Juuso Toivanen

Domain controllerien varmuuskopiointi ja vikatilanteista palauttaminen

Tradenomi, tietojen-käsittely

Syksy 2016

KAJAANIN
AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

TIIVISTELMÄ

Tekijä(t): Toivanen Juuso

Työn nimi: Domain controllerien varmuuskopiointi ja vikatilanteista palauttaminen

Tutkintonimike: Tradenomi, tietojenkäsittely

Asiasanat: Palvelin, vikatilanteista palautuminen, varmuuskopiointi, palautus, domain controller

Tämä opinnäytetyö on toteutettu selvitystyönä Kajaanin ammattikorkeakoululle. Työssä on pyritty selvittämään Windows Server 2012 R2 domain controllerien varmuuskopioinnin ja palautuksen menetelmiä. Tekstissä on käyty läpi myös palvelimien toimintaa organisaatiossa sekä mahdollisia ongelmatilanteita, mitä palvelimet voivat kohdata elinkaarensa aikana. Palvelimien ongelmatilanteista palautumista työssä on selvitetty sekä teorian että käytännön keinoin. Teoriaosuudessa on kirjoitettu palautumisen suunnittelusta, varmuuskopiointivaihtoehdoista sekä palautusmenetelmistä. Työssä läpi käydyt varmuuskopiointivaihtoehdot ovat täysi varmuuskopio, Active Directoryn varmuuskopio sekä tiedostojen ja kansioiden varmuuskopio. Palautusmenetelmät ovat täysi palautus, Active Directoryn palautus, tiedostojen ja kansioiden palautus sekä domain controllerin palautus uudelleen asentamalla. Käytännön osiossa on selvitetty esimerkkien keinoin Windows Server 2012 R2 domain controllerien eritasoiset varmuuskopioinnit sekä palautus, esittäen myös varmuuskopiointiohjelman asennus ja käyttö sekä poistetun objektin palautus Active Directoryn roskakorista.

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Author(s): Toivanen Juuso

Title of the Publication: Backup and recovery solutions for domain controllers

Degree Title: Bachelor of Business Information Technology

Keywords: Server, disaster recovery, backup, recovery, domain controller

This thesis was commissioned by the Kajaani University of Applied Sciences. The purpose of the work is to investigate backup and recovery solutions for Windows Server 2012 R2 domain controllers. This thesis also explains the server functions in an organization and possible problems that can be encountered during their lifecycle.

The research aims to investigate server disaster recovery in theory and practice. The theory part includes disaster recovery planning, backup choices and recovery procedures. The backup choices introduced in this work are full backup, Active Directory backup and backups of files and folders. The introduced recovery solutions are using full backup, system state backup, backups of files and folders and also recovery of a domain controller by reinstalling the operating system. The aim of the practical part is to investigate different backup and recovery solutions for Windows Server 2012 R2 domain controllers by using examples. It also includes the installation of a backup program called Windows Server Backup and recovering deleted objects from Active Directory Recycle Bin.

SISÄLLYS

1 JOHDANTO 1

2 PALVELIN ORGANISAATIOSSA 2
2.1 Palvelimien ja työasemien erot 2
2.2 Windows-palvelimen roolit 4
2.3 Toimialueet 5
2.4 Mahdolliset ongelmatilanteet palvelimissa 6

3 VIKATILANTEISTA PALAUTUMINEN 7
3.1 Suunnitelma vikatilanteista palautumiseen 7
3.2 Suunnitelman hyödyt 8
3.3 Suunnitelman laatiminen 9
3.4 Suunnitelmassa huomioonotettavat asiat 10

4 DOMAIN CONTROLLERIN VARMUUSKOPIOINTIVAIHTOEHDOT 12
4.1 Täysi varmuuskopio 13
4.2 Active Directoryn varmuuskopiointi 14
4.3 Tiedostojen ja kansioiden varmuuskopiointi 14

5 DOMAIN CONTROLLERIN PALAUTUSMENETELMÄT 15
5.1 Täysi palautus 15
5.2 Active Directoryn palautus 15
5.3 Tiedostojen ja kansioiden palautus 16
5.4 Domain controllerin palautus uudelleenasentamalla 16

6 DOMAIN CONTROLLERIN VARMUUSKOPIOINTI KÄYTÄNNÖSSÄ 18
6.1 Windows Server Backup -ohjelman asennus 18
6.2 Domain controllerin täysi varmuuskopiointi Windows Server Backup -ohjelmalla 19
6.3 Active Directoryn varmuuskopiointi Windows Server Backup –ohjelmalla 23
6.4 Tiedostojen ja kansioiden varmuuskopiointi Windows Server Backup –ohjelmalla 25

7 DOMAIN CONTROLLERIN PALAUTUS KÄYTÄNNÖSSÄ 26
7.1 Poistetun objektin palautus Active Directoryn roskakorista 26
7.2 Domain controllerin palautus täydestä varmuuskopiosta 28

7.3 Active Directoryn palauttaminen varmuuskopiosta 32
7.3.1 Ei-autoritäärinen palautus 32
7.3.2 Autoritäärinen palautus 35
7.4 Tiedostojen ja kansioiden palautus varmuuskopiosta 36

8 YHTEENVETO 38

LÄHTEET 40

SYMBOLILUETTELO

Cluster = Useasta palvelimesta yhdistetty resurssikokonaisuus.

Domain = toimialue, sisältää keskitetyn hallinnan käyttäjätunnuksille, työasemille, palvelimille sekä tulostimille.

DMZ (Demilitarized Zone) = Fyysinen tai looginen aliverkko, johon sijoitetaan organisaation palvelut, jotka tarvitsevat suoran yhteyden internettiin.

ESXi, Hyper-V = Hypervisor eli alusta virtuaalikoneille.

Forest = Active Directoryn ylin taso, joka sisältää toimialueet, konfiguraatiot ja ohjelmistotiedot.

FTP (File Transfer Protocol) = Protokolla, jota käytetään tiedostojensiirrossa palvelimelta työasemalle.

GUI (Graphical User Interface) = Graafinen käyttöliittymä.

GPO (Group Policy Object) = Käytetään käyttäjäasetusten, käyttöjärjestelmien sekä ohjelmistojen hallinnassa Active Directoryssa.

RAID (Redundant Array of Independent Disks) = Useita erillisiä kovalevyjä yhdistettynä yhdeksi loogiseksi levyksi.

TCP/IP (Transmission Control Protocol / Internet Protocol) = IP-protokolla vastaa päätelaitteiden osoitteistamisesta ja pakettien reitittämisestä verkossa, TCP-protokolla vastaa päätelaitteiden välisestä tiedosiirtoyhteydestä.

UPS (Uninterruptible Power Supply) = Laite, joka toimii varavirtana siihen kytketyille laitteille sähkökatkosten aikana sekä tasaa jännitettä.

VHD (Virtual Hard Drive) = Tiedostotyyppi, jota käytetään yleensä virtuaalisen tietokoneen kovalevynä.

.NET Framework= Ohjelmistokomponenttikirjasto, jota Microsoft Visual Studio -ympäristössä kehitetyt ohjelmistot käyttävät.

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on selvittää Windows Server 2012 R2 domain controllerien varmuuskopioinnin ja palautuksen menetelmiä. Oma mielenkiintoni sekä opettajan toive selvittää kyseiseen aiheeseen liittyvät asiat ohjasivat minut kirjoittamaan Windows-palvelinympäristöjen ongelmatilanteisiin varautumisen suunnittelusta ja ongelmatilanteiden jälkeisen palautumisen toteutuksesta. Tämä opinnäytetyö on tehty Kajaanin ammattikorkeakoululle. Aihe on valittu yhteistyössä opettajani Timo Partasen kanssa.

Työn teoreettisessa osuudessa käsitellään palvelimien roolia organisaatiossa, vertaillaan palvelimia työasemiin sekä esitellään mahdollisia ongelmatilanteita palvelimissa. Osuudessa käydään läpi myös vikatilanteisiin varautumista, suunnittelua sekä vikatilanteista palautumista. Lisäksi työssä käsitellään domain controllerien varmuuskopioinnin vaihtoehdot Windows Server Backup -ohjelmalla sekä palautusmenetelmiä ongelmatilanteiden jälkeen.

Käytännön osio sisältää Windows Server 2012 R2 domain controllerien varmuuskopioinnin ja palautuksen menetelmiä käytännössä. Tässä opinnäytetyössä käydään läpi täyden varmuuskopioinnin ja palautuksen, yksittäisten tiedostojen ja kansioiden varmuuskopioinnin ja palautuksen sekä järjestelmän tilan varmuuskopioinnin ja Active Directoryn palautuksen ei-autoritäärisesti sekä autoritäärisesti. Lisäksi käytännön osiossa käsitellään Windows Server Backup -ohjelman asennus sekä Active Directoryn roskakorin käyttö objektin palauttamiseen.

2 PALVELIN ORGANISAATIOSSA

Palvelimet ovat osa organisaation infrastruktuuria, ja ne tarjoavat erinäisiä palveluja palvelimen roolista riippuen kuten organisaatiotason tietoteknistä hallintaa, käyttäjähallintaa, datan tallennustilaa, ohjelmistoja sekä tietoteknistä kommunikaatiota. Palvelimia on olemassa eri käyttöjärjestelmillä kuten Linux, Mac ja Windows. Tässä työssä käsitellään Windows-palvelimen rooleja sekä toimintoja. Windows-palvelimista on useita versioita, joita on päivitetty vuosien varrella sisältämään enemmän ominaisuuksia, pyrkien kuitenkin vakaaseen suorituskykyyn. Tällä hetkellä dokumentoidut versiot ovat Windows Server 2003, 2008 ja 2012 sekä näistä päivitetyt R2-versiot. (Microsoft.)

Windows Server 2012 -käyttöjärjestelmästä on neljä eri versiota, joista voi valita sopivimman organisaation tarpeisiin. Versiot ovat Datacenter, Standard, Essentials ja Foundation. Datacenter-versio on suunniteltu suuren mittakaavan virtualisoiduille ympäristöille. Standard-versio on ympäristöille, joissa ei käytetä virtualisointia vaan palvelimet asennetaan suoraan raudan päälle. Se on sopiva pienempiin infrastruktuureihin tai sivutoimistoihin. Essentials-versio on suunniteltu pienemmille yrityksille, joissa on enintään 25 käyttäjää. Foundation-versio tarjoaa vain yleisimmät Windows Server -palvelut ja siinä käyttäjämäärä on rajoitettu 15:een. (Hester, M & Henley, C. 7.)

2.1 Palvelimien ja työasemien erot

Palvelimet eroavat työasemista sekä rauta-, komponentti- että käyttöjärjestelmätasolla. Kuvassa 1 on normaali tornimallinen palvelin. Se on ulkomuodoltaan samankaltainen kuin työasema, joskin usein kooltaan hieman isompi ja painavampi. Tornimallinen palvelin on yleensä käytössä, kun ei ole tarvetta useammalle palvelimelle. Organisaation tarpeiden kasvaessa siirrytään palvelinkaappeihin sekä useampaan kaappiin sijoitettavaan palvelimeen. Kuvassa 2 on ohuempi, palvelinkaappiin sijoitettava malli. (Dell.)

Kuva 1. Tornipalvelin

Kuva 2. Palvelinkaappiin sijoitettava malli

Komponenttitasolla erilaisuutena on se, että palvelimet on suunniteltu käsittelemään erilaisia tehtäviä kuin työasemat, jolloin komponentit eroavat tehoiltaan ja toiminnaltaan. Palvelimien prosessointitehoa pyritään parantamaan lisäämällä ydinten määrää prosessorissa. Palvelimen prosessorissa on lisäksi suurempi välimuisti kuin työaseman prosessorissa. Lisäksi palvelimen keskusmuisti on nopeampaa ja kalliimpaa kuin työasemassa, koska palvelin suorittaa useita tehtäviä jatkuvasti yhtä aikaa. Useimmissa palvelimissa on myös kahdennettu virransyöttö, jolloin yhden virtalähteen hajotessa toinen pystyy syöttämään tarvittavan virran palvelimelle eikä toiminta katkea. Palvelimen näytönohjaimet eivät ole yleensä kovin tehokkaita, koska niissä ei käytetä graafisesti raskaita ohjelmistoja. Yksi suurimmista eroista palvelimen ja työaseman välillä on tallennustilan levyjärjestelmä. Kun työasemassa on yleensä yksi kovalevy, palvelimissa on puolestaan useampia kovalevyjä, jotka on konfiguroitu näkymään käyttäjälle yhtenä levynä. Tätä järjestelmää kutsutaan sanalla RAID. RAID-taso 1 peilaa kahta levyä, jolloin toisen hajotessa sama data on edelleen tallessa ehjällä levyllä. RAID-taso 5 on monimutkaisempi, sisältäen vähintään kolme kovalevyä, ja se kestää minkä tahansa levyn rikkoutumisen. Molemmat suojaavat datan menetyksiltä, mutta taso 5 antaa enemmän tallennustilaa ja se toimii nopeammin. RAID-tasoja on lisäksi useampia eri tarkoituksiin. (Dell)

Palvelimissa on toimittajasta riippuen lisäksi rautaan sisäänrakennettuja hallintatyökaluja, joita työasemissa ei ole. Näitä ovat esimerkiksi HP:n Integrated Lights

Out (iLO) ja Dellin Integrated Dell Remote Access Controller (iDRAC). HP:n iLO antaa mahdollisuuden monitoroida ja hallita palvelinta etäyhteydellä. Yksi sen pääominaisuuksista on palvelimen tilan monitorointi. Monitorointi sisältää asennetut ohjelmistot ja versiot sekä lämpötilan, tuulettimien, muistin, verkon, prosessorien, virransyötön, tallennustilan ja asennettujen lisälaitteiden tilanteet. Lisäksi iLO:n voi konfiguroida lähettämään hälytyksiä järjestelmänvalvojalle, jos jossain mainituista asioista ilmaantuu ongelmia tai poikkeamia (Hewlett Packard Enterprise. 19.). Dellin iDRAC on ominaisuuksiltaan käytännössä samanlainen kuin HP:n iLO (Dell, 2014. 16.)

2.2 Windows-palvelimen roolit

Windows-palvelimille voi asettaa rooleja, jotka määrittävät mitä toimintoja palvelin suorittaa, ja mitä palveluita se tarjoaa organisaatiolle tai sen asiakkaille. Yhdellä palvelimella voi olla yksi tai useampi rooli riippuen siitä, kuinka ja missä mittakaavassa IT-infrastruktuuri halutaan toteuttaa. Kuvassa 3 näkyvät pääroolit ovat asetettavissa Windows Server 2012 -palvelimiin. (Hester, M & Henley, C. 7.)

Rooli	Toiminnot
Active Directory Domain Services	Käyttäjähallinta ja SSO
Active Directory Lightweight Directory Services	Kevyempi versio AD DS:stä
Active Directory Certificate Services	Sertifikaatit ja datan kryptauksessa käytetyt avaimet
Active Directory Federation Services	SSO kirjautuminen domainien välillä sekä web-pohjainen SSO
Active Directory Rights Management	Valtuutus- ja vahvistuspalvelu
Application Server	.NET rajapintaa käyttävien ohjelmien toiminta palvelimella
DHCP Server	Automatisoidut TCP/IP jakelupalvelut
DNS Server	Nimenselvityspalvelu
Fax Server	Faxin perustoiminnot palvelimella
File and Storage Services	Tiedostojärjestelmien palvelut
Hyper-V	Virtuaalikoneiden luonti ja hallinta
Network Policy and Access Services	Reitittäminen ja etäyhteydet
Print and Document Services	Keskitetty hallinta tulostuspalvelimelle ja tuslotimille
Remote Access	Etäyhteyspalvelut
Remote Desktop Services	Etätyöpöytäyhteys palvelimelle
Volume Activation Services	Keskitetty hallinta ohjelmistojen lisensoinnille
Web Server (IIS)	Ydininfrastruktuuri web-palvelimelle
Windows Deployment Services	Käyttöjärjestelmien jakelu ja asennus verkossa
Windows Update Services (WSUS)	Hallintarakenne Microsoftin päivityksille verkon yli työasemille

Kuva 3. Windows Server 2012 -roolit.

