetuille virtuaalikoneille voidaan määritellä yhteisiä resursseja vSphere-ympäristössä.
RID Master	(Relative Identifier). Ohjauspalvelimen FSMO-rooli, jonka tehtävänä on jakaa muille ohjauskoneille RID-tunnuksia, joita ne käyttävät SID-tunnusten (Security Identifier) tekemiseen aktiivihakemiston objekteille.
RPC	Remote Procedure Call. Protokolla jonka avulla ohjelma voi pyytää palveluita toisilta koneilta tietoverkon yli.
Schema	Tässä yhteydessä aktiivihakemiston kaava. Sisältää aktiivihakemiston objektit ja niihin liitettävissä olevat attribuutit.
Schema Master	FSMO-rooli, joka hallinnoi aktiivihakemiston kaavaa ja siihen liittyviä tietoja.

Security descriptor	Sisältää objektin tietoturvaan liittyvät määrittelyt. Näitä ovat esimerkiksi SID-tunnukset ja Access List-tiedot.
Site	Palvelinympäristön osa, joka on määritelty fyysisen sijainnin tai nopeiden tietoliikenneyhteyksien takia loogiseksi kokonaisuudeksi. Site-tietoja käytetään replikoinnin reitittämiseen.
Site link bridgehead	Ohjauskone, joka huolehtii intersite-replikoinnista alueiden välillä.
SMB	Server Message Block. IBM:n ja Microsoftin kehittämä hajautettu levyjärjestelmä.
SMPT	Simple Mail Transfer Protocol. TCP-pohjainen sähköpostipalvelimien käyttämä protokolla.
Store and Forward	Menetelmä, jossa ohjauskoneet tallentavat muutokset ensin omaan tietokantaansa ja välittävät tiedot sitten eteenpäin. Näin alkuperäistä palvelinta ei tarvita tiedon eteenpäin siirtämiseen.
System State Recovery	System State -varmuuskopion palautus korjaa palvelimelle asennetut roolit ja aktiivihakemiston tietokannan.
SYSVOL	System Volume on jaettu hakemisto, joka sijaitsee ohjauskoneilla ja sisältää kirjautumis-skriptit (Logon Scripts) ja ryhmäkäytännöt, eli Group Policy Objects (GPO).
TCP	Transmission Control Protocol. Kuljetuskerroksen verkkoprotokolla jonka tehtävänä on luoda yhteydet tietokoneiden välille IP-paketteja käyttäen. Huolehtii vianhallinnasta ja luotettavuudesta.
Template	Tässä opinnäytetyössä virtuaalikoneesta ja sen asetuksista luotu pohja, jota voidaan käyttää uusien virtuaalikoneiden alustamisessa.
USN Journal	Update Sequence Number Journal, NTFS-levyjärjestelmän ominaisuus, joka pitää kirjaa levyille kirjoitetuista muutoksista.

Windows Backup	Windows-palvelinten ohjelma, jonka avulla tietokoneista voidaan tehdä varmuuskopioita.
PowerShell	Microsoftin komentotulkki Windows-käyttöjärjestelmiin.
Virtualisointi	Tekniikka, jossa fyysisten laitteiden resursseja jaetaan käyttöön ohjelmallisesti.
WMware	Virtualisointi ratkaisuja tarjoava yritys.
vSphere	VMwaren ohjelmisto virtuaalikoneiden hallintaan.
X.500	Vanha hakemistopalveluiden käsittelyyn tarkoitettu standardi.

Liite 2. Windows Domain & Forest Functional levels

Taulukko 1. Toimialueen toiminnallisuustasojen ominaisuudet (Microsoft 2014a & Microsoft 2018c)

Domain Functional level	Available Features	Supported DC operating systems
Windows 2000 native	-Default AD DS services. -Universal groups for both distribution and security groups. -Group nesting. -Group conversion between security and distribution groups. -SID history.	Windows Server 2008 R2 Windows Server 2008 Windows Server 2003 Windows 2000
Windows Server 2003	-Renaming Domain controllers (Netdom.exe). -Logon timestamp updates. -Set userPassword attribute as the effective password on inetOrgPerson. -Redirect Users and Computers containers. -Authorization Manager can store its authorization policies in AD DS. -Constrained delegation. -Selective authentication.	Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008 Windows Server 2003
Windows Server 2008	-Distributed File System (DFS) replication support for SYSVOL. -Domain-based DFS namespaces. -Advanced Encryption Standard (AES 128 and AES 256) support for the Kerberos. -Last Interactive Logon In-	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008

	formation. -Fine-grained password policies. -Personal Virtual Desktops.	
Windows Server 2008 R2 (Haaga-Helia Domain level)	-User logon method authentication. -Automated SPN update. -Windows PowerShell cmdlets for AD.	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2
Windows Server 2012	-The KDC support for claims, compound authentication, and Kerberos armoring. -Dynamic Access Control.	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012
Windows Server 2012 R2	-DC-side protections for Protected Users. -Authentication Policies. -Authentication policy Silos.	Windows Server 2016 Windows Server 2012 R2
Windows Server 2016	-New Kerberos and NTLM features.	Windows Server 2016

Taulukko 2. Metsän toiminnallisuustasojen ominaisuudet (Microsoft 2014a & Microsoft 2018c)

Forest Fuctional Level	Available Features	Supported DC operating systems
Windows 2000 Native	-All default AD DS features.	Windows Server 2008 R2 Windows Server 2008 Windows Server 2003 Windows 2000
Windows Server 2003	-Forest Trust. -Domain rename. -Linked-value replication. -Read-only Domain Controllers (RODC). -Improved Knowledge Consistency Checker (KCC) algorithms and scalability.	Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008 Windows Server 2003

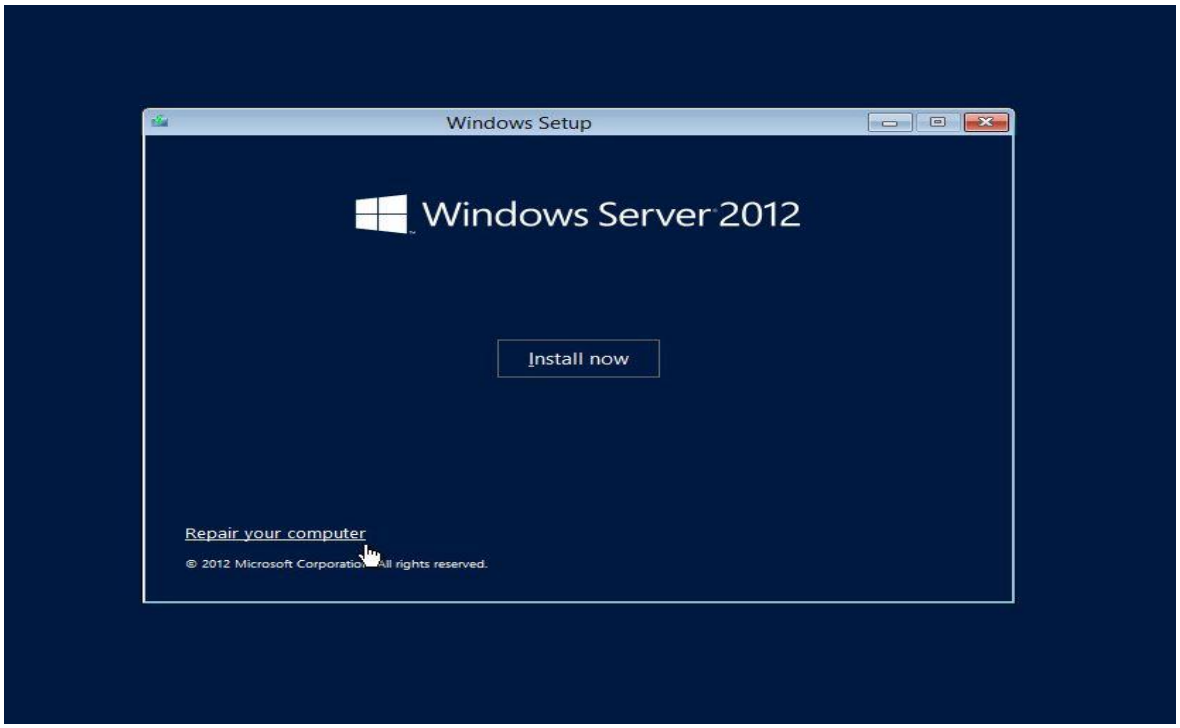
	-Create instances of the dynamic auxiliary class named dynamicObject in a domain directory partition. -The ability to convert an inetOrgPerson object instance into a User object instance. -The ability to create instances of new group types to support role-based authorization (application basic groups and LDAP query groups). -Deactivation and redefinition of attributes and classes in the schema. -Domain-based DFS namespaces running in Windows Server 2008 Mode, which includes support for access-based enumeration and increased scalability.	
Windows Server 2008	-No new features.	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008
Windows Server 2008 R2 (Haaga-Helia Forest Level)	-**Active Directory Recycle Bin**, which provides the ability to restore deleted objects in their entirety while AD DS is running.	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2
Windows Server 2012	-No new features.	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012

Windows Server 2012 R2	-No new features.	Windows Server 2012 R2
Windows Server 2016	-Privileged access management (PAM) using Microsoft Identity Manager (MIM).	Windows Server 2016

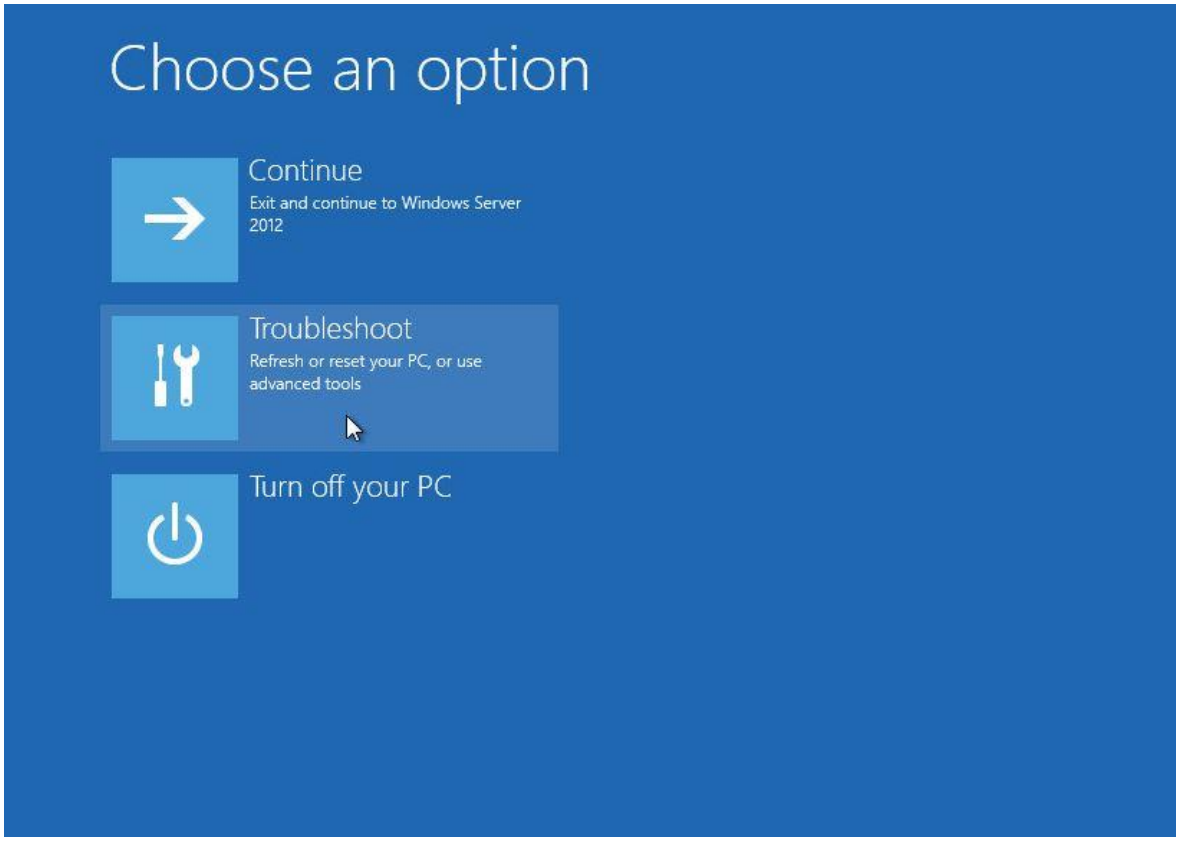
Liite 3. Windows-käyttöjärjestelmän palauttaminen Backup-tiedostosta

Tämä liite sisältää Windows-käyttöjärjestelmän palauttamisessa tehdyt työvaiheet ruutukaappauksina. Kuvat ovat järjestyksessä ja erillisiä selitteitä ei ole, sillä kysymyksessä on perustason asennustehtävä.

