Toni Anttila

Palvelimien lokiasetusten selvittäminen ja uudistaminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

22.3.2015

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Toni Anttila Palvelimien lokiasetusten selvittäminen ja uudistaminen 34 sivua + 2 liitettä 22.3.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Tomi Reiman, Tietoturva-asiantuntija Jukka Louhelainen, Lehtori

Insinöörityön tavoitteena on selvittää Cygaten nykyisten käytössä olevien palvelimien lokienkeräys-asetukset ja päivittää ne vastaamaan nykyisiä vaatimuksia. Työn toisena tavoitteena on saada lokiasetukset uusien palvelimien käyttöönottoprosessiin.

Työn alkuvaiheessa kartoitettiin nykyinen tilanne Windowsin Audit policyn osalta. Windows-palvelimien nykyiset asetukset todettiin täyttävän asetetut vaatimukset eikä näihin asetuksiin koettu tarvetta tehdä muutoksia. Linux-palvelimien lokiasetusten nykytilanne selvitettiin ja ne todettiin riittäviksi.

Työtä varten perustettiin virtuaalinen testiympäristö Audit policyn testausta varten. Testauksien tarkoituksena oli tutustua lokitapahtumiin sekä selvittää testiin liittyviä lokitapahtumia. Luotiin testauksia varten kaksi virtuaalipalvelinta, joista toinen toimi DC:na ja toinen liitettiin perustettuun domainiin. Toteutettiin yksinkertaisia testejä tapahtumien luomiseksi ja analysoitiin testiin liittyviä lokitapahtumia.

Testit onnistuivat hyvin, ja saatiin selkeät lokitapahtumat. Osa testeistä jätettiin tekemättä, koska ne olisivat vaatineet muutoksia, joiden selvittäminen ja tekeminen olisivat vaatineet aikaa. Työn valmistumisen takarajaa oli kertaalleen jouduttu siirtämään, jonka vuoksi päädyttiin yksinkertaisempiin testauksiin.

Avainsanat	Lokien keräys, lokitapahtuma, Audit policy

Author(s) Title Number of Pages Date	Toni Anttila Examining and updating servers log configuration 34 pages + 2 appendices 22 March 2015
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Data Networks
Instructor(s)	Tomi Reimain, Security specialist Jukka Louhelainen, Senior Lecturer

The purpose of the bachelor thesis was the survey of the current configuration for log collection of Cygate's servers and update configuration, if it meets the current requirements. The secondary purpose was to implement log configuration to the process of setting up new servers to the network to have one common log collecting configuration.

The first task was to find out the current configuration of Audit policy used in Windows servers. Linux servers were not included in the study, but the current configuration was examined. Current Windows Audit policy configurations were discovered to meet the current requirements and changes were not needed.

A test environment was then created to test Audit policy audit events. The purpose of the tests was to explore log events and find out any related events for the certain test. The Virtual environment created included two servers: Domain controller and domain member server. A simple test was made to trigger audit events. All tests were successful and the log events were analyzed. It was decided to leave out few tests, because it would have taken a significant amount of time to solve how to configure the settings to able log the events.

Keywords	Log event, Audit policy

Sisällys

Lyhenteet

DC	Domain Controller. Domain-palvelin, jossa AD DS sijaitsee.
AD DS	Active Directory Domain Services. Domainin ja siihen liittyvien resurssien hallinta.
UDP	User Datagram Protocol. Käytetään Syslogien välittämisprotokollana, joka perustuu epäluotettavaan lähetykseen.
TCP	Transmission Control Protocol. Tiedon luotettavaan lähetykseen käytettävä protokolla.
GPO	Group Policy. Hallitaan käyttäjien ja tietokonetilien toimia domainissa.
DoS	Denial of Service. Palvelunestohyökkäys.
DNS	Domain Name Service. Nimipalvelin, joka selvittää nimen perusteella IP-osoitteen.
DHCP	Dynamic Host Configuration Protocol. IP-osoitteiden jakamiseen käytettävä protokolla.

1 Johdanto

Insinöörityön tarkoituksena on selvittää Cygaten käytössä olevien palvelimien lokien keräyksen nykyiset asetukset sekä selvittää, minkälaisia tapahtumia asetuksilla voidaan kerätä. Työn yhtenä tavoitteena on saada palvelimien käyttöönottoprosessia varten oletuslokiasetukset.

Palvelimet koostuvat lähinnä Windows- ja Linux-järjestelmistä. Windows-palvelimista käytössä on 2008 ja 2012 versioita. Työssä selvitetään Windowsin Audit policyn määritetyt asetukset ja selvittää, minkälaisia tapahtumia asetukset valvovat. Tarpeen vaatiessa asetuksia päivitetään vastaamaan asettuja vaatimuksia. Työssä ei ole tarkoitus ottaa kantaa kerättäviin lokitietoihin, vaan määrittää tarvittavat asetukset suunniteltujen vaatimuksien pohjalta.

Työn lopussa luotiin testiympäristö, jonka tarkoituksena on testata Audit policya sekä tutustua lokitapahtumiin ja selvittää muut testiin liittyvät tapahtumat. Tapahtumia analysoitiin testiympäristössä olevalla SIEM-järjestelmällä.

Työ rajattiin käsittämään lokiasetuksien selvittämiseen sekä asetuksille tehtäviin muutoksiin. Työssä selvitettiin Windows- ja Linux-palvelimien asetukset, mutta muutokset rajattiin vain Windows-palvelimiin.

2 Lokien keräys ja hallinnointi

2.1 Lokitapahtumat

Loki on tallenne tapahtumasta, joka on esiintynyt organisaation järjestelmässä tai verkossa. Loki sisältää lokimerkintöjä ja jokainen merkintä on oma tapahtuma sisältäen tiedot kyseisestä tapahtumasta. Alun perin lokeja käytettiin selvittämään vikatilanteita, mutta nykypäivänä lokit palvelevat muitakin toimintoja organisaatiossa kuten järjestelmän optimointia ja verkon suorituskykyä sekä käyttäjien toimien kirjausta ja tarjoaa tärkeää tietoa haitallisten toimintojen tutkimista varten. [1.]

Lokitapahtuma on tietokoneen, verkonlaitteen tai ohjelmiston yms. muodostama tapahtumatieto. Se, mikä tapahtuma on, riippuu sen muodostavasta lähteestä. Lokiviesti voi olla esimerkiksi käyttöjärjestelmän sisään- tai uloskirjautumistieto tai levyjärjestelmän muodostama lokiviesti virheen tapahtumisesta. [2, s. 2-3.]

Lokitieto on lokiviestistä otettu informaatio, jossa ilmenee, miksi tapahtuma on muodostettu. Esimerkiksi käyttäjän kirjautuessa käyttöjärjestelmään tallentuu siitä lokitapahtuma järjestelmään, joka pitää sisällään tiedot tapahtumasta. Lokiviesti sisältää aina vähintään aikaleiman, koska tapahtuma on alkanut ja mistä se on peräisin eli lähteen. Yleensä lähde on joko IP-osoite tai isäntä-nimi. Viimeisenä ovat tarkemmat tiedot tapahtumasta. Lisäksi lokiviestissä voi myös olla seuraavia muitakin lisätietoja kuten kohdeosoite, lähde- ja kohdeportti, käyttäjätunnus, ohjelmannimi. [2, s. 2-3., s. 6.]

Lokiviestit voidaan jakaa seuraaviin yleisiin luokkiin: [2, s. 3]

- Informatiivinen (Informational): Viesti ilmoittaa käyttäjälle tai ylläpitäjälle normaalista toiminnasta [3.].

- Testaus (Debug): Yleensä ohjelmistojen muodostamia lokiviestejä vianselvityksen ja tunnistamista varten.

- Varoitus (Warning): Ilmoittaa järjestelmän kadottaneen tai tarvitsevan jotain osaa, mutta varoituksen ilmestyminen ei häiritse sen toimintaa.

- Virhe (Error): Välittää viestin tapahtuneessa virheestä järjestelmän eri tasoilta. Yleensä vaatii lisäselvitystä, ja virhe välittää aloituspisteen, josta lähdetään etsimään ongelmaa.

- Hälytys (Alert): Tarkoitettu ilmoittamaan jostain kiinnostavasta tapahtumasta. Hälytykset yleisesti muodostuvat tietoturvaan liittyvistä laitteista ja järjestelmistä.

2.2 Lokienhallinnan infrastruktuuri

Lokienhallinnan infrastruktuuri koostuu laitteistosta, ohjelmistosta, verkosta ja muodostamiseen, lähettämiseen, säilyttämiseen, analysointiin, lokin poistamiseen käytettävästä mediasta. Organisaatioilla on yksi tai useampi lokienhallintaan käytössä oleva järjestelmä. Lokienhallinnan infrastruktuuri koostuu tyypillisesti kolmesta tasosta. Ensimmäinen taso on lokien muodostus taso. Se koostuu isäntälaitteesta, joka muodostaa tapahtuman. Jotkin isännät suorittavat ohjelmistoa tai palvelua mahdollistamaan lokien toimittamisen seuraavalle tasolle.

Seuraavalla tasolla analysoidaan ja säilytetään lokeja. Toisella tasolla toimii yksi tai useampi lokipalvelin, joka vastaanottaa lokit ensimmäisen tason laitteilta. Tapahtumia siirretään reaaliajassa tai tietyllä viiveellä. Myös voidaan ajastaa tai odottaa, että saadaan tietty määrä täyteen, jonka jälkeen lähetään.

Kolmannella tasolla suoritetaan lokien valvontaa. Se koostuu konsoleista, joilla voidaan valvoa ja katsella lokitietoja ja automatisoitujen analyysien tuloksia. Lokienhallintakonsoleilla voidaan muodostaa raportteja lokitapahtumista. Joissakin lokienhallintakonsoleista voidaan myös hallita lokipalvelimia ja käyttäjiä.

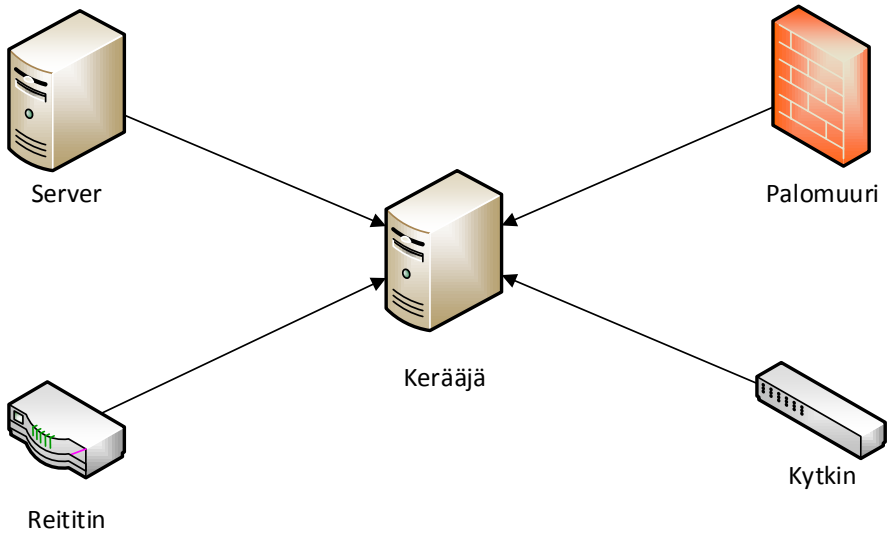
Toisesta tasosta on olemassa erilaisia variaatioita aina yksinkertaisesta lokipalvelimesta, joka kerää lokitapahtumat. Monimutkaisemmat ratkaisut sisältävät useita lokipalvelimia, joilla jokaisella on oma tehtävä. Tehtävänä voi olla palvelimien suorituskykytapahtumien kerääminen, analysointi ja lyhytaikainen varastointi. Toisen palvelimen tehtävä on hoitaa pitkäaikainen säilyttäminen.

Yksi vaihtoehto on, että jokainen lokipalvelin kerää tietyiltä isänniltä tapahtumia ja tekee näille analysointia sekä säilyttää tapahtumat. Tällä saadaan aikaan redundanttisuutta. Käyttäjä voi vaihtaa vara lokipalvelimelle, mikäli sen primääri palvelin on tavoittamattomissa. Lisäksi voidaan myös määrittää lokipalvelimet jakamaan tapahtumat toisilleen, millä saadaan myös redundanttisuutta parannettua.