Ydinversio Windows Server 2012 (Server Core) on toinen vaihtoehto käyttöjärjestelmän asennuksesta. Se ei sisällä graafista käyttöliittymää vaan sitä hallitaan komentoriviltä. Ydinversio sisältää rajoitetusti toimintoja, ja siihen voi asentaa myöhemmin halutessaan graafisen käyttöliittymän. Tämän version hyviä puolia ovat ylläpidon ja turvallisuusriskien pienempi määrä. Se ei tarvitse myöskään yhtä paljon päivityksiä pysyäkseen ajan tasalla. Ydinversio sisältää kuvassa 4 mainitut 13 roolia, joista suurin osa on samoja kuin kokoversiossa. (Hester, M & Henley, C. 9-10.)

Kuva 4. Windows Server 2012 ydinversion roolit.

2.3 Toimialueet

Toimialueet ovat käytössä yleensä yli 10 käyttäjän ympäristössä, koska se tuo seuraavat hyödyt organisaatiolle; käyttäjien ja käyttöoikeuksien keskitetty hallinta, keskitetty järjestelmien suojaus ja hallinta Group Policy Objecteilla (GPO) sekä muut palvelut, jotka ovat riippuvaisia Active Directorysta. Yhdessä toimialueessa on yleensä kaksi domain controlleria, jotka replikoivat niissä olevan tiedon keskenään. Organisaation Forestissa voi olla yksi tai useampi toimialue. Useampaa toimialuetta voidaan käyttää tapauksissa, joissa on tarve säilyttää vanha toimialue

uuden rinnalla tai toimialueessa on niin paljon tietoliikennettä, että yhteys ei riitä replikoinnin toteuttamiseen. (Minasi, M & Greene, K & Booth, C. 260-261.)

Järkevin tapa rakentaa Active Directory on kuitenkin käyttää yhtä toimialuetta, ellei edellä mainitut tai jotkin muut syyt pakota käyttämään useampaa. Yhden toimialueen hyötyjä ovat halvempi hinta, helpompi hallinta ja helpompi palautus. Jokainen ylimääräinen palvelin maksaa organisaatiolle lisää, koska voidaan tarvita lisää rautaa, lisenssejä, ohjelmistoja sekä työaikaa tai työntekijöitä hallintaan. Vaikka palvelimet voidaan virtualisoida, jäljelle jää silti tallennustilan hankkiminen ja hallintaan menevät kustannukset. Jokainen Forestiin lisättävä toimialue lisää hallittavia objekteja sekä haasteita käyttöoikeuksiin liittyen. Lisäksi Active Directory on haastava tehtävä palauttaa ongelmien ilmentyessä, jolloin on helpompi palauttaa yksi kuin useampi toimialue. (Minasi, M & Greene, K & Booth, C. 261-262.)

2.4 Mahdolliset ongelmatilanteet palvelimissa

Koska tässä työssä käsitellään Windows Server 2012 R2 domain controllerien ongelmatilanteista palautumista, tässä kappaleessa esitetään, millaisia ongelmia palvelin voi mahdollisesti kohdata elinkaarensa aikana.

Tapahtumia, jotka voivat johtaa palvelimen ongelmatilanteeseen, ovat luonnolliset tekijät kuten vesivahingot, järistykset tai tulipalot, jolloin komponentit voivat vahingoittua. Lisäksi ongelmatilanteeseen voi johtaa verkkoyhteyksien ja virransaannin keskeytyminen sekä rikollinen tai tahallista vahinkoa tuottava toiminta (Varghese, M. 3.). Myös tekniset viat kuten komponenttien hajoaminen vanhentumisen tai kulumisen myötä voivat johtaa tilanteeseen, jolloin palvelimen toiminta on uhattuna (Gregory, P. H. 10.).

3 VIKATILANTEISTA PALAUTUMINEN

Vikatilanteista palautuminen on Mathew Varghesen mukaan prosessi, joka varmistaa organisaation toiminnan jatkuvuuden teknisen tai luonnollisen vahingon tapahtuessa. Prosessi keskittyy vikatilanteesta palautumiseen niin lyhyessä ajassa kuin mahdollista. Tehokkaan palautumisen varmistaminen kustannustehokkaasti mahdollisimman lyhyessä ajassa voi varmistaa laatimalla suunnitelman palautumista varten. Tämä termi on englanniksi Disaster recovery planning. (Varghese, M. 1.)

Miriam Kahn on esittänyt, että tällaisen tapahtuman selvittämisessä on neljä vaihetta: vikailmoituksen huomioiminen, tapahtuneen vahingon arviointi, palautuksen aloittaminen sekä palautusprosessi, joka sisältää palveluiden ja tietojen toiminnan palauttamisen. (Mallery, M. 14.)

Tapahtumia jotka voivat johtaa vikatilanteeseen ovat luonnolliset katastrofit, kuten tulvat, tornadot ja maanjäristykset. Myös tulipalot, yhteyksien ja virransaannin keskeytyminen ja rikollinen tai tahallista vahinkoa tuottava toiminta saattavat johtaa vikatilanteeseen (Varghese, M. 3.). Lisäksi tekniset viat voivat johtaa tilanteeseen, jolloin organisaation toiminnan jatkuvuus on uhattuna. Katastrofin vaikutukset voivat olla suoraa vahinkoa rakennuksille ja laitteistoille tehden niistä käyttökelvottomia tai luoksepääsemättömiä. Parhaimmassa tapauksessa katastrofit aiheuttavat pienempiä harmeja kuten sähkö- ja kommunikaatioyhteyksien katkoksia (Gregory, P. H. 10.).

3.1 Suunnitelma vikatilanteista palautumiseen

Suunnitelmaa laatiessa pyritään tunnistamaan tavat, joilla voidaan käsitellä järjestelmien käyttökatkot ja vahingot (Varghese, M. 6.). Organisaatiot ilman suunnitelmaa ovat suurissa vaikeuksissa tapaturman sattuessa. Olettaen, että organisaatiolla on järjestelmien toiminta-aikaan sidottuja kriittisiä prosesseja, tapaturmasta toipuminen on lähes mahdotonta. Vaikka organisaatiolla olisikin suunnitelma, heillä voi silti olla vaikeuksia ongelmien ilmentyessä. Suunnitelma antaa kuitenkin

mahdollisuuden toipua kriittisestäkin vahingosta. Suunnitelman laatiminen oli aiemmin vapaaehtoista, joskin aiheellista. Nykyään niitä alkaa kuitenkin esiintyä jo standardeissa ja säännöksissä, kuten PCI DSS, ISO27001, BS25999, NFPA 1620 ja HIPAA Security Rule. Peter Gregory arvelee, että tulevaisuudessa yhä useampi datan turvallisuuteen liittyvä laki sisältänee vikatilanteista palautumisen suunnittelun. (Gregory, P. H. 12.)

Seuraavassa esitetään Peter Gregoryn esimerkki tapahtumista ilman suunnitelmaa ja suunnitelman kanssa: Jos palvelin kaatuu ja sen sisältämä data korruptoituu, ilman palautumissuunnitelmaa voi kestää useita päiviä rakentaa data uudestaan varmuuskopiotallenteesta. Hyvän suunnitelman kanssa palautus onnistuu varapalvelimelta. Lisäksi tahallisesti aiheutetun vian tapahtuessa suunnitelman mukaisesti lyhyellä aikavälillä varmuuskopioitu tieto on nopeampaa palauttaa. (Gregory, P. H. 16.)

3.2 Suunnitelman hyödyt

Hyötyjä suunnitelman laatimisessa ovat Mathew Varghesen mukaan liiketoiminnan jatkuvuus tunnistamalla ja takaamalla kriittisten resurssien, toimintojen ja järjestelmien toimivuus ja vakaus, jolloin myös asiakkaan intressit ovat turvattuja. Suunnitelman laatiminen etukäteen myös minimoi rahalliset tappiot vahingon tapahtuessa. Myös yksittäisten ongelmakohtien tunnistaminen suunniteltaessa hyödyttää organisaatiota, kun tiedostetaan, missä toiminnoissa ja prosesseissa esiintyvät ongelmat ovat tuhoisimpia organisaation toiminnalle. Katastrofien varalle tehty suunnitelma vähentää mahdollista paniikkia ongelmien ilmentyessä. Se vähentää myös ongelmien ratkaisuaikaa merkittävästi. (Varghese, M. 6.)

Prosessien analysointi voi hyödyttää liiketoimintaa siinä määrin, että siitä voi löytyä kehitettäviä osa-alueita. Tämä johtaa myös yleensä IT-järjestelmien kehittämiseen ja parempaan varmistamiseen, esimerkiksi kahdentamiseen sekä kahdennettujen järjestelmien sijoittamiseen fyysisesti eri paikkoihin. Kehittyneempi teknologia takaa paremman toimintavarmuuden ja voi johtaa pienempään määrään katkoksia.

Prosessien ja teknologian kehittyessä myös sisäiset sekä asiakkaille tarjotut palvelut paranevat. Hyvä palautumissuunnitelma voi myös antaa organisaatiolle kilpailuetua, koska laadulla voi kilpailla hintaa vastaan varsinkin kriittisissä palveluissa. (Gregory, P. H. 13.)

3.3 Suunnitelman laatiminen

Palautumissuunnitelmaa laatiessa on Mathew Varghesen mukaan kolme strategiaa: ehkäisevä, ennakoiva ja lieventävä. Ehkäisevässä strategiassa paneudutaan estämään ongelmien syntyminen. Tämän saavuttaakseen organisaation tulee ottaa käyttöön suunnitellut toimenpiteet varmistamaan, että toimet ja järjestelmät, joista organisaatio on riippuvainen, ovat luotettavia. Kaiken kaikkiaan tällä pyritään vähentämään hallittavissa olevien ongelmien syntyminen. Ennakoivassa strategiassa pyritään selvittämään, mitkä ovat oikeat toimintatavat ongelmien ilmentyessä, mikä kehittyy yleensä kokemuksen ja tiedon kautta. Lieventävässä strategiassa selvitetään tavat, joilla voidaan minimoida väistämättömän ongelman vaikutus toimintaan. (Varghese, M. 7, 8.)

Peter Gregory esittää teoksessaan, että suunnitelman tulisi sisältää seuraavat asiat: toimintaohje ongelmasta tiedottamiseen, henkilöiden yhteystiedot hätätilanteessa, hätätilanteen johtohenkilöiden ja järjestelmien palauttamisen vastuuhenkilöiden tiedot, toimintaohje vahinkojen kartoittamisesta, järjestelmän palautus- ja uudelleenkäynnistysohjeet sekä siirtyminen takaisin normaaliin toimintaan. Lisäksi suunnitelman tulisi olla aina ongelmatilanteesta palautumisesta vastaavien henkilöiden ulottuvilla. Sen saatavuus pelkästään organisaation intranetistä tai tiedostopalvelimelta ei ole missään tapauksessa suositeltavaa, koska juuri nuo palvelut voivat olla ongelmasta johtuen tavoittamattomissa, jolloin suunnitelmaan ei pääse käsiksi. Suunnitelma suositellaan jaettavan kyseisille henkilöille esim. paperilla, CD-levyllä, USB-tikulla jne. (Gregory, P. H. 24.)

3.4 Suunnitelmassa huomioonotettavat asiat

Esimerkkejä suunnitelman ennaltaehkäisevistä tekijöistä ovat Peter Gregoryn mukaan varavirran sekä useamman kommunikaatioreitin suunnittelu. Hän mainitsee myös varmuuskopioiden ja kahdennettujen järjestelmien sijoittamisen fyysisesti toiseen sijaintiin (Gregory, P. H. 24.).

Varavirtajärjestelmät, kuten esimerkiksi UPS, jotka käynnistyvät päävirran katketessa, vähentävät sähkökatkosten vaikutusta palvelujen saatavuuteen. UPS on hyvä lyhyiden sähkökatkosten vaikutusten vähentämiseen, koska se varaa virtaa akkuihinsa ja pystyy takaamaan järjestelmien toiminnan omalla virrallaan päävirran katketessa (Wallace, M. & Webber, L. 151.). Virransyötön lisäksi UPS myös tasoittaa sähköverkon virtapiikkejä, jotka voivat vahingoittaa palvelimien komponentteja (Alertra).

Kahdennetut järjestelmät eri paikkakunnilla - tai jopa eri maissa - ja säännöllinen varmuuskopiointi ovat tärkeiden järjestelmien kannalta yksi parhaimmista tavoista taata minimaalinen vika-aika järjestelmiin ja nopea palautuminen vikatilanteista. Internetin välityksellä tarjotut palvelut asiakkaalle voivat sijaita fyysisesti missä tahansa, jos yhteydet toimivat ja palvelut on suunniteltu hyvin eikä yhteyden viive vaikuta palvelujen toimivuuteen. (Gregory, P. H. 24.)

Ihmiset tekevät virheitä, tietomurtoja tapahtuu ja kovalevyjä hajoaa. Siksi datan varmuuskopiointi on äärettömän tärkeää ja ainoa mahdollisuus palauttaa menetetty data. Hyvin suunniteltu ja toteutettu varmuuskopiointikäytäntö on organisaatiolle erittäin tärkeää. Varmuuskopiot tärkeimmistä järjestelmistä ja datasta olisi suositeltavaa ottaa vähintään kerran vuorokaudessa. (Varghese, M. 124-125.)

Varmuuskopiointi sisältää datan, esimerkiksi dokumentit ja sähköpostit. Myös käyttöjärjestelmien ja ohjelmistojen varmuuskopiointi on tärkeää varsinkin ennen järjestelmiin tehtäviä muutoksia. Näin ongelmien ilmaantuessa voidaan palata alkuperäiseen tilanteeseen varmuuskopiosta. Varmuuskopioinnin voi toteuttaa kokonaisvaltaisena kopiointina, jolloin kaikki data tallennetaan, tai vaihtoehtoisesti tallentaa täyden varmuuskopion päälle vain ne tiedostot, joihin on tehty viime aikoina muutoksia. (Varghese, M. 125-126.)

Varmuuskopiointi voidaan toteuttaa Peter Gregoryn mukaan vanhanaikaisesti magneettinauhalla tai nykyään suosiossa olevilla kovalevyillä, jotka voidaan helposti irrottaa tai kytkeä tallennuslaitteeseen. Kestävä tapa varmuuskopiointiin on rakentaa useamman kovalevyn RAID-tallennusjärjestelmä, jossa hajonnut kovalevy voidaan vaihtaa uuteen menettämättä dataa. Järjestelmään voidaan myös sisällyttää kahdennetut virtalähteet ja palvelinyhteydet sekä virtualisoitu tallennuskapasiteetti, jota voidaan joustavasti lisätä tallennustilan lähestyessä loppua. Varmuuskopioitua dataa voidaan myös suojata kahdentamalla, jolloin varmuuskopiot ovat vaihtoehtoisella palvelimella, josta palautus onnistuu lähes reaaliajassa ongelman ilmentyessä. (Gregory, P. H. 176, 179-180.)