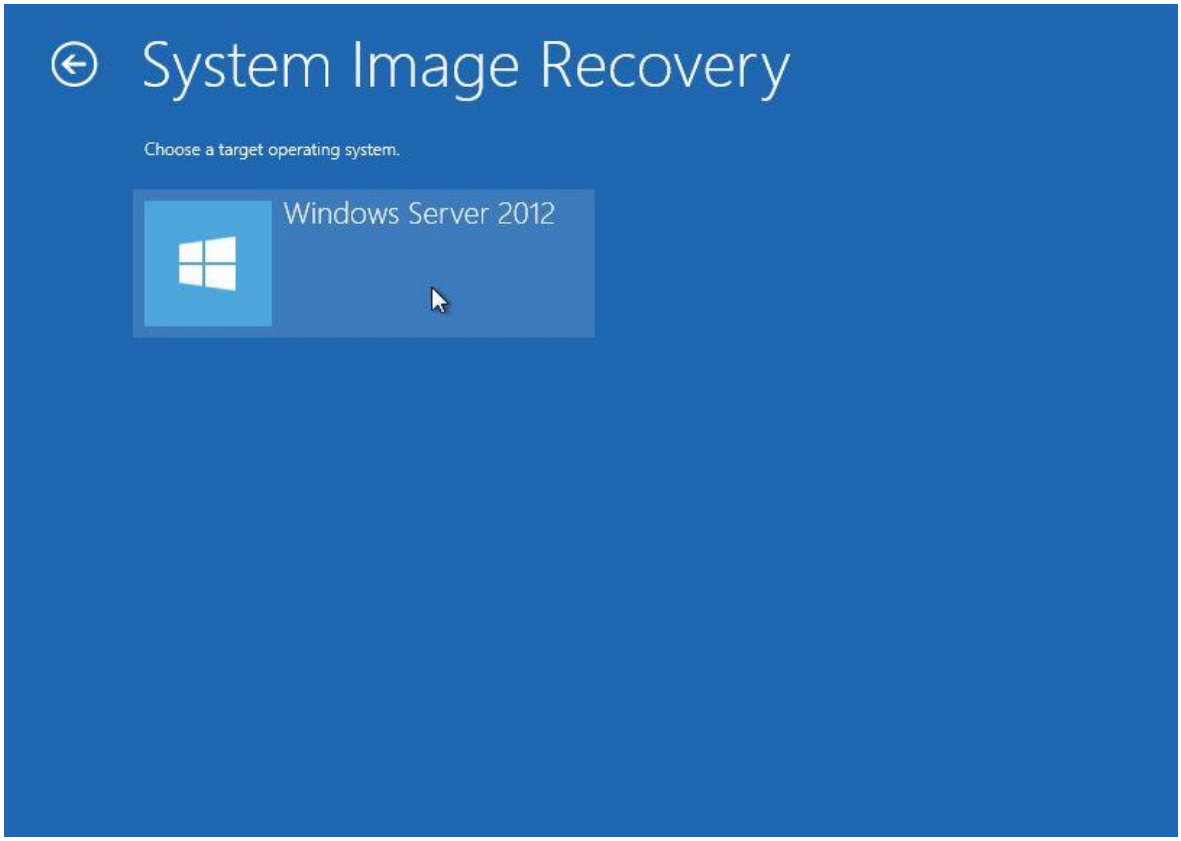
Kuva 3-1



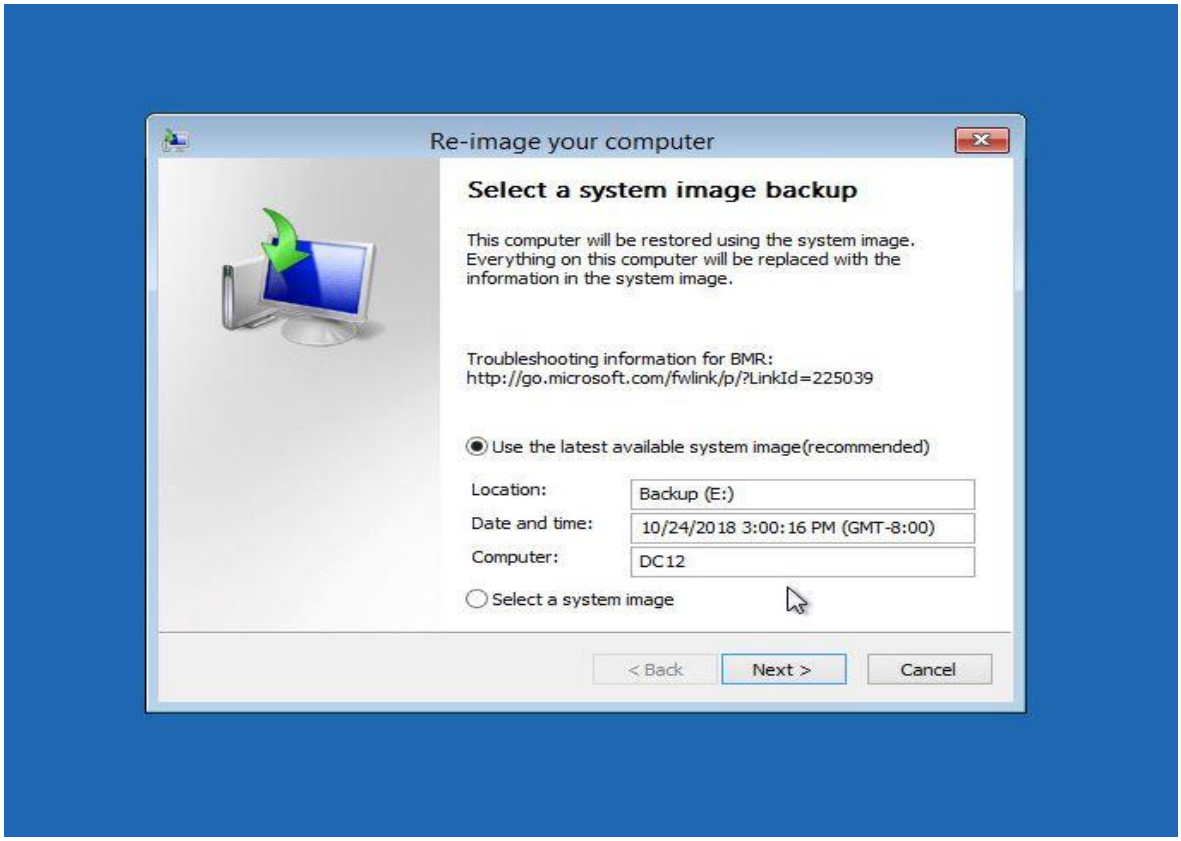
Kuva 3-2



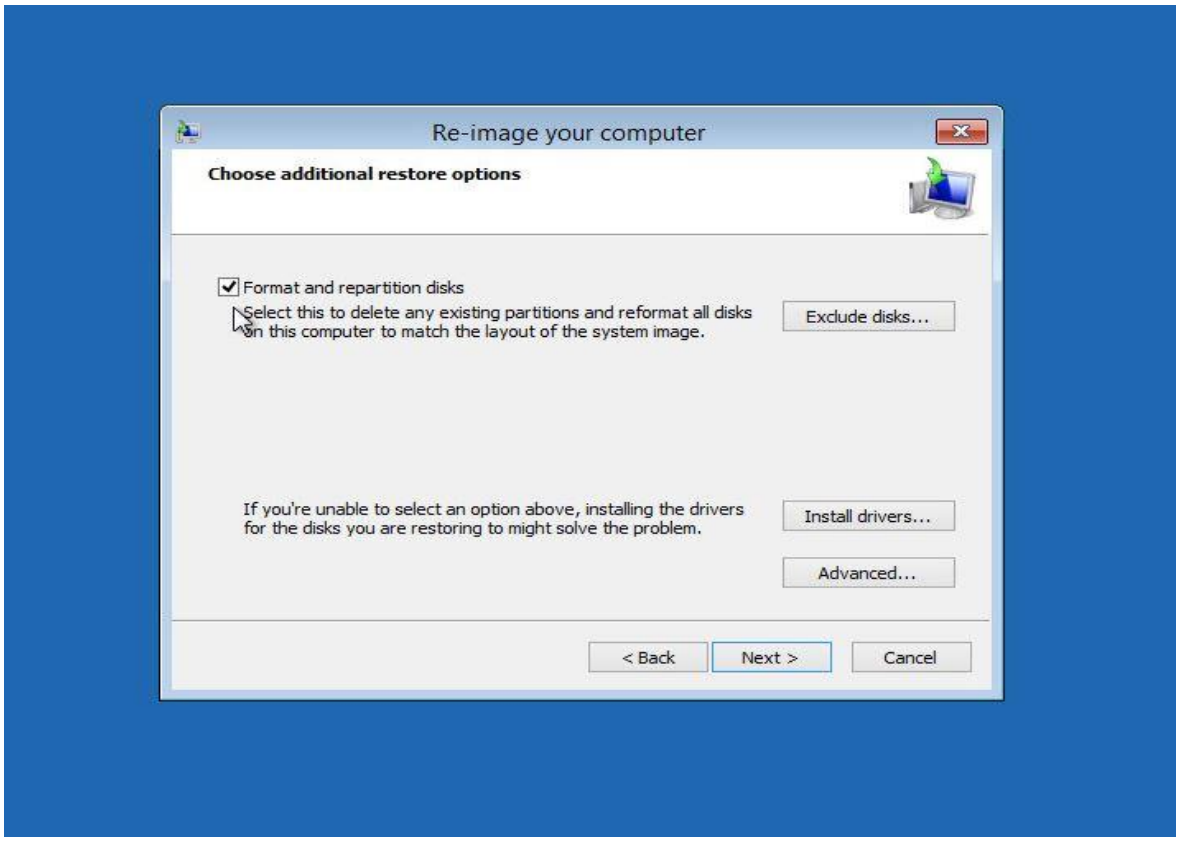
Kuva 3-3



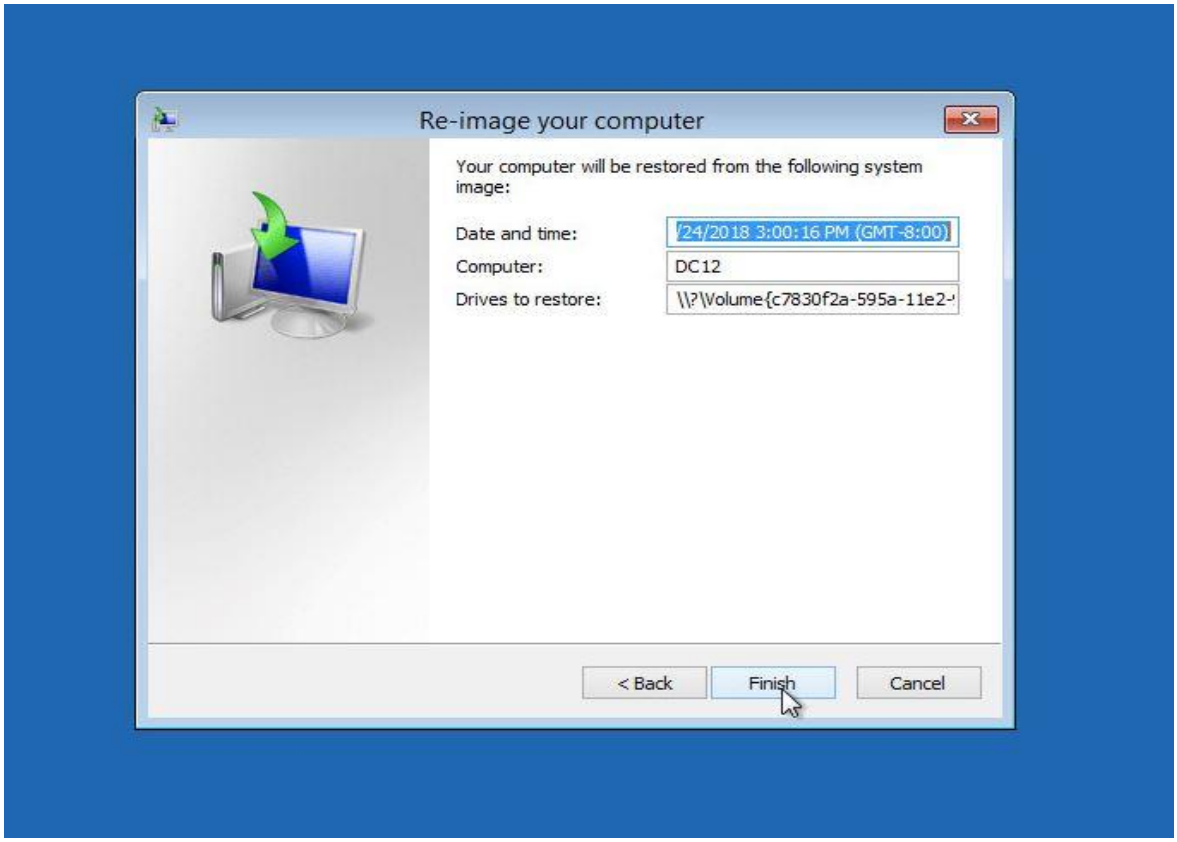
Kuva 3-4



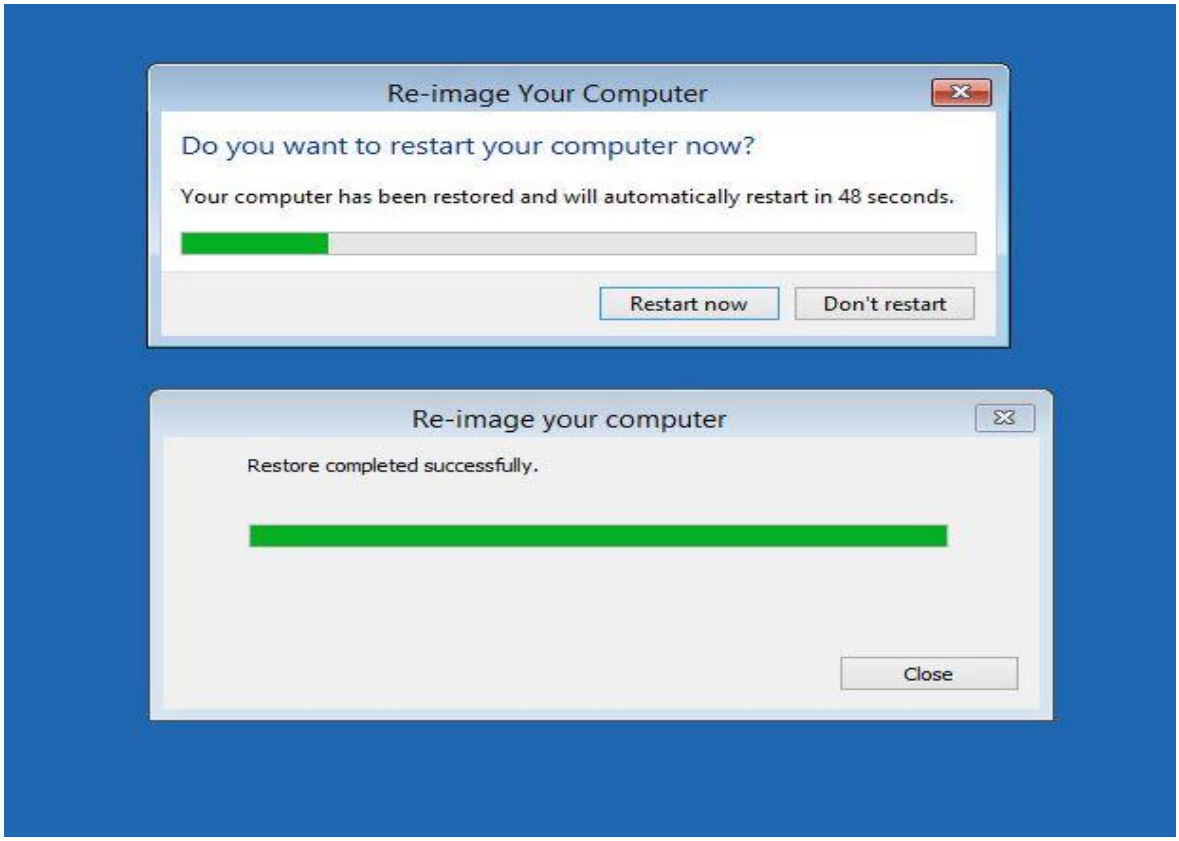
Kuva 3-5



Kuva 3-6



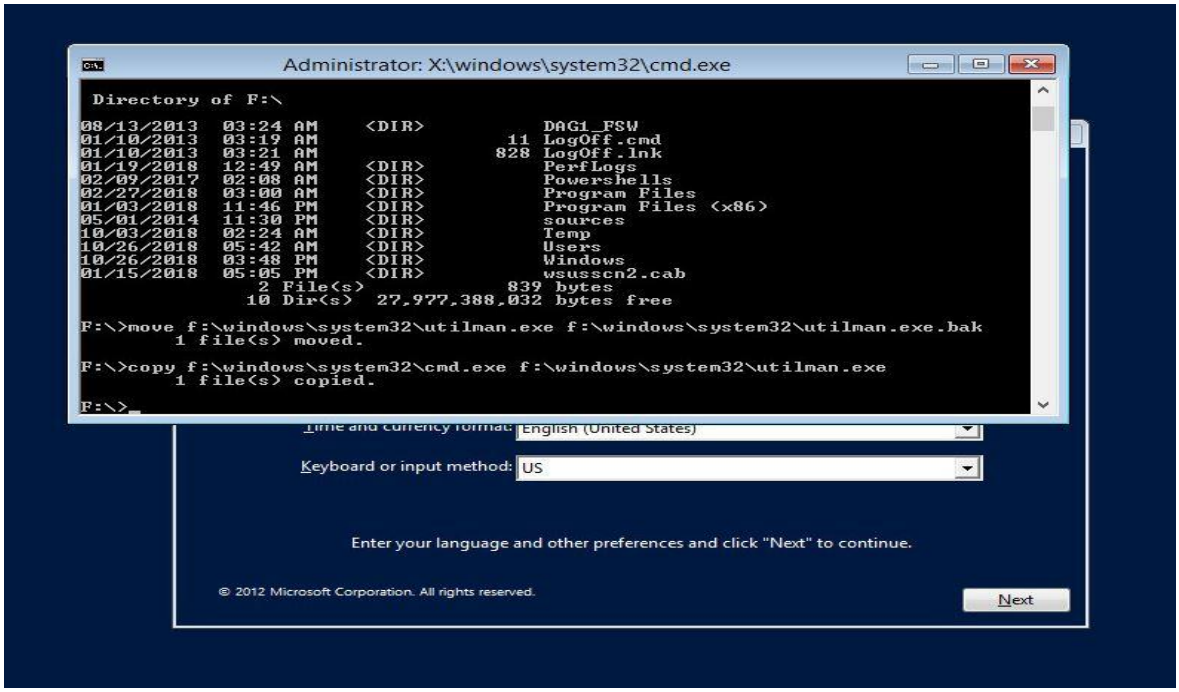
Kuva 3-7



Kuva 3-8

Liite 4. Salasanan haltuunotto käynnistyslevyn avulla

Tässä liitteessä on kuvattu, miten toimialueen salasanan saa otettua haltuun Windows-käynnistyslevyn avulla. Kuvat on numeroitu ja niitä selvennetään kuvatekstein. Windows Setup -ohjelmassa komentokehote käynnistyy näppäimillä ”shift+F10”.

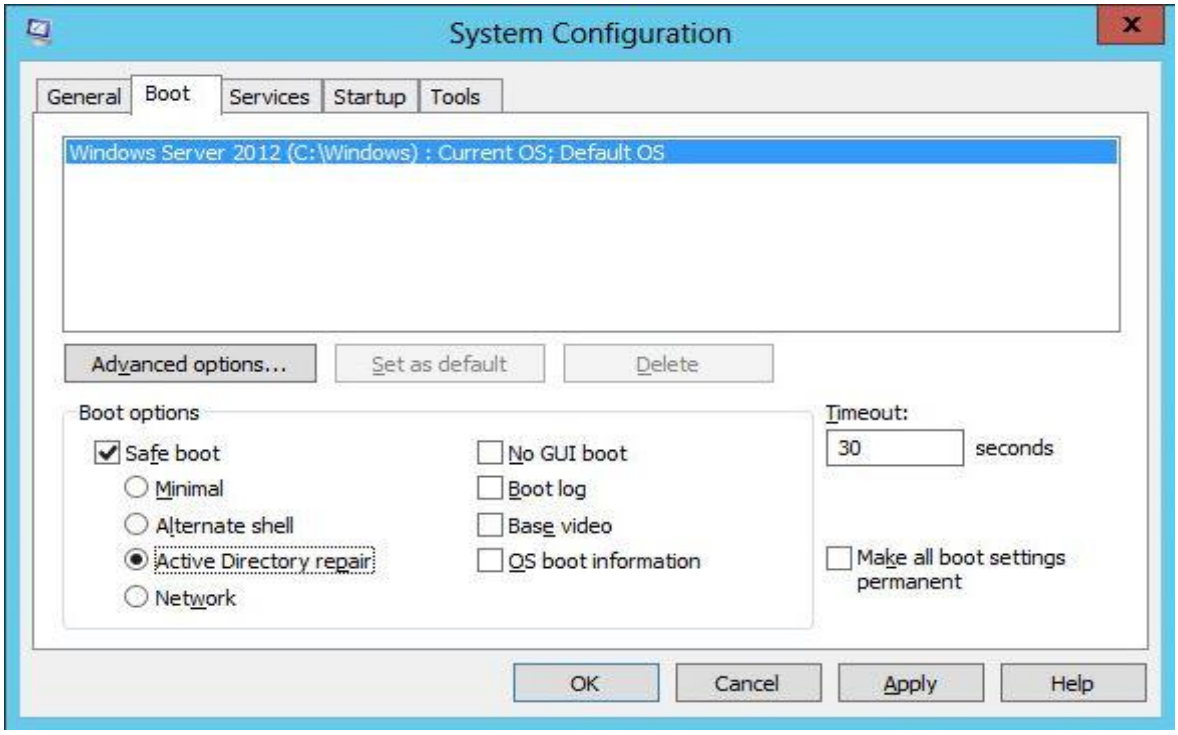


Kuva 4-1 Komentokehotteen kopiointi helppokäyttötyökalujen päälle

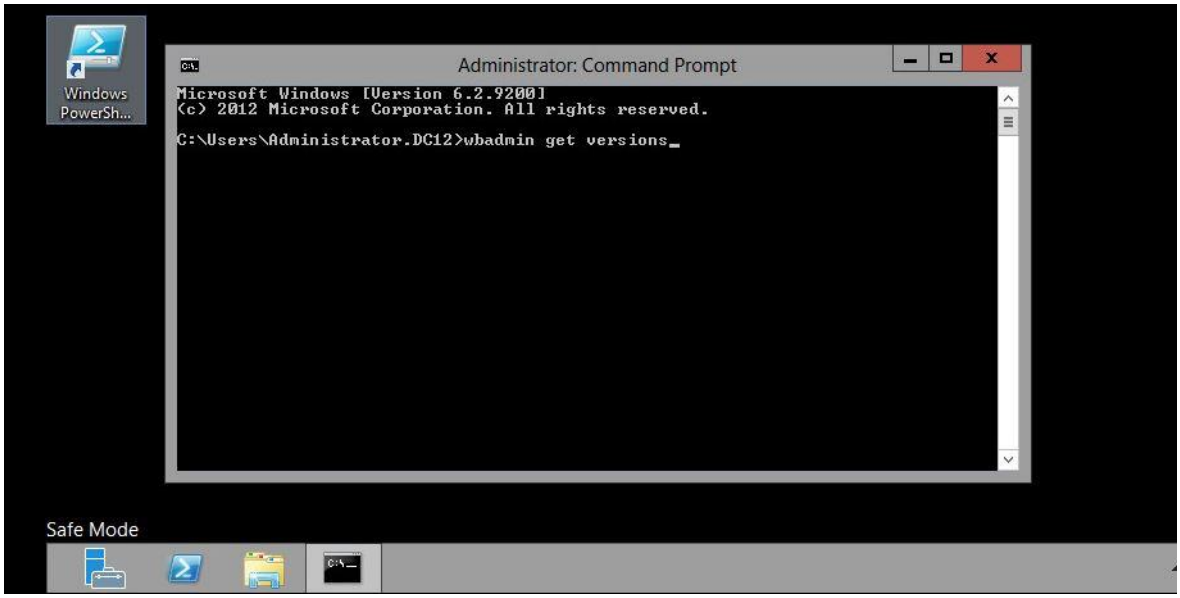
Kuva 4-2 Administrator-salasanan vaihtaminen komennolla ”net user” kirjautumisruudussa.

Liite 5. System State Recovery

Tässä liitteessä on System State Recovery –palautuksen työvaiheet. System State Recovery palauttaa aktiivihakemiston tietokannan varmuuskopiosta. Kuvat on numeroitu ja niissä on seliteteksti.

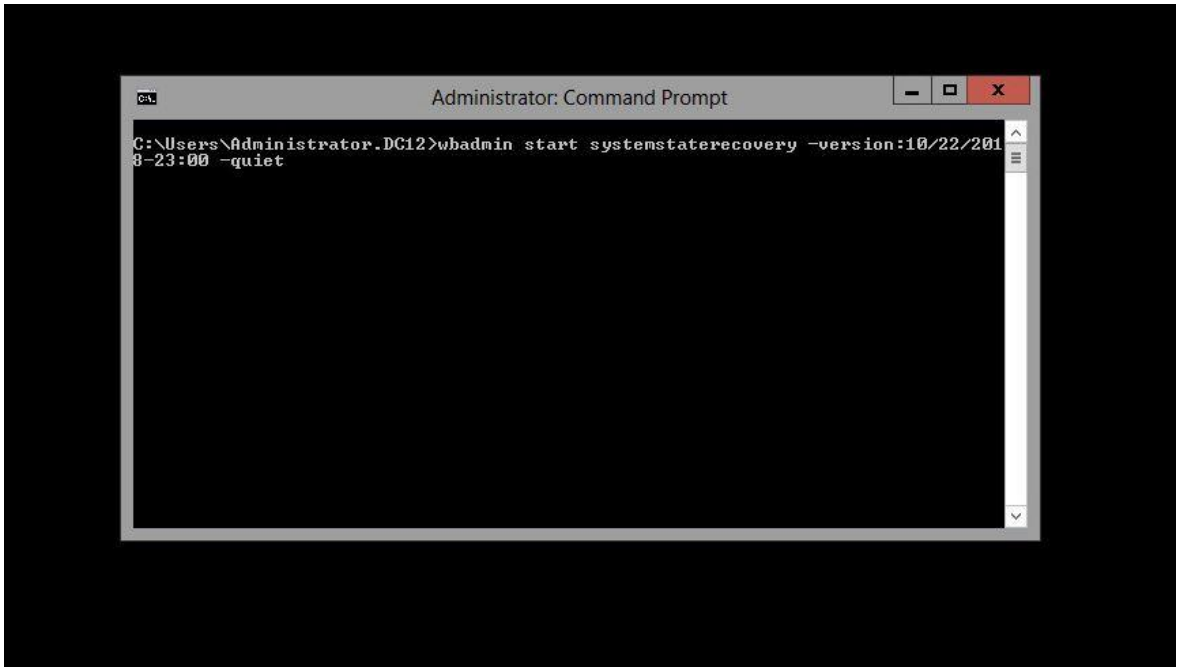


Kuva 5-1 Tietokoneen käynnistäminen Active Directory repair –tilaan System Configuration ikkunassa

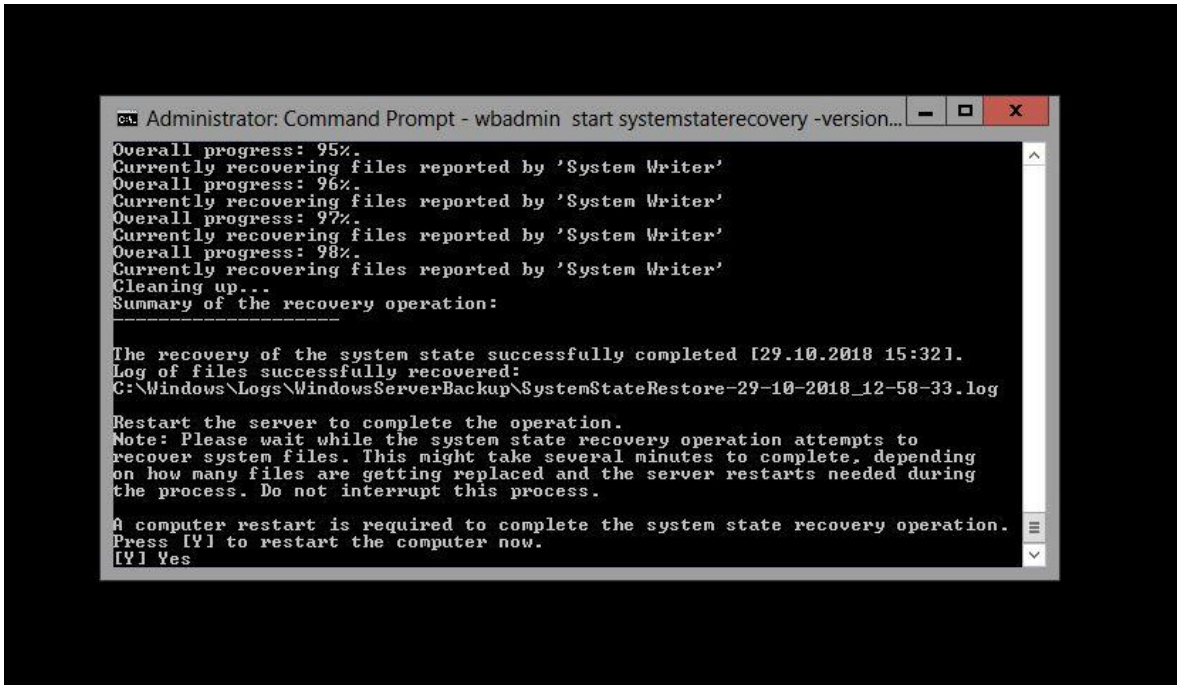


Kuva 5-2 Tallennettujen varmuuskopioversioiden selvittäminen wbadmin-komennolla, joka on varmuuskopiointiin ja palauttamiseen käytettävä komento

Kuvassa 5-3 nähtävälle komennolle annetaan parametrina sen varmuuskopion nimi, josta palauttaminen halutaan suorittaa. Eri versiot selvitettiin edellisessä kuvassa 5-2 näkyvällä komennolla.