Lisäksi voidaan tehdä kaksitasoinen lokipalvelinjärjestelmä, jossa ensimmäisen tason lokipalvelimet vain vastaanottavat tapahtumia lokien muodostajilta ja lähettävät joko kaikki tai osan tapahtumista eteenpäin toisen tason lokipalvelimille. Tietyissä ratkaisuissa ensimmäinen taso toimii vain välimuistina lokitapahtumille, yksinkertaisesti vastaanottaa ja välittää tapahtumat seuraavalle tasolle. Ratkaisu mahdollistaa toisen tason palvelimien suojauksen suorilta hyökkäyksiltä ja hyödyllinen, kun verkossa on luotettavuus ongelmia lokien muodostajien ja toisen tason lokipalvelimien välillä. Tässä tapauksessa välimuistipalvelimien sijaitseminen luotetussa lähiverkossa mahdollistaa lokien muodostajien lähettämisen välimuistipalvelimille, jotka voivat lähettää lokit, kun yhteydet sen sallivat keskitetyille lokipalvelimille. [1.]

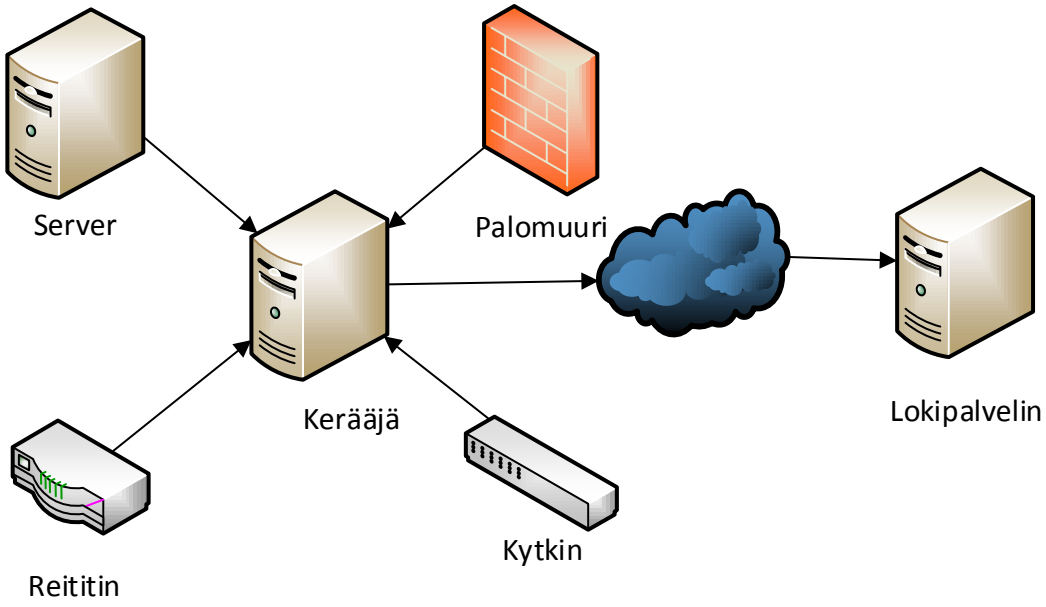
2.3 Lokitiedon lähettäminen ja kerääminen

Lokien lähettäminen ja kerääminen on varsin yksinkertainen asia käsitteellisellä tasolla. Tietokone tai laite toteuttaa lokialijärjestelmän, josta se muodostaa viestejä aina, kun määritykset täyttyvät. Määritykset riippuvat käytettävästä laitteesta. Ne voivat olla käyttäjän määrittelemiä tai kovakoodattuja laitteeseen. Lokeille tulee olla jokin paikka, johon ne kerätään. Yleensä tätä tehtävää suorittaa siihen varattu kerääjä tai jaettu lokipalvelin, johon kerääjä välittää lokeja. Kerääjä on yleensä Unix-järjestelmä tai Windows-palvelin. [2, s. 4.]



Kuva 1. Lokitapahtumien paikallinen keskitetty keräys.

Kuvassa 1 on lähiverkossa sijaitseva kerääjä johon lokiviestit kerätään. Vain paikalliset laitteet välittävät lokit.



Kuva 2. Lokien kerääminen keskitetylle lokipalvelimelle

Kuvassa 2 käytetään jaettua lokipalvelinta. Laitteet siirtävät lokiviestit paikalliselle kerääjälle, joka välittää viestit eteenpäin jaetulle lokipalvelimelle varastointia varten. Lokipalvelimelle on etuna, että se ei rajoitu vain paikallisten laitteiden lokien keräykseen.

Voidaan kerätä lokeja julkisen verkon kautta paikallisilta kerääjiltä. Kerääjälle saavutetaan seuraavia etuja. Se mahdollistaa keskitetyn paikan, jossa voidaan säilyttää useiden kohteiden lokit sekä sen vuoksi tarjoaa varmuuskopiot näistä. Sen lisäksi kerääjällä pystytään analysoimaan kertyneitä lokeja. [2, s. 4.]

2.4 Syslog

Lokiviestien yleisin lähettämistapa on käyttää Syslog-protokollaa. Syslog on standardiin perustuva lokiviestin vaihtaja, jota käytetään yleensä Unix-pohjaisissa järjestelmissä. Syslogia voidaan myös käyttää Windows-järjestelmissä ja muissa ei Unix-järjestelmissä. Myös tavallisia käyttökohteita ovat verkonlaitteet reitittimet ja palomuurit yms. Käytetään vianselvitykseen ongelmatilanteissa, tunkeutumisen havaitsemista varten, toimintojen hallintaan sekä valvontaan.

Syslog perustuu asiakas-palvelin-tyyppiseen toteutukseen, joka käyttää User Datagram Protokollaa (UDP). Moni avoin ja kaupallinen Syslog-toteutus tukee Transmission Control Protokollaa (TCP) viestien varmistettua toimittamista varten. Asiakaskomponentilla tarkoitetaan laitetta, joka muodostaa ja lähettää lokiviestit kohti kerääjää. Lokit voidaan varastoida kerääjällä tai ne voidaan välittää eteenpäin jaetulle lokipalvelimelle, jossa tapahtuu pitkäaikaisempi säilytys. [1, s. 4.; 2.; 4.]

Lokiviestin yleisimmin sisältävät kentät:

- ominaisuus
- vakavuus
- aikaleima
- lähde
- merkki
- viesti.

Kaikki kentät eivät kuitenkaan ole aina välttämättä käytössä, vaan kenttien käyttö riippuu olemassa olevasta toteutuksesta ja konfiguraatiosta. Kenttien avulla lokiviestejä voidaan suodattaa ja prosessoida. [4.]

Syslogin huonoja puolia on, että se ei ole täysin turvallinen, koska mikä tahansa laite voi lähettää syslog-viestejä palvelimelle. Tämä voidaan estää käyttämällä pääsyn estolistoja palvelimelle. Näin vain tietyistä kohteista hyväksytään lokit. UDP:lla käytettäessa ei voida olla varmoja, että vastaanottaja vastaanottaa viestit, mikä tekee siitä epäluotettavan. Koska viestikenttä ei ole standardisoitu, saattaa viesti olla ihmiselle ymmärtämättömässä muodossa.

2.5 Windows Event Log

Microsoft on toteuttanut oman lokijärjestelmän lokitietojen keräystä varten, mikä on nimeltään Windows Event Log. Event Log-lokit voidaan muuntaa Syslogeiksi, joita varten on olemassa ilmais- ja kaupallisohjelmia niiden muuntamiseksi, josta ne siirretään Syslog-palvelimelle. [2, s. 4]

Windowsissa kerätään viisi erilaista tapahtumatyyppiä: [5.]

- Virhe: Ilmoittaa merkittävästä tapahtumasta, kuten palvelu on epäonnistunut käynnistyksen yhteydessä tai tietoa on kadonnut.

- Varoitus: Ei välttämättä merkittävä vaan ilmoittaa jotain tapahtuvan tulevaisuudessa kuten esimerkiksi kovalevyllä on tila loppumassa.

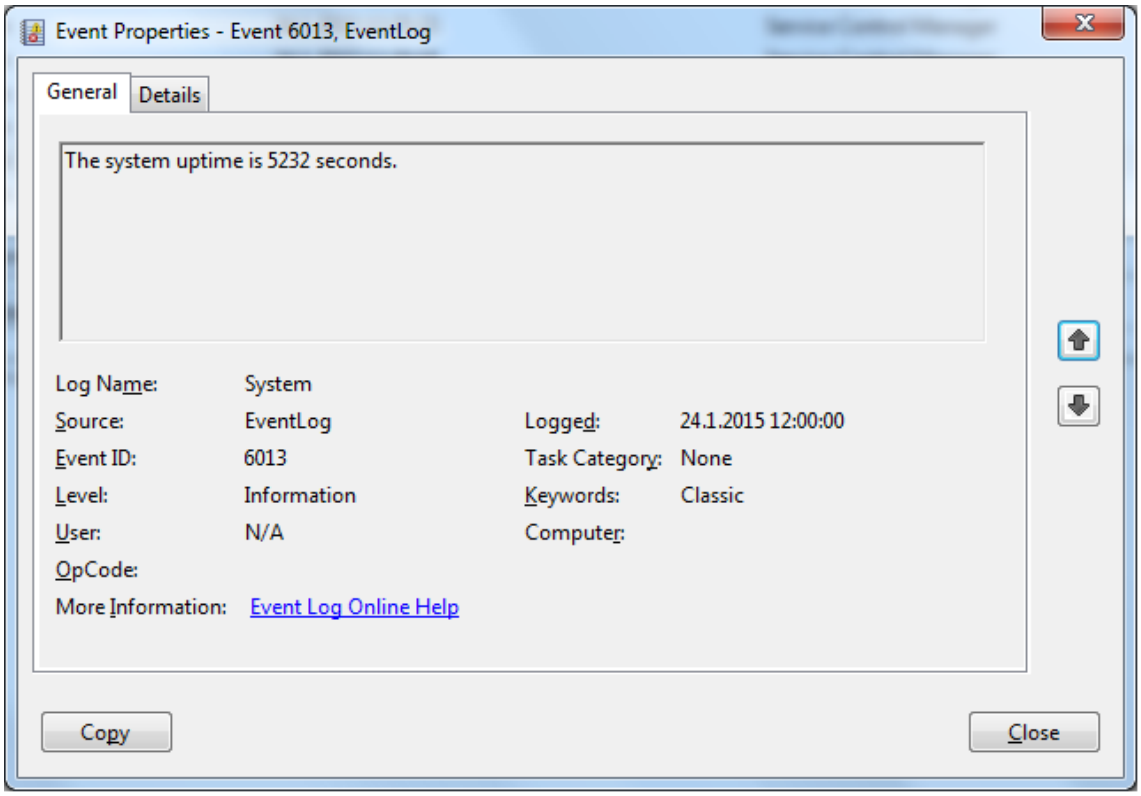
- Informatiivinen: Onnistuneesta tapahtumasta muodostuva ilmoitus.

- Valvonta (Onnistunut): Valvoo onnistuneita tapahtumia kuten kirjautumiset.

- Valvonta (Epäonnistunut): Valvoo epäonnistuneita tapahtumia kuten kirjautumiset.

Tapahtumalokeja pystytään keräämään:

- Ohjelmistoista, mikä sisältää ohjelmien tapahtumat.
- Tietoturvallisuus, mikä sisältää tapahtumia kirjautumisista sekä tapahtumista liittyen resursseihin kuten tiedostojen poistaminen.
- Järjestelmä, mikä sisältää tapahtumia järjestelmän komponenteista.
- Mukautettu, mikä sisältää tapahtumia ohjelmistoista, jotka muodostavat mukautettu lokeja.



Kuva 3. Esimerkki Event viewerin turvallisuustapahtumasta.

Kuvassa 3 on esimerkki järjestelmän muodostamasta ilmoitustasontapahtumasta, mikä ilmoittaa, kuinka kauan järjestelmä on ollut ylhäällä. Lähteenä on eventlog, joka tapahtuman on muodostanut. EventID on kyseisen tapahtuman tunniste ja jokaisella tapahtumalla on oma tunnisteensa. Lisäksi vielä näytetään tapahtuman kellonaika ja mistä se on peräisin.

2.6 Prosessi ja haasteet

Toimivan ja onnistuneen lokienhallintaprosessin aikaansaamiseksi tulee organisaation suunnitella käytännönprosessi, jolla suoritetaan lokien hallintaa. Osana tätä prosessia tulee selvittää organisaation vaatimukset ja tavoitteet lokien keräyksen suhteen. Niiden perusteella tulee organisaation kehittää politiikka tarvittavista vaatimuksista ja tarpeellisista suosituksista lokien toiminnallisuuksista sisältäen lokien muodostamisen, lähetyksen, säilyttämisen, analysoinnin ja hävittämisen. Lisäksi tulee huolehtia, että politiikka noudattaa ja tukee lokienhallinta vaatimuksia sekä suosituksia. Organisaation johdon tulisi tarjota tarvittava tuki suunnitteluun, politiikan ja menetelmän kehitykseen. Myös tulee ottaa huomioon suunnittelussa organisaation alaa koskeva lainsäädäntö ja määräykset lokien keräämisen suhteen. Lisäksi lokienhallintaa ja niiden tarkastamiseen tulee kiinnittää tarvittavat resurssit, jotka käyvät lokitapahtumia säännöllisesti läpi.