Varmuuskopiointi on erittäin tärkeä osa palvelimen ongelmista palautumisen onnistumisen varmistamista. Joissain tilanteissa, kuten laiterikoissa tai tietokantojen korruptoitumisessa, varmuuskopiosta palauttaminen voi olla ainoa tapa varmistaa organisaation palvelimien toiminnan jatkuvuus. Määrittelemällä palvelimille säännölliset varmuuskopioinnit voidaan vähentää palvelimen häiriöaikaa ongelmien ilmaantuessa. (Alertra)

4 DOMAIN CONTROLLERIN VARMUUSKOPIOINTIVAIHTOEHDOT

Palvelimien varmuuskopioinnissa on tilanteesta riippuen eri vaihtoehtoja. Varmuuskopiointitavan määrittelee se, kuinka usein Active Directoryyn tehdään muutoksia sekä mitä dataa ja ohjelmistoja palvelin sisältää (Minasi, M & Greene, K & Booth, C. 1576). Microsoftin suosittelema tapa on käyttää Windows Server Backup -ohjelmistoa (Microsoft, 2013), mutta jos organisaatiolla on tarve vanhanaikaisempaan ratkaisuun, kuten magneettinauhalle tallentamiseen, tällöin on käytettävä toista ratkaisua, esimerkiksi Microsoft System Center 2012 R2 Data Protection Manager (Minasi, M & Greene, K & Booth, C. 1556.).

Domain controllerien varmuuskopiointi on kriittinen toimenpide jokaiselle organisaatiolle. Varmuuskopiot suojaavat datan menettämiseltä palvelimen häiriötilanteessa tai hallintavirheessä. Häiriötilanteen tai hallintavirheen, kuten tahattoman käyttäjien tai muiden objektien poiston tapahtuessa, on tarpeellista palauttaa domain controller tilanteeseen, jossa virhettä ei ole vielä tapahtunut. Tuettu tapa domain controllerin palauttamiseen on käyttää Active Directory -yhteensopivaa varmuuskopiointiohjelmistoa, kuten Windows Server Backup. (Microsoft, 2013.)

Virtualisoitua domain controlleria varmuuskopioidessa ja palauttaessa vältettäviä käytäntöjä ovat mm. Snapshotin sekä VHD-tiedoston käyttäminen varmuuskopiona. VHD-tiedoston tallennuksen jälkeen se sisältää vanhentunutta tietoa, koska se ei sisällä Active Directoryssa tehtyjä muutoksia tallennuksen jälkeen. Tämä voi johtaa replikoinnin epäonnistumiseen palauttamisen jälkeen, koska palautetun domain controllerin datassa on eroavaisuuksia toimivaan domain controlleriin. Sama pätee Snapshotin palauttamiseen aiempaan ajankohtaan. (Microsoft, 2013.)

Huomioon otettava asia varmuuskopiointia suunniteltaessa on lisäksi se, että varmuuskopion ottaminen vaatii paljon resursseja palvelimelta. Tämän vuoksi varmuuskopiointi on hyvä ajoittaa siten, että palvelimen palveluilla ei olisi silloin paljon aktiivisia käyttäjiä, esimerkiksi yöllä. Jos varmuuskopiointi suoritetaan aikana, jolloin palveluita käytetään, voivat käyttäjät valittaa palveluiden hitaasta toiminnasta, ja heidän järjestelmässä tekemänsä asiat voivat hidastaa varmuuskopiointia. (Minasi, M & Greene, K & Booth, C. 1559.)

Domain controllerien varmuuskopiointiin on useampia eri tapoja. Nämä toimenpiteet voidaan tehdä joko Windows Server Backup -ohjelmasta, komentoriviltä tai Powershellillä. Varmuuskopio voi sisältää järjestelmän tilan, valitut kovalevyt, tiedostot ja kansiot tai kaikki edellä mainitut. Varmuuskopiot voidaan ottaa Windows Server Backup -ohjelmalla tilanteesta riippuen järjestelmässä oleville kovalevyille tai siirrettäville kovalevyille. Suositeltu tallennustapa on ottaa varmuuskopiot useille siirrettäville kovalevyille, jotta osa niistä voidaan siirtää fyysisesti eri paikkaan säilytettäväksi, vaihtaen levyjä säännöllisin väliajoin. Lisäksi Microsoft on mahdollistanut varmuuskopioiden tallentamisen pilveen Windows Azure Backup -lisäpalikalla. Myös Windows Server 2008 R2:ssa tullut Active Directory -roskakori on hyvä ottaa käyttöön ympäristöissä, joissa se on mahdollista. (Minasi, M & Greene, K & Booth, C. 1557-1577.)

4.1 Täysi varmuuskopio

Täyden varmuuskopion ottaminen palvelimesta on yksi helpoimmista ja parhaista tavoista varmistaa palauttamisen onnistuminen. Täysi varmuuskopio sisältää palvelimen kaikki levyosiot, tietokannat sekä järjestelmän sen hetkisen tilanteen. Täydestä varmuuskopiosta voidaan palauttaa yksittäisiä tiedostoja ja kansioita tai kokonaisia levyosioita, jos palvelimen kovalevy vioittuu. Siitä voi tehdä palautuksen myös tilanteessa, jossa koko palvelin rautoineen on vaihdettu. Haittana täydessä varmuuskopiossa on sen koko sekä aika, joka menee palauttamiseen. Mark Minasi, Kevin Greene ja Christian Booth suosittelevat kirjassaan Mastering Windows Server 2012 R2 ulkoisen USB- tai eSATA-kovalevyn käyttämistä varmuuskopiointiin. Heidän mukaansa paras varmuuskopiointijärjestelmä sisältää useita ulkoisia kovalevyjä, joita käytetään vuorotellen ja varastoidaan toiseen rakennukseen nostaen näin suojauksen tasoa vikatilanteita varten. Windows Server Backup osaa automaattisesti konfiguroinnin jälkeen tunnistaa levyt, joita käytetään varmuuskopiointiin, käyttäen paikalla olevaa levyä ja tehden siihen tilaa uudelle varmuuskopiolle poistamalla vanhemmat varmuuskopiot uuden tieltä. (Minasi, M & Greene, K & Booth, C. 1557.)

4.2 Active Directoryn varmuuskopiointi

Windows Server Backup -ohjelmalla voidaan ottaa varmuuskopio järjestelmän tilasta, jota käytetään Active Directoryn palauttamiseen. Tämä varmuuskopio sisältää Active Directoryn tietokannan (Ntds.dit), rekisterin, COM+ rekisteröinnin tietokannan, Active Directory Certificate Services -tietokannan, käynnistystiedostot, SYSVOL -kansion, Cluster -palvelun tiedot, järjestelmän tiedostot, jotka ovat suojattuna Windows Resource suojauksella sekä Microsoft Internet Information Services hakemiston. (Minasi, M & Greene, K & Booth, C. 1576.)

Active Directoryn palauttaminen tarvitsee ongelmien ilmaantuessa vähintään järjestelmän tilan varmuuskopion. Active Directory voidaan toki palauttaa myös täydestä varmuuskopiosta, koska se sisältää myös järjestelmän tilan varmuuskopion. Kannattavan varmuuskopion tyyppi domain controllereille riippuu siitä, kuinka paljon muutoksia tietokantaan ja dataan tehdään tai mitä ohjelmistoja palvelimelle on asennettu. (Minasi, M & Greene, K & Booth, C. 1576.)

4.3 Tiedostojen ja kansioiden varmuuskopiointi

Kolmas vaihtoehto Windows Server Backup -ohjelmalla varmuuskopiointiin on valittujen tiedostojen ja kansioiden varmuuskopiointi. Tätä tapaa käytetään, kun halutaan varmistaa datan säilyvyys tilanteissa, joissa sitä muutetaan jatkuvasti eikä olla niinkään kiinnostuneita palauttamaan käyttöjärjestelmää. Pelkän datan varmuuskopiointi voi olla hyödyllistä tapauksissa, joissa käyttöjärjestelmä voidaan palauttaa levykuvasta, minkä jälkeen data palautetaan varmuuskopiosta. (Minasi, M & Greene, K & Booth, C. 1566.)

5 DOMAIN CONTROLLERIN PALAUTUSMENETELMÄT

Tässä osiossa esitellään eri vaihtoehdot domain controllerin palauttamiseksi ongelmatilanteen jälkeen. Nämä tavat ovat täysi palautus, Active Directoryn palautus, tiedostojen ja kansioiden palautus sekä palautus uudelleenasentamalla palvelin. Lisäksi osiossa käsitellään, missä tilanteessa kutakin palautusmenetelmää yleensä käytetään.

5.1 Täysi palautus

Pahimmassa tilanteessa, jossa Active Directoryn tietokanta on korruptoitunut, palvelimen komponentit hajonneet tai toimialueeseen ei muuten pääse käsiksi, se täytyy palauttaa varmuuskopiosta. Tässä tapauksessa käytetään käyttöjärjestelmän asennusmediaa ja täyttä varmuuskopiota järjestelmän palauttamiseksi tilanteeseen, jolloin se vielä toimi. Tämä järjestelmän palauttamistapa on kohdistettu pienemmille ympäristöille, eikä se ole toteuttamiskelpoinen suuremmissa ympäristöissä, joissa on useampia domain controllereja. (Minasi, M & Greene, K & Booth, C. 1562.)

5.2 Active Directoryn palautus

Active Directoryn palauttamiseen varmuuskopiosta on kaksi tapaa. Nämä tavat ovat autoritäärinen ja ei-autoritäärinen palautus. Molemmat palautukset täytyy tehdä Directory Services Restore Modessa (DRSM), joka vaatii palvelimen uudelleenkäynnistämisen kyseiseen tilaan. (Minasi, M & Greene, K & Booth, C. 1580.)

Ei-autoritäärisessä palautuksessa domain controller palautetaan tilaan, jossa se oli varmuuskopiota otettaessa. Kun domain controller on palautettu, se replikoi tietokantansa muilta domain controllereilta sen hetkisen Active Directory -tietokannan mukaiseksi. (Minasi, M & Greene, K & Booth, C. 1580.)

Autoritäärinen palautus antaa mahdollisuuden palauttaa Active Directoryn objekteja, jotka on poistettu tietokannasta, mutta ei anna replikoinnin toiselta palvelimelta päällekirjoittaa palautettuja objekteja. Sen sijaan palautetut objektit replikoituvat autoritäärisesti muille domain controllereille toimialueessa. (Minasi, M & Greene, K & Booth, C. 1580.)

5.3 Tiedostojen ja kansioiden palautus

Yksittäisten tiedostojen ja kansioiden palautus on useille järjestelmänvalvojille tavanomainen tehtävä. Käyttäjä on saattanut vahingossa poistaa tärkeän dokumentin, jota hän huomaakin tarvitsevansa. Palautus voidaan tehdä helposti ja nopeasti, jos kansio tai kovalevy, jossa dokumentti sijaitsee, on varmuuskopioitu ennen tiedoston poistamista. (Minasi, M & Greene, K & Booth, C. 1567.)

5.4 Domain controllerin palautus uudelleenasentamalla

Domain controllerin palautus uudelleen asentamalla on sama prosessi kuin uuden luominen, eikä palautusta tarvitse tässä tapauksessa tehdä varmuuskopiosta. Edellä mainittu tapa palauttaa domain controller on riippuvainen Active Directoryn replikoinnista, ja jotta tätä tapaa voidaan käyttää, tulee Active Directoryssa olla toinen, ehjä domain controller. Tämä on ainut tapa palauttaa domain controller, josta ei ole varmuuskopioita. Lisäksi tätä tapaa voidaan käyttää ei-autoritäärisen palautuksen sijaan silloin, kun varmuuskopiointimediaa ei ole saatavilla. Domain controllerin palautus uudelleen asentamalla ei tulisi kuitenkaan olla vastine säännöllisten varmuuskopioiden ottamiselle. (Microsoft, 2009.)

Tätä tapaa käytettäessä domain controller vaatii täyden käyttöjärjestelmän uudelleen asentamisen, ja on suositeltavaa, että ennen kuin asennus tehdään, palvelimen kovalevy formatoidaan. Ennen formatointia tulee kuitenkin varmistaa, että kaikki tärkeä data on siirretty kovalevyltä talteen. Lisäksi tässä tavassa tulee pois-

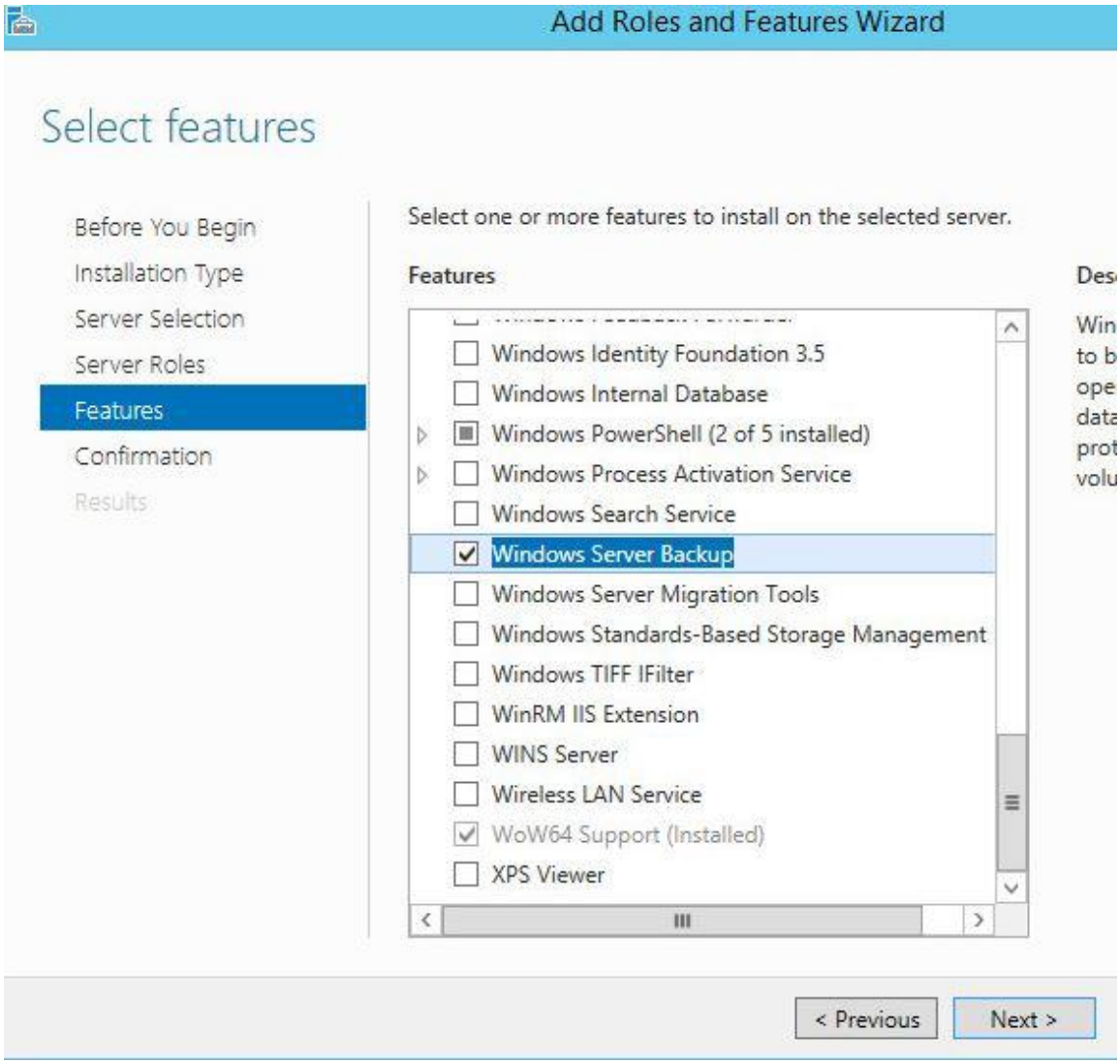
taa palvelimen metadata Active Directorysta toisella domain controllerilla. Jos palautettava palvelin halutaan nimetä eri nimiseksi kuin poistettu, täytyy myös poistaa vanhan palvelimen objekti Active Directorysta. (Microsoft 2009)

6 DOMAIN CONTROLLERIN VARMUUSKOPIOINTI KÄYTÄNNÖSSÄ

Työn käytännön osuudessa pyritään selvittämään, kuinka Windows Server 2012 R2 domain controllerin varmuuskopiointi käytännössä tehdään ja mitä asioita tätä tehdessä tulee ottaa huomioon, jotta voidaan välttyä mahdollisilta ongelmilta. Työssä käydään läpi domain controllerin varmuuskopiointi ja palautus, koska siinä tulee ottaa enemmän asioita huomioon kuin normaalin palvelimen palautuksessa. Työn käytännön osuutta varten on asennettu kaksi virtuaalista Windows Server 2012 R2 domain controlleria koulun ESXi-hostille käyttäen VMwaren vSphereä.