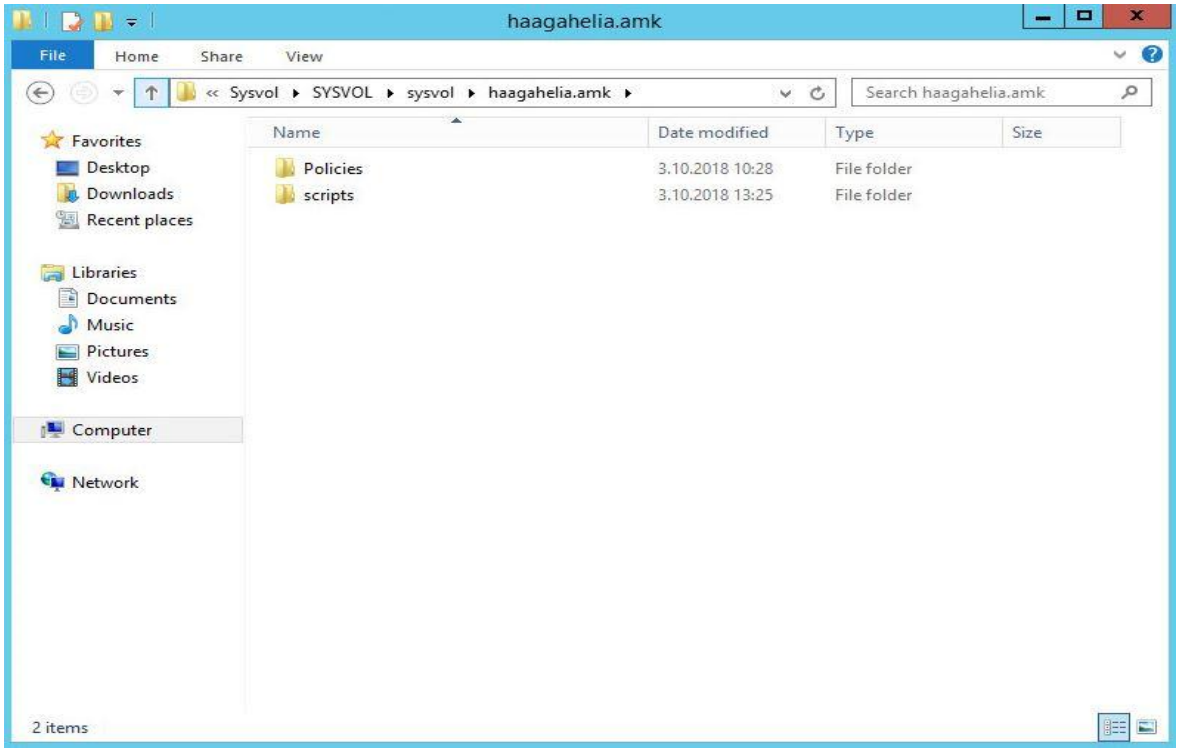
Kuva 5-3 System State Restore –palautuksen aloittaminen komentokehotteella



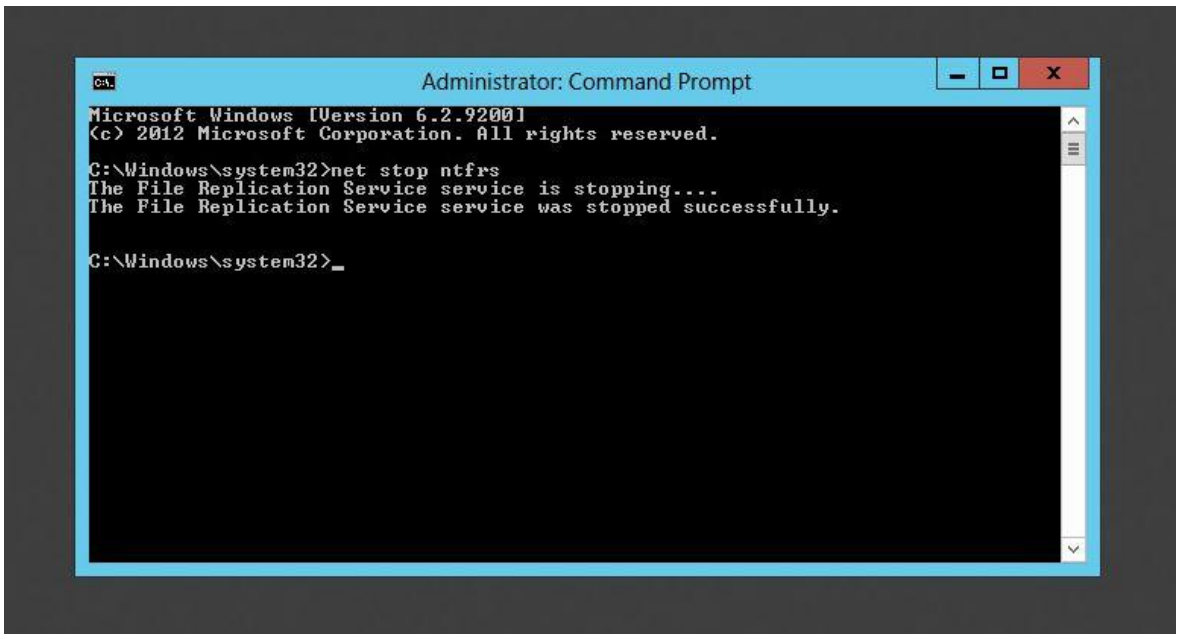
Kuva 5-4 Palautus on onnistunut ja kone täytyy käynnistää uudelleen

Liite 6. SYSVOL authoritative restore

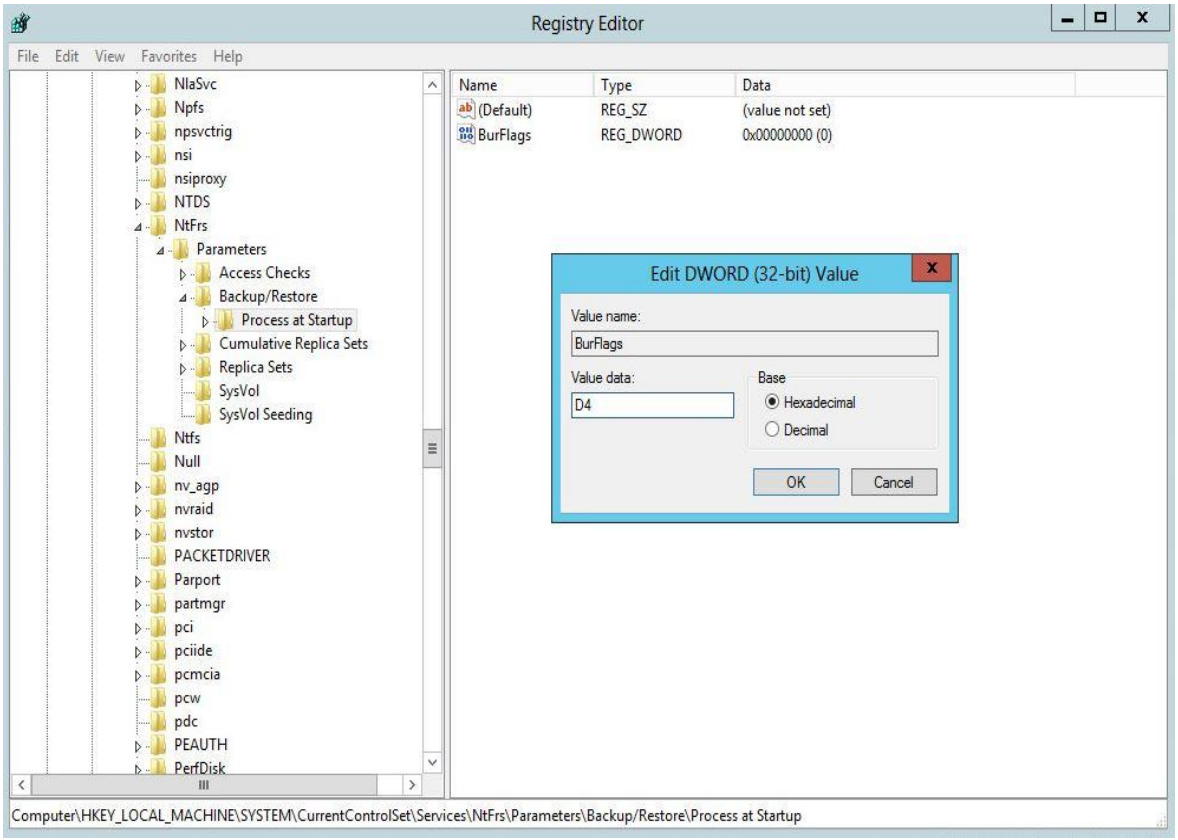
Tässä liitteessä kuvataan SYSVOL-kansion toiminnan palauttamiseen liittyvät työvaiheet. Jotta kansio saadaan System State Recoveryn jälkeen toimimaan, on sille tehtävä ns. authorative restore.



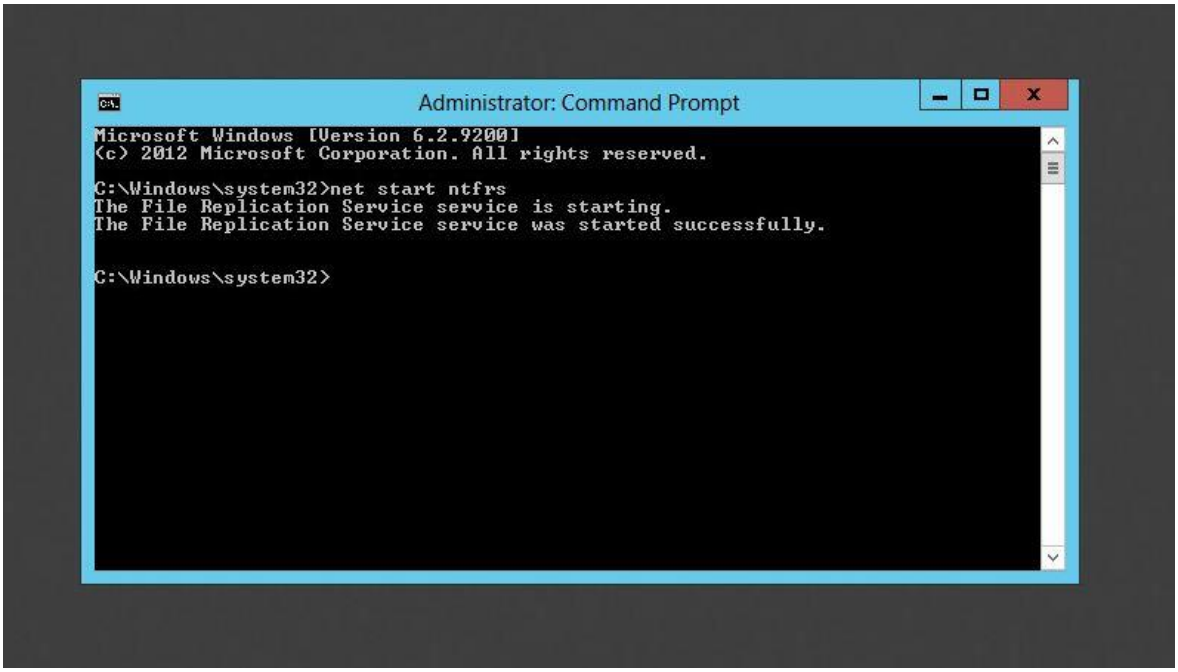
Kuva 6-1 SYSVOL-kansion sisältö



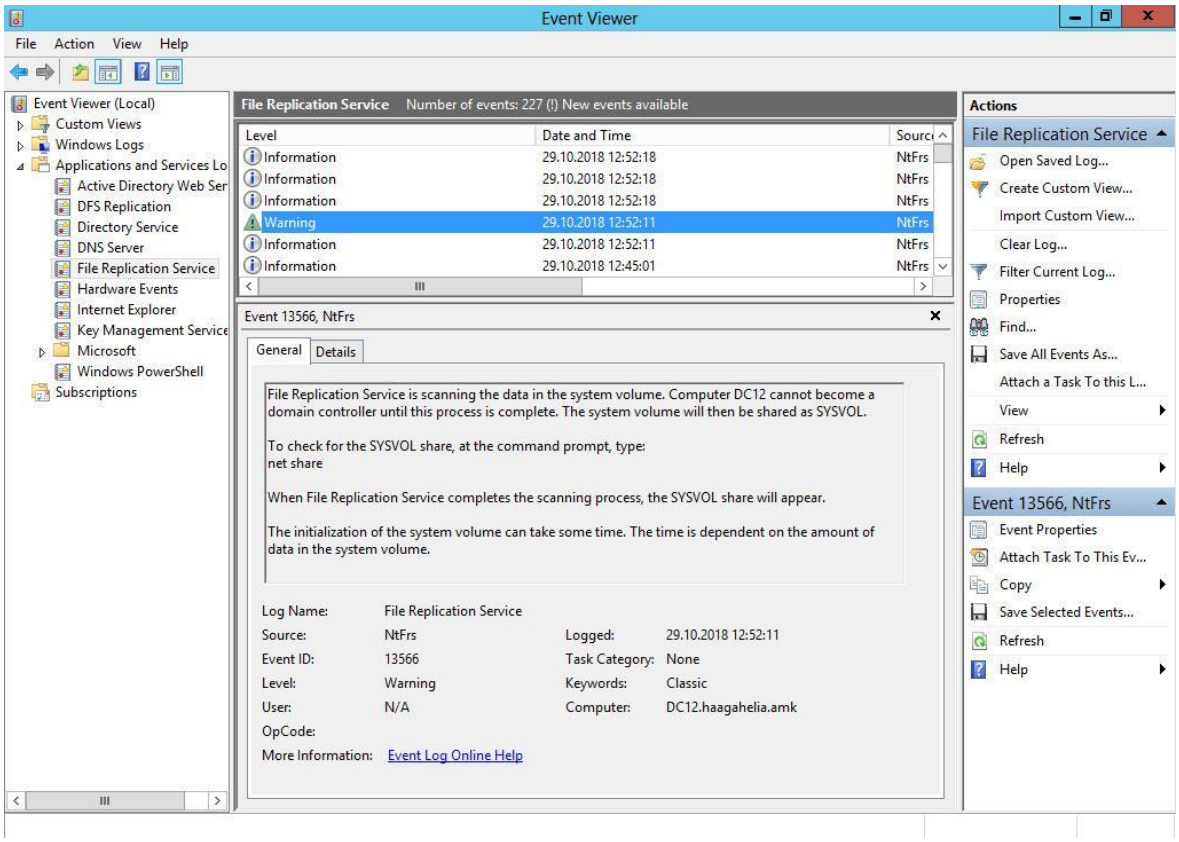
Kuva 6-2 FRS-palvelun pysäyttäminen ennen palautusta



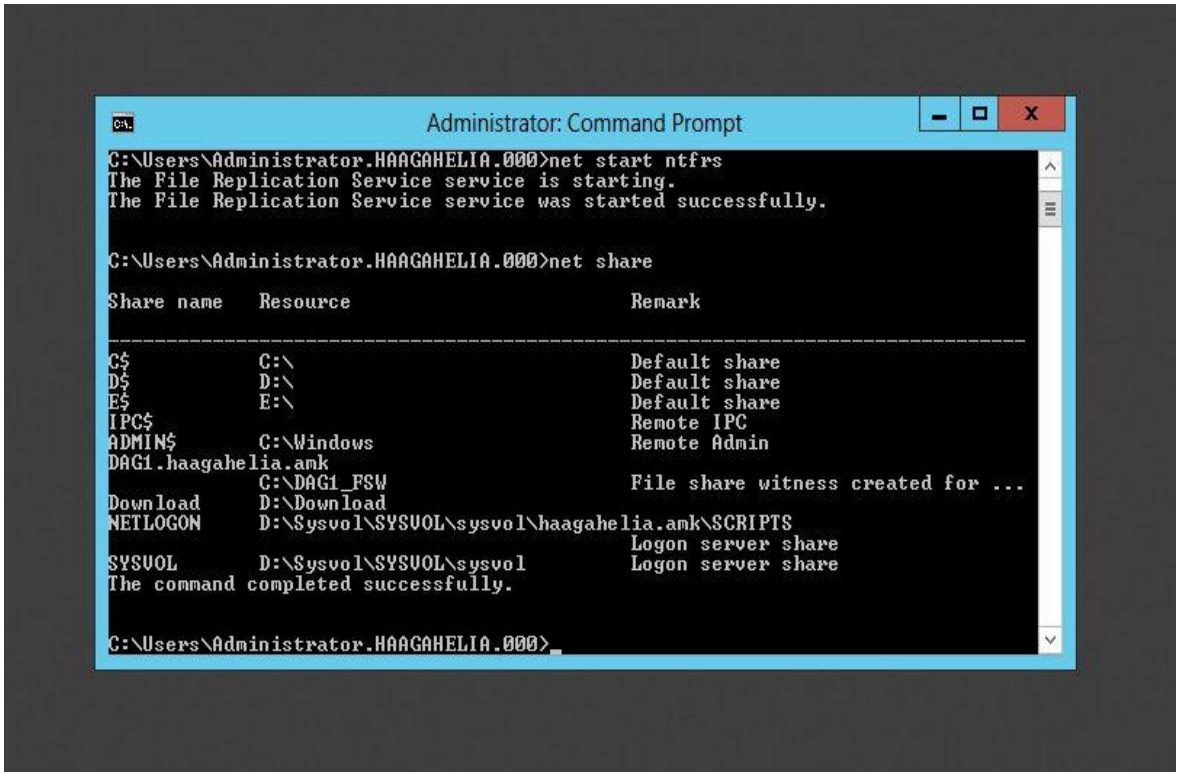
Kuva 6-3 BurFlags-muuttujalle annetaan rekisterissä arvo ”D4”, joka merkitys on ”authorative”. Osoite rekisterissä on nähtävissä alareunassa.