Suurin osa organisaatioista kohtaa samanlaisia ongelmia lokienhallinnan suhteen, kuinka tehokkaasti tasapainottaa lokien keräykseen käytettävien rajallisten resurssien määrä loputtomassa lokien tulvassa. Tyypillisiä haasteita, joihin organisaatiot törmäävät ovat lukuisat lokien lähteet, jotka vaativat hallinnan koko organisaation laajuudelta. Lisäksi yksittäinen lähde saattaa kerätä useita lokeja, kuten ohjelmiston keräämät tunnistetiedot yhteen lokiin ja verkon aktiivisuudesta toiseen lokiin.

Epäjohdonmukaiset lokien sisällöt luovat haasteita lokien hallintaa koskien. Jokainen lähde sisällyttää tapahtumaan tietyn osan, kuten IP-osoitteen ja käyttäjänimen. Tehokkuuden kannalta jokainen lähde valitsee sen pohjalta, mikä on sille tärkeintä. Sen vuoksi voi olla vaikeaa yhdistää kahden eri lähteen lokitapahtumaa, koska ne saattavat sisältää eri tietoja tai tiedot voivat esiintyä eri muodossa, kuten päivämäärä eri järjestyksessä.

Jokainen lokia muodostava lähde käyttää sisäistä kelloaan lokien aikaleimoihin. Jos kellon aika on epätarkka, aiheuttaa se myös lokitapahtumalle epätarkan ajan. Tämä luo haasteita lokien analysoinnissa varsinkin, kun analysoidaan useista lähteistä tapahtumia.

Useat lokien lähteet käyttävät erilaisia lokimuotoja lokitapahtumille. Osa voi olla ihmiselle luettavassa muodossa, kun taas osa saattaa olla binäärisessä muodossa. Sen

vuoksi organisaatiot yleensä muuntavat lokit tiettyyn formaattiin, jolla saadaan pidettyä lokien yhtenäisyys.

Lokit saattavat sisältää arkaluontoista tietoa, kuten järjestelmän tai verkon turvallisuuteen liittyvää tietoa. Tämän takia loki tulee suojata tietomurroilta luotettavuuden ja eheyden varmistamiseksi. Lokit saattavat tarkoituksellisesti tai tarkoituksettomasti sisältää esimerkiksi salasanoja ja käyttäjänimiä tai sähköpostien sisältöä. [1.]

3 Audit policy

Windows Audit policyllä kerätään Windowsin turvallisuuteen liittyviä tapahtumia. Valvonnan käyttöönotolla saadaan esiin mahdolliset tietoturvaongelmat. Samalla se mahdollistaa todisteiden saamisen murtoyrityksistä. Tapahtumat kerätään Windowsin Event Login-turvallisuustapahtumiin. Audit policy koostuu yhdeksästä eri tapahtumasta joita voidaan valvoa. [6.]

Audit policy tapahtuma kategorian valvontaa määritellään kolmella eri asetuksella jotka ovat [6]

- **Success**. Luo tapahtuman onnistuneesta toiminnasta.
- **Failure**. Luo tapahtuman epäonnistuneesta toiminnasta.
- **No auditing**. Asetuksella ei valvota tapahtumia.

Mikäli Audit policy ei ole konfiguroitu, esimerkiksi tietomurron tai sen yrityksen sattuessa, on vaikeaa tai mahdotonta havaita sellaista toimintaa. Toisaalta, jos Audit policy on määritelty keräämään kaikki tapahtumat, voi sekin estää löytämästä oleellisia asioita suuren tapahtumien määrän joukosta.

Audit policyllä voidaan altistaa tietokone DoS-hyökkäykselle, jos Audit: Shut down system immediately if unable to log security audits -asetus on päällä. Kyseessä on palvelunestohyökkäys, jonka tarkoituksena on saada tietokone sammumaan. Tietokoneeseen suoritetaan useita vääriä kirjautumisia. Näin saadaan loki täyttymään, jonka jälkeen Audit Policy ei voi enää kirjata uusia tapahtumia. Tuloksena tietokone sammuttaa

itsensä kyseisen asetuksen takia. Audit policyssa on yhdeksän eri valvottavaa tapahtumakategoriaa: [6]

Audit logon events

Valvoo niiden tietokoneiden sisään- ja uloskirjautumisia, jotka käydään todentamassa valvontaa keräävältä tietokoneelta.

Account management

Valvotaan kaikkia käyttäjänhallintaan liittyviä tapahtumia. Valvottaviin tapahtumiin kuuluu käyttäjäryhman tai käyttäjän lisääminen, muuttaminen ja poistaminen sekä salasanan muuttaminen.

Audit directory services access

Valvoo käyttäjien pääsyä Active Directoryn objekteihin, joihin on liitetty SACL. SACL on lista käyttäjistä ja ryhmistä joista objektiin kohdistuvat toimista valvonta suoritetaan.

Audit logon events

Valvoo käyttäjien sisään- ja uloskirjautumisia niistä käyttäjistä, jotka sijaitsevat tietokoneessa, johon kirjaudutaan.

Audit object access

Valvoo käyttäjien objekteihin pääsyistä kuten tiedostojen, kansioiden, rekisteriavaimien ja printterien, joihin on asetettu SACL määrittämään, mitä tapahtumia valvotaan.

Audit policy change

Valvoo kaikkia käyttäjien oikeuksiin tehtäviä, Windowsin palomuuriin, Audit policyyn tai Trust policyihin tehtäviä muutoksia.

Audit privilege use

Valvoo käyttäjän käyttöoikeuksiin liittyviä tapahtumia. Tapahtuma muodostetaan aina, kun käyttäjä suorittaa toimenpiteen käyttöoikeuksillaan joko hyväksytysti tai hylätysti. Valvontaa käyttöön ottaessa kannattaa harkita, koska tapahtumien määrä on suuri ja niitä on vaivalloista käsitellä.

Audit process tracking

Valvoo tapahtumia, kuten ohjelmien aktivointia, prosessin sulkua ja epäsuoria objektien käsittelyjä. Se on hyödyllinen vianetsintää varten, koska saadaan tarkempia tietoja prosesseista, jotka käynnistyivät ja milloin ne käynnistyivät. Tyypillisesti valvonta ei suoriteta, koska tapahtumien määrä on suuri.

Audit system events

Audit system events kerää valvontatapahtumia käyttäjien tietokoneiden uudelleen käynnistämisestä ja sammuttamisesta sekä tapahtumista, jotka vaikuttavat tietokoneen turvallisuuteen tai turvallisuuslokeihin.

Audit policyn yhdeksän tapahtumakategorian sijasta voidaan käyttää laajennuttua Audit policya, jolloin voidaan säätää jokaista 53 asetusta erikseen. Laajennetun Audit policyn etu on, että voidaan tarkasti valita vain tietyt tapahtumat, joita halutaan valvoa. Osassa tapahtumakategorioissa on oletuksena asetuksia päällä, jotka keräävät suuren määrän tapahtumia ja peittävät allensa kiinnostavat tapahtumat. [7.]

4 Nykytilanne

4.1 Linux-palvelimien Syslog-konfiguraatio

Linux-palvelimille on määritelty lokien keräystä varten Syslog.conf-tiedosto, jolla määritellään, mitä tapahtumia kerätään.

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*             /dev/console
```

Edellä olevalla kern.* voitaisiin kerätä kerneliin liittyvät lokitapahtumat, mutta rivi on määritelty kommentiksi. Sen vuoksi se ei kerää lokitapahtumia ollenkaan.

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none       /var/log/messages
```

Kaikki info ja sitä korkeamman prioriteetin tapahtumat kerätään tiedostoon messages. Rivillä on myös määritelty, että mail-, authpriv- ja cron-tapahtumia ei kerätä ollenkaan.

```
# The authpriv file has restricted access.
authpriv.*          /var/log/secure
```

Rivillä määritellään kaikki vakavuudet authpriv-tapahtumista, jotka kerätään secure-tiedostoon. Authpriv sisältää tunnistautumiseen ja turvallisuuteen liittyvät tapahtumat.

```
# Log all the mail messages in one place.
mail.*                          /var/log/maillog
```

Rivillä määritetään kaikki vakavuudet mail-tapahtumista ja ne kerätään maillog-tiedostoon.

```
# Log cron stuff
cron.*                          /var/log/cron
```

Määritetään cron-tapahtumien keräys kaikilta vakavuuksilta, jotka kerätään cron-tiedostoon. Cron-tapahtumat ovat kelloon liittyviä.

```
# Everybody gets emergency messages
*.emerg                         *
```

Kaikki emergency-vakavuuden tapahtumat lähetetään kaikkien käyttäjien konsoleille. Kyseisiä tapahtumia muodostuu, kun järjestelmä ei ole vakaa.

```
# Save news errors of level crit and higher in a special file.
uucp,news.crit                  /var/log/spooler
```

Kaikki uucp ja news critically tai sitä korkeammat tapahtumat kerätään spooler-tiedostoon.

```
# Save boot messages also to boot.log
local7.*                        /var/log/boot.log
```

Edellä olevat määritykset ovat perusmäärityksiä Syslog.conf-tiedostossa. Kaikista oleellisin osa syslog.conf-tiedostosta on alla olevat kaksi riviä, joissa määritellään tapahtumia, jotka välitetään kerääjälle. Edellä olevat jäävät vain paikallisesti tapahtumia keräävälle palvelimelle. Se ei kuitenkaan haittaa vaan toimii myös varmuuskopiona.

```
#Forward logs to collector
*.info                          @loghost
```

Rivillä määritetään kaikkien tapahtumien info tai sitä korkeampien vakavuuksien kerääminen. Tapahtumat välitetään kerääjälle eteenpäin. Kyseisen rivi ei tallenna tapahtumia paikallisesti. Osa näistä tapahtumista myös kerätään paikallisesti, jolloin saadaan varmuuskopiot ainakin osasta lokitapahtumia.

Nykyisillä määrityksillä kerätään kaikki lokitapahtumat, jolloin mikään oleellinen tapahtuma ei jää puuttumaan. Toisaalta juuri sen vuoksi suurten tapahtuma määrien sekaan voi kadota jokin tärkeä tieto, jota haluttaisiin hyödyntää. Lisäksi kaikkien tapahtumien kerääminen asettaa vaatimuksia tallennustilan riittävyydelle. Tapahtumia tulee pystyä varastoimaan vuoden ajan, mikä jo osaltaan asettaa vaatimuksia tallennustilalle. Mielestäni määrityksiä voisi kohdentaa tarkemmiksi.

4.2 Windows palvelimien Audit policy -asetukset

Windows-palvelimien osalta keskitytään Audit policyn määrityksiin. Taulukossa ovat nykyiset asetukset

Taulukko 1. Windows palvelimien audit policy -asetukset.

Sääntö	Asetus
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory services	Failure
Audit logon events	Success. Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

Audit policy on määritelty valvomaan tapahtumia erittäin kattavasti. Kirjautumistietoja kerätään niin paikallisesti kuin myös domainiin kirjautuessa. Kirjautumistietojen valvonta on ehdottoman tärkeää, jotta voidaan nähdä, ketä on kirjautunut sekä pystytään huomaamaan myös tarvittaessa luvattomat pääsynyritykset. Lisäksi valvotaan käyttäjien- ja ryhmienhallintaa, mikä on tietoturvan kannalta tärkeää. Molemmista valvotaan onnistuneet ja epäonnistuneet yritykset.

Active Directory objektien osalta valvotaan objektien muutosyrityksiä eli esimerkiksi GPO:den. Toisaalta olisi hyvä myös olla tieto siitä, kuka on muokannut AD:n objekteja.

Policy change valvotaan kummatkin tapahtumat, jolloin saadaan tieto esimerkiksi Audit policyn tehtävistä muutoksista.

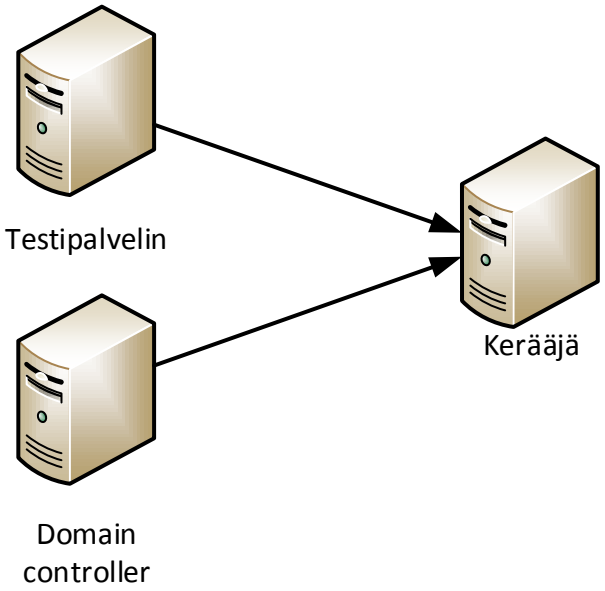
System event saadaan tärkeää tietoa järjestelmästä kuten sen käynnistymisistä. Lisäksi sillä saadaan tärkeää informaatiota prosesseista, jotka yrittävät suorittaa toimenpidettä, mihin ei ole oikeutta. Tällä voidaan paljastaa esimerkiksi haitallinen ohjelma.