6.1 Windows Server Backup -ohjelman asennus

Windows Server Backup on Active Directory -yhteensopiva varmuuskopiointiohjelmisto, joka voidaan asentaa domain controllerille hallintavalikosta. Asennus on nopea ja suoraviivainen. Ensin avataan hallintavalikko, valitaan sieltä Add Roles and Features -vaihtoehto ja valitaan asennuksessa Features-valikon kohdalla tarvittava asennuspaketti, kuten kuvassa 5 on nähtävissä. Asennus kestää vain pari minuuttia.



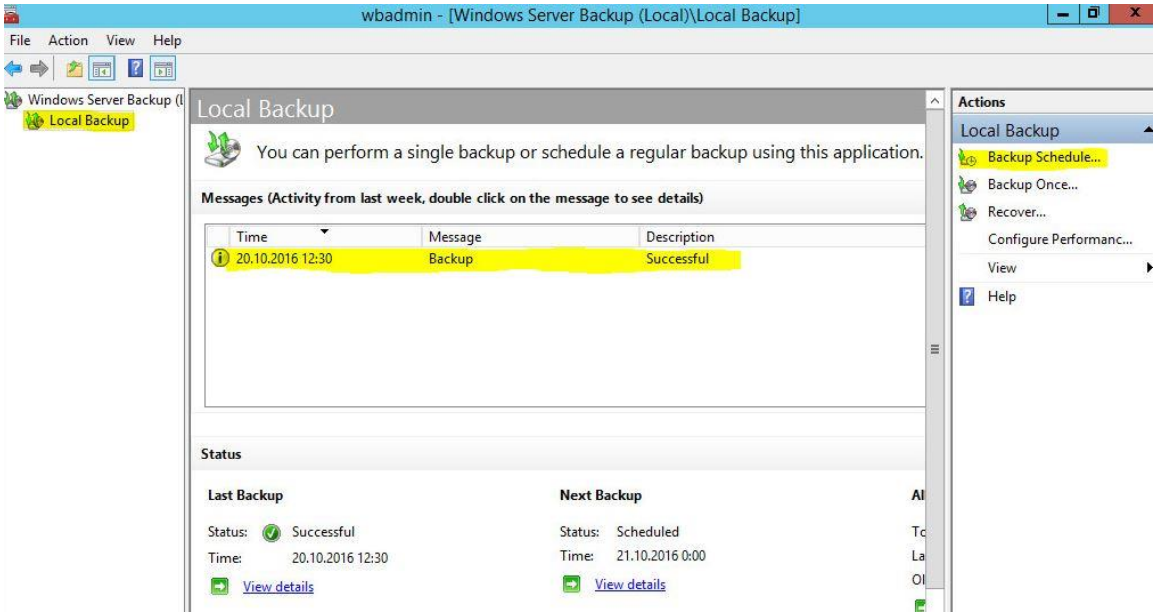
Kuva 5. Windows Server Backup -ohjelman asennus.

6.2 Domain controllerin täysi varmuuskopiointi Windows Server Backup -ohjelmalla

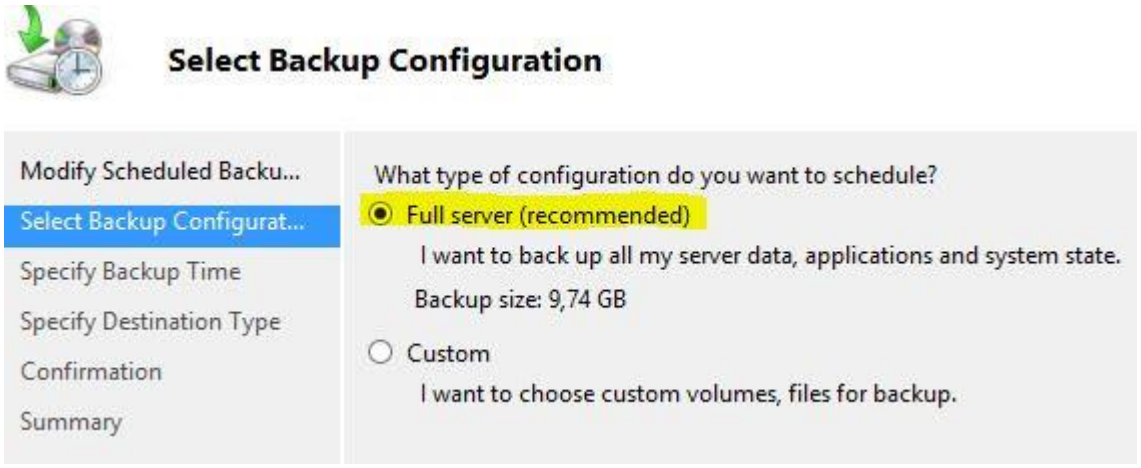
Tässä esimerkissä on käytetty järjestelmän rajoituksista johtuen varmuuskopiointiin aiemmin palvelimelle lisättyä ylimääräistä virtuaalista kovalevyä suositellun siirrettävän kovalevyn sijaan. Varmuuskopiointi Windows Server Backupilla tehdään käynnistämällä ohjelma palvelimen Tools-valikosta. Ohjelmassa valitaan vasemmalla hiiren painikkeella vasemmasta laidasta ”Local Backup”, jonka jälkeen ruudun oikeaan laitaan tulee näkyviin ”Backup Schedule” –valikko, joka on nähtävissä kuvassa 6. Tällä työkalulla voidaan valita, mitä, milloin ja mihin varmuuskopioidaan.

Täyden varmuuskopion ottamisessa valitaan vaihtoehto ”Full server (recommended)”, kuten kuvassa 7. Seuraavassa kohdassa valitaan aika, jolloin varmuuskopiot tallennetaan kuvan 8 mukaisesti.

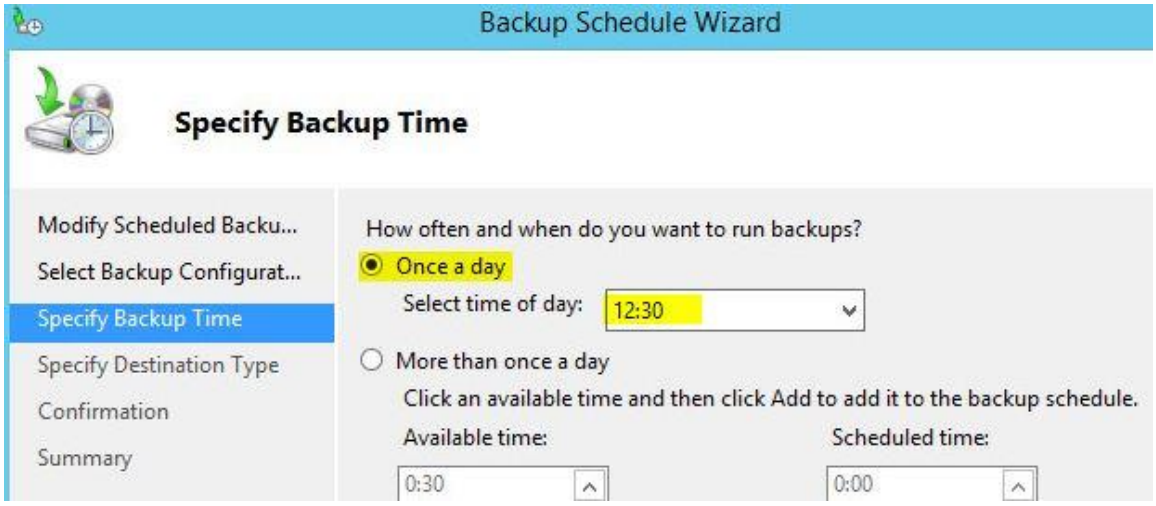
Esimerkissä valitaan varmuuskopioinnin ajaksi 12:30 aikataulusyistä, koska palvelimella ja toimialueella ei ole muita käyttäjiä. Seuraavassa kohdassa valitaan, millaiselle alustalle varmuuskopiointi tehdään, kuten nähdään kuvassa 9. Tähän valitaan ylin, suositeltu vaihtoehto. Viimeisenä valitaan levy, johon varmuuskopiot otetaan. Tämä toimenpide näkyy kuvassa 10. Tämän jälkeen saadaan kuvan 11 mukainen varmistus, onko varmuuskopioinnin ajastuksen luominen onnistunut. Varmuuskopioinnin onnistuminen voidaan todeta Windows Server Backup -ohjelman tapahtumalokista, joka on näkyvissä kuvassa 6.



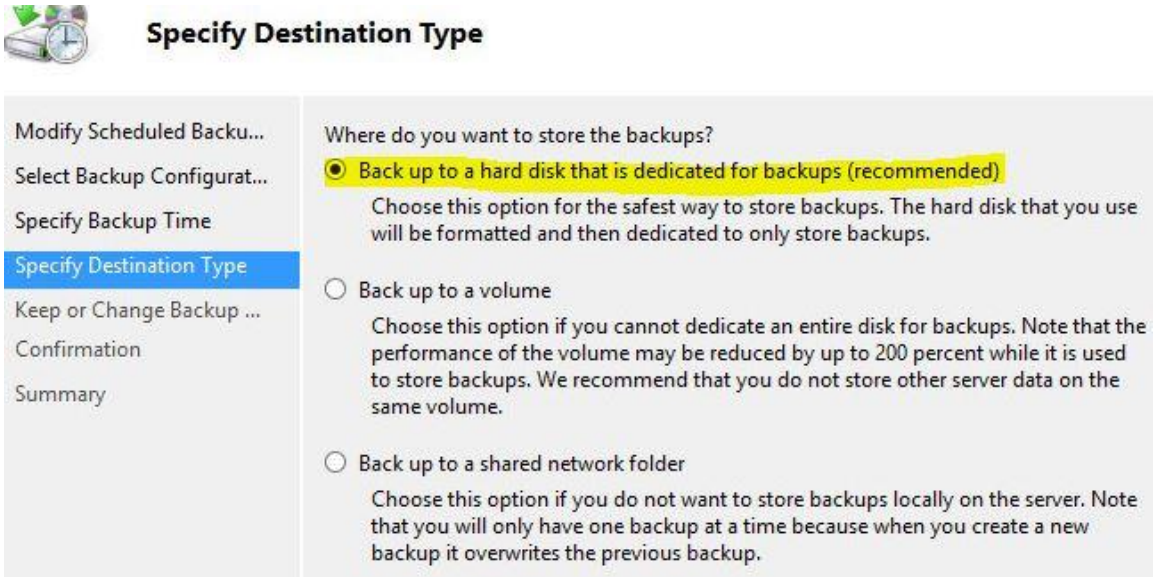
Kuva 6. Windows Server Backup GUI ja varmuuskopioinnin onnistumisen toteaminen



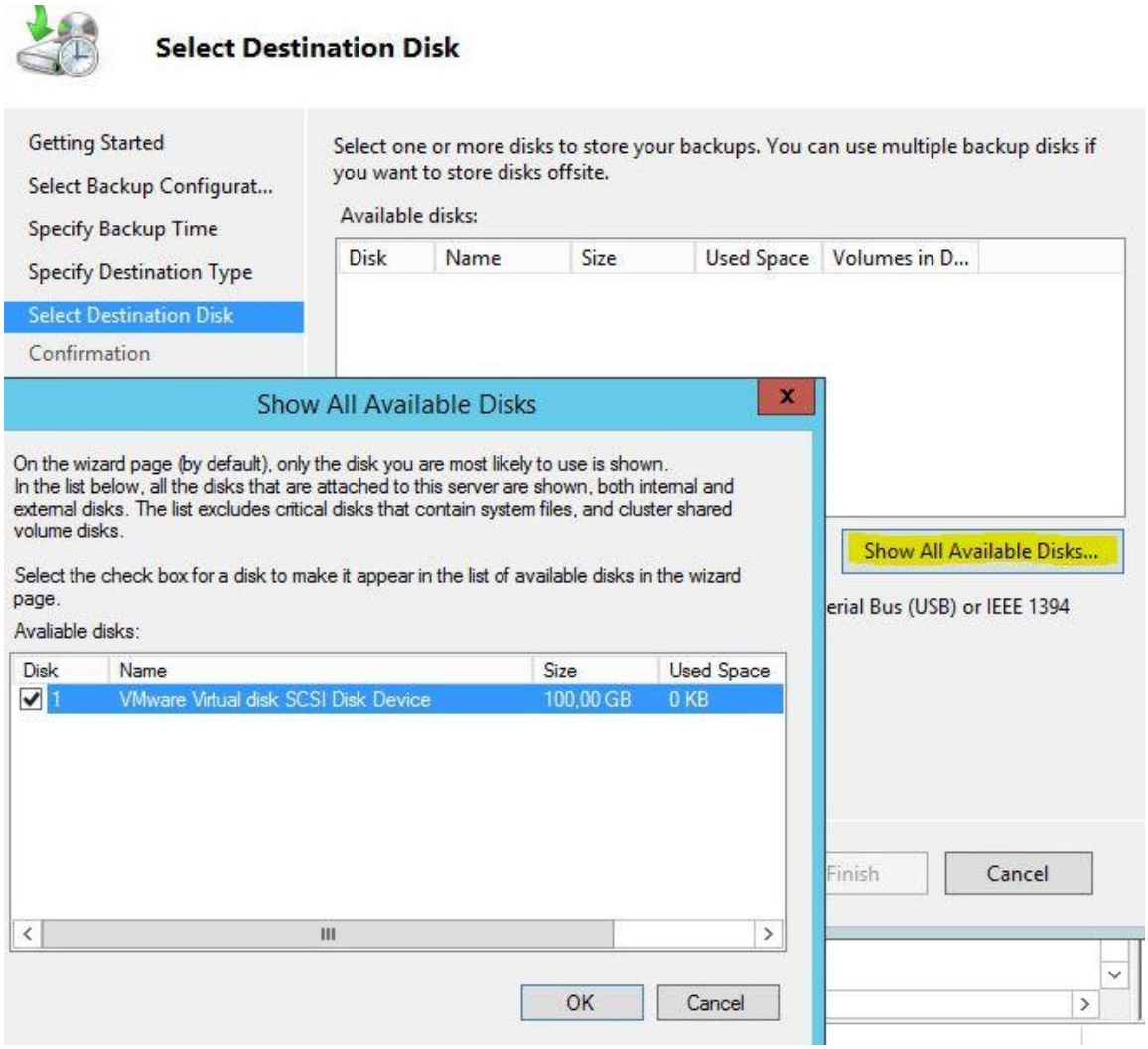
Kuva 7. Valitaan, mitä varmuuskopioidaan.