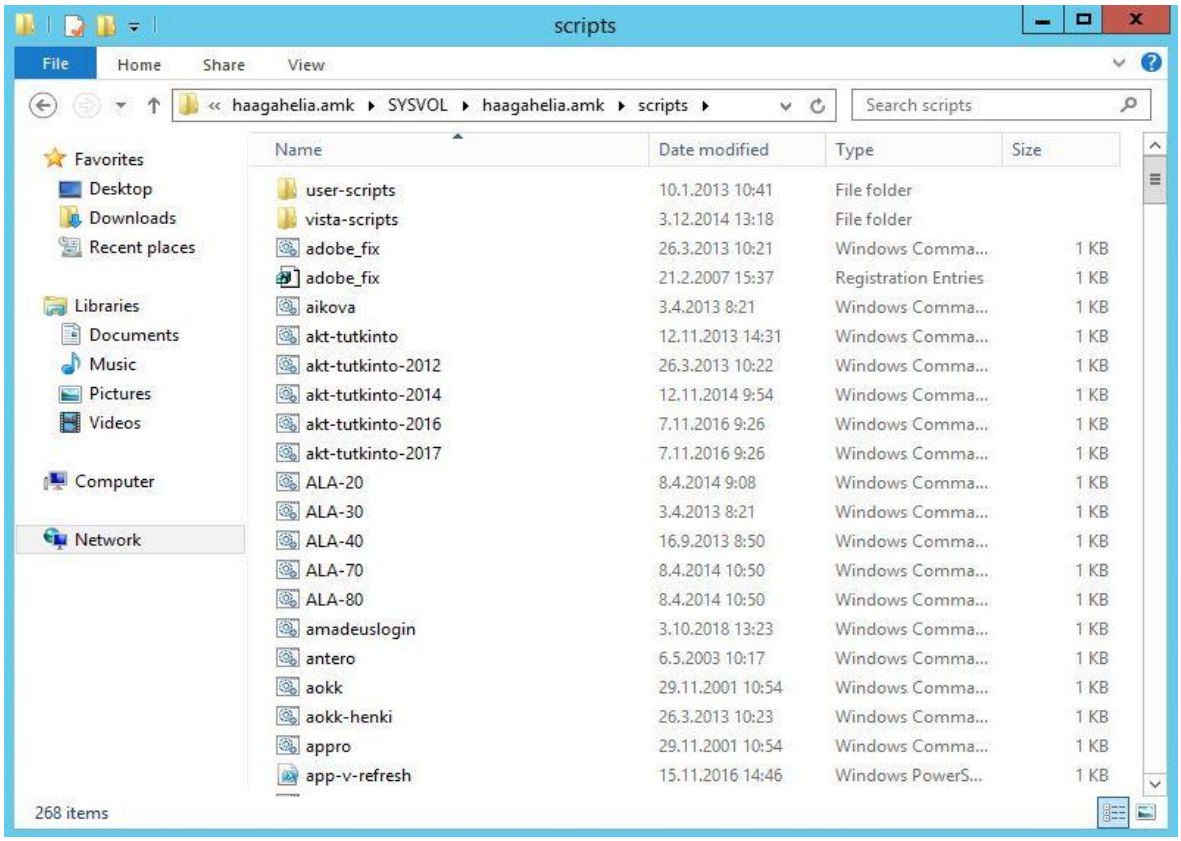
Kuva 6-4 Rekisterimuutosten jälkeen replikointi kytketään takaisin päälle



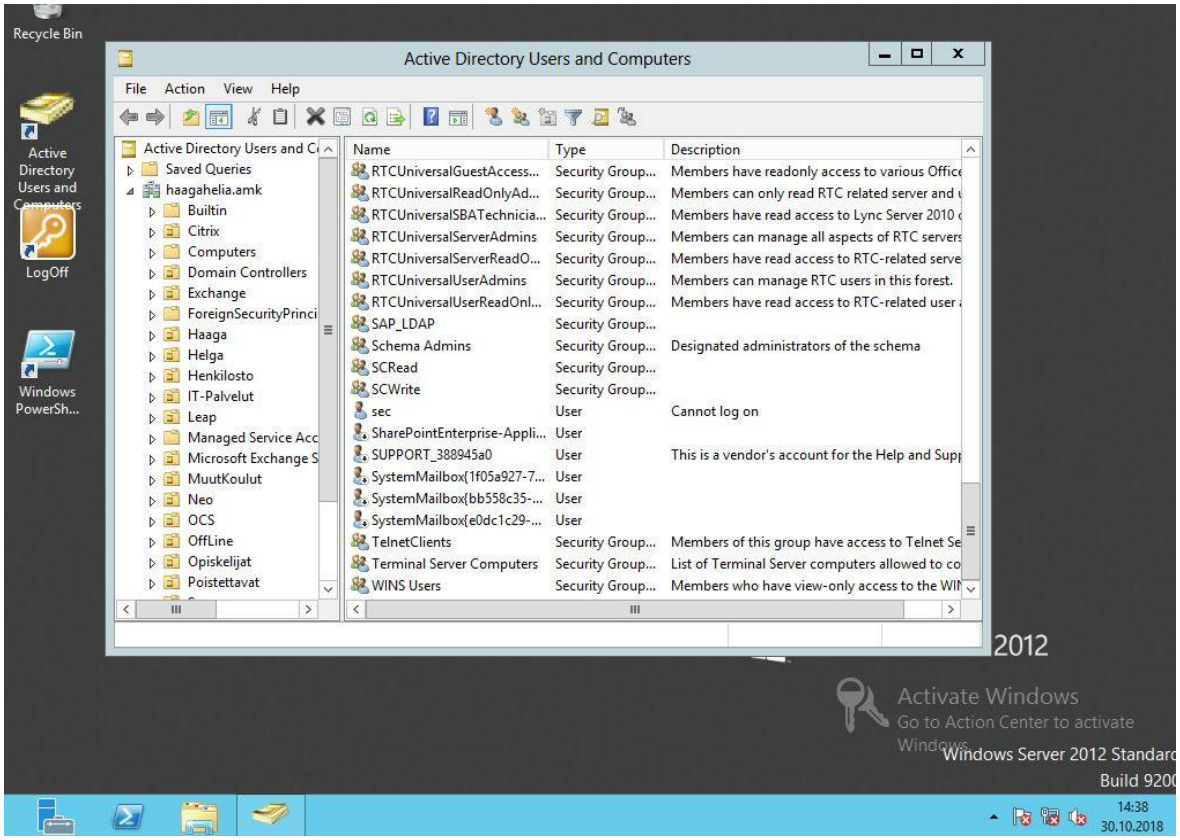
Kuva 6-5 Muutosten voimaantuleminen kestää hetken ja Event Viewer varoittaa tästä



Kuva 6-6 Käytettävä SYSVOL-kansio voidaan tarkastaa komennolla ”net share”



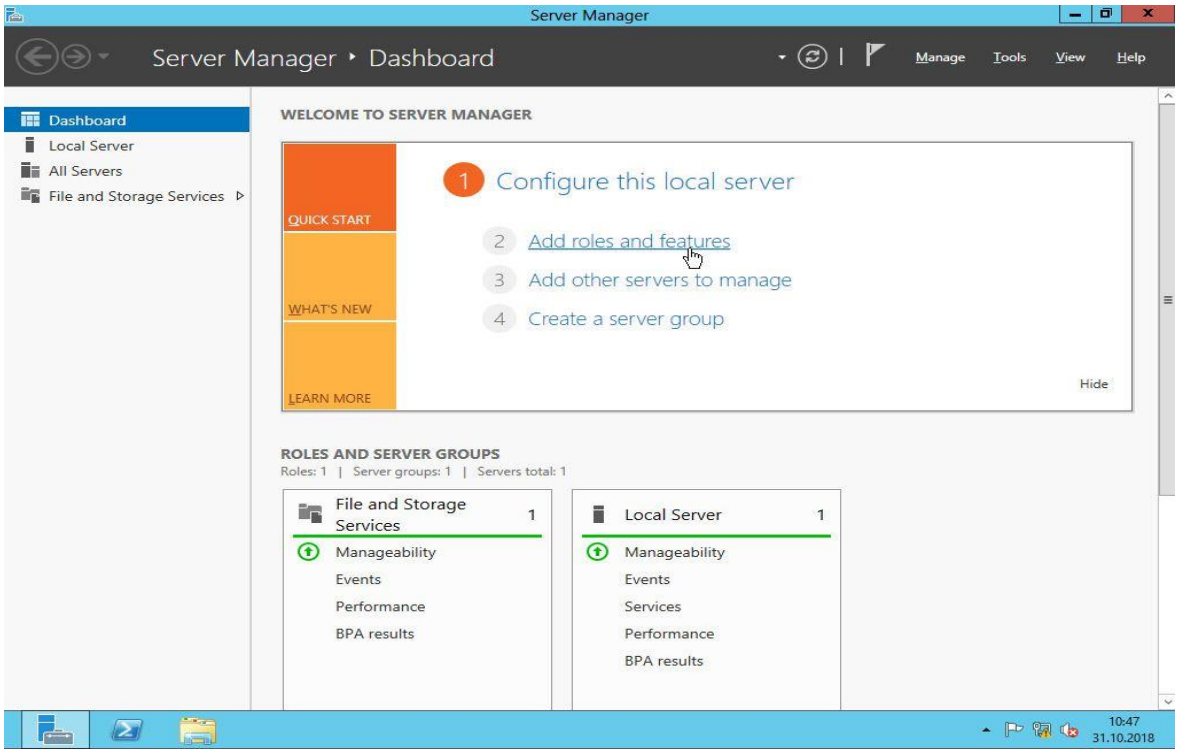
Kuva 6-7 Työvaiheiden jälkeen SYSVOL-kansiossa näkyy tiedostoja



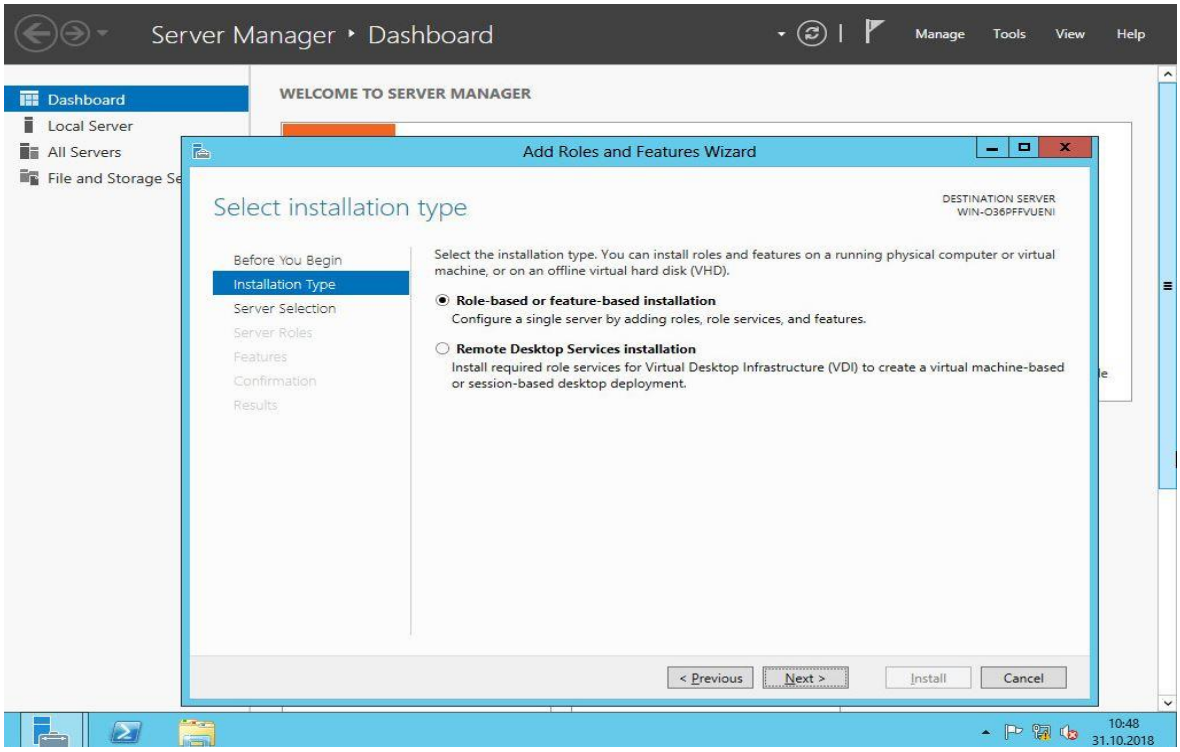
Kuva 6-8 Lopuksi on tarkistettava, että aktiivihakemisto aukeaa ja toimii normaalisti

Liite 7. AD DS –palveluiden asentaminen ohjauskoneelle

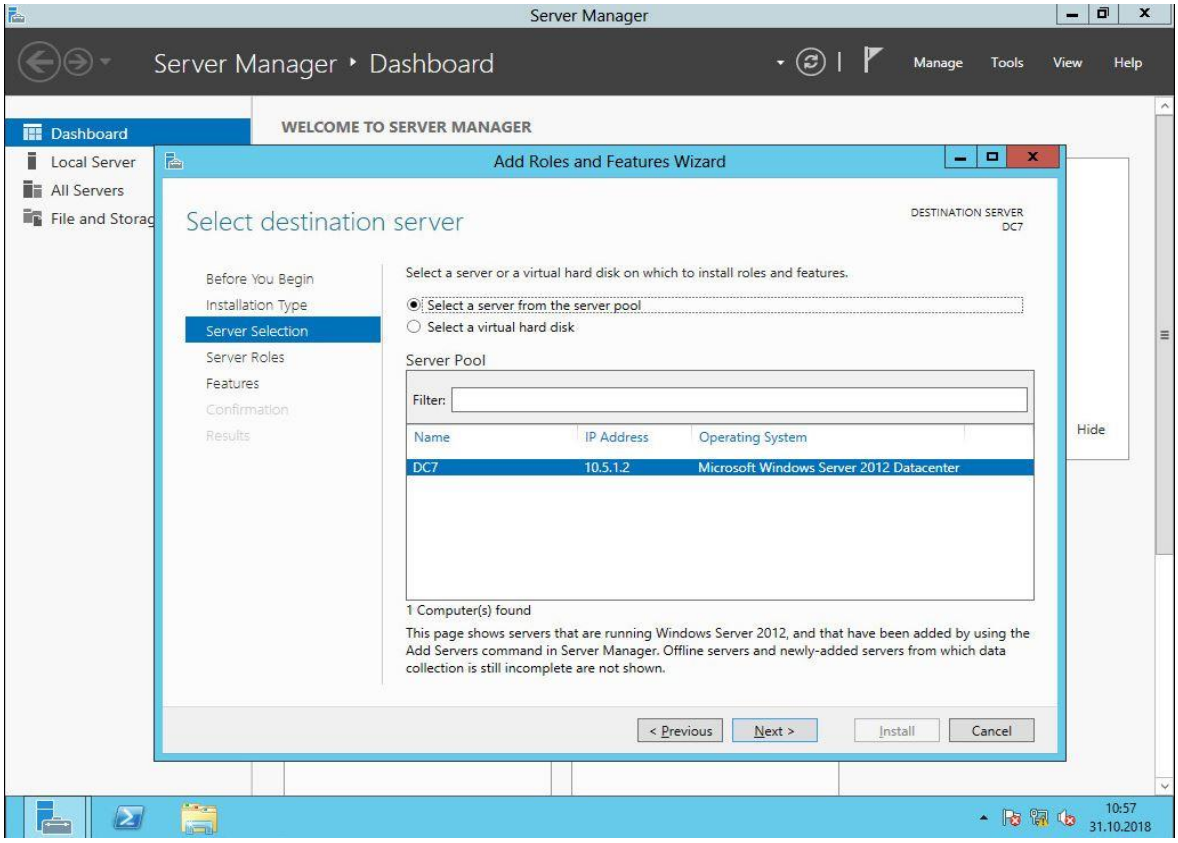
Aktiivihakemistoroolin asentaminen ohjauskoneelle on helppoa asennusvelhon avulla. Tässä liitteessä ovat ruutukaappaukset tarvittavista asetuksista.