Audit object access on jätetty valvomatta. Tällä estetään suurien tapahtumalokien määrä, mikäli sen valvonta on lisätty monelle kohteelle. Pahimmassa tapauksessa tällä saadaan järjestelmän suorituskykyä hidastettua. Lisäksi Audit process tracking on pois käytöstä, mikä valvoo prosessien suorittamista. Se on hyödyllinen tietyissä tapauksissa, mutta muodostaa suuria määriä tapahtumia.

5 Testiympäristö ja testaukset

5.1 Testiympäristö

Insinöörityötä varten luotiin Windows-palvelinympäristö lokitapahtumien testausta varten. Tarkoituksena on testata Windowsin Audit policya. Tarkoitus on tehdä testejä, joilla saadaan valvontatapahtuma aikaiseksi. Testillä saatua tapahtumaa tarkastellaan SIEM-järjestelmässä ja etsitään testiin liittyviä muita tapahtumia. Tällä saadaan hieman tietoa siitä, minkälaisia tapahtumia milläkin testillä saadaan.



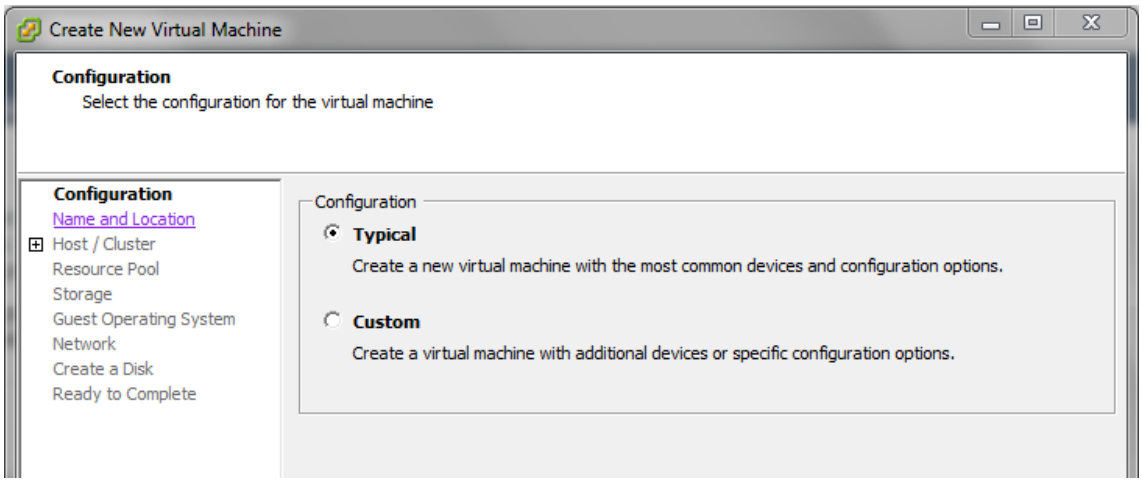
Kuva 4. Testiympäristö.

Testiympäristö koostuu kolmesta palvelimesta. Palvelimista yksi on kerääjä, johon lokitiedot välitetään kahdelta palvelimelta. Kahdesta muusta palvelimesta toisesta perustetaan Domain Controller AD-domainiin ja toinen palvelin liitetään tähän domainiin. Testipalvelimena toimivalle asennetaan agentti-sovellus, jolla lokit muunnetaan syslog-muotoon, jonka jälkeen ne lähetetään testiympäristön kerääjälle.

5.2 Testiympäristön asennukset

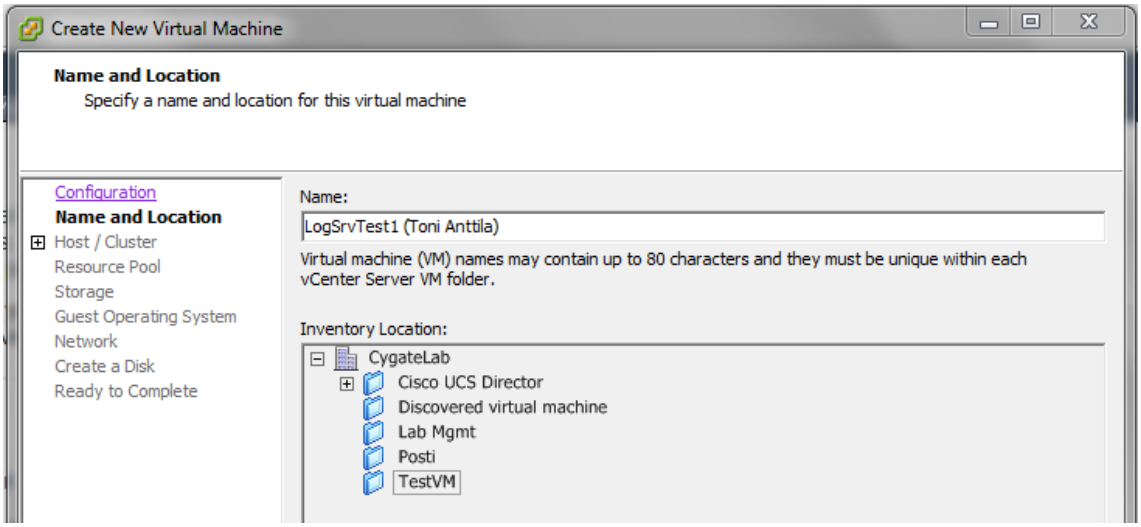
Testausympäristö luodaan VMWare vSpheren virtuaaliympäristöön, johon perustetaan kolme virtuaalikonetta. Lokikerääjän asennus on rajattu insinöörityöstä pois. Kahden Windows-palvelimien asennus käydään läpi työssä. Virtuaalikoneiden asennukset ja niihin asennettava käyttöjärjestelmä on sama asetuksineen. Siksi yhden asennuksen dokumentointi riittää.

Asennus aloitetaan luomalla virtuaalikone. Asennustavaksi valitaan tyypillinen, koska tällä asetuksella saadaan helposti tarvittavat asetukset valmiiksi käytettävää käyttöjärjestelmää varten.



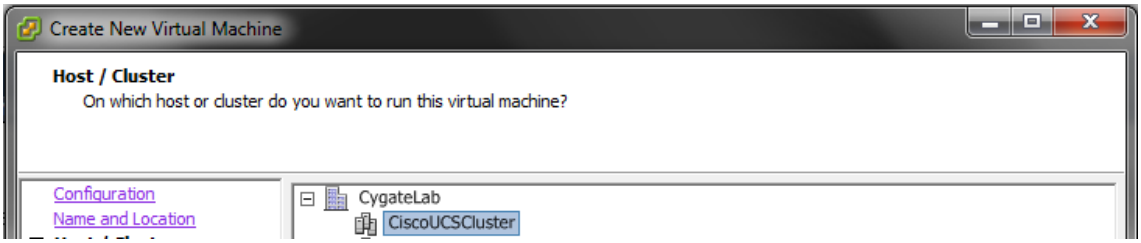
Kuva 5. Virtuaalikoneen asennuksen tyypin valinta.

Seuraavaksi nimetään virtuaalikone, jolla se erotetaan muista virtuaalikoneista.



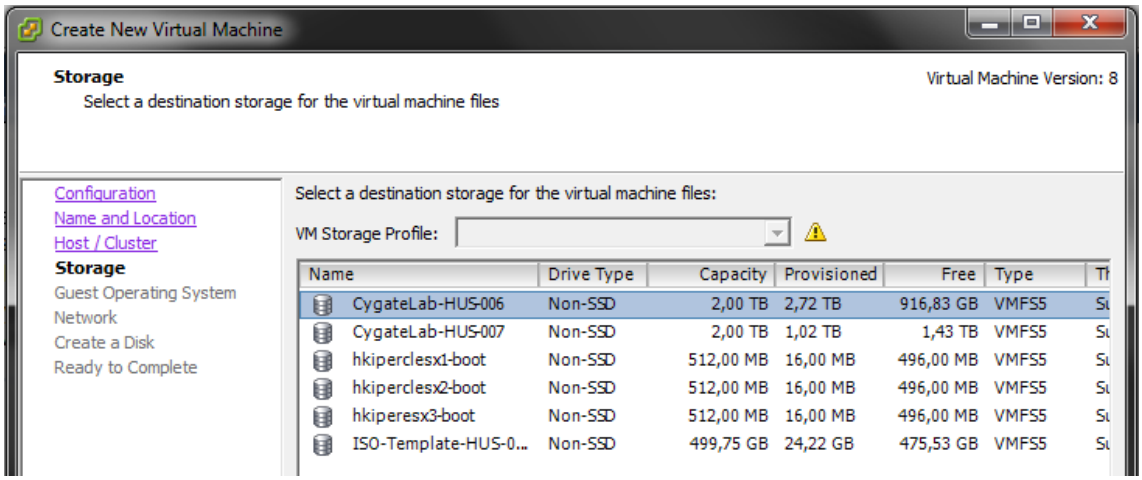
Kuva 6. Virtuaalikoneen nimeäminen.

Seuraavassa vaiheessa valitaan alusta, jonka resursseja luotu virtuaalikone tulee käyttämään.



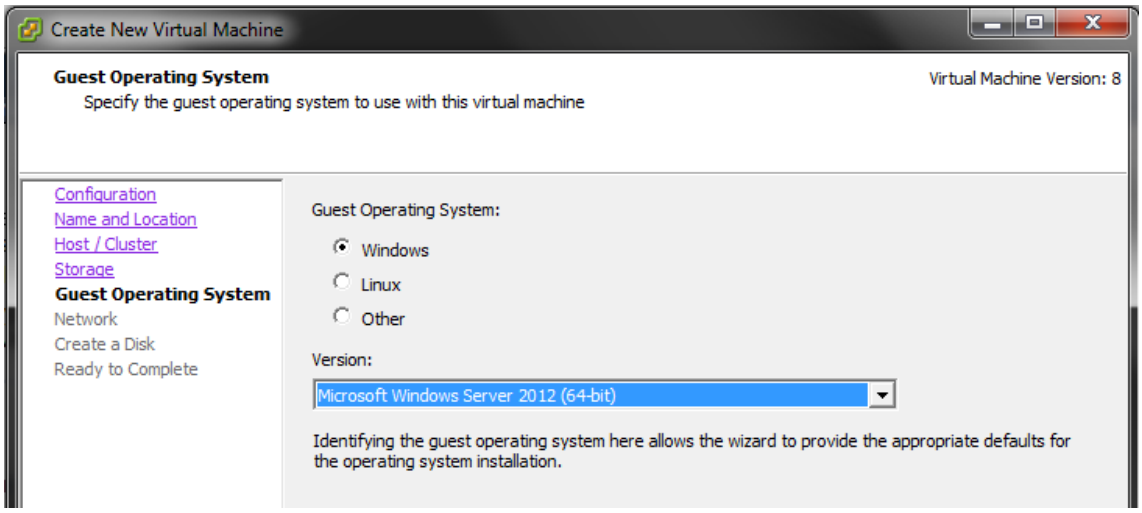
Kuva 7. Resurssialustan valinta.

Tämän jälkeen määritellään käytettävä levyjärjestelmä, minkä tallennustilaa hyödynnetään.