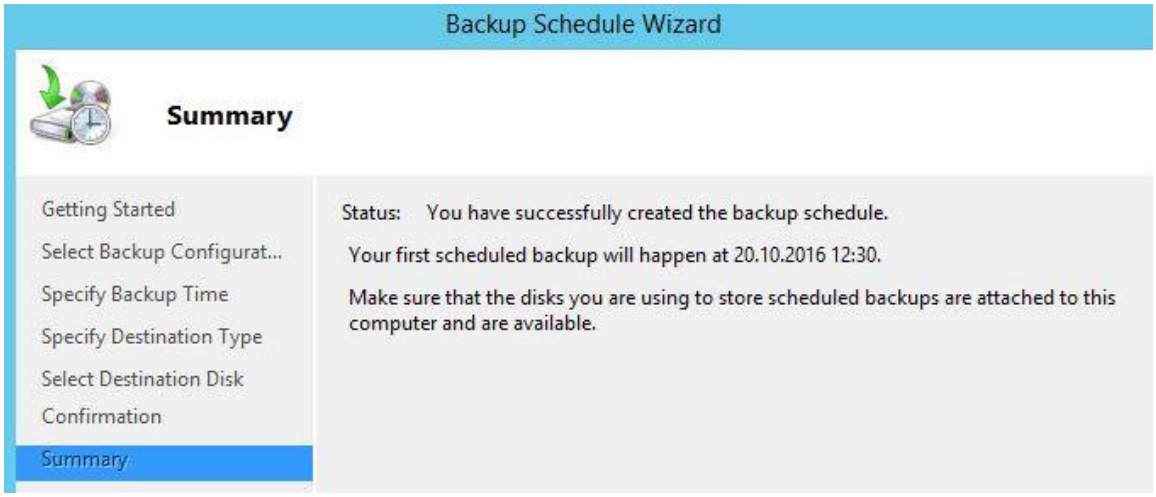
Kuva 8. Valitaan kellonaika varmuuskopioinnille.



Kuva 9. Valitaan tallennuskohteen tyyppi.



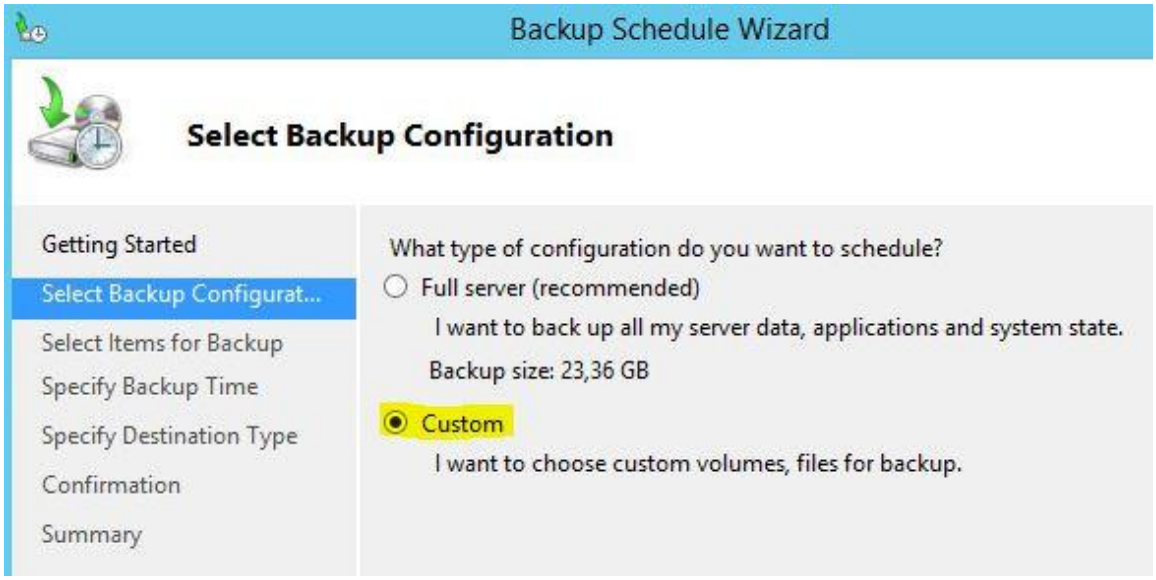
Kuva 10. Valitaan levy, johon varmuuskopiointi tehdään.



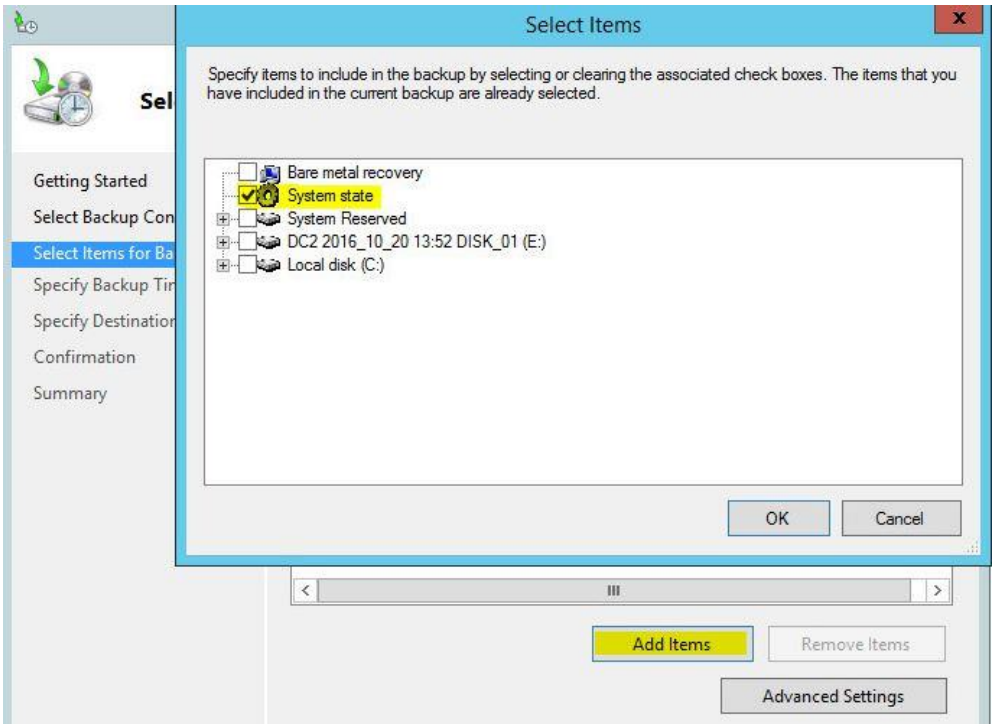
Kuva 11. Varmistus varmuuskopioinnin ajastuksen onnistumisesta.

6.3 Active Directoryn varmuuskopiointi Windows Server Backup –ohjelmalla

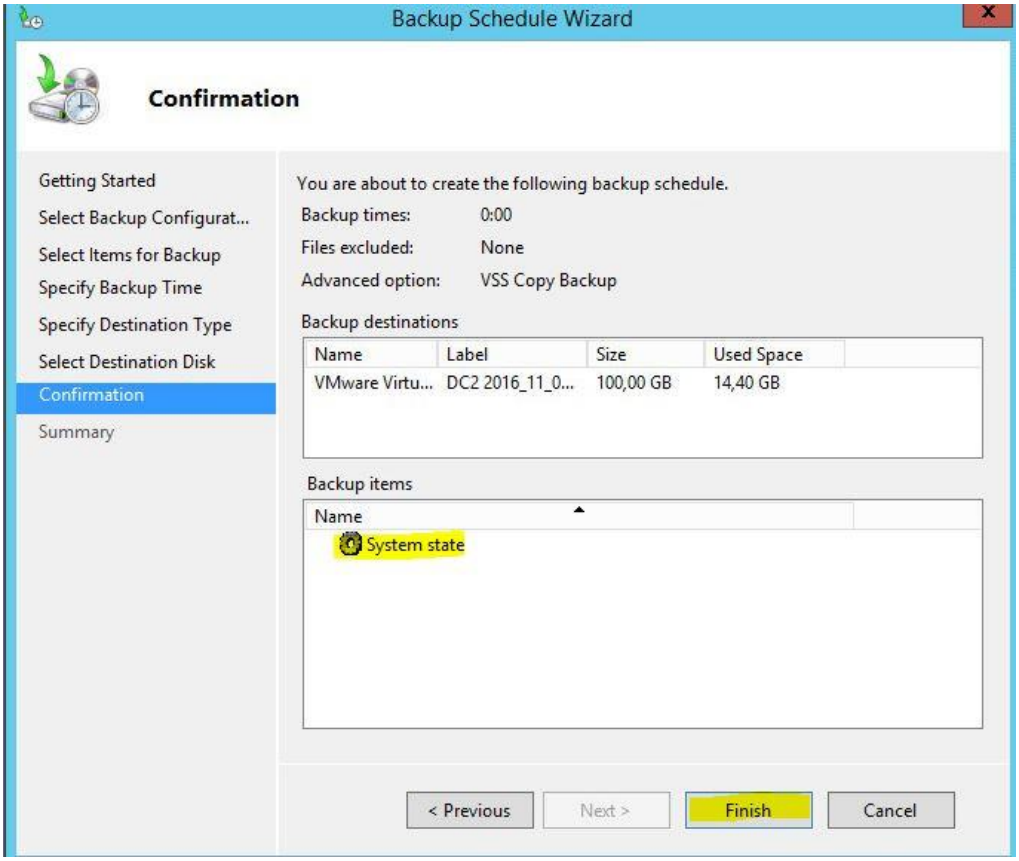
Järjestelmän tilan varmuuskopiointi antaa mahdollisuuden palauttaa Active Directoryn tietokanta ongelmien ilmaantuessa. Tämä varmuuskopiointi toteutetaan seuraavasti: Ensin käynnistetään Windows Server Backup -ohjelma kuten edellisessä kappaleessa. Tässäkin esimerkissä valitaan oikeasta laidasta ”Backup Schedule” toiminto, jonka jälkeen valitaan haluttu varmuuskopiointimalli. Kuten kuvassa 12 näkyy, valitaan vaihtoehto ”Custom”. Seuraavaksi valitaan, mitä varmuuskopioon sisällytetään. Valitaan kuvan 13 mukaisesti ”Add Items”, josta valitaan varmuuskopioitavaksi ”System state”. Seuraavaksi valitaan kovalevy, mihin varmuuskopiot otetaan sekä hyväksytään valinnat. Kuvassa 14 on nähtävissä valintojen viimeistely. Kun varmuuskopiointi on suoritettu, siitä tulee ilmoitus Windows Server Backup -ohjelmaan, kuten nähdään aiemmassa kuvassa 6.



Kuva 12. Valitaan varmuuskopion tyypiksi ”Custom”.



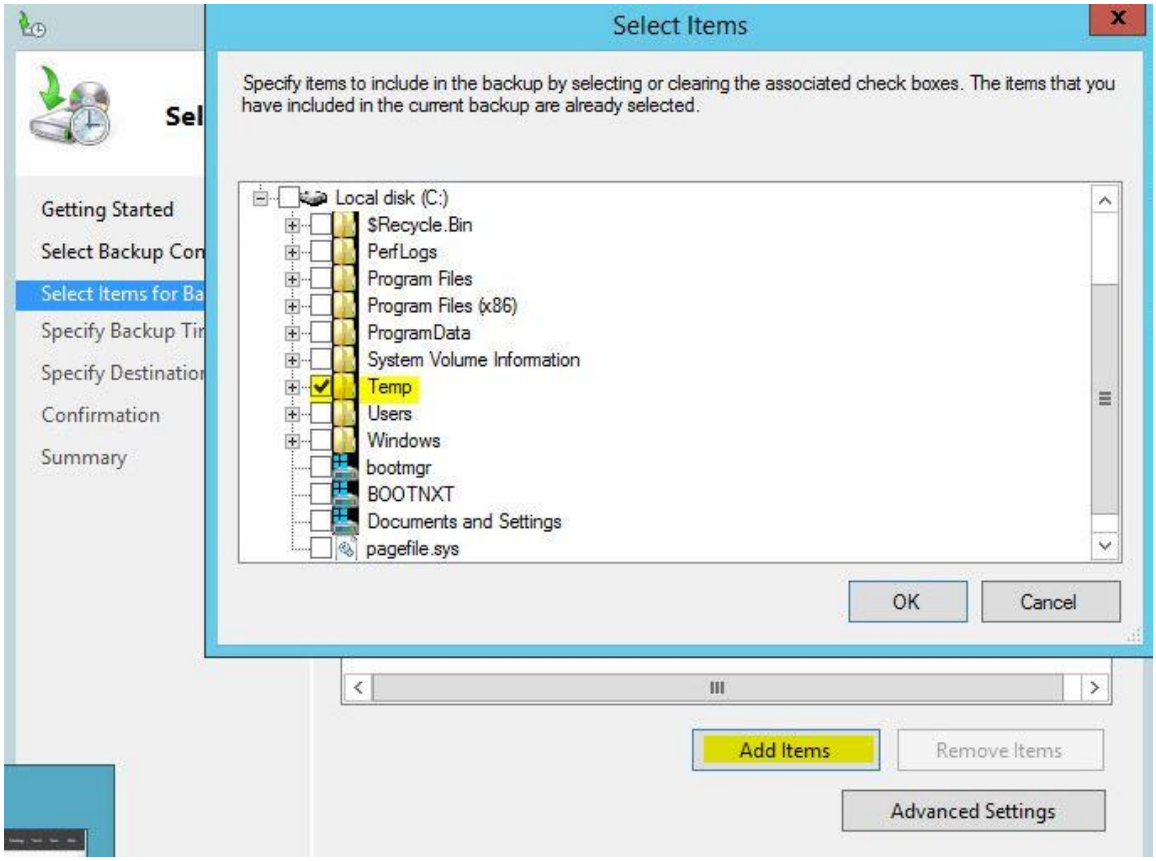
Kuva 13. Valitaan, mitä halutaan varmuuskopioida.



Kuva 14. Järjestelmän tilan varmuuskopioinnin viimeistely.

6.4 Tiedostojen ja kansioiden varmuuskopiointi Windows Server Backup –ohjelmalla

Windows Server Backup -ohjelmalla voi varmuuskopioida täyden- ja järjestelmän tilan varmuuskopioiden lisäksi myös yksittäisiä tiedostoja ja kansioita. Tämä tapahtuu kuten edellä mainitut varmuuskopioinnit Windows Server Backupin päänäkymästä valitsemalla oikeasta reunasta tarpeen mukaan joko ”Backup Schedule” tai ”Backup Once”. Valinnat tehdään kuten aiemmassakin esimerkissä, tällä kertaa kuitenkin valitsemalla haluttu kansio tai tiedosto järjestelmän tilan sijaan. Kuten kuvassa 15 nähdään, esimerkiksi on valittu Temp-kansio. Tämä kansio palautetaan myöhemmin varmuuskopiosta kansion poistamisen jälkeen. Toiminto viedään loppuun valitsemalla varmuuskopioinnin aika sekä kovalevy, johon varmuuskopio otetaan sekä hyväksymällä valinnat.