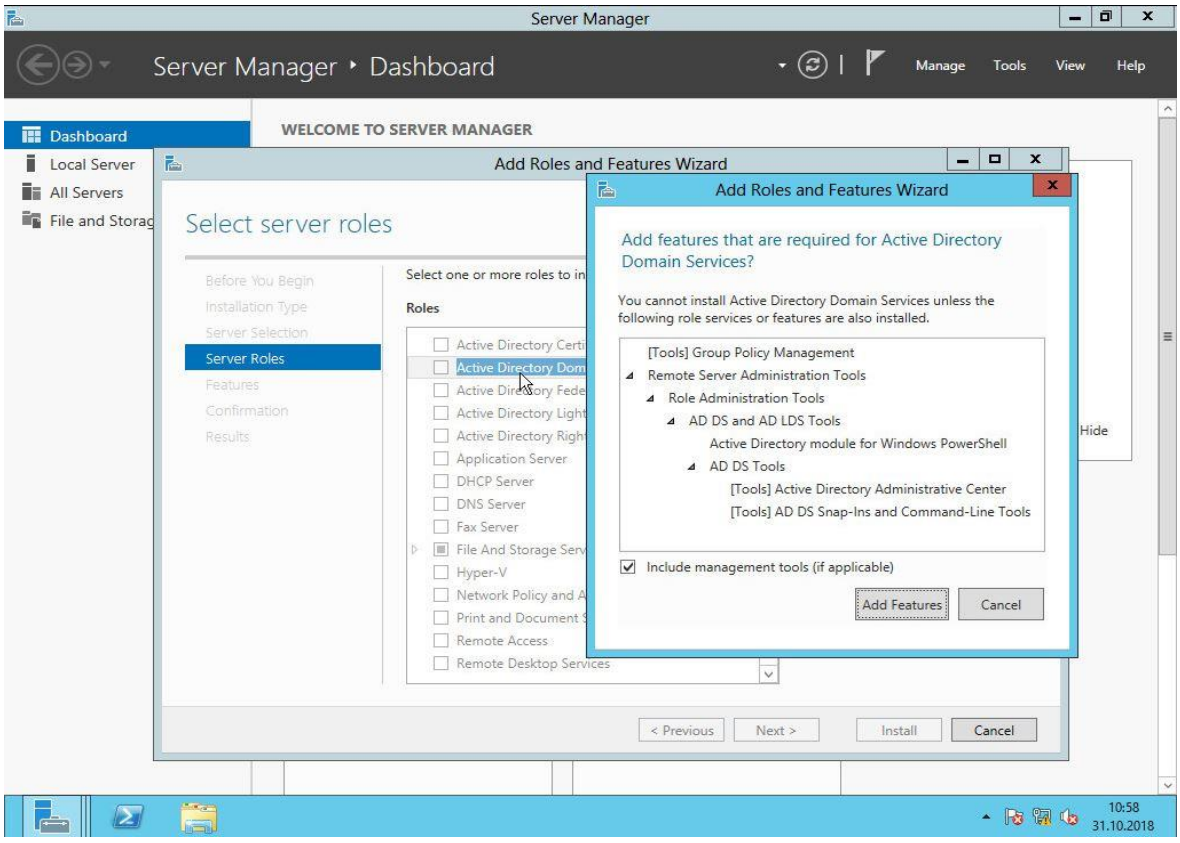
Kuva 7-1



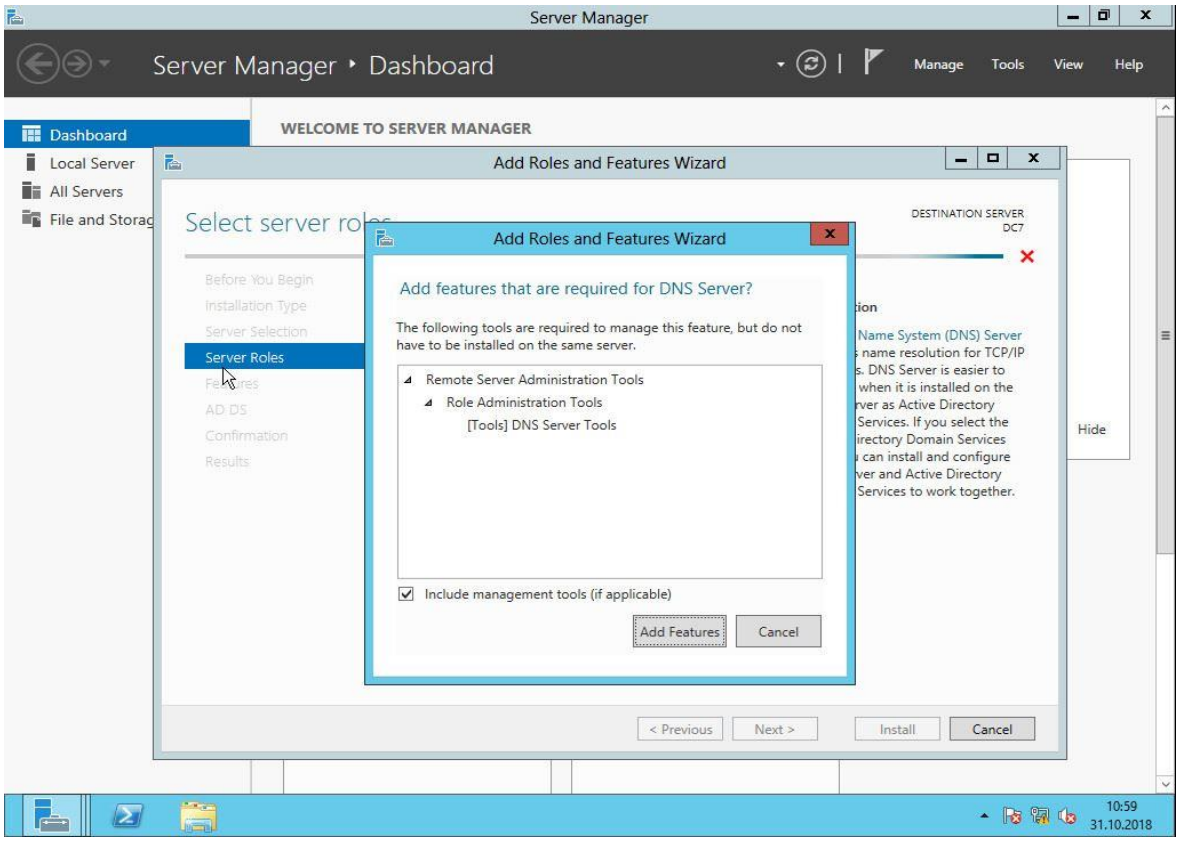
Kuva 7-2



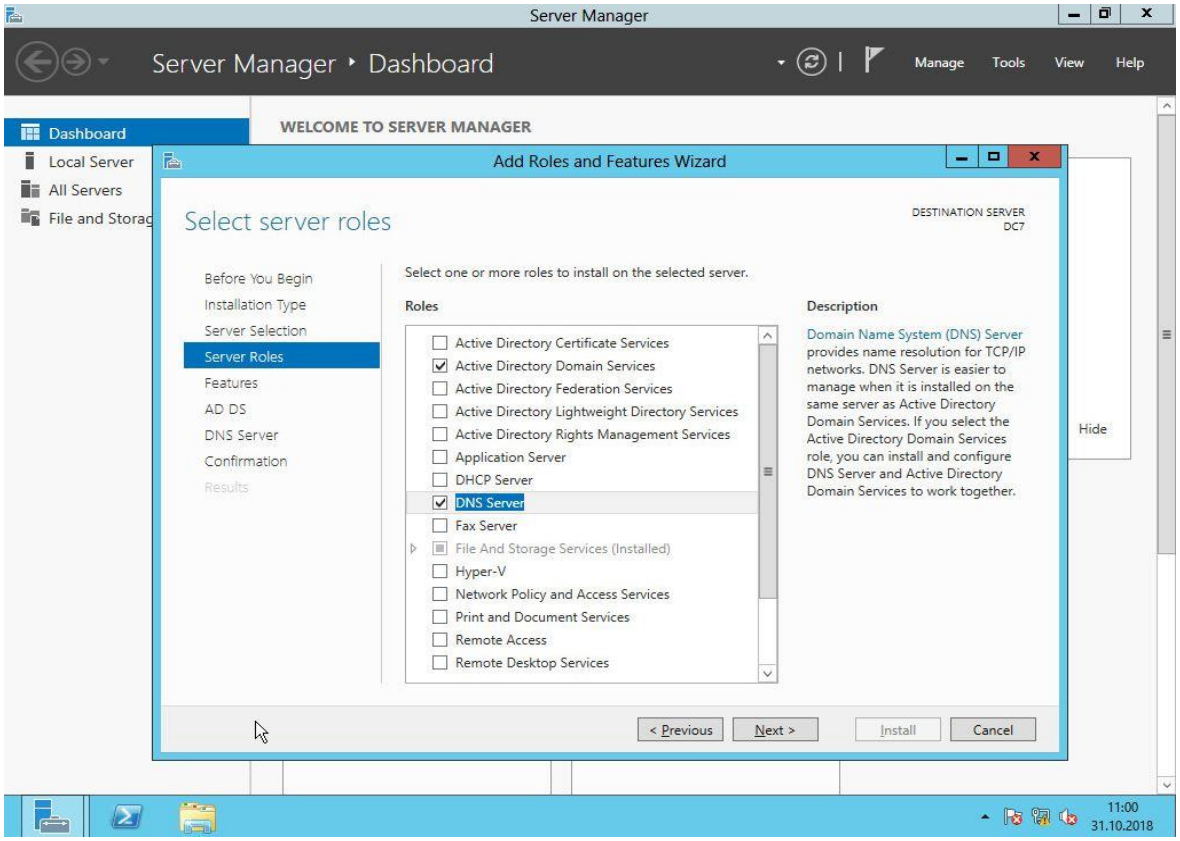
Kuva 7-3



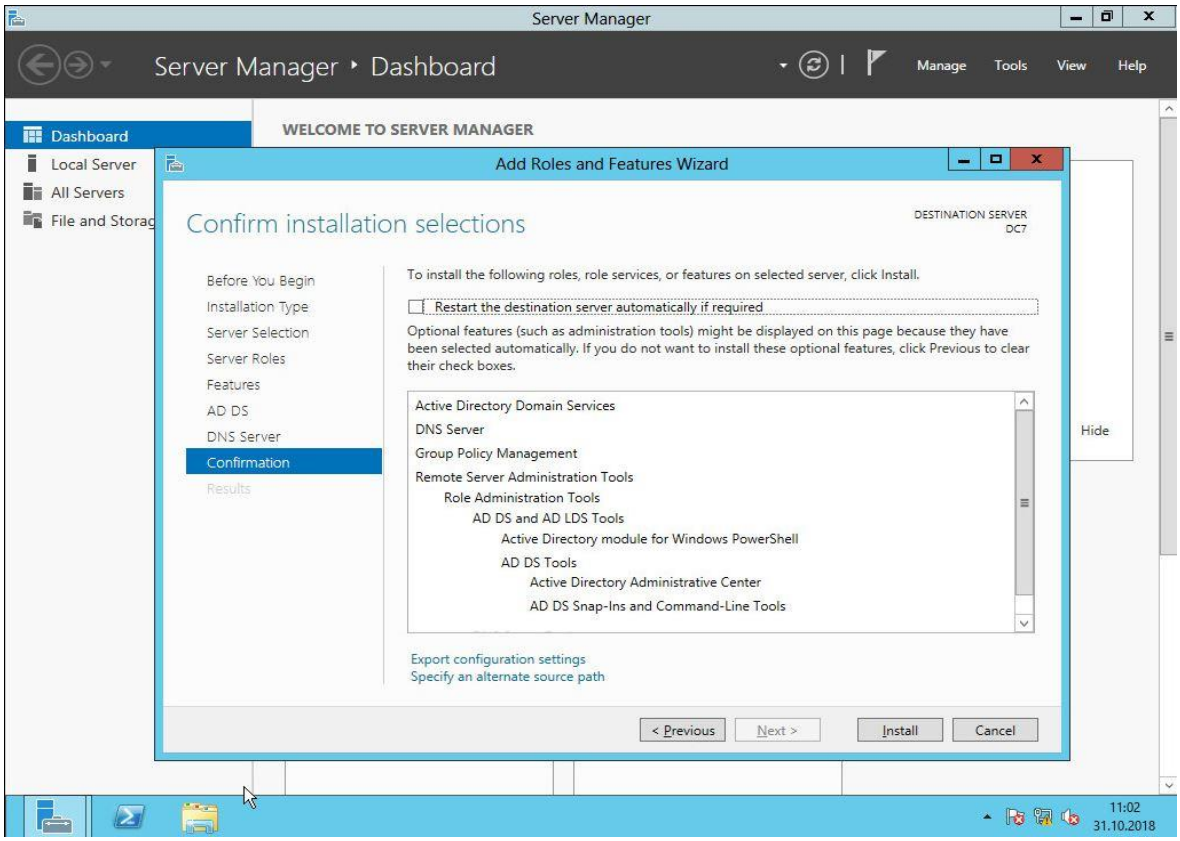
Kuva 7-4



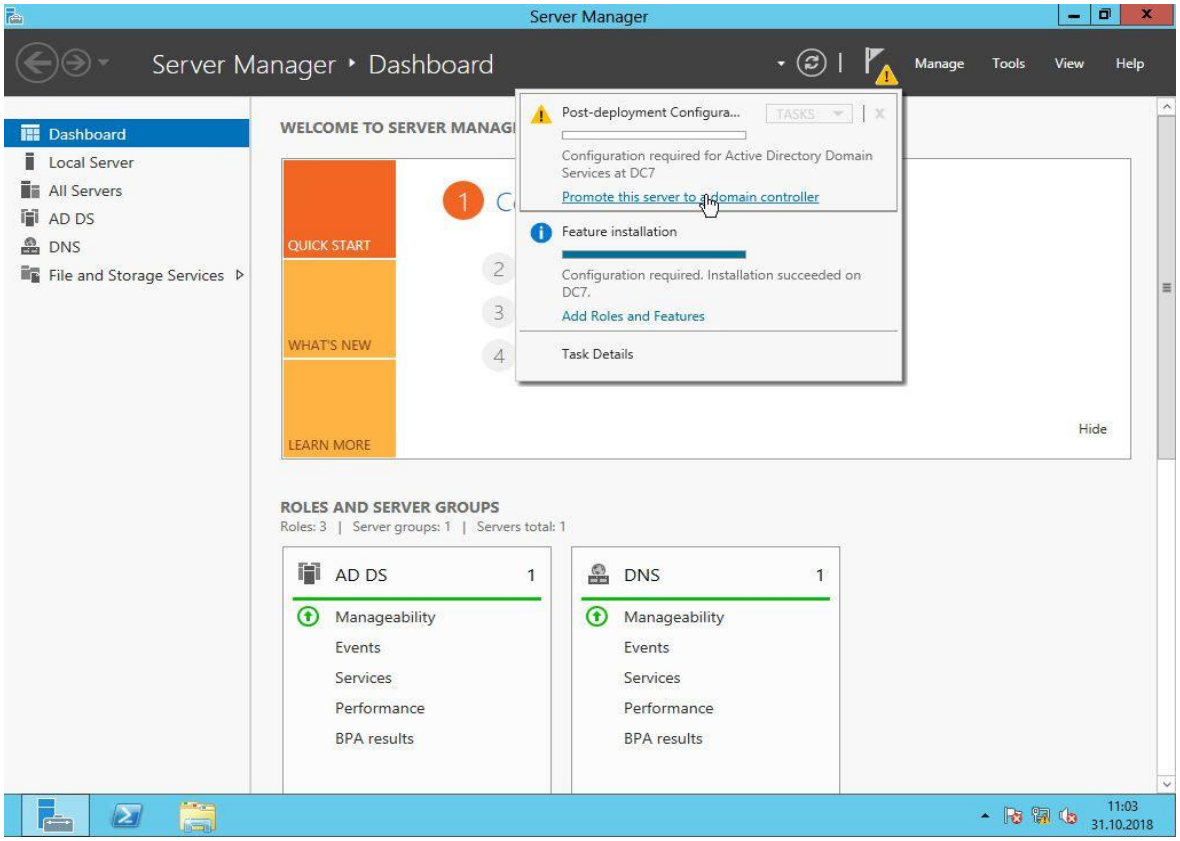
Kuva 7-5



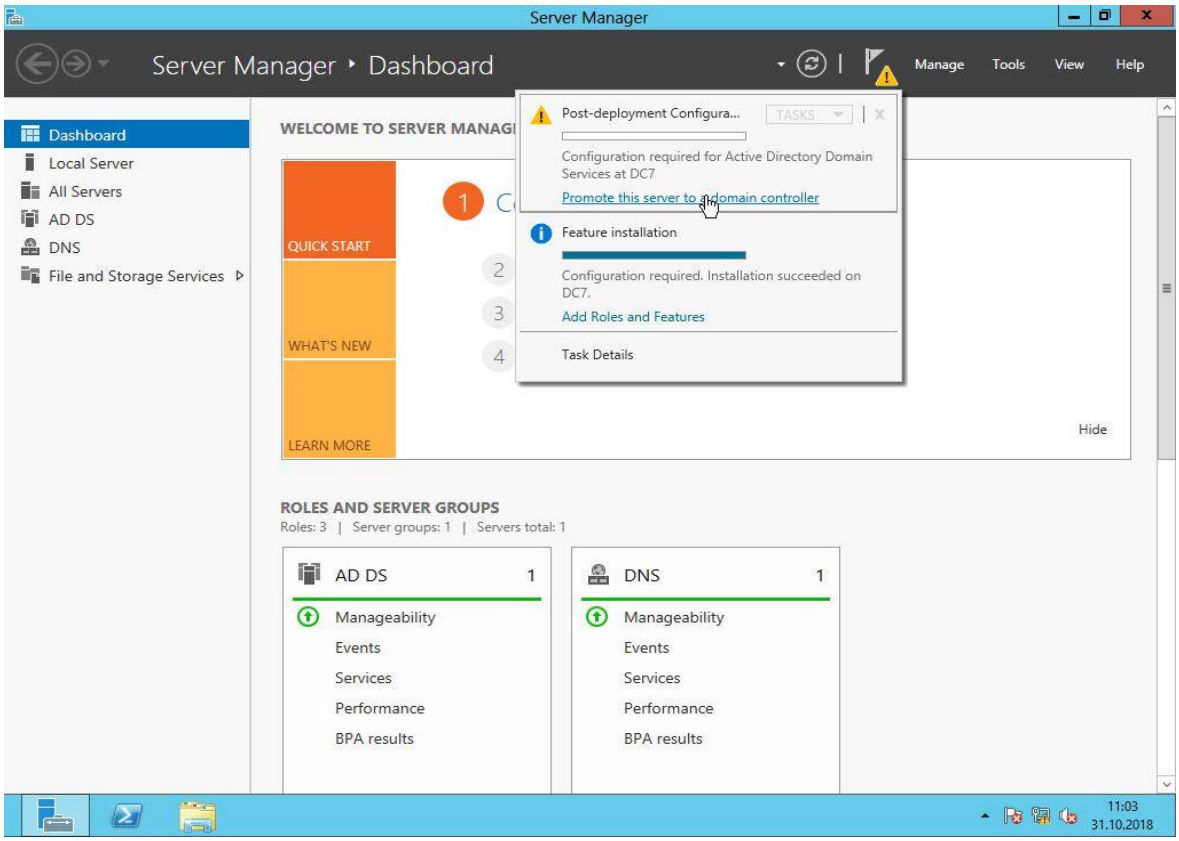
Kuva 7-6



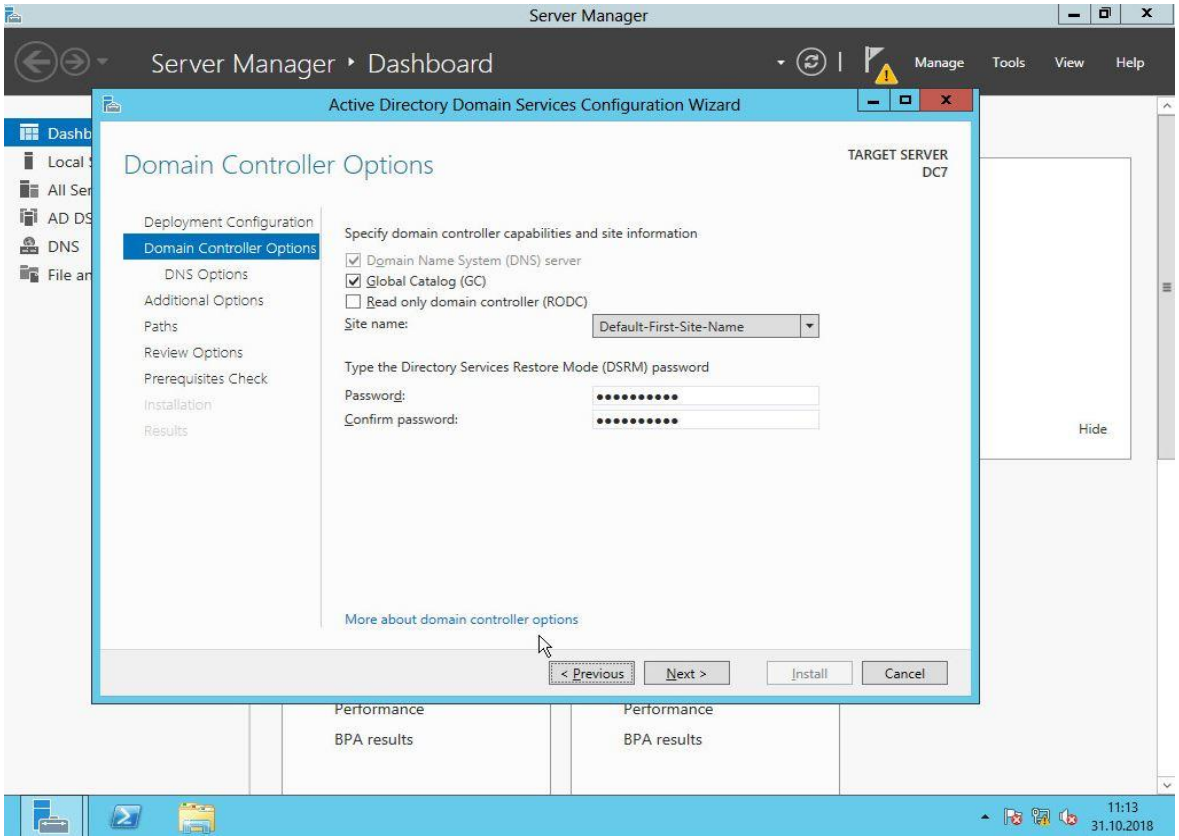
Kuva 7-7



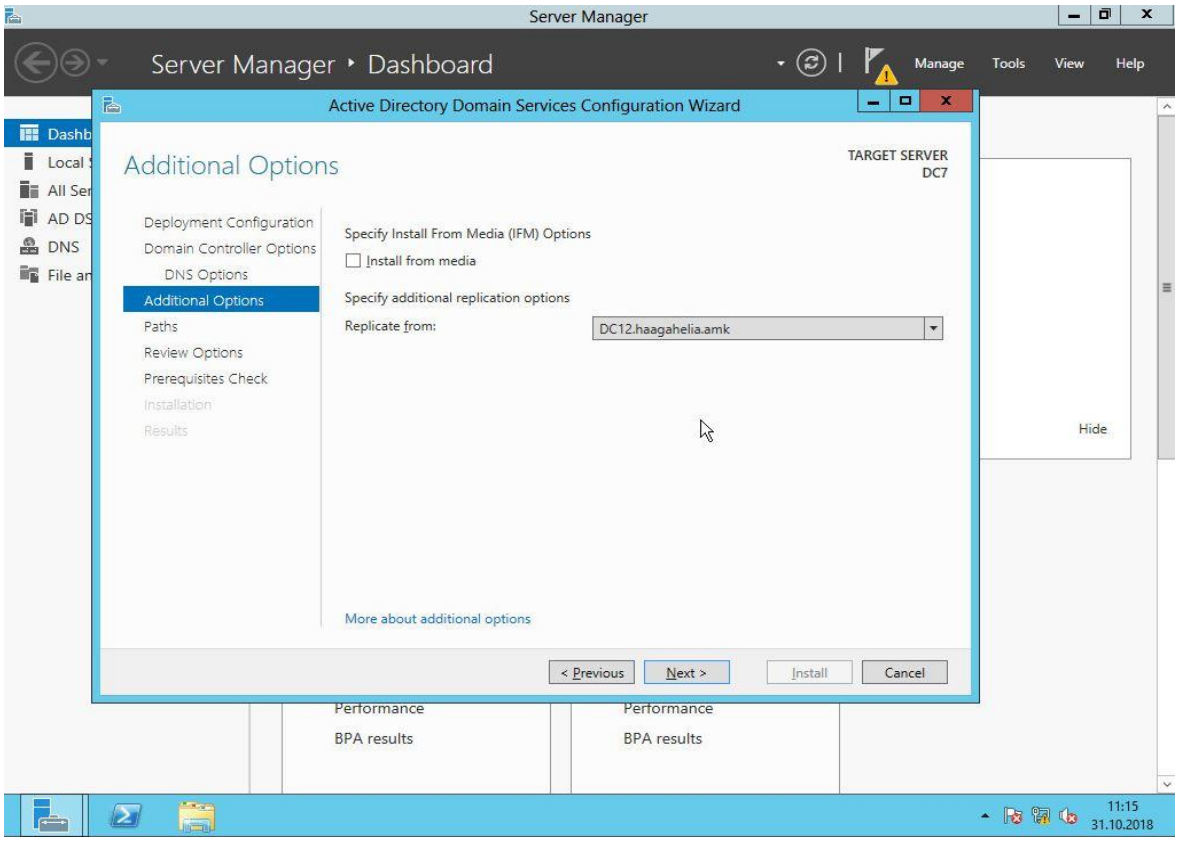
Kuva 7-8



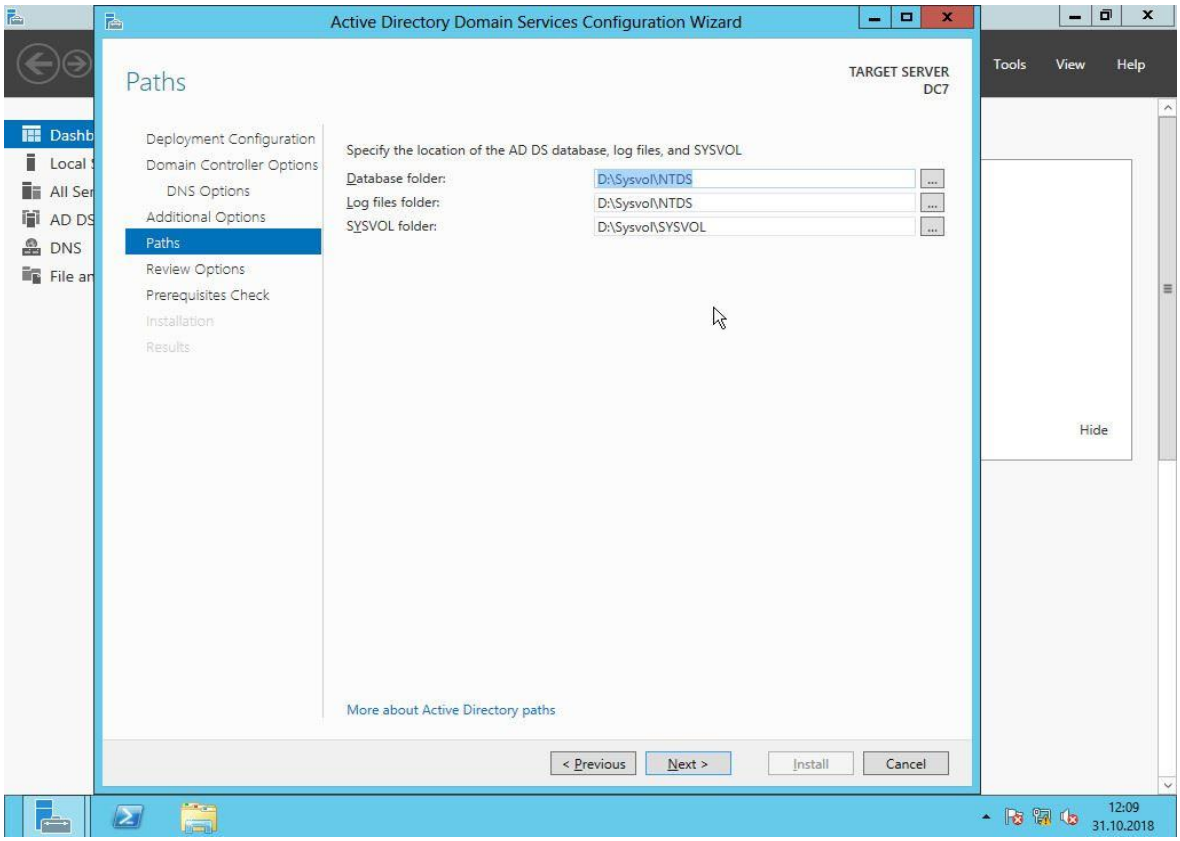
Kuva 7-9



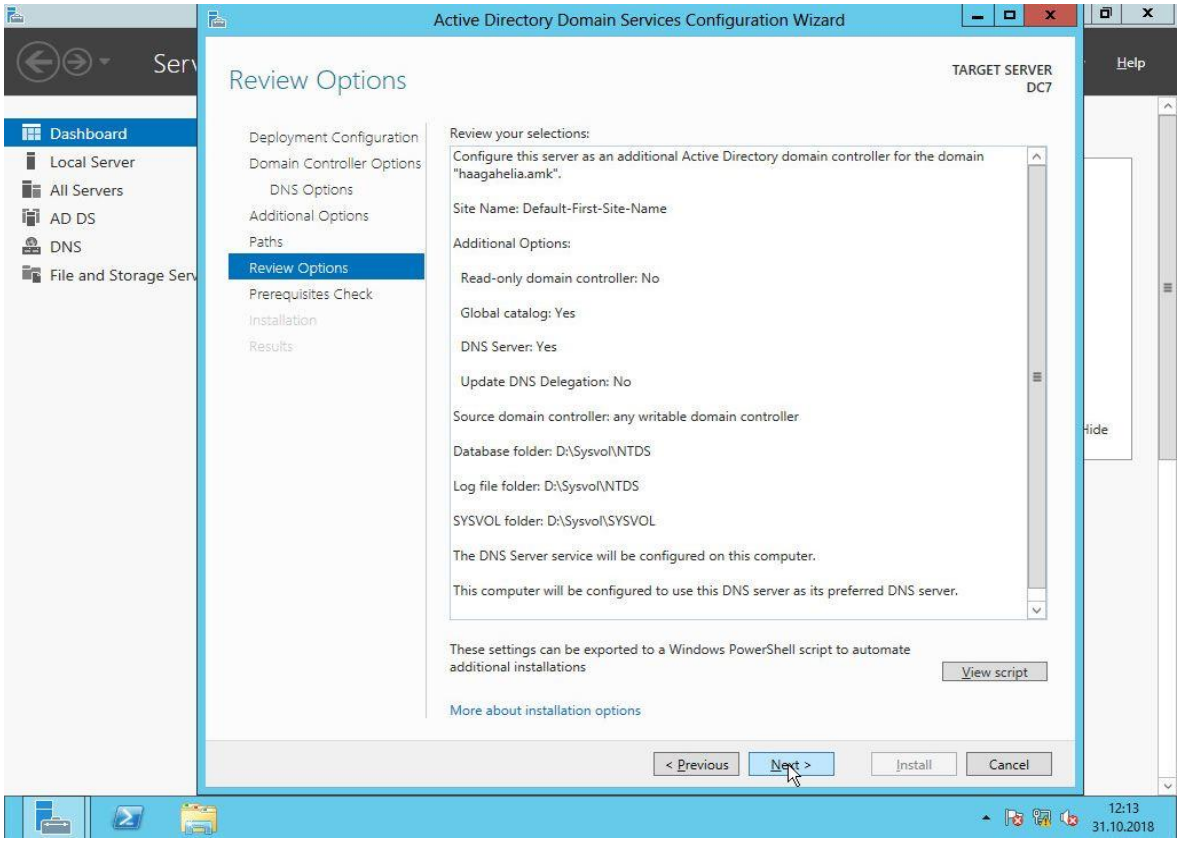
Kuva 7-10



Kuva 7-11



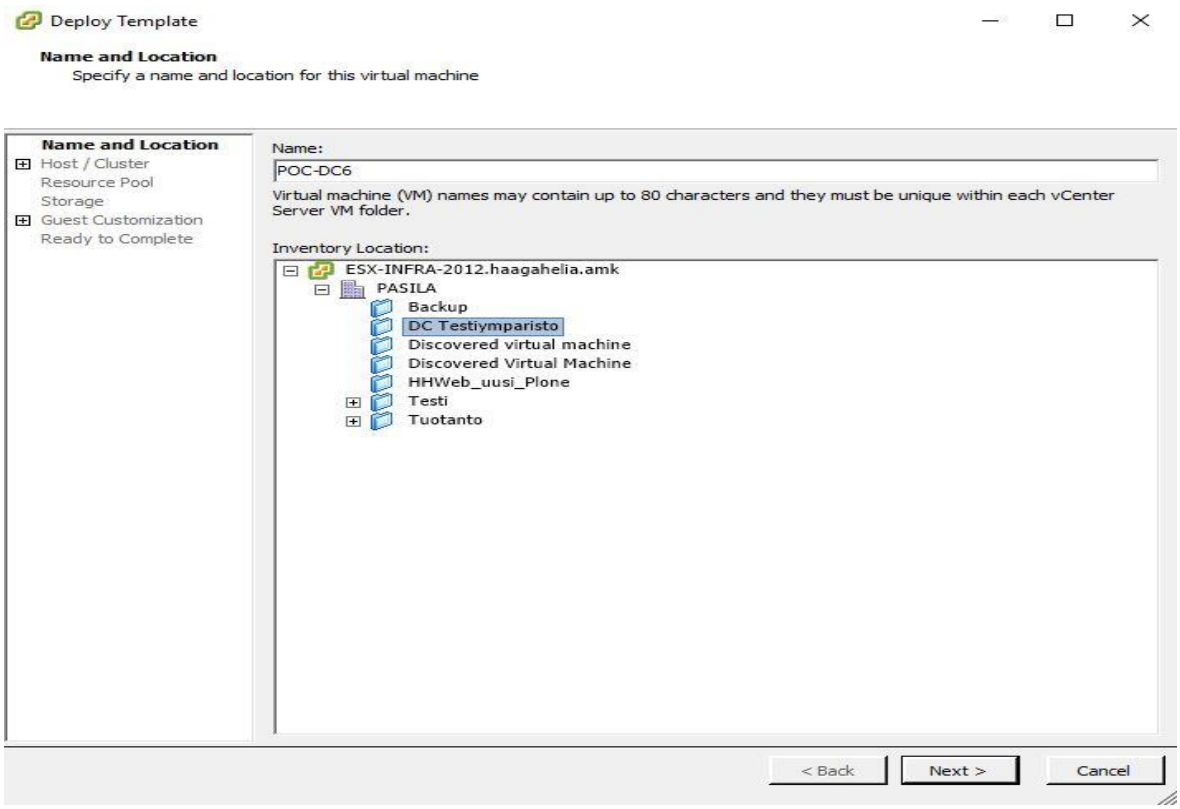
Kuva 7-12


Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
DC7
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Configure this server as an additional Active Directory domain controller for the domain "haagahelia.amk".
Site Name: Default-First-Site-Name