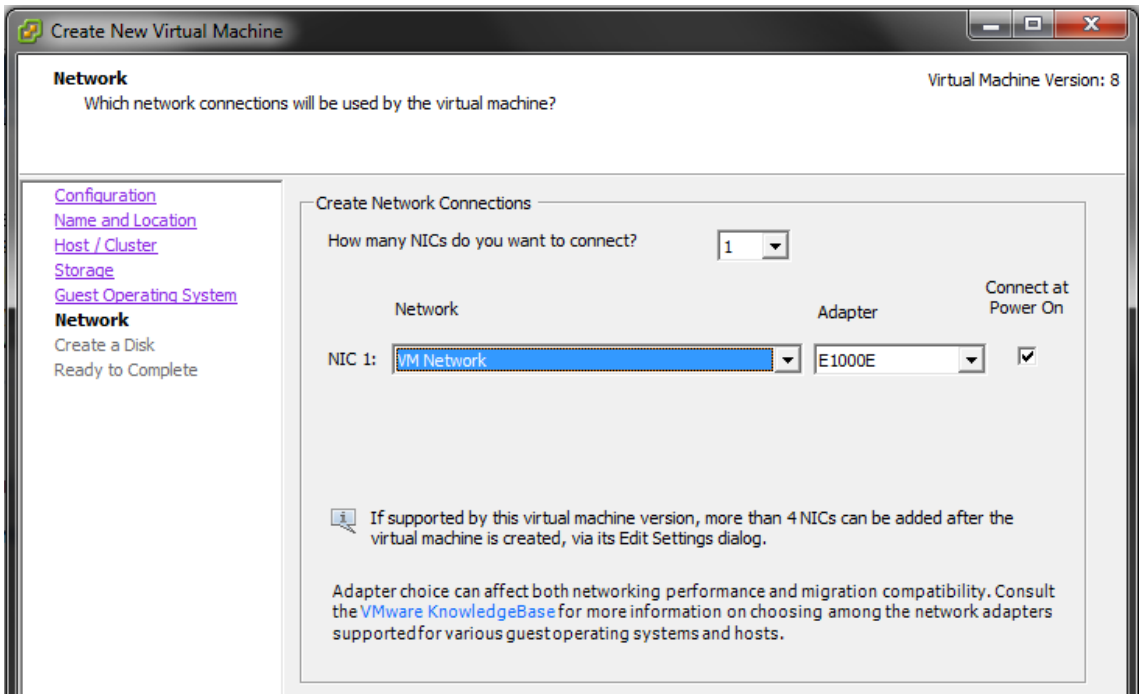
Kuva 8. Käytettävän levyjärjestelmän valinta.

Tämän jälkeen valitaan virtuaalikoneeseen asennettava käyttöjärjestelmä. Tässä virtuaalikoneessa sekä toisessa tullaan käyttämään Windows Server 2012 R2 (64-bit) -versiota. Asetus varaa automaattisesti tarvittavan muistimäärän ja prosessorin sekä tekee muut tarpeelliset määritykset kyseistä käyttöjärjestelmää varten.



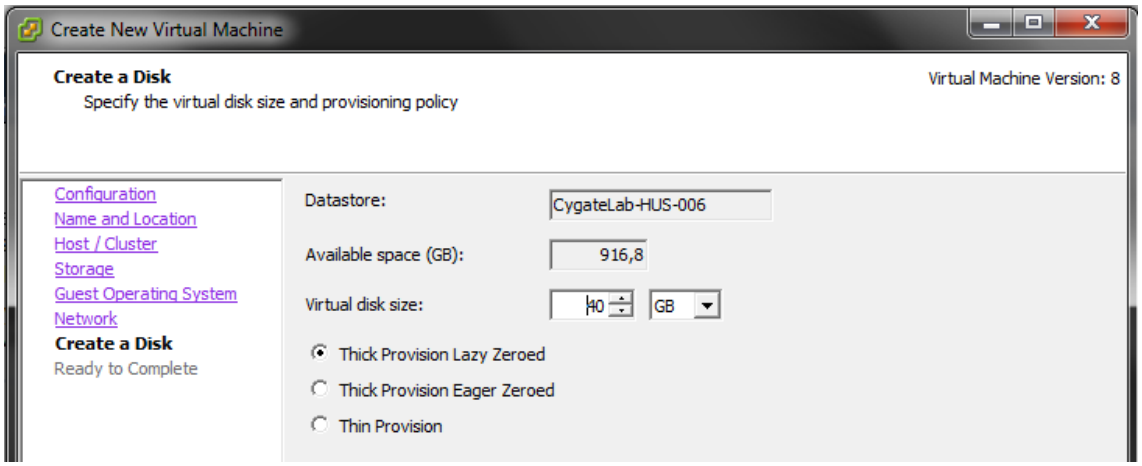
Kuva 9. Käyttöjärjestelmän valinta.

Tämän jälkeen valitaan käytettävä verkkoadapteri, joka jätetään tässä vaiheessa vielä oletukseksi. Myöhemmin tullaan määrittelemään oikea adapteri käyttöön sekä IP-osoitteet. Adaptereita ei tarvita kuin yksi, koska tarvetta kuorman jakamiseen tai redundattisuuteen ei ole.



Kuva 10. Verkkoadapterin määrittäminen.

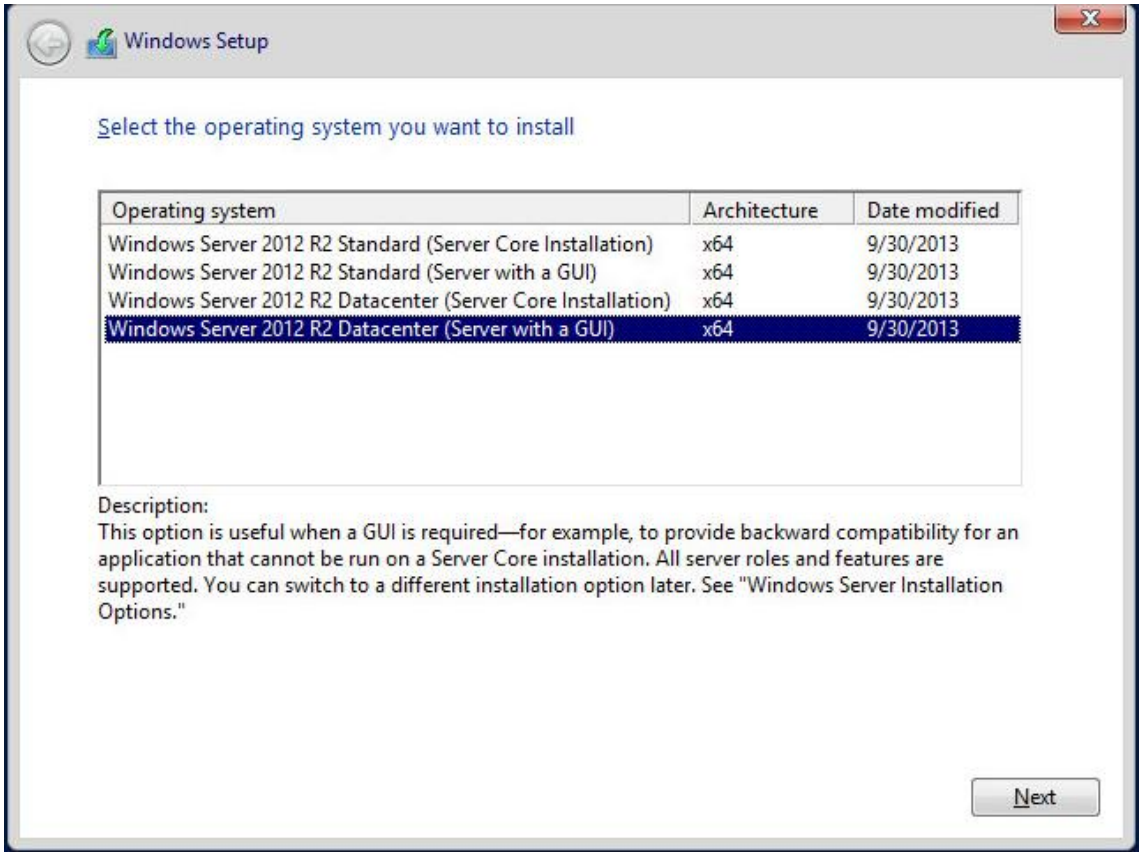
Viimeisessä vaiheessa määritellään kovalevyn koko. Levyn kooksi määritettiin 40 Gb ja käytetään Thick provisiointia eli tila otetaan suoraan käyttöön levyjärjestelmästä.



Kuva 11. Levyn provisiointi ja tilan määrittäminen.

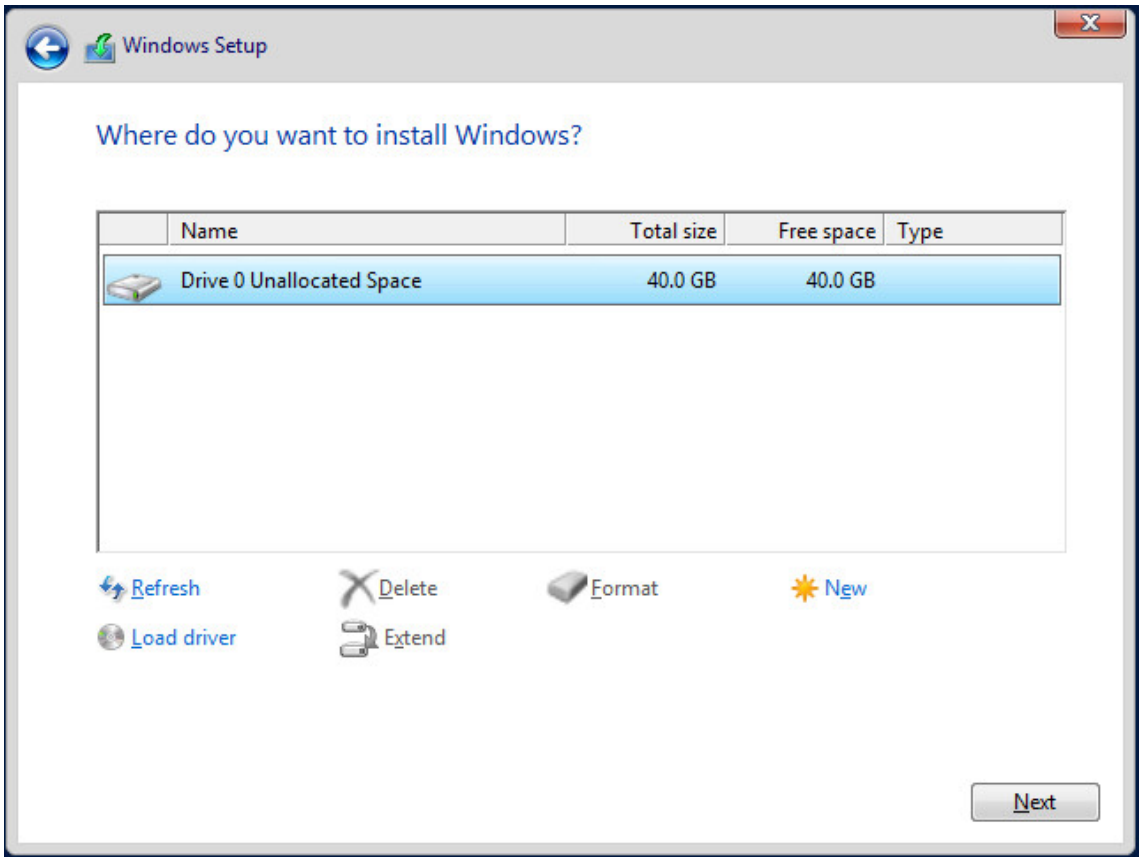
Tämän jälkeen nähdään vielä kooste valituista asetuksista. Seuraavaksi asetukset hyväksytään, jonka jälkeen virtuaalikone luodaan.

Virtuaalikoneen asennuksen jälkeen asennetaan siihen käyttöjärjestelmä. Virtuaalikoneeseen ladataan image, josta asennetaan käyttöjärjestelmä. Käyttöjärjestelmäksi asennetaan Windows Server 2012 R2 Datacenter graafisella käyttöliittymällä.



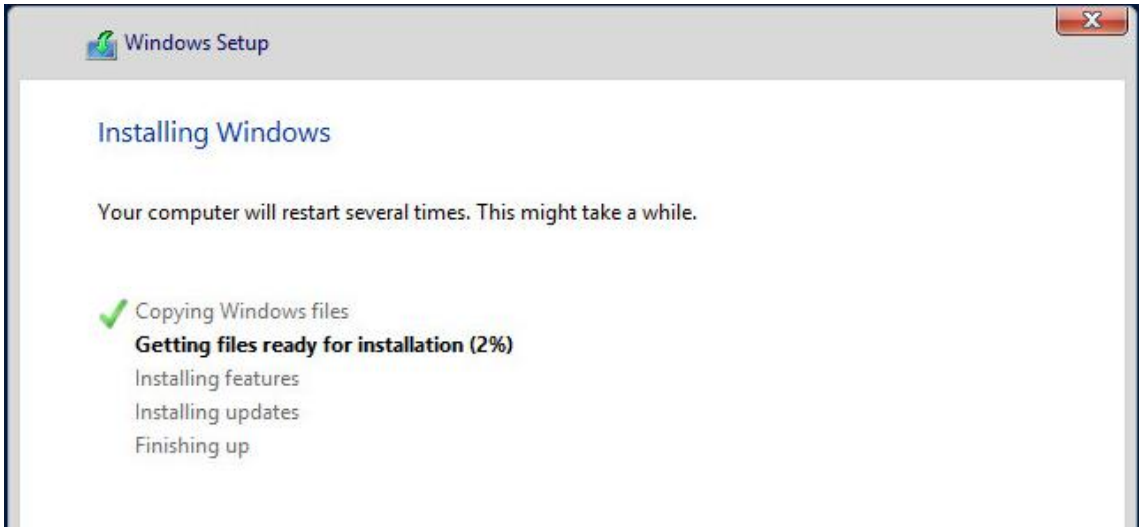
Kuva 12. Käyttöjärjestelmän valinta.