Kuva 15. Kansion valitseminen varmuuskopioitavaksi.

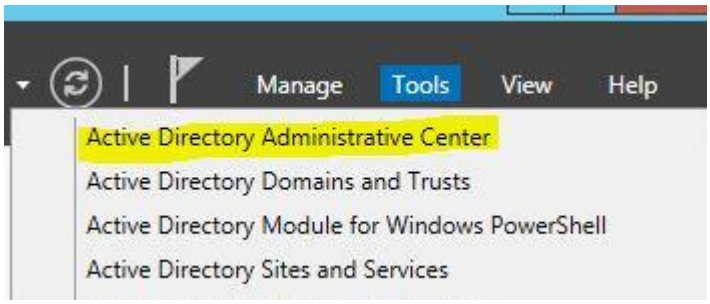
7 DOMAIN CONTROLLERIN PALAUTUS KÄYTÄNNÖSSÄ

Tässä osuudessa pyritään esittämään, kuinka Windows Server 2012 R2 domain controllerin palautus käytännössä tehdään ja mitä asioita tätä tehdessä tulee ottaa huomioon, jotta voidaan välttyä mahdollisilta ongelmilta. Lisäksi tässä osiossa selitetään Active Directory -roskakorin käyttö tilanteissa, joissa se on kannattavaa.

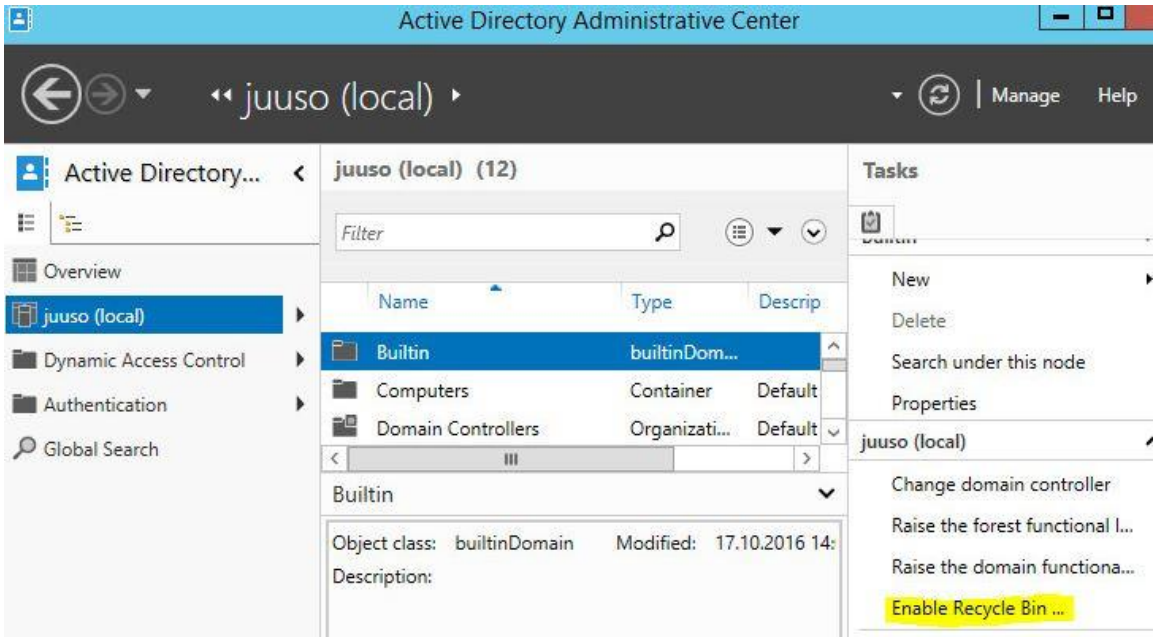
7.1 Poistetun objektin palautus Active Directoryn roskakorista

Yleisimmässä tapauksessa, jossa on esimerkiksi vahingossa poistettu käyttäjä Active Directorysta, palauttamisen helpoin tapa on käyttää Active Directoryn roskakoria. Jos järjestelmänvalvojalla on edelleen pääsy toimialueeseen, roskakori on nopein tapa tehdä yksittäisen objektin palautus, jos virhe huomataan heti. Tämä vaatii sen, että roskakori on otettu käyttöön ennen kuin virhe on tapahtunut. Vaatimus tämän ominaisuuden käytölle on vähintään yksi Windows Server 2012 R2 domain controller, jossa on Active Directory Administrative Center. Muiden domain controllerien on oltava Windows Server 2008 R2 tai uudempia. Lisäksi Active Directoryn Forestin täytyy olla toiminnalliselta tasoltaan vähintään Windows Server 2008 R2 tai uudempi. (Minasi, M & Greene, K & Booth, C. 1577-1578.)

Active Directoryn roskakori otetaan käyttöön Active Directory Administrative Centeristä, joka sijaitsee kuvassa 16 nähtävässä Tools-valikossa. Administrative Centerin käynnistyttyä valitaan sen vasemmasta reunasta paikallinen toimialue, ja tämän jälkeen roskakori otetaan käyttöön valitsemalla oikeasta reunasta ”Enable Recycle Bin”, joka näkyy kuvassa 17. Tämän jälkeen odotetaan, että valinta replikoituu myös toiselle domain controllerille tai tehdään replikointi manuaalisesti.

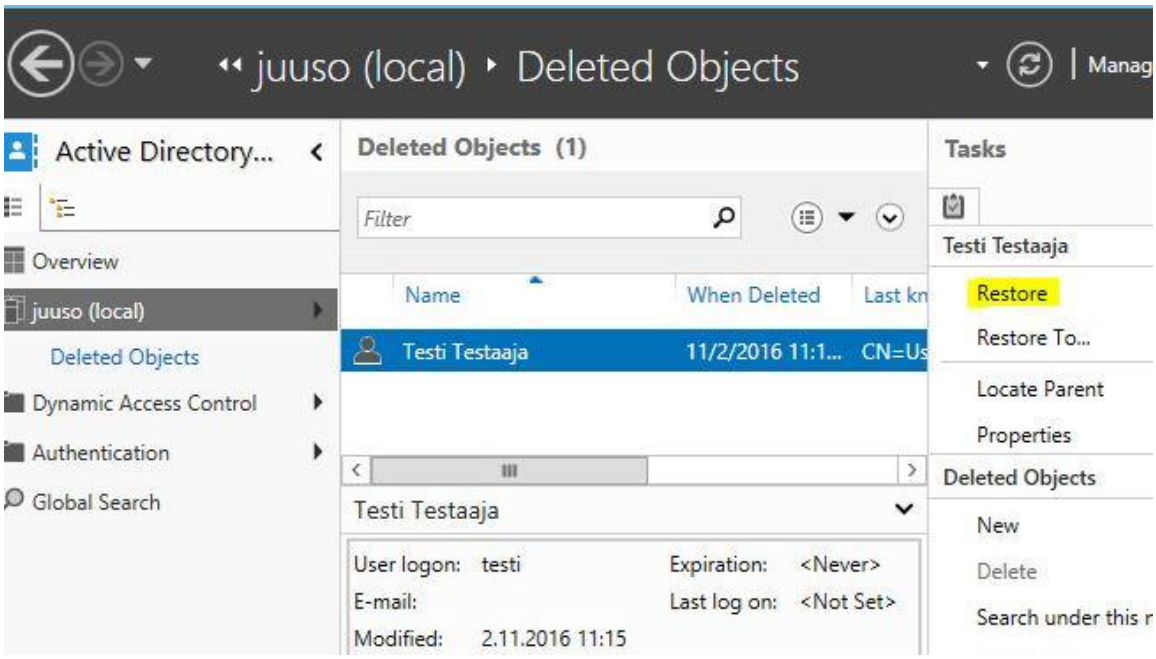


Kuva 16. Active Directory Administrative Centerin käynnistys.



Kuva 17. Active Directoryn roskakorin käyttöönotto.

Poistetun objektin palautus tapahtuu avaamalla ”Deleted Objects” -kansio Administrative Centerin keskinäkymästä. Täältä valitaan palautettava objekti ja klikataan ruudun oikeasta reunasta, kuvassa 18 näkyvästä ”Restore”-painikkeesta. Tämän jälkeen voidaan todeta objektin palautuminen sille kuuluvasta paikasta, tässä tapauksessa Active Directory Users and Computers.



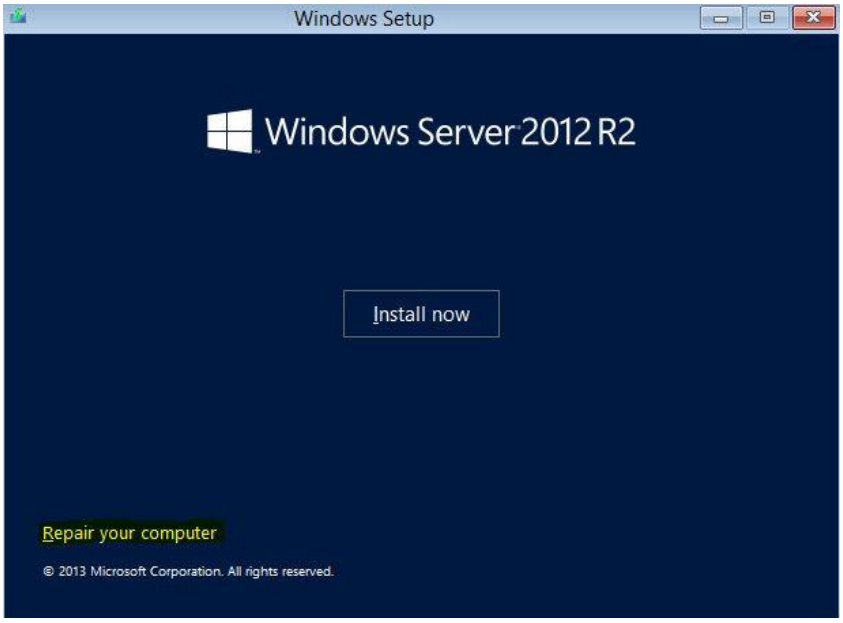
Kuva 18. Objektin palautus roskakorista.

7.2 Domain controllerin palautus täydestä varmuuskopiosta

Tässä esimerkissä on kaksi replikoivaa Domain Controlleria, DC1 ja DC2. Molemmista on otettu täydet varmuuskopiot niille osoitetuille ylimääräisille virtuaalisille kovalevyille. Palautus tapahtuu käynnistämällä palvelin sen käyttöjärjestelmän asennusmedialta, tässä tapauksessa Windows Server 2012 R2.

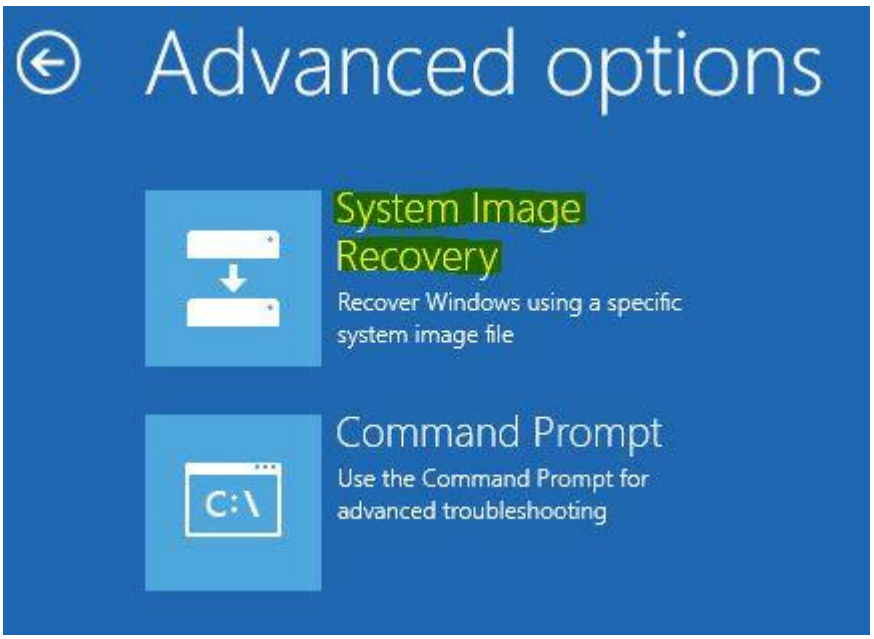
Palvelimen käynnistyessä asennusmedialta valitaan ensiksi kieliasetukset, ja seuraavasta kohdasta ”repair your computer” -valinta oikeasta alakulmasta, joka on nähtävissä kuvassa 19. Seuraavaksi valitaan kuvan 20 mukaisesti ”Troubleshoot”, eli ongelmanratkaisu, jonka jälkeen ”System Image Recovery” kuten kuvassa 21. Tämän jälkeen valitaan kuvan 22 mukaisesti, mihin varmuuskopion versioon järjestelmä halutaan palauttaa. Tässä esimerkissä on valittu viimeisin varmuuskopio, koska sen tiedetään toimivan. Tässä kohtaa voidaan palata tarvittaessa myös aiempiin varmuuskopioihin. Ylimääräisissä palautusvalinnoissa rastitetaan kohta ”Format and repartition disks”. Tämä on nähtävissä kuvassa 23. ”Exclude disks” -valintaa voidaan käyttää, jos halutaan palauttaa esimerkiksi vain käyttöjärjestelmä

eikä koskea muilla kovalevyillä sijaitsevaan dataan. Lopuksi voidaan todeta palvelin uudestaan käynnistämällä, onko toimenpide onnistunut.

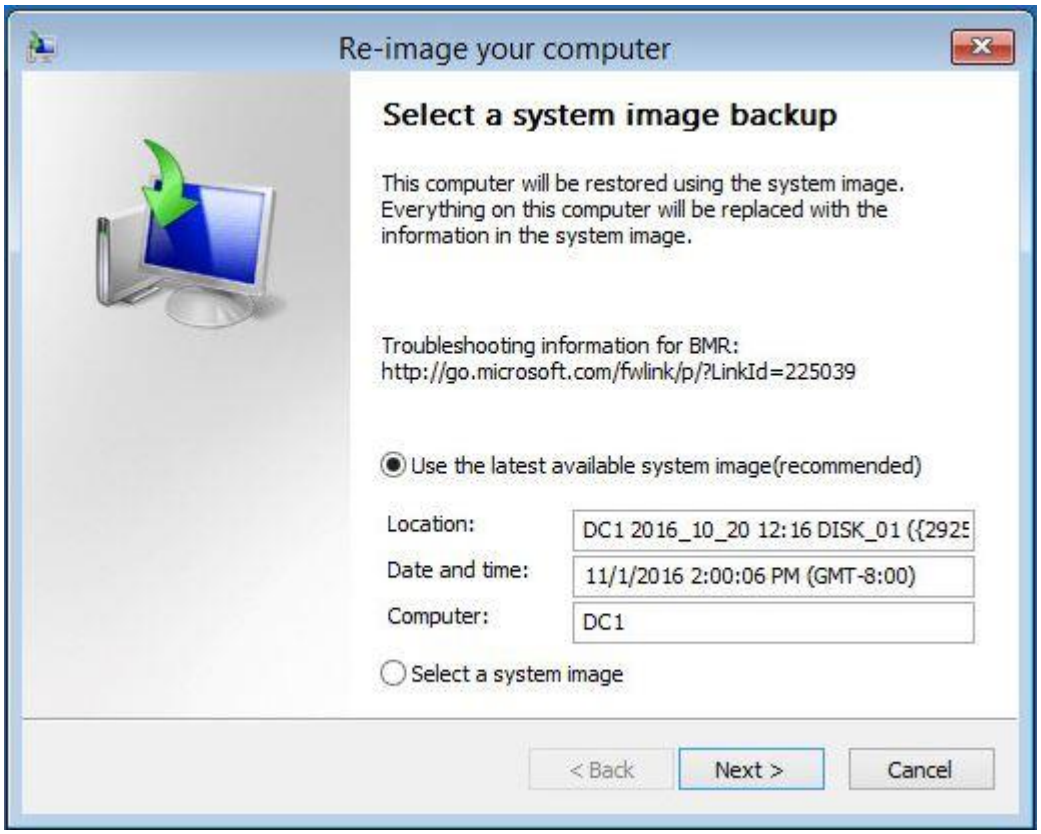


Kuva 19. Valitaan tietokoneen korjaus.