Additional Options:
Read-only domain controller: No
Global catalog: Yes
DNS Server: Yes
Update DNS Delegation: No
Source domain controller: any writable domain controller
Database folder: D:\Sysvol\NTDS
Log file folder: D:\Sysvol\NTDS
SYSVOL folder: D:\Sysvol\SYSVOL
The DNS Server service will be configured on this computer.
This computer will be configured to use this DNS server as its preferred DNS server.
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options
< Previous
Next >
Install
Cancel
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Serv
Help
12:13
31.10.2018

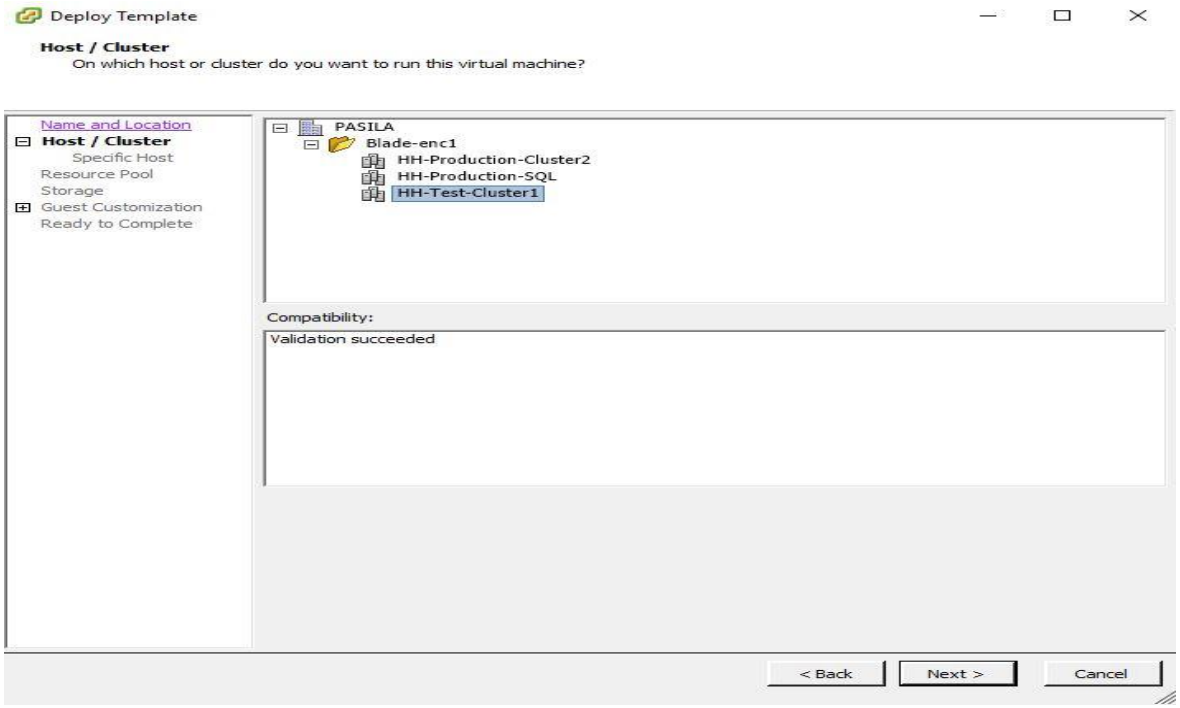
Kuva 7-13

Liite 8. Virtuaalikoneen luominen valmiin pohjan avulla

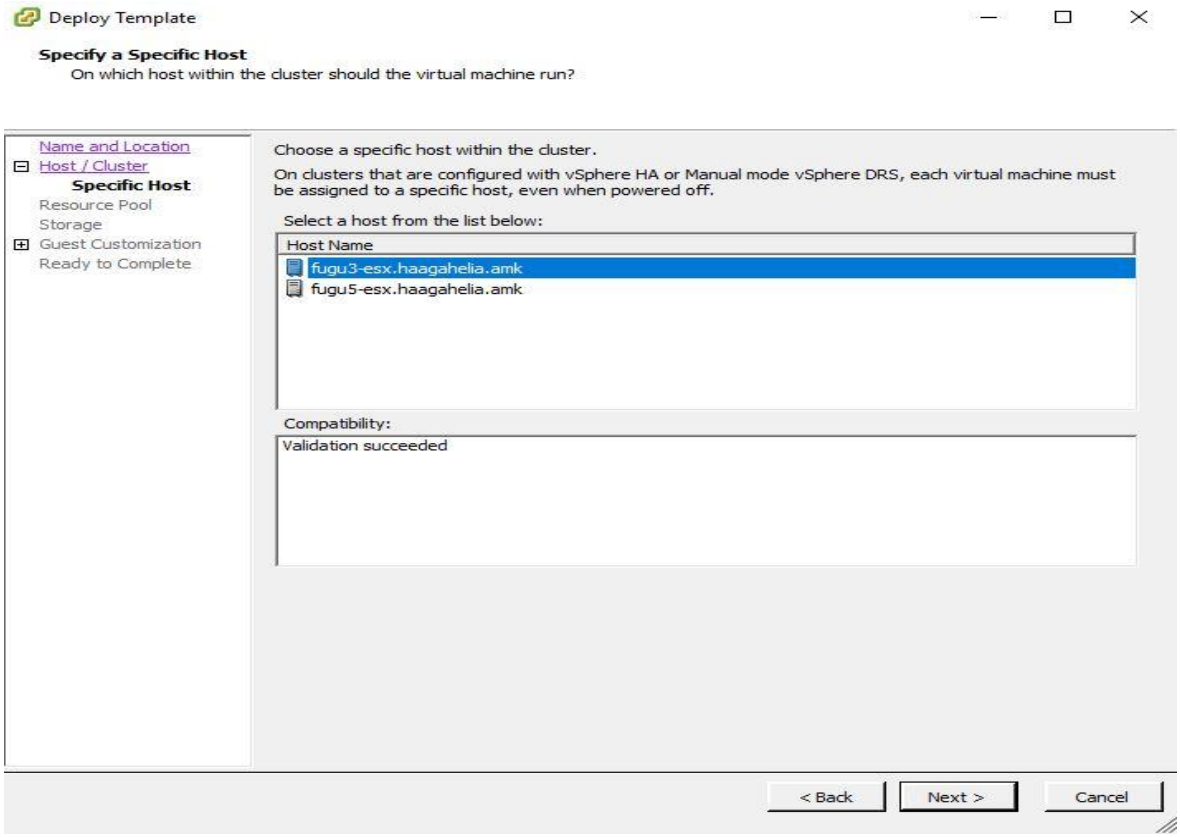
Tässä liitteessä on kuvattu työvaiheet, joiden avulla luodaan virtuaalipalvelin valmiista pohjasta vSphere-ympäristössä.