Seuraavaksi valitaan, tehdäänkö päivitys vai muokattu asennus. Valitaan jälkimmäinen, koska koneessa ei ole aikaisempaa käyttöjärjestelmää. Sen jälkeen valitaan, mihin osioon asennetaan ja voidaan tehdä uusia osioita. Asennetaan olemassa olevalle osiolle.



Kuva 13. Levyn valinta asennusta varten.

Tämän jälkeen käynnistyy käyttöjärjestelmän asennus. Asennuksen jälkeen kone käynnistyy uudelleen, jonka jälkeen käyttöjärjestelmä latautuu.

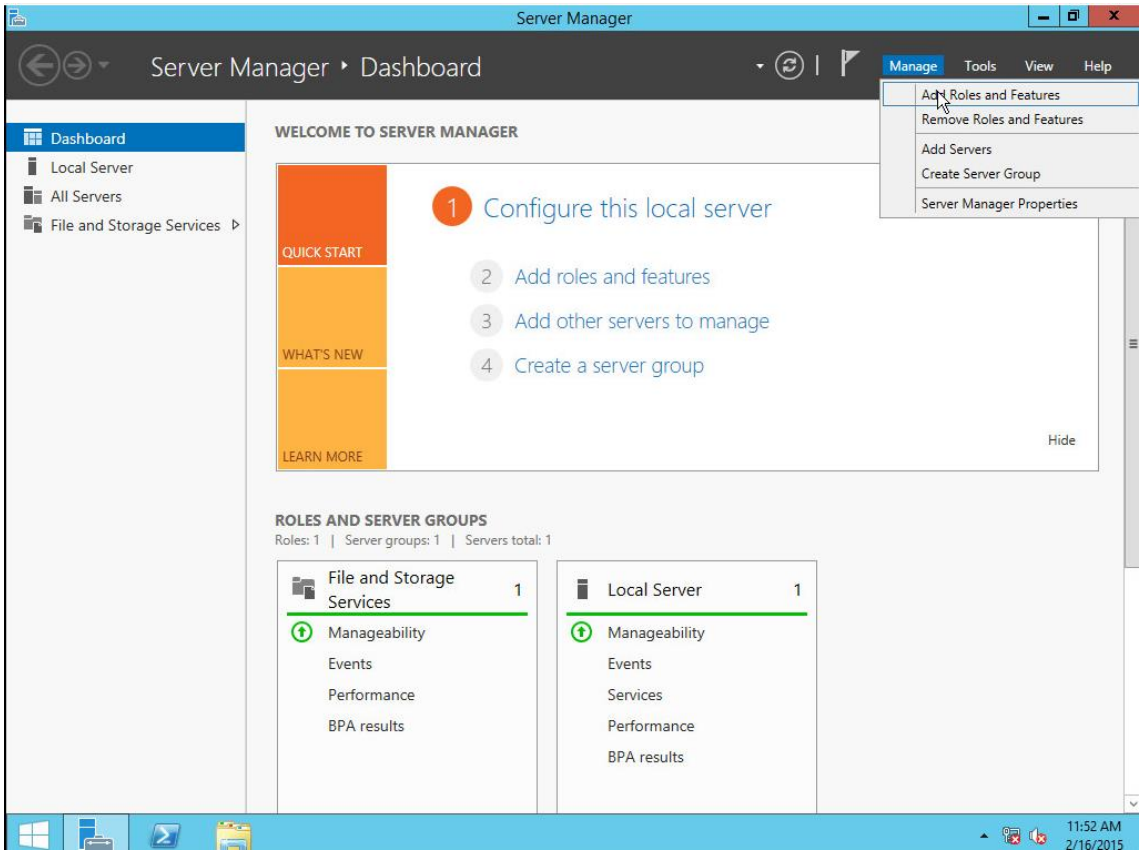


Kuva 14. Käyttöjärjestelmän asennusvaihe.

5.3 Domain Controller

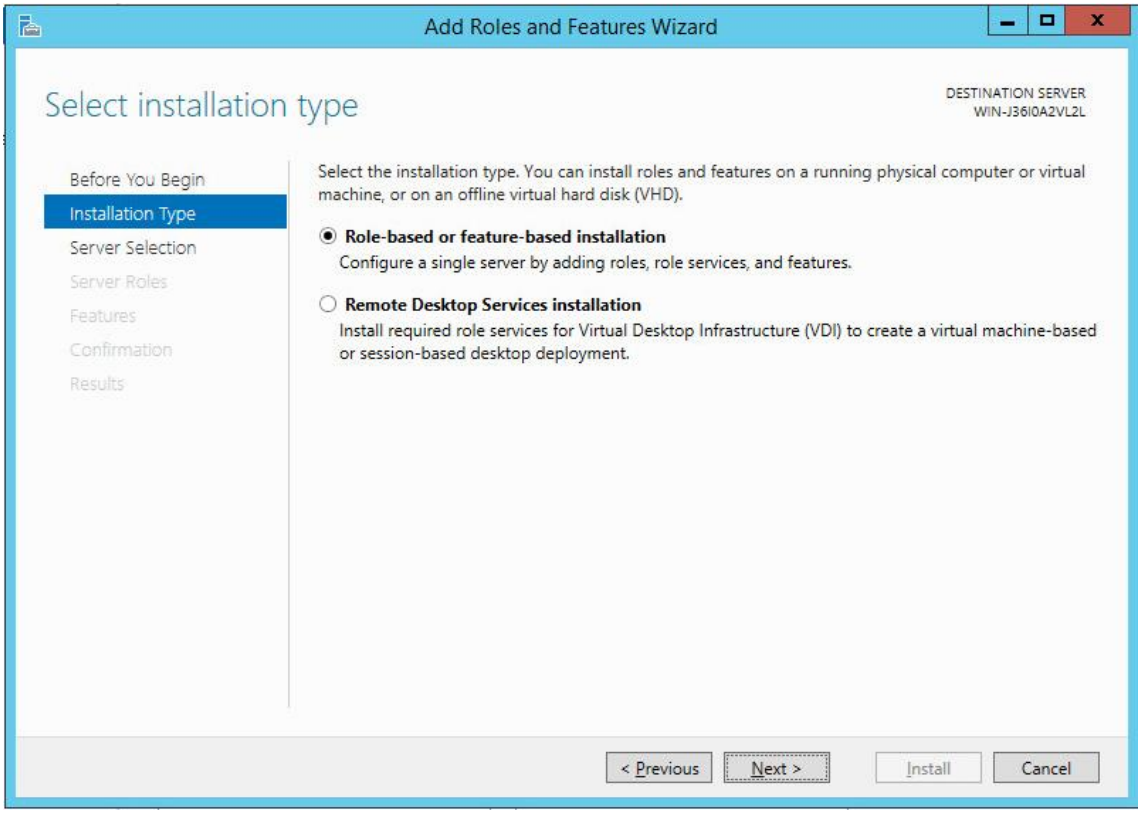
Käyttöjärjestelmän asennuksen jälkeen asennetaan toiselle palvelimista AD DS -rooli sekä DNS. Roolien asennuksien jälkeen palvelimesta tehdään Domain controller, josta voidaan domainia hallita ja muuttaa siihen liittyviä asetuksia.

Roolit asennetaan Server managerin kautta, valitsemalla Manage -> Add Roles and Features -kohdasta. [8]



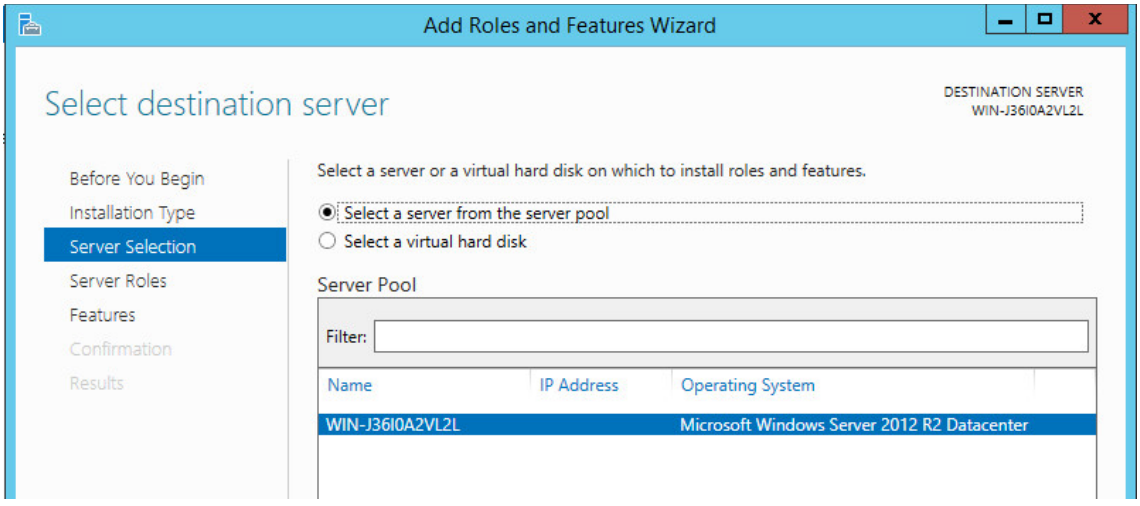
Kuva 15. Roolien asennus.

Asennetaan ensimmäisenä Active directory Domain Services, jossa säilytetään domainiin liittyviä objekteja sekä välittää Domain Controllerille tietoja oikeuksista. Valitaan ensimmäinen valinta, eli asennetaan paikalliselle koneelle.



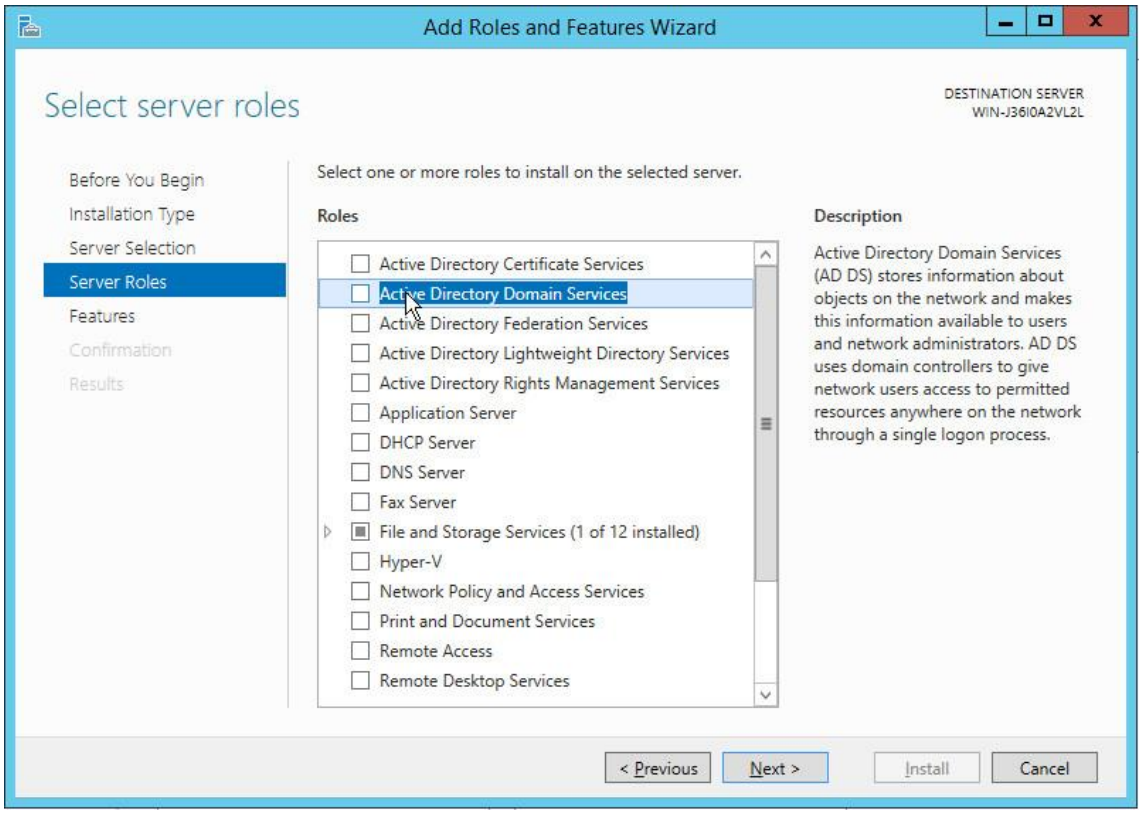
Kuva 16. Asennustyypin valinta.

Seuraavaksi valitaan, mille palvelimelle asennus halutaan suorittaa. Tässä vaiheessa palvelinta ei ollut vielä nimetty, vaan sillä oli Windowsin määrittämä oletusnimi. Myöhemmin nimi vaihdettiin kuvaavammaksi.