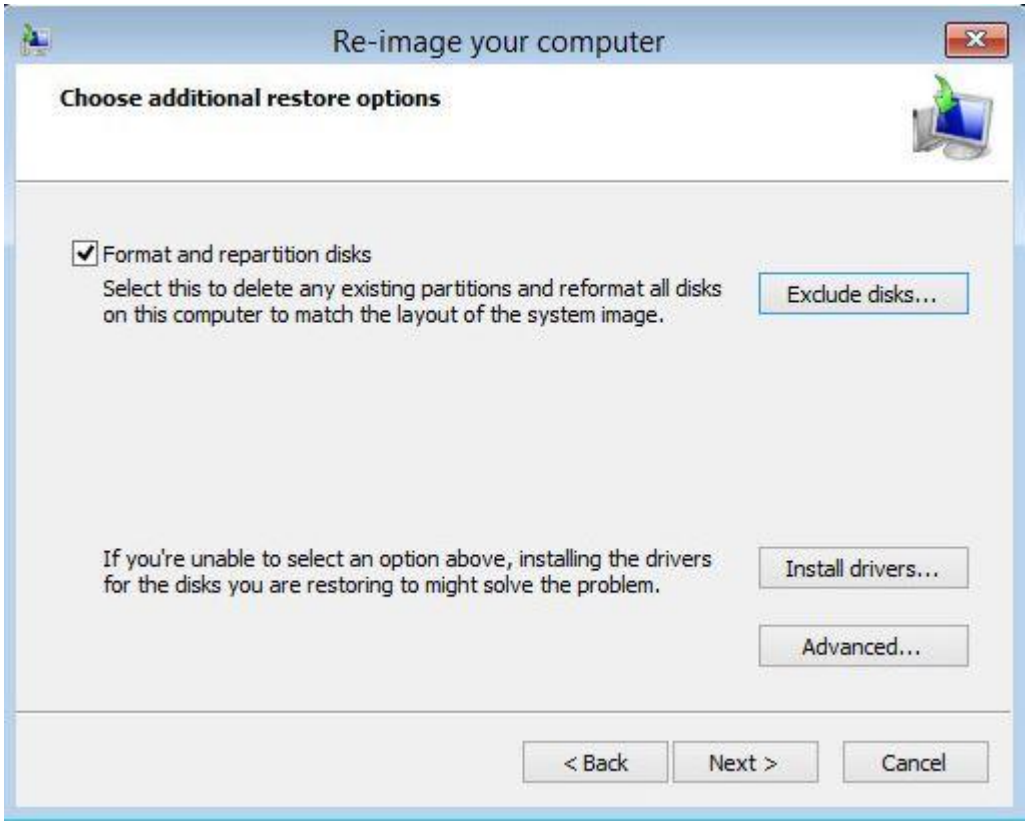
Kuva 20. Valitaan ongelmanratkaisu.



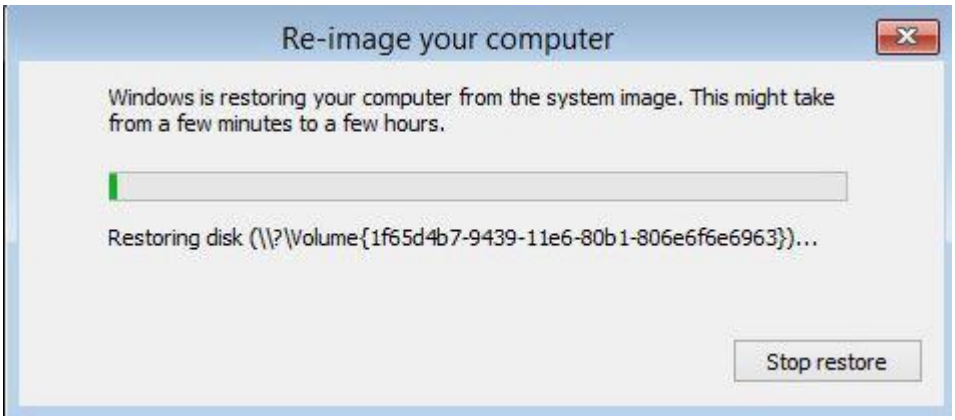
Kuva 21. Valitaan palautus varmuuskopiosta.



Kuva 22. Valitaan haluttu varmuuskopio palautusta varten. Tässä tapauksessa valittiin viimeisin varmuuskopio.



Kuva 23. Valitaan levyjen formatointi ja uudelleen partitiointi.



Kuva 24. Järjestelmän palauttaminen valitusta varmuuskopiosta käynnissä.

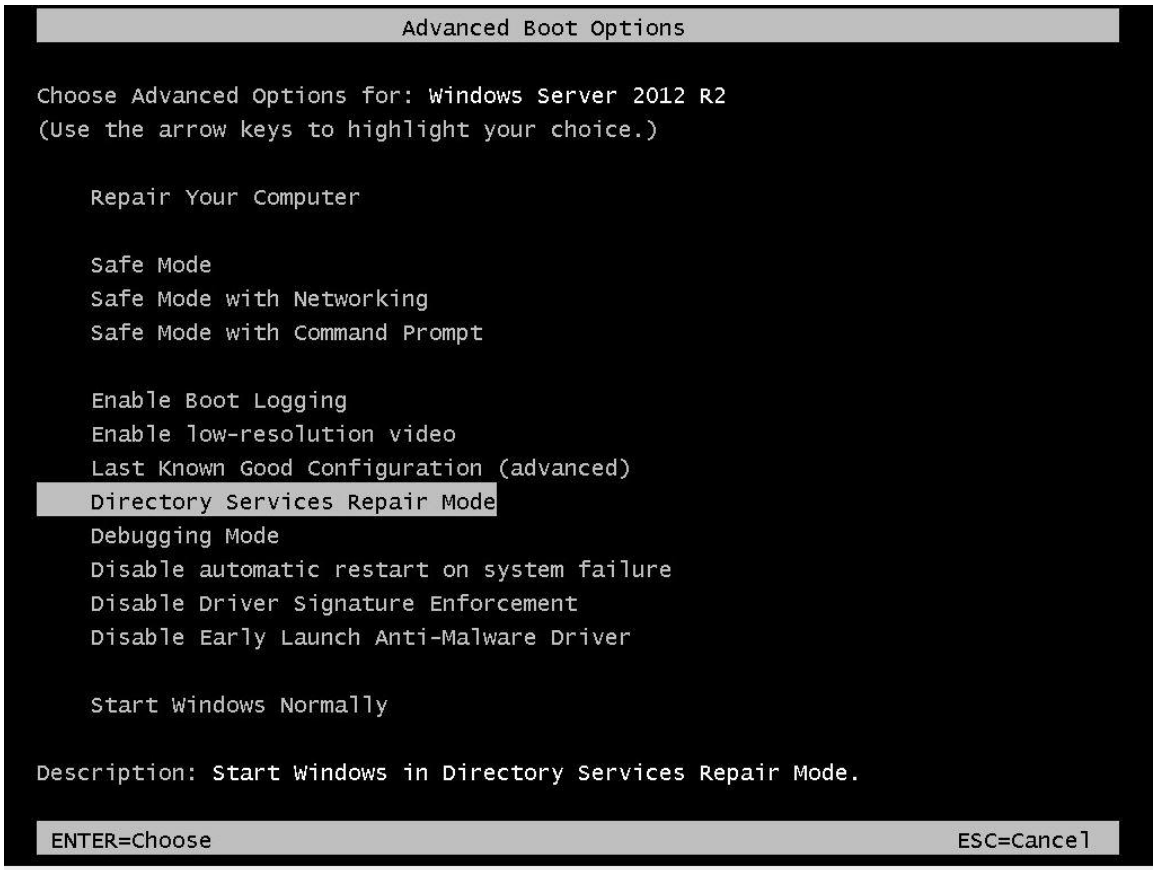
Esimerkkitapauksessa palautus onnistui ongelmitta ja DC1-palvelimelle palautettu järjestelmä replikoi muutokset, jotka oli tehty Active Directoryyn palautetun varmuuskopion ottamisen jälkeen DC2-palvelimelta.

7.3 Active Directoryn palauttaminen varmuuskopiosta

Tässä osiossa palautetaan poistettu Active Directoryn objekti järjestelmän tilan varmuuskopiosta. Esimerkissä käytetään molempia tapoja palauttaa Active Directory. Nämä tavat ovat ei-autoritäärinen sekä autoritäärinen palautus.

7.3.1 Ei-autoritäärinen palautus

Ei-autoritäärinen palautus aloitetaan käynnistämällä palvelin uudelleen ja painamalla käynnistysvaiheessa F8-näppäintä. Tällä saadaan näkyviin palvelimen käynnistysvalinnat. Tässä esimerkissä, koska palvelin on virtualisoitu, koneen käynnistyessä painetaan Esc-näppäintä, jonka jälkeen päästään valikkoon, josta voidaan tehdä samat valinnat. Tästä valikosta valitaan Directory Services Repair Mode kuten kuvassa 25, ja syötetään sisäänkirjautumisen yhteydessä DRSM-käyttäjänimi ja salasana. DRSM-käyttäjänimi on esimerkissä DC2\Administrator, kuten kuvassa 26 nähdään.



Kuva 25. Palvelimen käynnistysvalinnat.

Kuva 26. Sisäänkirjautuminen DRSM-käyttäjänimellä ja salasanalla.

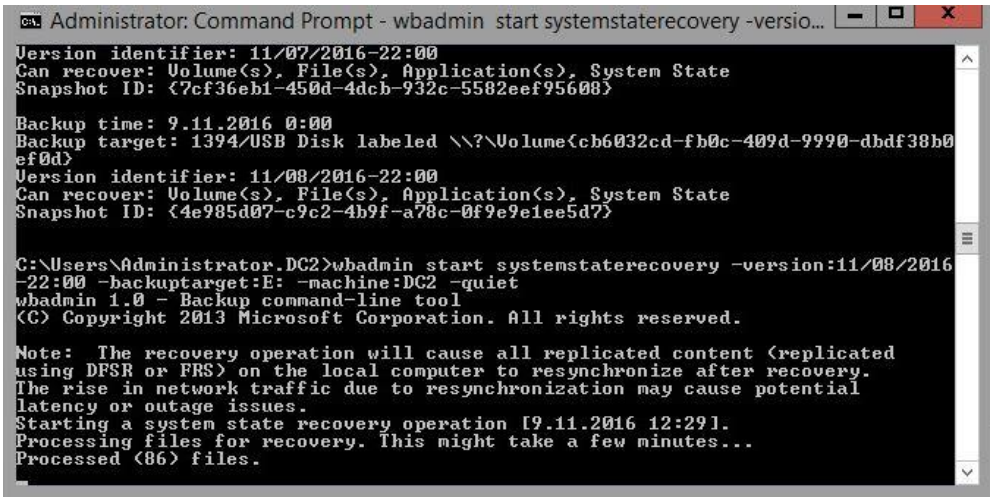
Palvelimen käynnistyttyä DRSM-tilaan avataan komentokehote. Tähän kirjoitetaan komento, joka hakee varmuuskopioille määrätyltä kovalevyltä siellä sijaitsevat varmuuskopioversiot, esimerkiksi:

wbadmin get versions –backutarget :E: -machine:DC2

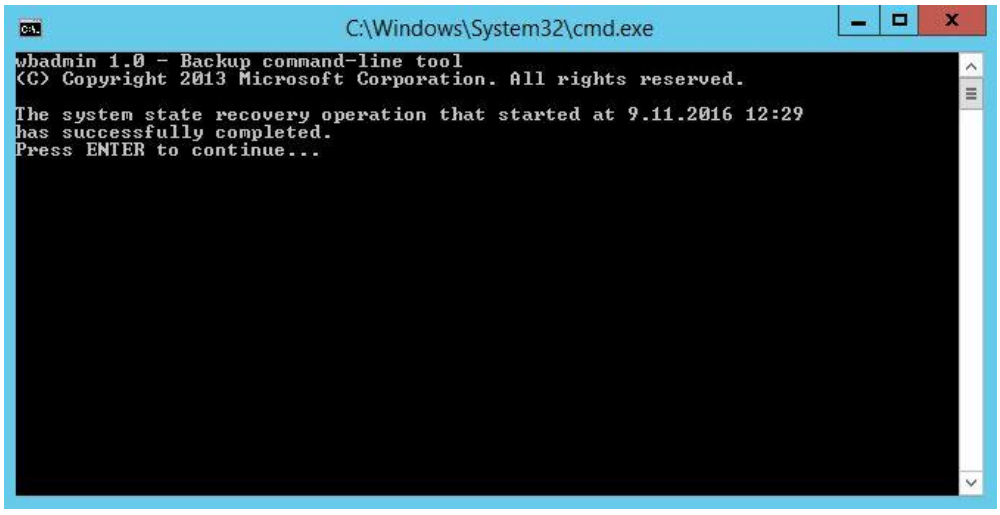
Seuraavaksi kirjoitetaan komento, joka aloittaa palautuksen halutusta järjestelmän tilan varmuuskopiosta, esimerkiksi:

wbadmin start systemstaterecovery –version:11/08/2016-22:00 –backuptarget:E: -machine:DC2 -quiet

Tämän komennon syöttämisen jälkeen palautus lähtee käyntiin, kuten nähdään kuvassa 27. Palautuksen lopuksi järjestelmä antaa ilmoituksen, että palautus on onnistunut, kuten kuvassa 28. Jos tämän jälkeen haluaa tehdä autoritäärisen palautuksen, palvelinta ei tule käynnistää uudelleen. Kun palvelin käynnistetään uudelleen, AD DS ja Active Directory Certificate Services havaitsevat, että on tapahtunut järjestelmän tilan palautus, ja ne tekevät automaattiset eheystarkistukset tietokantoihinsa.



Kuva 27. Järjestelmän tilan palautuksen aloitus.



Kuva 28. Järjestelmän tilan palautuksen onnistumisen ilmoitus.