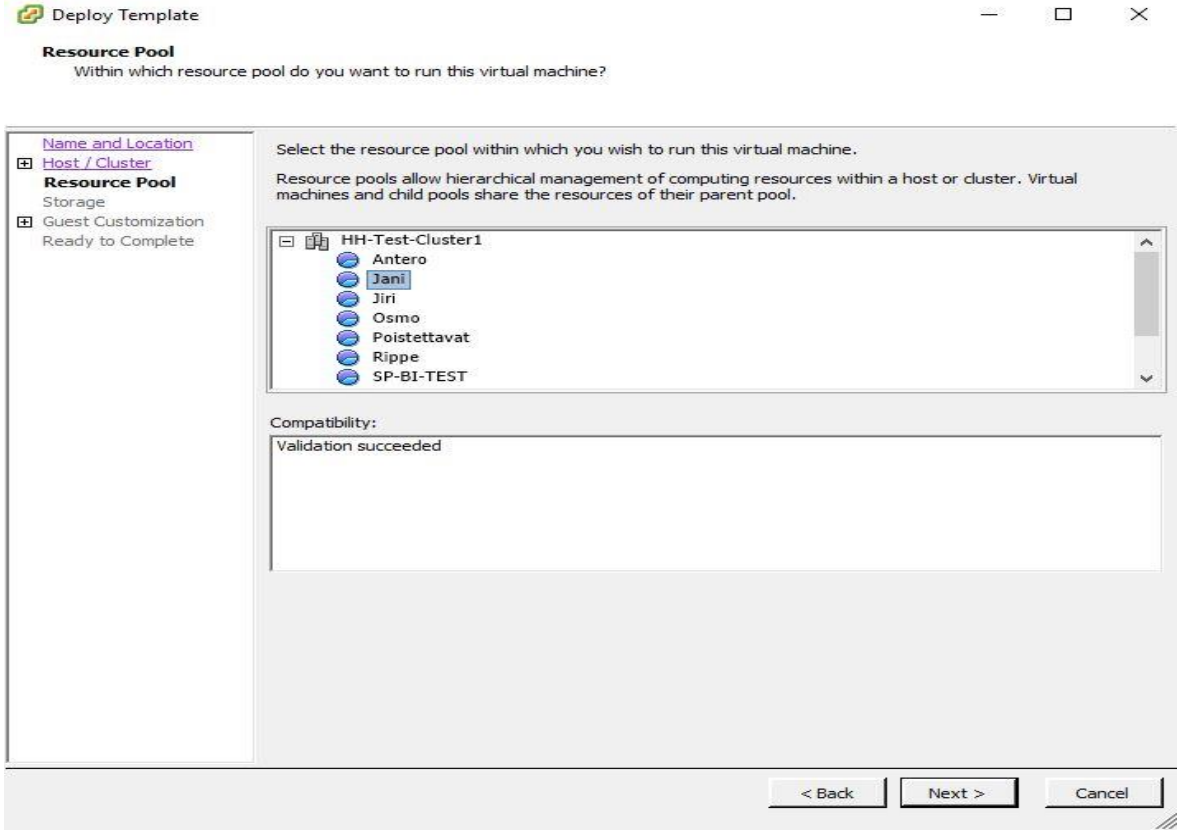
Kuva 8-1



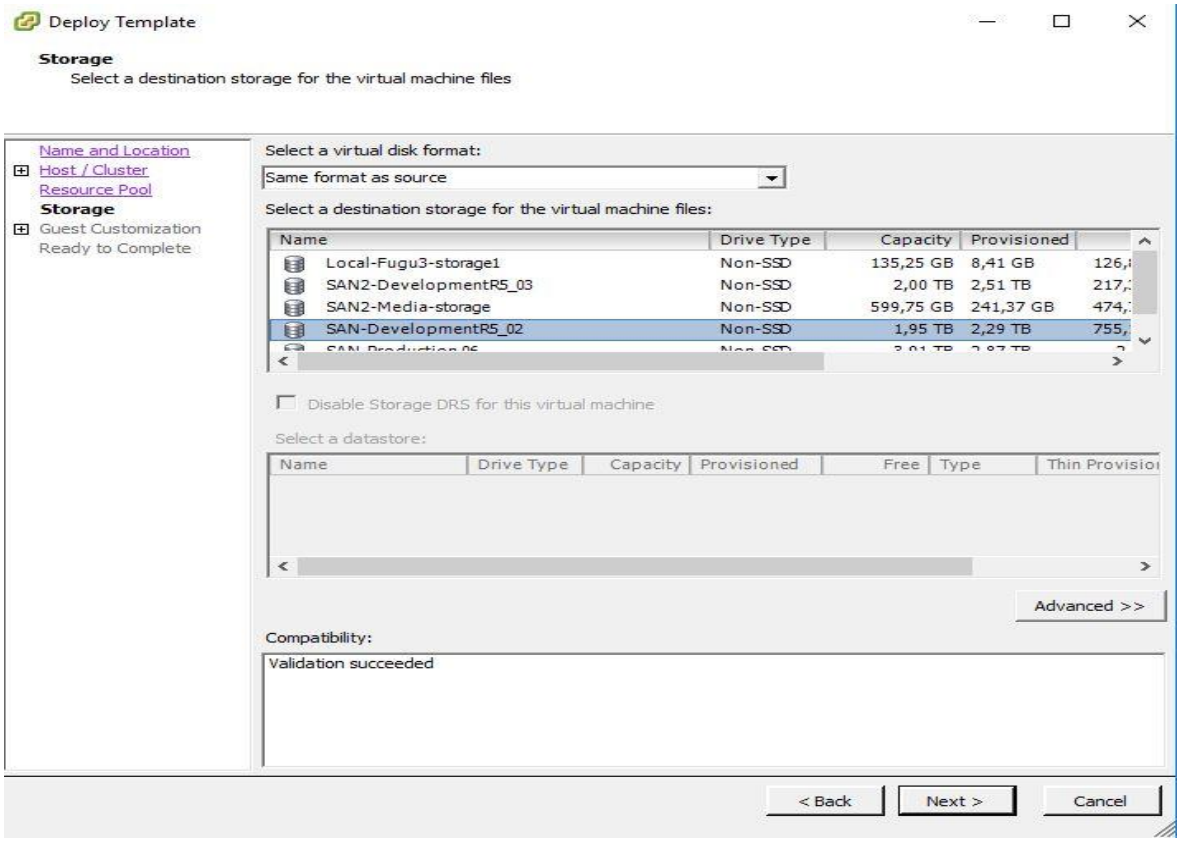
Kuva 8-2



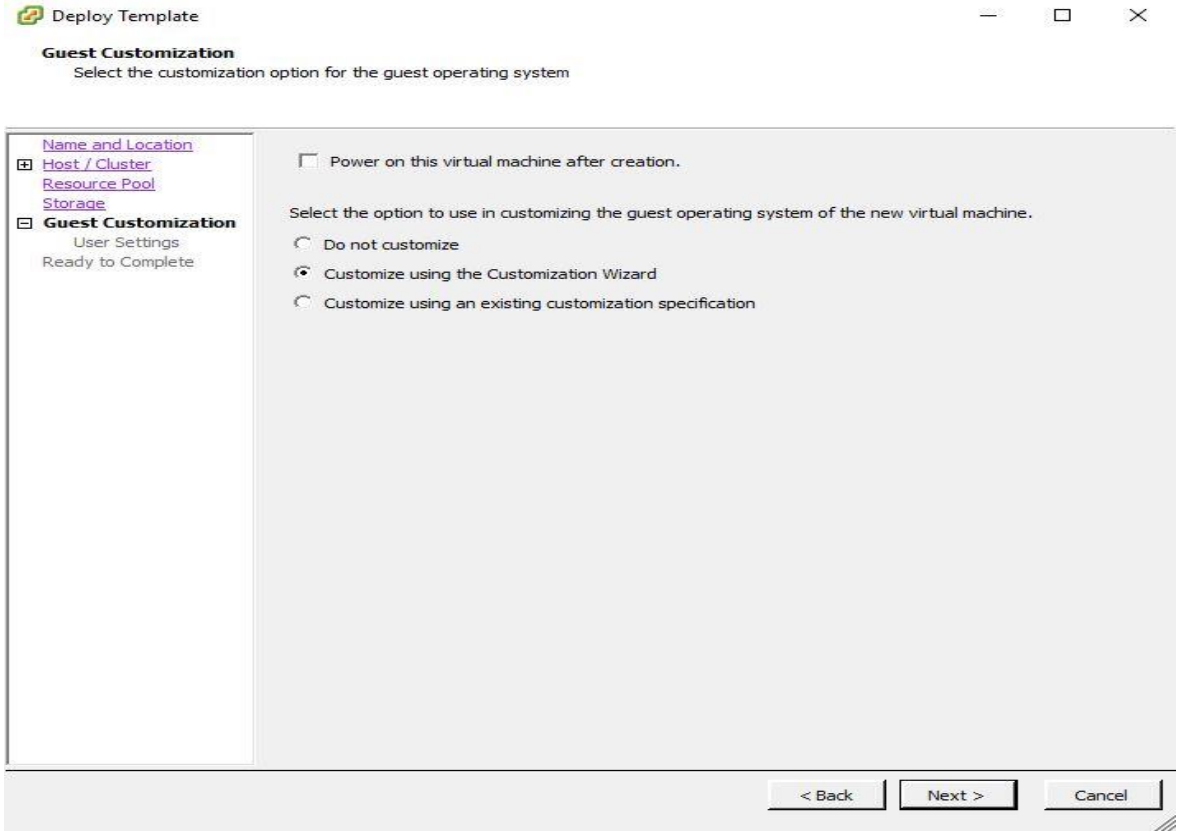
Kuva 8-3



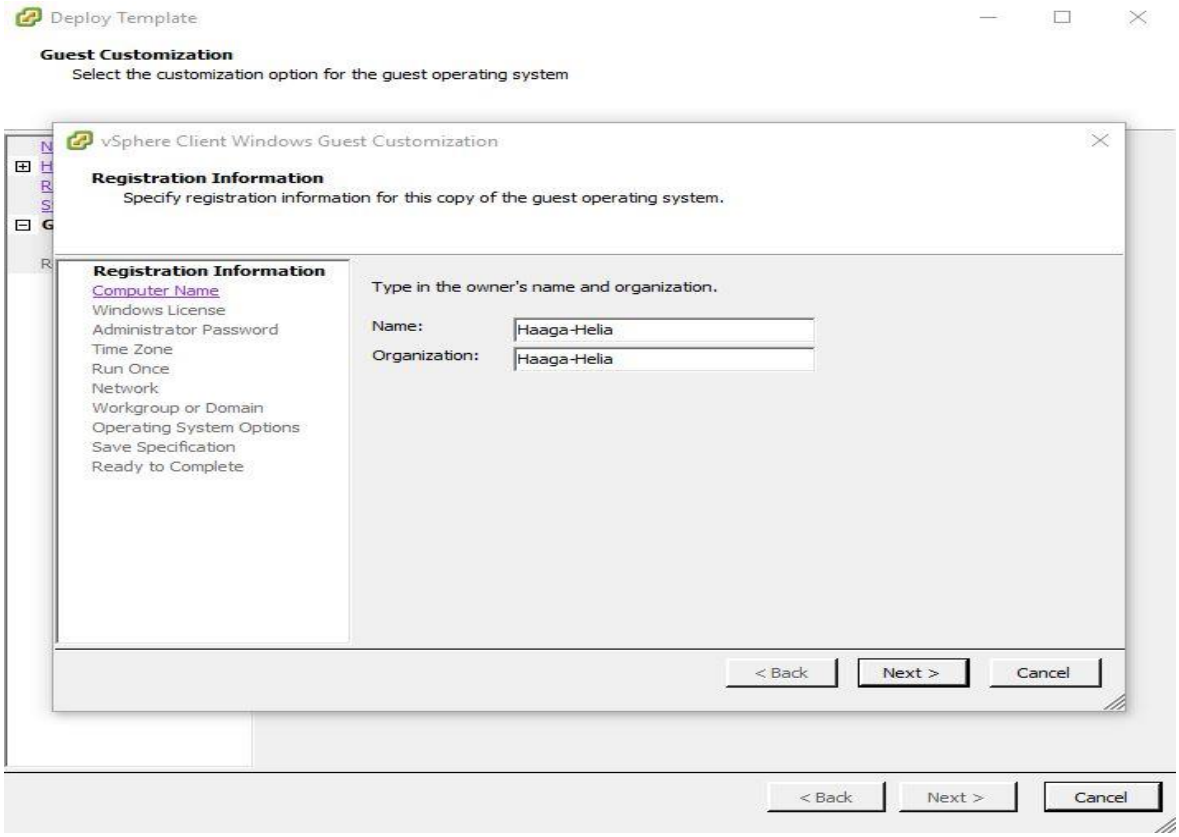
Kuva 8-4



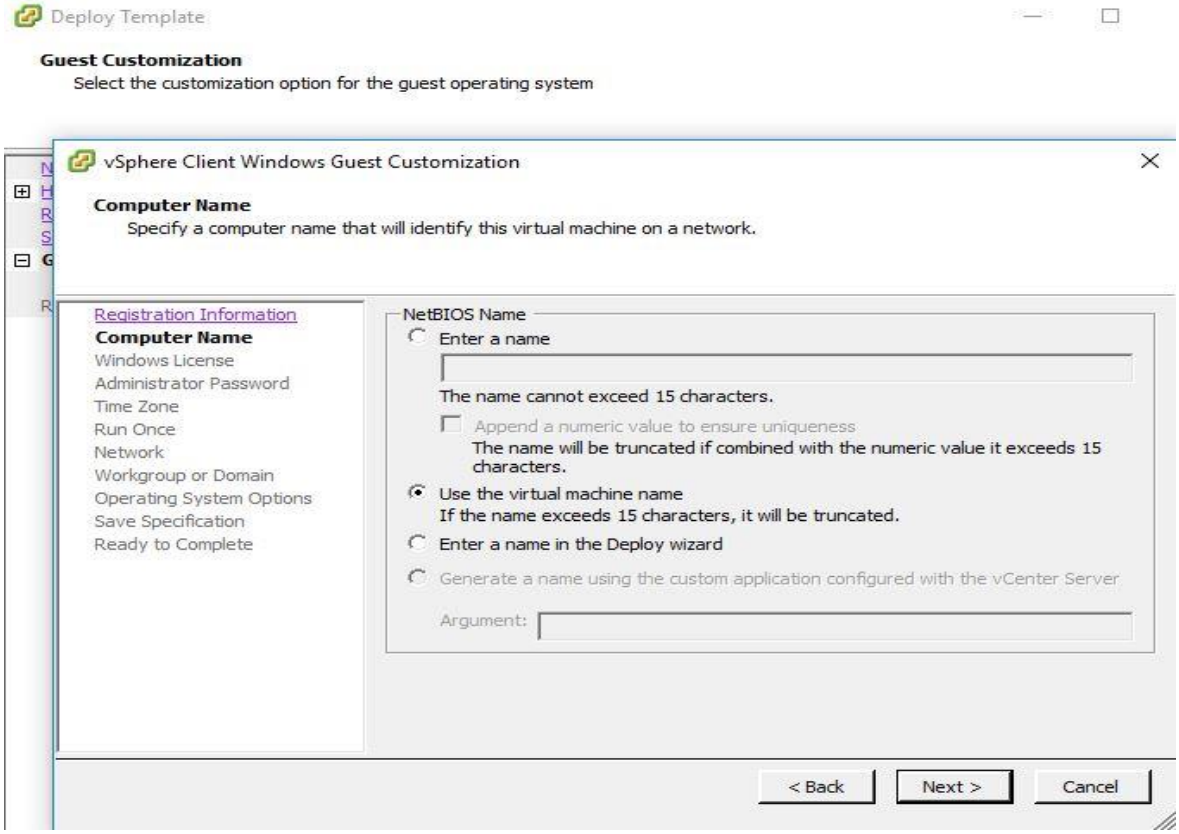
Kuva 8-5



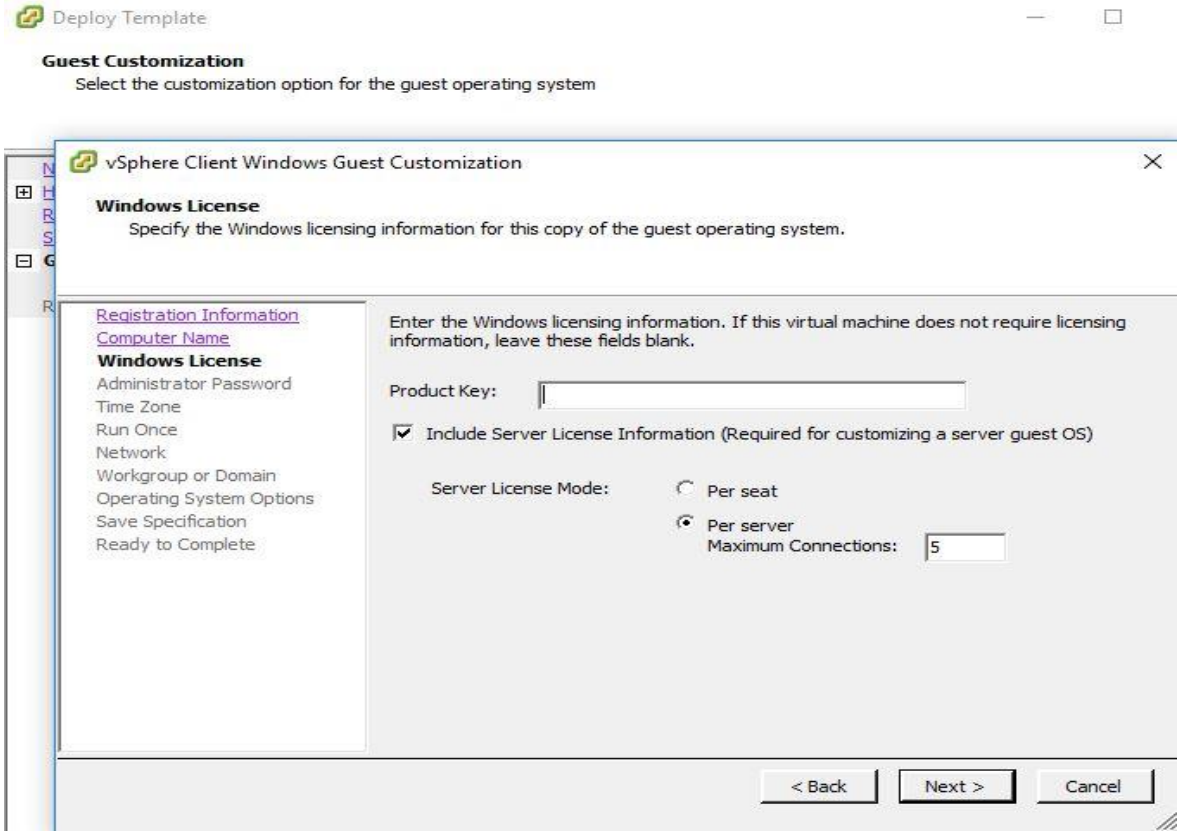
Kuva 8-6



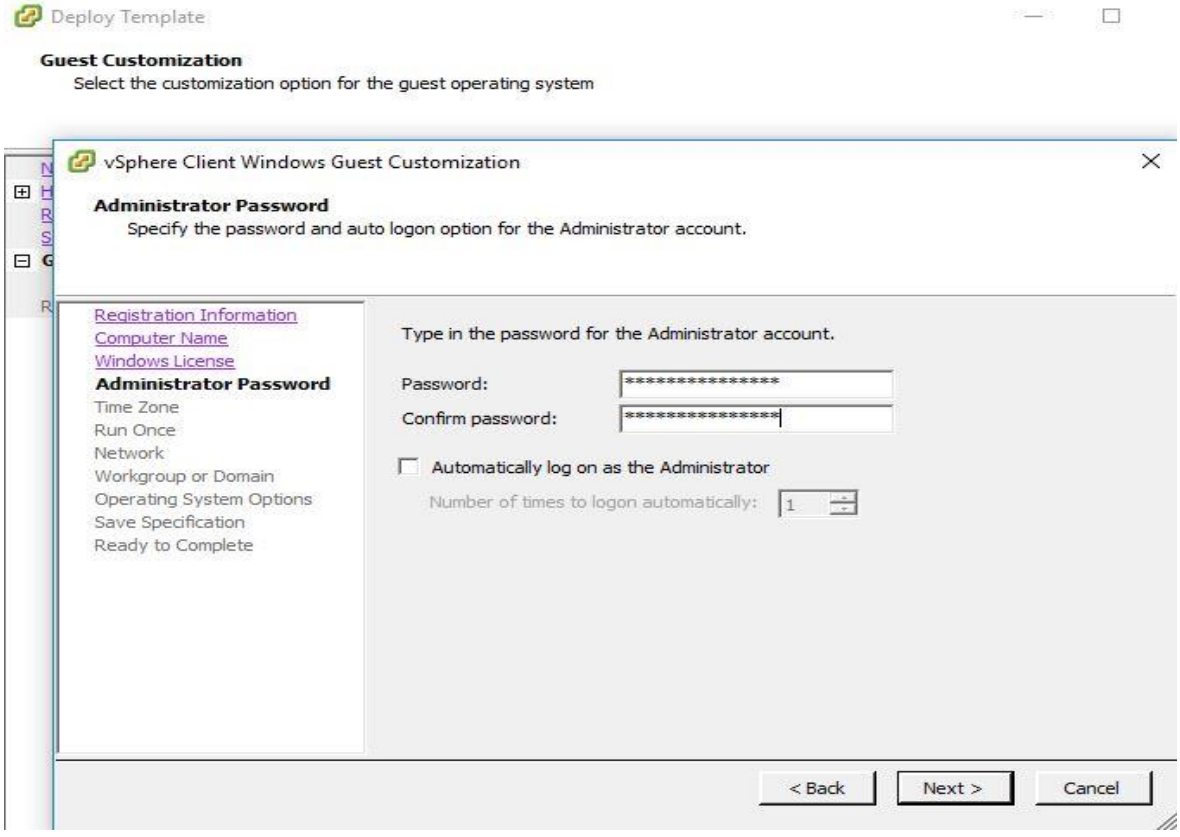
Kuva 8-7



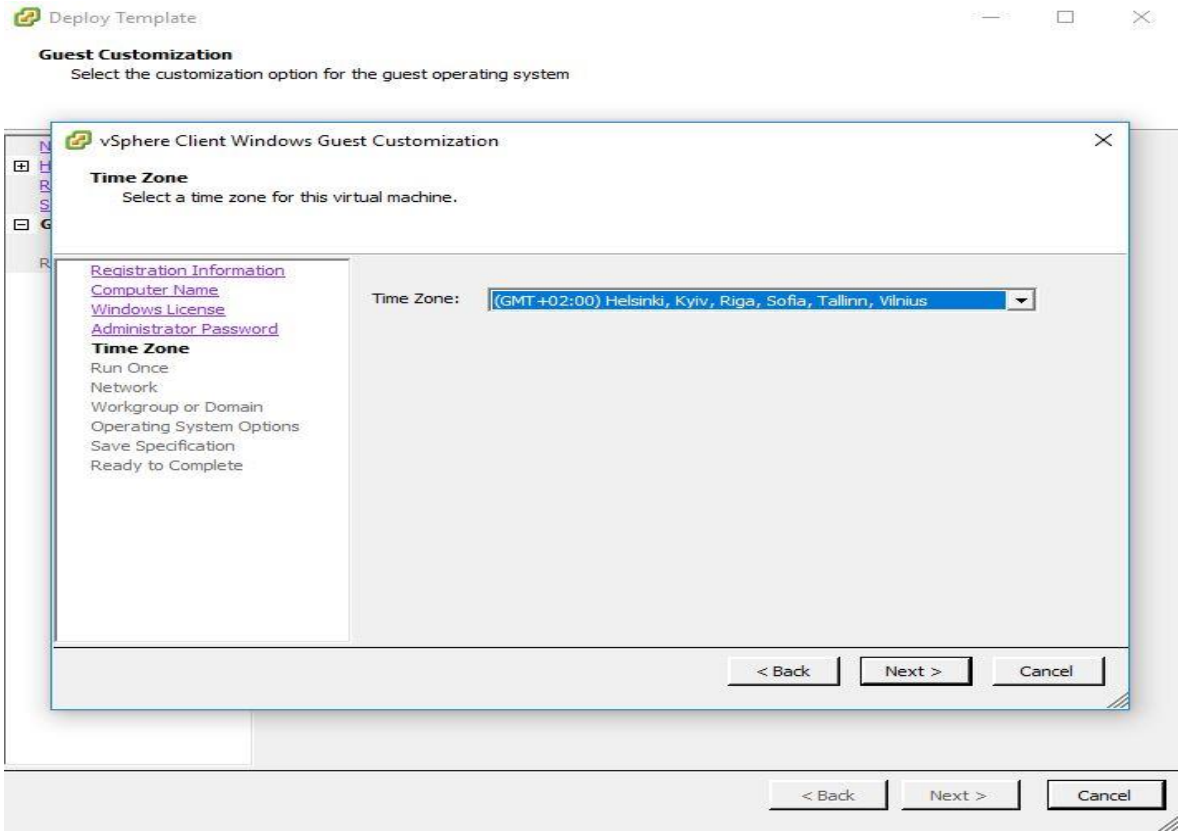