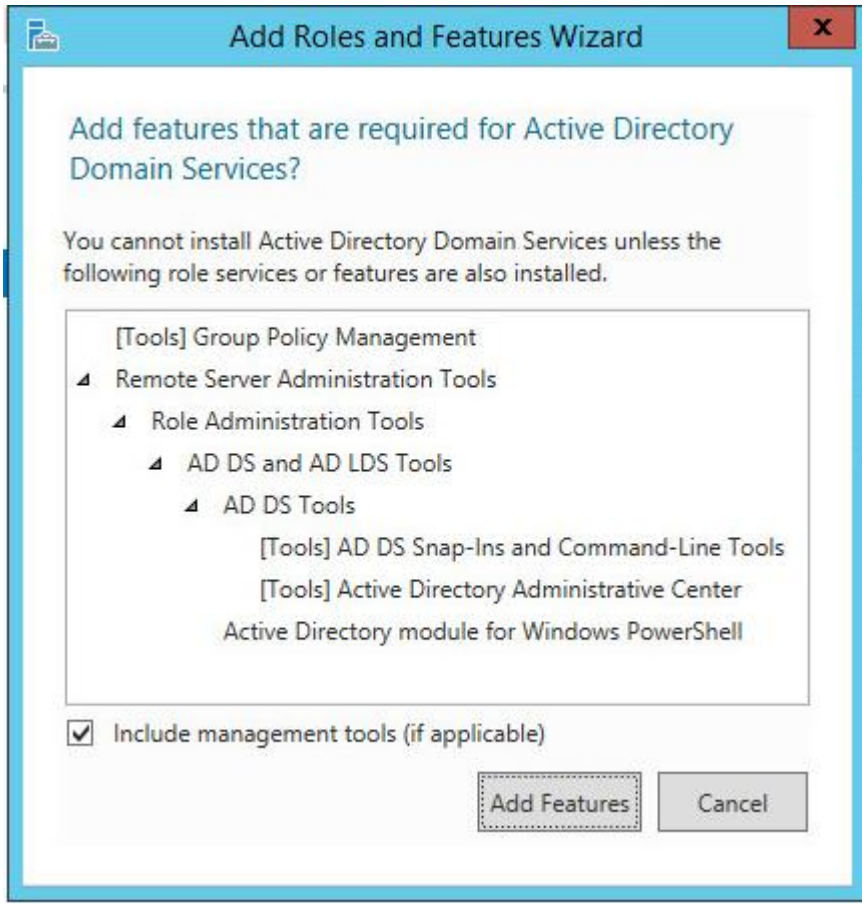


Kuva 17. Palvelimen valinta johon rooli asennetaan.

Seuraavaksi valitaan asennettavat roolit. Asennetaan AD DS- ja DNS-roolit.

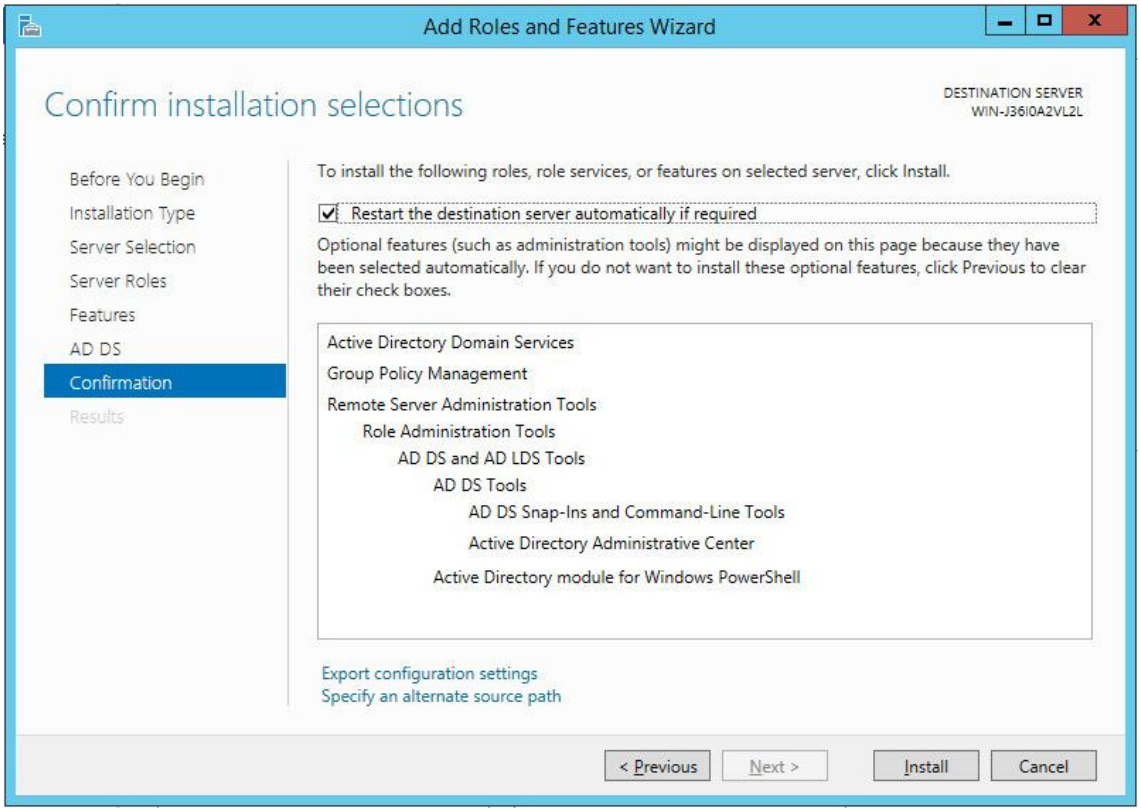


Kuva 18. AD DS -roolin asennuksen valinta.



Kuva 19. Roolia varten asennettavat hallintatyökalut.

Roolin valinnan jälkeen saadaan kuvan 17 mukainen ilmoitus, jossa vaaditaan hallintatyökalujen asentaminen. Nämä tulee hyväksyä, jotta AD DS -asennus voidaan suorittaa tai muuten asennus ei onnistu.

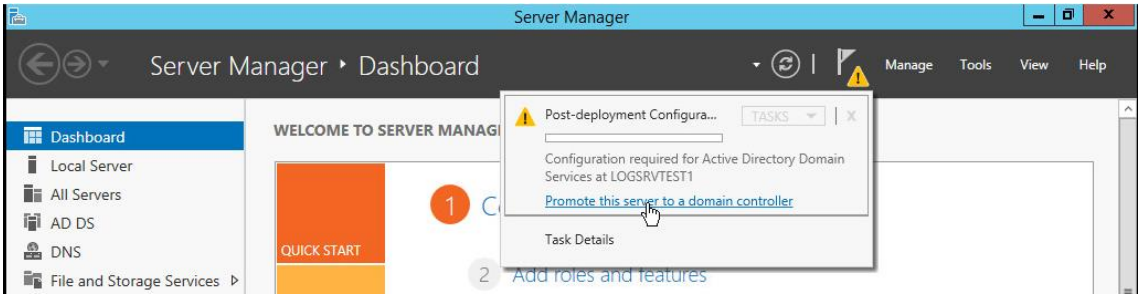


Kuva 20. Roolin asennuksen vahvistaminen.

Viimeinen vaihe asennuksessa on roolin asentamisen vahvistaminen. Tällöin voidaan valita koneen automaattinen uudelleenkäynnistys roolin asennuksen jälkeen. Valittiin kyseinen asetus, koska palvelin on testikäytössä ja se voidaan käynnistää aiheuttamatta katkosta. Tällä varmistutaan siitä, että tarvittava uudelleenkäynnistys ei jää tekemättä, koska se voisi johtaa siihen, että rooli ei toimi ennen uudelleen käynnistystä. Tällä estetään turha vianselvitys.

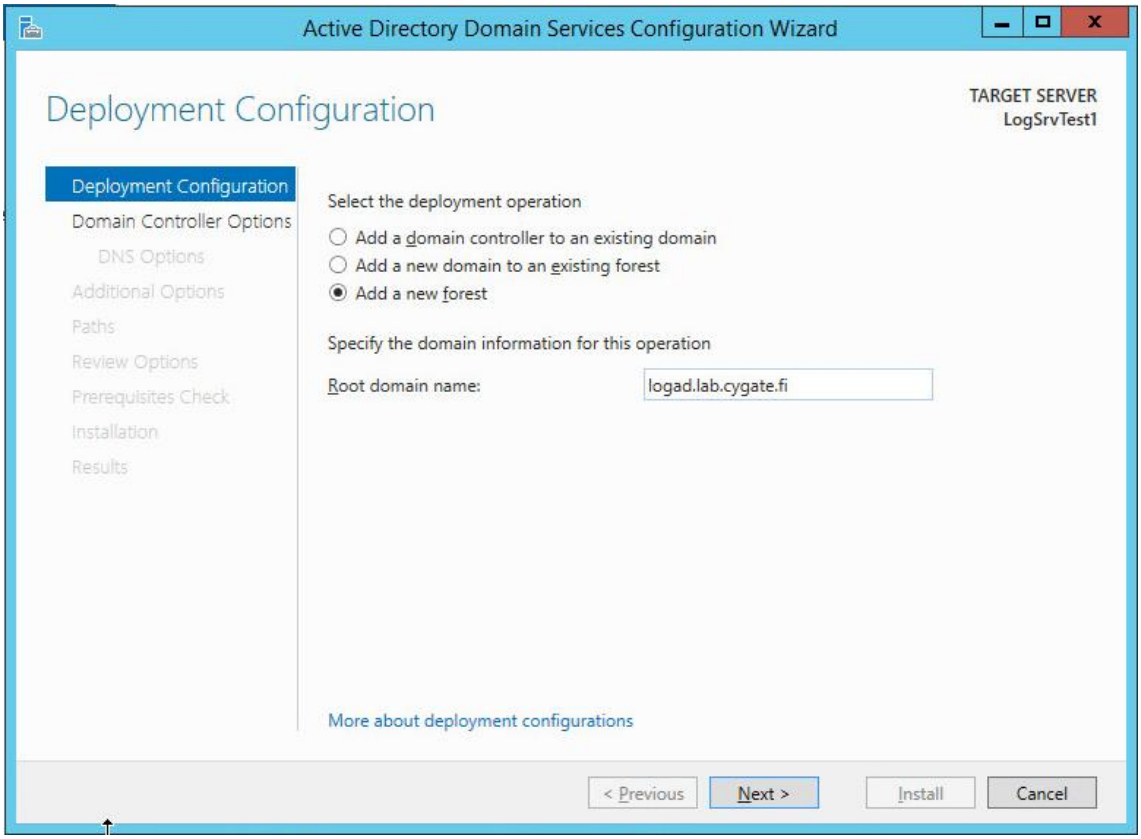
Tämän jälkeen asennettiin DNS-rooli, koska se vaaditaan domainia varten. Sen asentaminen tapahtuu samanlailla kuin AD DS -roolin asennus, ja se voidaan asentaa samanaikaisesti sen kanssa. DHCP:tä ei asennettu, koska domainiin ei tulla liittämään yhtään työasemaa, joihin tarvitsisi jakaa osoitteita. Kaikki palvelimet on määritetty kiinteillä IP-osoitteilla.

Ennen kuin palvelimesta tehdään Domain controller, määritetään palvelimelle kiinteä IP-osoite Local server -välilehdeltä sekä palvelimelle uusi nimi. Lisäksi määritetään DNS-palvelimen osoite, joka tässä tapauksessa on palvelimen IP-osoite. Domain Controllerin määrittäminen tehdään Server managerin kautta.



Kuva 21. Domain controllerin määrittäminen.

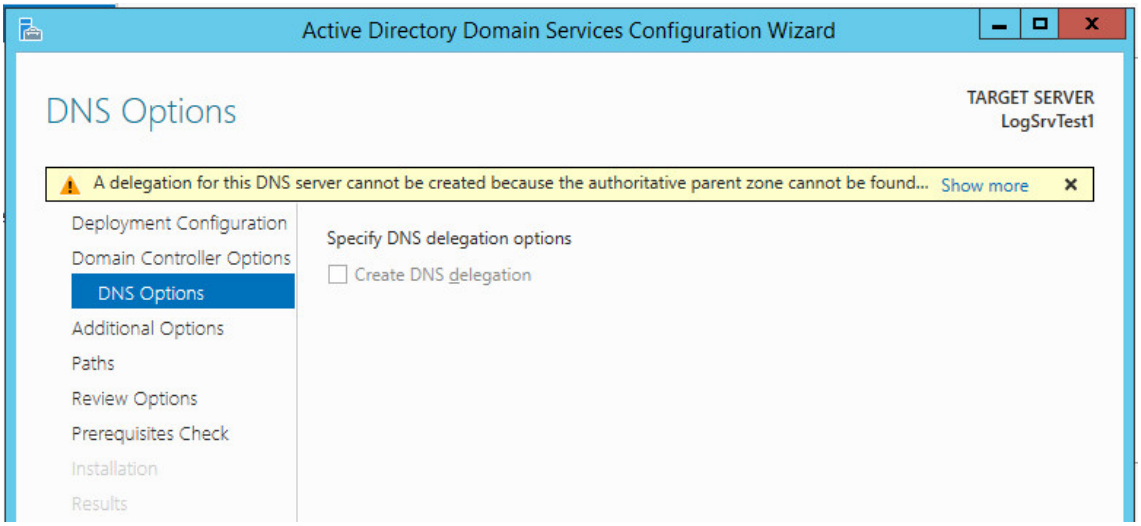
Luodaan uusi Forest, koska emme halua lisätä olemassa olevaan domainiin. Domainille annetaan juurinimeksi logad.lab.cygate.fi.