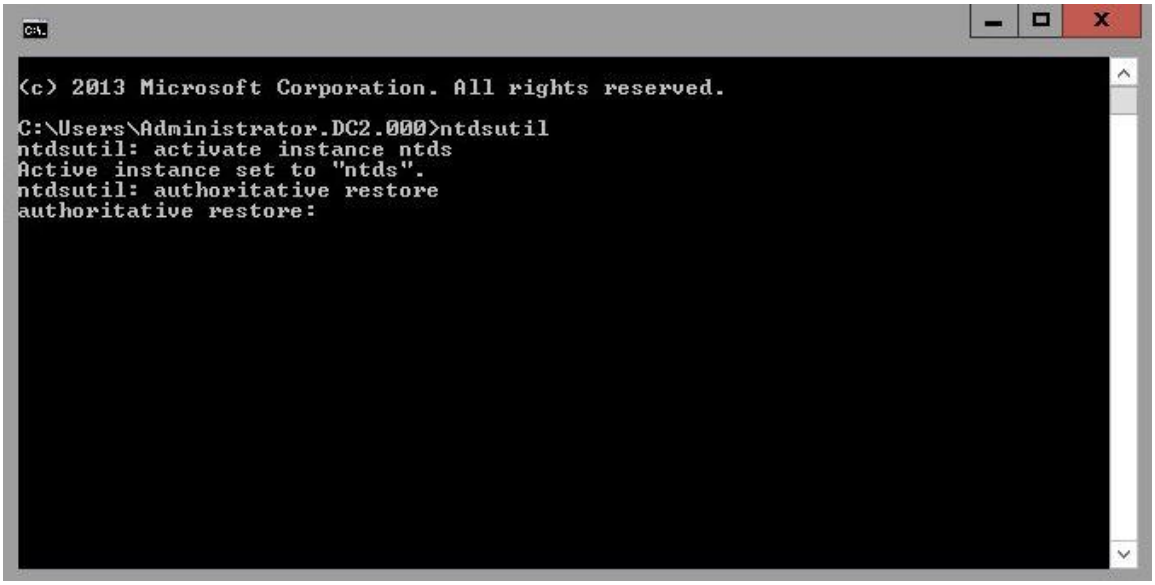
7.3.2 Autoritäärinen palautus

Autoritäärinen palautus tehdään jatkona ei-autoritääriselle palautukselle. Sen sijaan, että palvelin käynnistetään uudelleen ei-autoritäärisen palautuksen jälkeen, avataan uusi komentokehote järjestelmänvalvojan oikeuksilla. Seuraavaksi avataan komentokehotteessa ntdsutil, aktivoidaan ntds-instanssi sekä avataan autoritäärinen palautus kuvan 29 mukaisesti seuraavilla komennoilla:

ntdsutil

activate instance ntds

authoritative restore

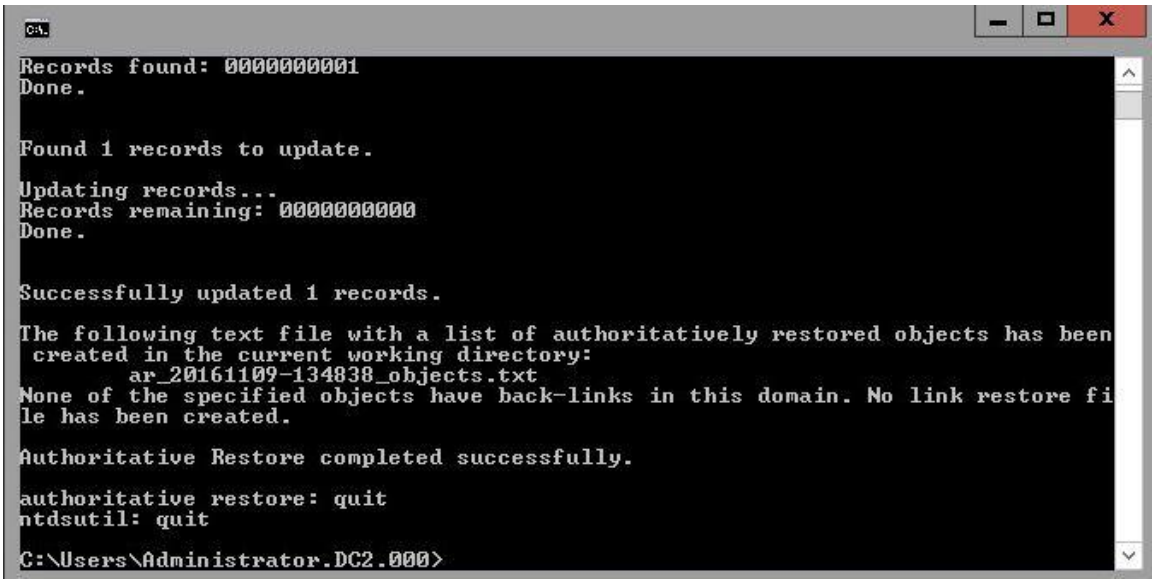


Kuva 29. Ntdsutil-valikko objektin palautusta varten.

Täältä voidaan palauttaa esimerkiksi poistettu organization unit (OU) tai käyttäjä. Esimerkissä palautetaan poistettu käyttäjä Testi Testaaja. Tämä tapahtuu kirjoittamalla komento:

restore object ”CN=Testi Testaaja,CN=Users,DC=juuso,DC=local”

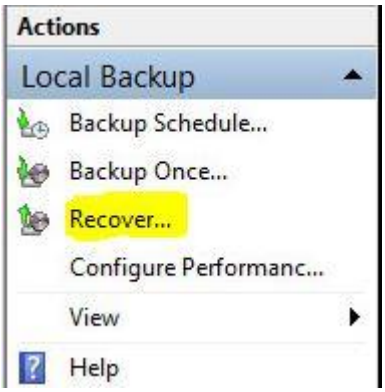
Tässä komennossa lainausmerkkien sisällä on palautettavan objektin täysi ”Distinguished Name (DN)”. Lopuksi onnistunut palautus antaa kuvan 30 mukaisen ilmoituksen, jonka jälkeen palvelimen voi käynnistää uudelleen.



Kuva 30. Ilmoitus objektin onnistuneesta palautuksesta.

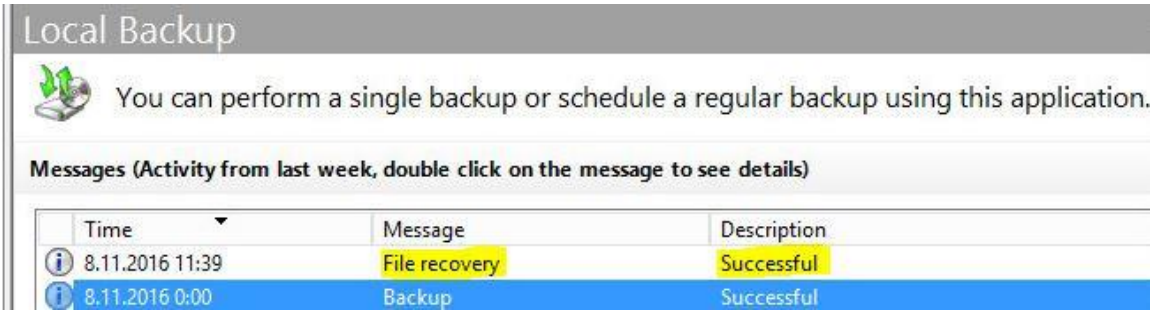
7.4 Tiedostojen ja kansioiden palautus varmuuskopiosta

Windows Server Backup -ohjelmalla palautus tapahtuu valitsemalla ohjelman oikeasta reunasta kuvan 31 mukaisesti ”Recover”. Seuraavaksi valitaan, mistä varmuuskopio haetaan ja valitaan kovalevy, joka sisältää varmuuskopion. Tämän jälkeen valitaan, minkä palvelimen dataa halutaan palauttaa ja mistä varmuuskopiosta. Tässä esimerkissä palvelin on DC1. Jos varmuuskopioita on useita, ohjelma hakee oletuksena niistä uusimman. Seuraavaksi valitaan, halutaanko palauttaa tiedostoja ja kansioita vai kokonaisia loogisia levyjä. Tässä esimerkissä palautetaan poistettu tiedosto, joten valitaan tiedostot ja kansiot. Tämän jälkeen voidaan selata varmuuskopion sisältämiä tiedostoja, ja hakea sieltä tarvittava dokumentti palautettavaksi kuten kuvassa 32. Seuraavassa kohdassa määritellään, minne tiedosto palautetaan, ja lopuksi hyväksytään palautus. Toiminnon onnistumisen voi varmistaa Windows Server Backup -ohjelman tapahtumalokista, kuten kuvassa 33 on nähtävissä, sekä navigoimalla kansioon johon tiedosto on määritelty palautettavaksi.



Kuva 31. Tiedostojen tai kansioiden palautus varmuuskopiosta.

Kuva 32. Valitaan palautettava tiedosto varmuuskopion sisällöstä.



Kuva 33. Palautuksen onnistumisen toteaminen Windows Server Backup -ohjelman tapahtumalokista.

8 YHTEENVETO

Palvelimessa toimii usein organisaation toiminnalle kriittisiä palveluita tai ohjelmistoja. Tämän vuoksi palvelinympäristön suunnittelu ja rakentaminen vikatilanteita kestäväksi sekä niistä nopeasti palautuvaksi on erittäin tärkeää. Palautumisen lisäksi ongelmia ennaltaehkäisevät tekijät ovat tärkeitä huomioon otettavia asioita.

Vikatilanteista palautumisen kannalta tärkeimmät tekniset huomioon otettavat asiat ovat järjestelmien kahdennus ja tietojen varmuuskopiointi. Mikäli palvelinta ei ole kahdennettu, eikä varmuuskopioita otettu ja sen kovalevyt esimerkiksi hajoavat, tietoja voi olla hyvin vaikeaa tai lähes mahdotonta saada enää pelastettua hajonneilta kovalevyiltä. Parhaassa tapauksessa jotain dataa saadaan pelastettua, mutta se vie luultavasti tuhottomasti aikaa ja vaivaa.

Kahdennus tulisi mahdollisuuksien mukaan toteuttaa siten, että toinen palvelimista sijaitsisi fyysisesti eri paikassa, jolloin palvelimen sijaintiin kohdistuvat uhkat, kuten luonnonkatastrofit, tulipalot tai vesivahingot eivät lamauta koko järjestelmää. Jos toista palvelinta uhkaa tällainen ongelma, ainakin toinen on turvassa sisältäen kaiken tarpeellisen datan, joka voidaan myöhemmin replikoida korvatulle palvelimelle.

Varmuuskopiointi tulisi suunnitella ja tehdä siten, että se olisi jatkuvaa ja sopivin aikavälein tallennettu. Yhden päivän vanhaan varmuuskopioon on huomattavasti kivuttomampaa palata kuin usean kuukauden takaiseen, jolloin järjestelmään on mahdollisesti tehty varmuuskopioinnin ottamisen jälkeen muutoksia, jotka täytyy ottaa huomioon ja tehdä uudestaan palautuksen jälkeen. Lisäksi varmuuskopioita olisi hyvä olla usealla eri kovalevyllä, jolloin voidaan pienentää riskiä datan menetyksiin. Jos varmuuskopiota on useammalla levyllä, yhden hajoaminen ei ole katastrofi, vaan se voidaan korvata uudella.

Windows Server Backup on mielestäni hyvä ja vaivaton varmuuskopiointiohjelma. Se osaa automaattisesti tunnistaa, mitkä sille kohdistetut varmuuskopiointikovalevyt ovat kytkettynä palvelimeen. Ohjelma poistaa automaattisesti kovalevyn täyttyessä vanhimman varmuuskopioista ja kirjoittaa sen päälle uusimman version.

Varmuuskopioinnissa käytettyjä levyjä siis voidaan vaihtaa vaivattomasti palvelimeen ja pois, säilytykseen erilliseen fyysiseen sijaintiin. Erillisessä sijainnissa säilytetyt varmuuskopiot myös vähentävät riskiä luonnollisista katastrofeista johtuvaan datan menetykseen.

Sain tässä työssä tehdyt käytännön osion esimerkkitapaukset toimimaan tarkoituksenmukaisella tavalla. Näihin tehtäviin liittyvät toimenpiteet oli esitetty hyvin teoksessa Mastering Windows Server 2012 R2, ja seuraamalla ohjeita sekä soveltamalla niitä esimerkkiympäristöön sopivaksi, ei käytännön osiota toteuttaessani ilmentynyt suurempia ongelmia vähäistä lisäselvitystyötä lukuun ottamatta.

Koen, että tässä työssä käsiteltyjä aiheita koskeva tiedonkeruu, testaus ja raportointi kasvattivat osaamistani tällä osa-alueella. Koen myös saavuttaneeni opinnäytetyöprosessille asettamani tavoitteet, jotka ovat työn laajuus sekä työssä kirjoitettuihin aiheisiin paneutumisen syvyys. Lisäksi lähdekritiikki ja tiedonhakutaitoni karttuivat tätä työtä tehdessä ja koen, että molemmista on hyötyä minulle jatkossa uraani ajatellen.

LÄHTEET

Alertra (16.9.2015) Understanding what Server Downtime is and how to minimize it. Haettu 8.11.2016, sivustolta alertra.com internetosoite: https://www.alertra.com/blog/2015/understanding-what-server-downtime-is-and-how-to-minimize-it

Dell. (12/2014). Integrated Dell Remote Access Controller 8 (iDRAC8) Version 2.05.05.05 User's Guide. Haettu 13.10. 2016, sivustolta dell.com internetosoite: http://topics-cdn.dell.com/pdf/idrac8-with-lc-v2.05.05.05_User's%20Guide_en-us.pdf

Dell. What Is a Server? Haettu 12.10. 2016, sivustolta dell.com internetosoite: http://www.dell.com/downloads/us/bsd/What_Is_a_Server.pdf

Gregory, P. H. (2011). For Dummies : IT Disaster Recovery Planning For Dummies (1). Hoboken, US: For Dummies. Retrieved from http://www.ebrary.com

Hester, M., & Henley, C. (2013). Microsoft Windows Server 2012 Administration Instant Reference (1). Somerset, US: Sybex. Retrieved from http://kamezproxy01.kamit.fi:2083

Hewlett Packard Enterprise. (10/2016). HPE iLO 4 User Guide. Haettu 13.10. 2016, sivustolta hpe.com internetosoite: http://h20566.www2.hpe.com/hpsc/doc/public/display?docId=c03334051

Mallery, M (2015) Technology Disaster Response and Recovery Planning : A LITA Guide. US: ALA TechSource. Retrieved from http://www.ebrary.com

Microsoft. (2013). Backup and Restore Considerations for Virtualized Domain Controllers. Haettu 28.10. 2016, sivustolta technet.microsoft.com internetosoite: https://technet.microsoft.com/en-us/library/d2cae85b-41ac-497f-8cd1-5fbaa6740ffe(v=ws.10)#backup_and_restore_considerations_for_virtualized_domain_controllers

Microsoft (9.1.2009) Restoring a Domain Controller Through Reinstallation. Haettu 8.11.2016, sivustolta technet.microsoft.com internetosoite: https://technet.microsoft.com/en-us/library/cc816620(v=ws.10).aspx

Microsoft. Windows Server. Haettu 12.10. 2016, sivustolta msdn.microsoft.com internetosoite: https://msdn.microsoft.com/en-us/library/dn636873(v=vs.85).aspx

Minasi, M., Greene, K., & Booth, C. (2013). Mastering Windows Server 2012 R2 (1). Somerset, US: Sybex. Retrieved from http://kamezproxy01.kamit.fi:2083

Varghese, M. (2002). Disaster Recovery. Boston, US: Course Technology / Cengage Learning. Retrieved from http://www.ebrary.com

VMware. VMware vSphere 4 – ESX and vCenter Server. Haettu 7.11.2016, sivustolta pubs.vmware.com internetosoite: https://pubs.vmware.com/vsphere-4-esx-vcenter/index.jsp#com.vmware.vsphere.resourcemanagement.doc_40/using_drs_clusters_to_manage_resources/t_create_affinity_rules.html

Wallace, M., & Webber, L. (2004). Disaster Recovery Handbook. New York, US: AMACOM Books. Retrieved from http://kamezproxy01.kamit.fi:2083