Kuva 8-8



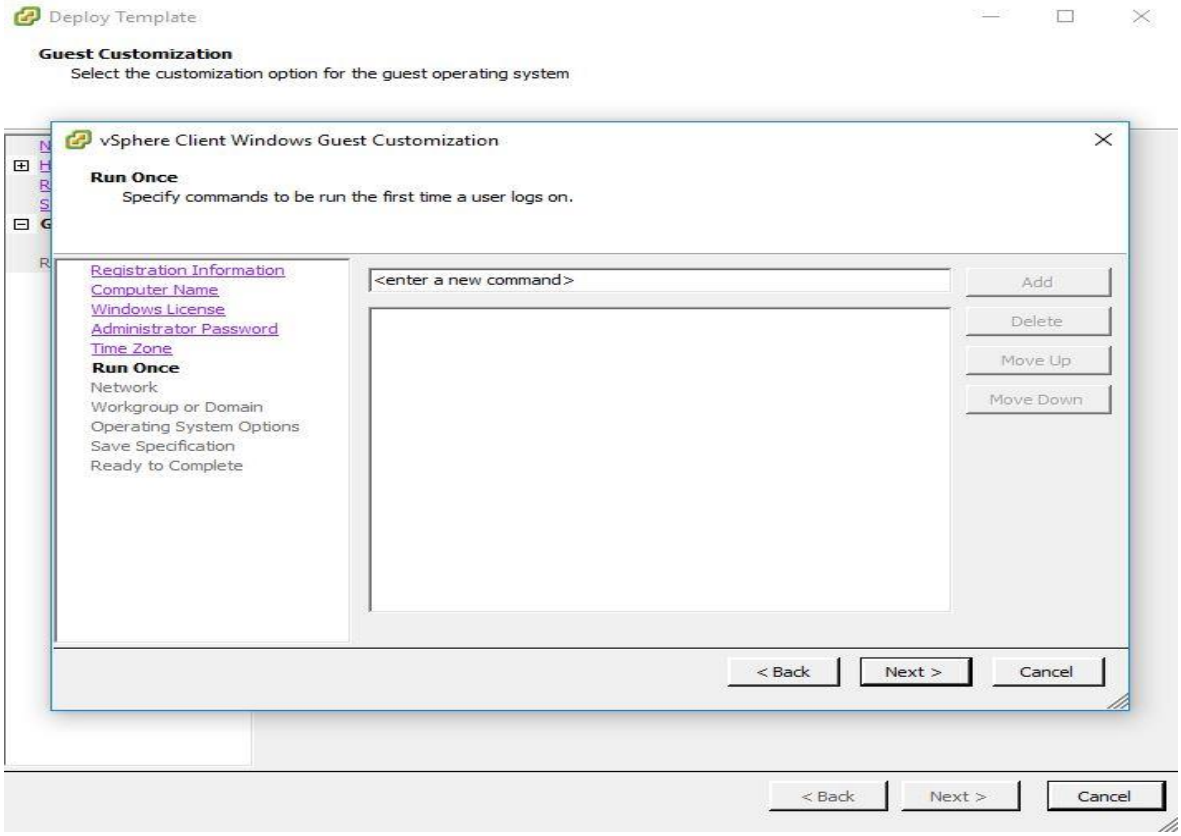
Kuva 8-9



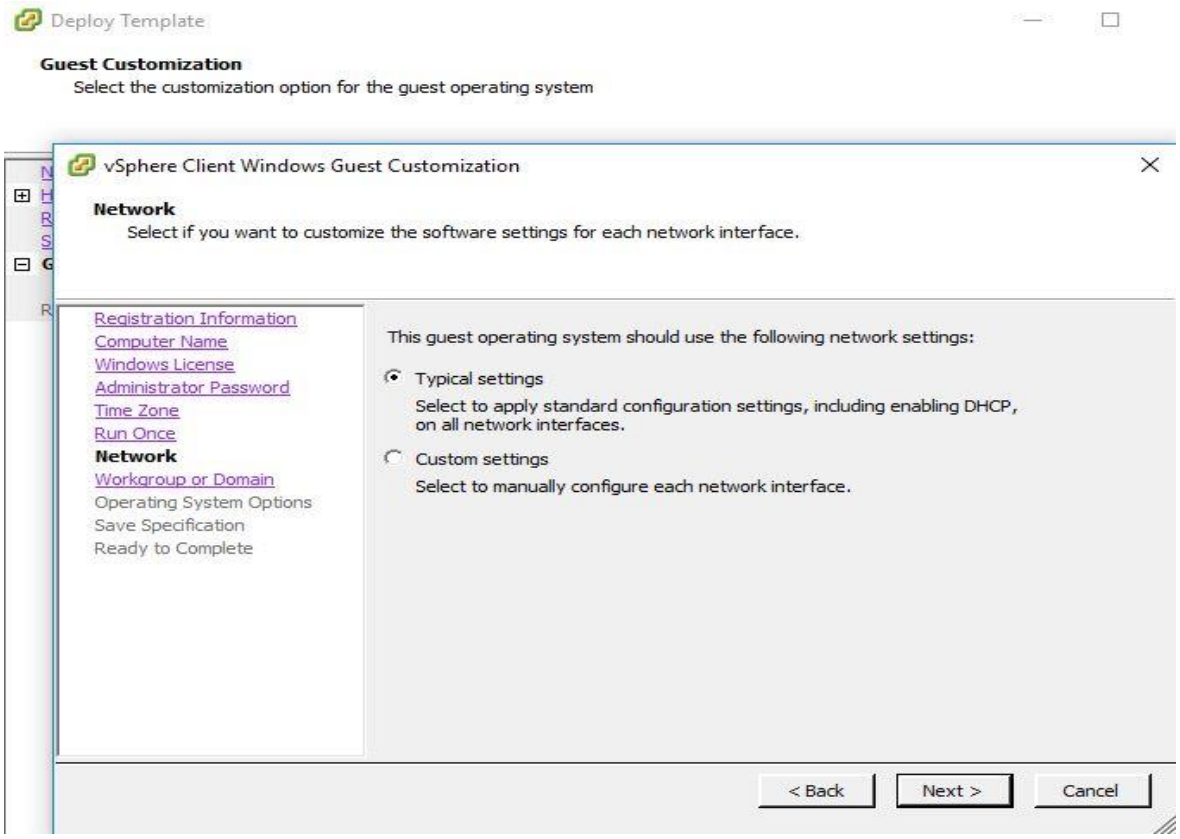
Kuva 8-10



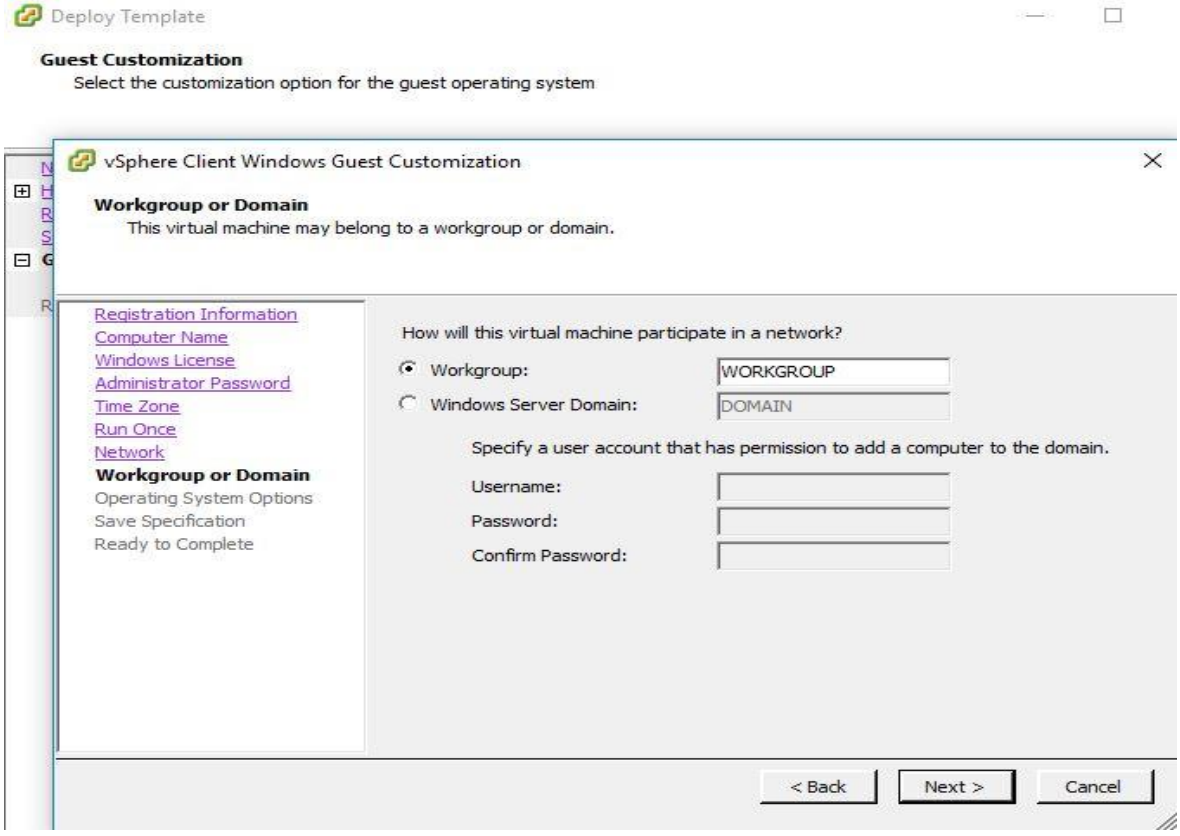
Kuva 8-11



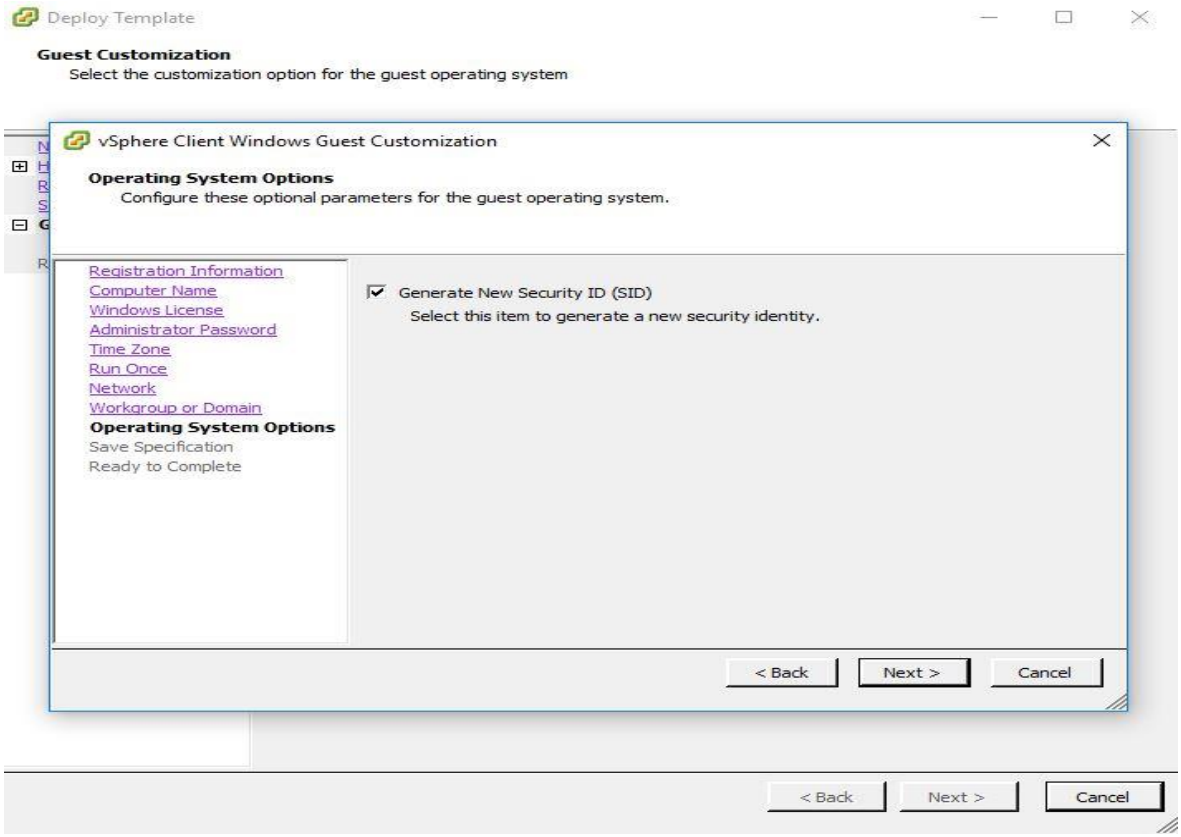
Kuva 8-12



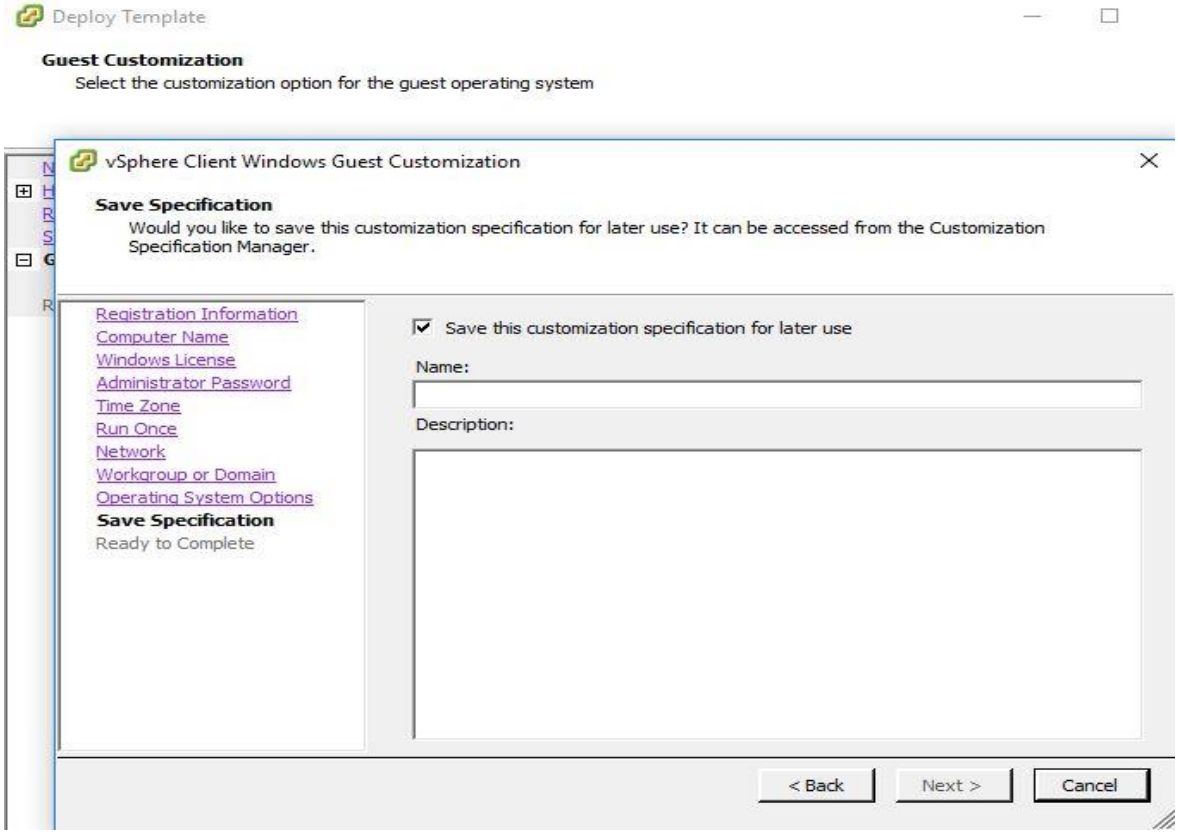
Kuva 8-13



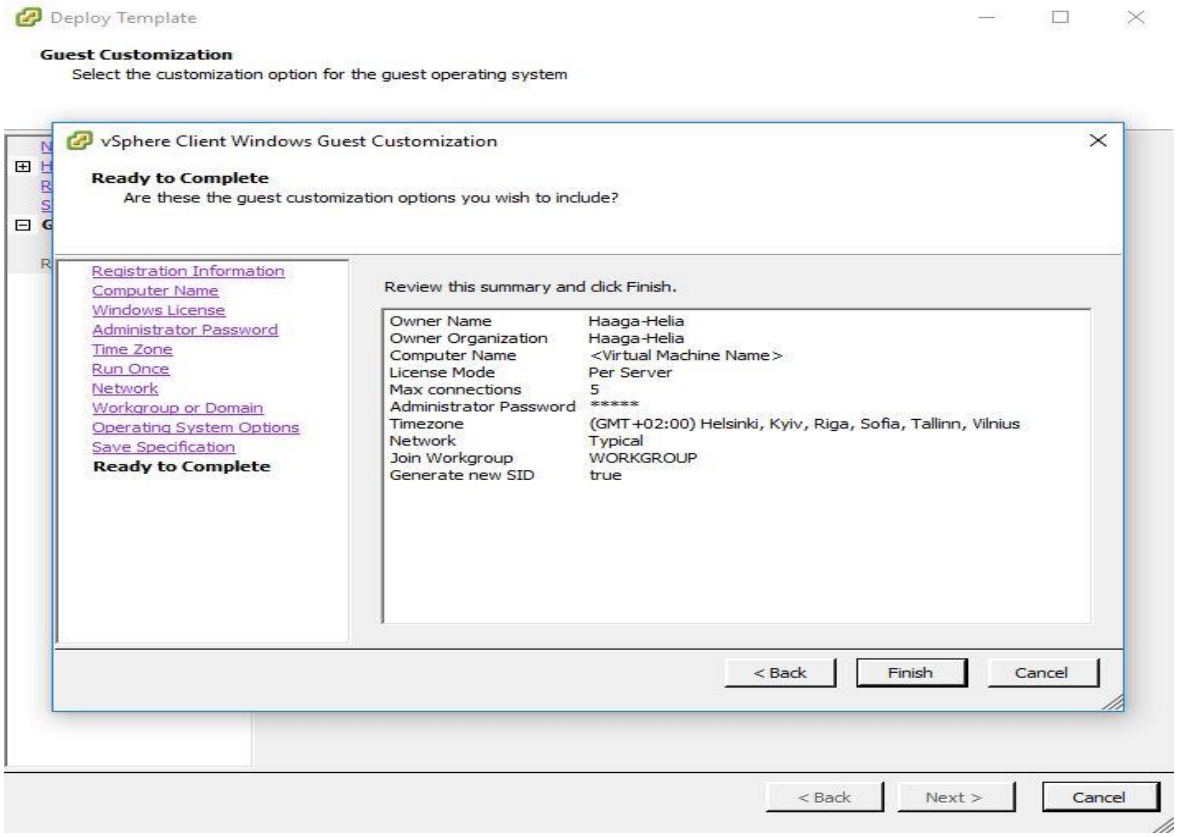
Kuva 8-14



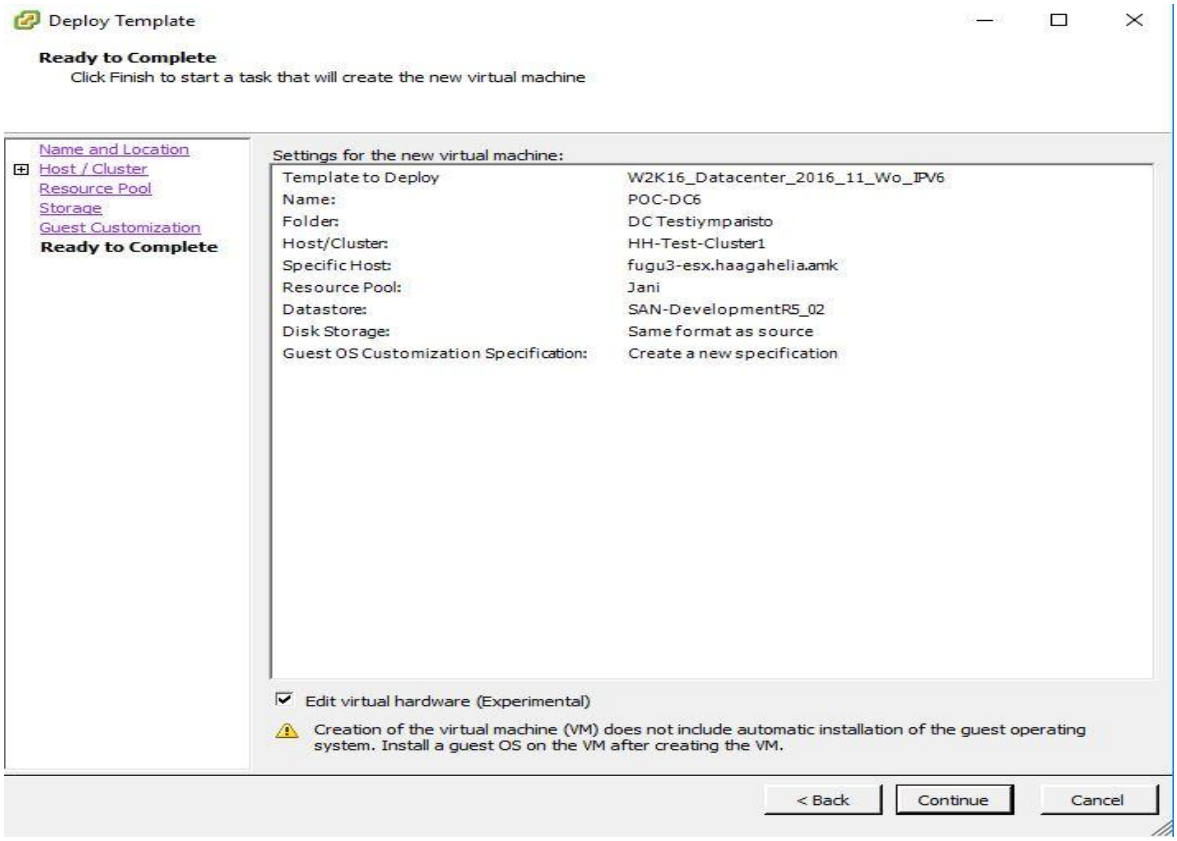
Kuva 8-15



Kuva 8-16



Kuva 8-17



Kuva 8-18