Kuva 22. Juuri-domainin nimeäminen.

Seuraavaksi määritetään Forestin ja Domainin toiminnallisuustasot. Asetus määrittelee, mitä käyttöjärjestelmä versioita sen tulee tukea, koska eri versioiden välillä saattaa olla eroja. Kummassakin palvelimessa on käytössä sama Windows Server 2012 R2 -käyttöjärjestelmä, joten asetusta ei tarvitse muuttaa.

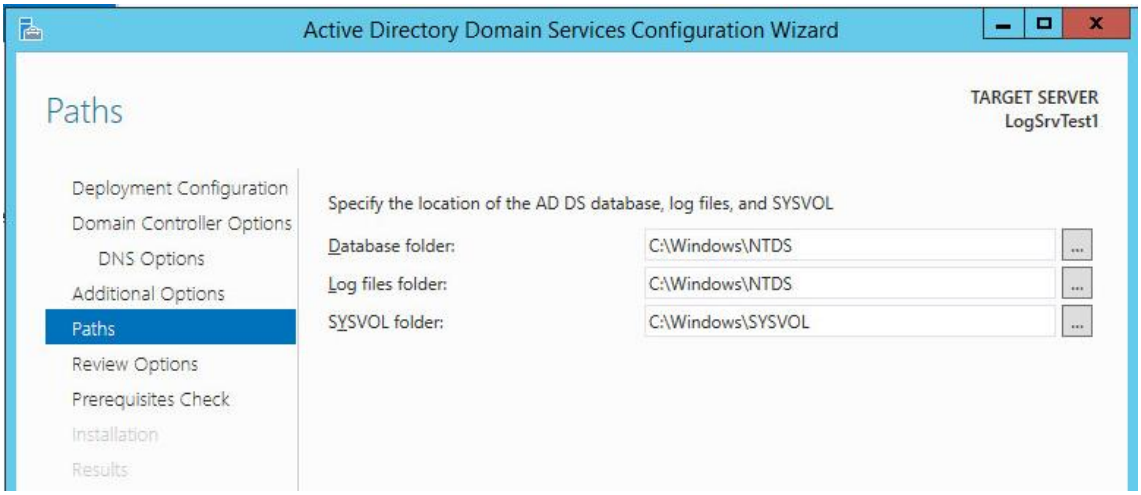
Seuraavaksi voidaan tehdä DNS:iä liittyviä delegointiasetuksia. Asennus antaa tässä vaiheessa virheilmoituksen, että delegointia ei voida suorittaa. Varoitus voidaan jättää huomioimatta, koska käytetään paikallista DNS-palvelinta.



Kuva 23. DNS-määrityksiin liittyvä virheilmoitus.

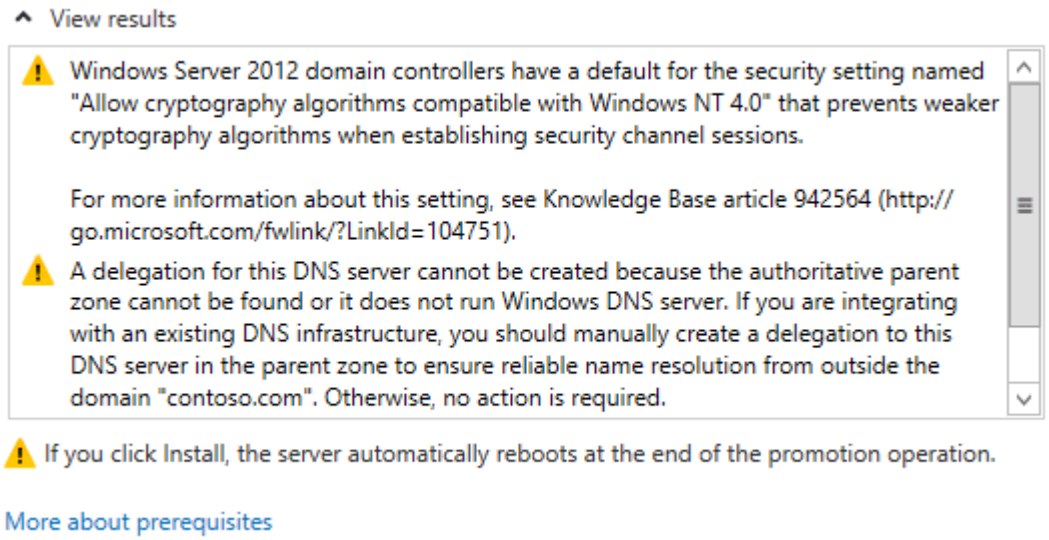
Seuraavaksi asennus määrittää automaattisesti NETBIOS-nimen, joka on LOGAD. Jos nimi halutaan muuttaa, saa se olla enintään 15 merkkiä pitkä.

Seuraavaksi valitaan, mihin AD DS -tietokanta, lokitiedostot ja SYSVOL sijoitetaan. Annetaan näiden olla oletuksina.



Kuva 24. Polkujen valinta.

Asennuksen seuraavassa vaiheessa on kooste valituista määrityksistä. Sen jälkeen asennus tekee tarkistuksen, voidaanko Domain controller -asennus suorittaa.



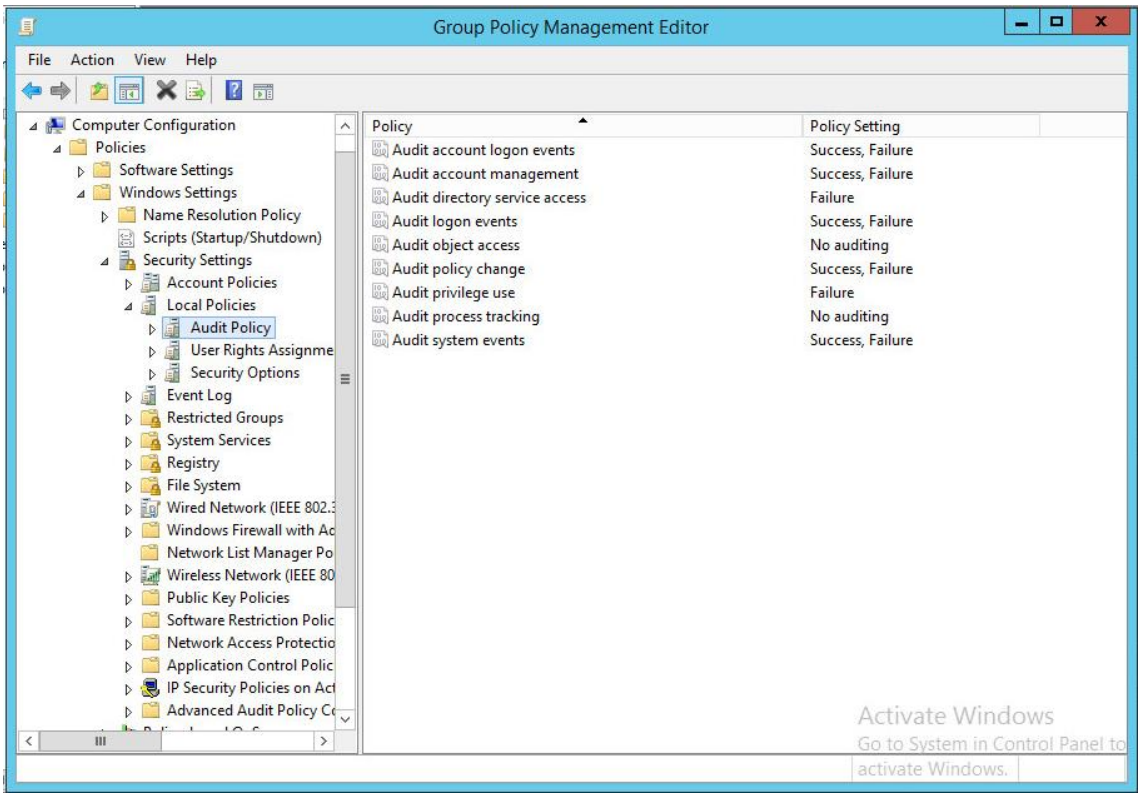
Kuva 25. Tarkistuksen löytämät virhekohdat.

Tarkistuksessa havaitaan todennäköisesti ainakin yksi virhe. Näistä virheistä ei tarvitse kuitenkaan välittää, ja asennus voidaan aloittaa. [9] Asennuksen valmistuttua palvelin käynnistyy uudelleen muutoksen voimaan saattamiseksi.

5.4 Testaukset

Tarkoituksena on suorittaa yksinkertaisia testejä, joilla testataan Audit policyn eri sääntöjä. Yksinkertaisia testejä tehdään sen vuoksi, että osa Audit policyn valvomista tapahtumista vaatii tehtäväksi muutoksia, kuten SACL:n määrityksiä. Näiden tekeminen ei aja varsinaista testien tarkoitusta, kun tapahtumia on tarkoitus alhaisella tasolla analysoida SIEM:ssa sekä tutkia, liittyykö niihin muita tapahtumia.

Testauksia varten DC:lla määriteltiin Default group policy Computer configuration – Windows settings – Security settings – Local policies alta löytyvään Audit policyn halutut asetukset. Käytetään asetuksia, jotka ovat käytössä yrityksen palvelimilla.



Kuva 26. Audit policy -määritykset

Tämän jälkeen, kun asetukset on määritelty, on ne tuotava palvelimille voimaan. Komentorivillä ajetaan komento gpupdate /force, joka pakottaa palvelimen päivittämään Group policy -asetukset.

Lokitapahtumien edelleenlähettämistä varten palvelimille asennettiin agentit, jotka muuntavat lokitapahtumat Syslog-muotoon ja lähettävät ne kerääjälle. Agentin konfiguraatio tiedostoon määritettiin liitteen 2 mukaiset asetukset.

Ensimmäisenä testattiin Account logon eventiä. Kirjauduttiin domainiin kuuluvalle palvelimelle domain-tunnuksella. Ensiksi tehtiin epäonnistunut kirjautumisyritys, jonka jälkeen onnistunut kirjautuminen. SIEM:stä nähdään, että tähän kirjautumiseen liittynyt tapahtuma muodostuu DC:ltä niin kuin sen kuuluukin, koska kirjautuminen vahvistetaan DC:lla. Yhteensä testistä muodostui kaksi tapahtumaa hylätty ja hyväksytty.

Toisessa testissä testattiin Account managementia. Luotiin DC:llä uusi käyttäjätunnus, josta muodostui useampi tapahtuma. Ensimmäinen merkintä on käyttäjän luonti, jonka

jälkeen seurasi neljä käyttäjää muuttavaa tapahtumaa. Nämä todennäköisesti ovat käyttäjänasetuksiin liittyviä määrityksiä, kuten käyttäjä ei voi muuttaa salasanaansa.

Hylättyä tapahtumaa en saanut tehtyä. Luotiin uutta käyttäjää, jolle annettu väärän pituinen salasana virheellisen tapahtuman aikaansaamiseksi. Palvelin antaa tästä virheilmoituksen, koska on annettu liian lyhyt salasana. SIEM:stä ei kuitenkaan löytynyt hylätysti luodusta käyttäjästä tapahtumia, vaan löytyi tiedot käyttäjän luonnista ja sen poistamisesta. Poistaminen johtui siitä, että käyttäjän luonti peruutettiin.

Kolmannessa testissä testattiin Audit logon eventsia. Ensimmäinen kirjautuminen tehtiin virheellisenä ja annettiin väärä salasana. Seuraavaksi kirjauduttiin oikealla salasanalla, jotta saadaan hyväksytty kirjautuminen. Logon events kerää kirjautumistapahtumat palvelimelta, johon kirjaudutaan. SIEM:stä nähtiin kaksi kirjautumista domainiin liitetyltä palvelimelta. Ensimmäinen tapahtuma oli epäonnistuneesta kirjautumisyrityksestä ja jälkimmäinen onnistuneesta. Kirjautuminen luo aina kaksi erillistä tapahtumaa. Tapahtumista toinen on ensimmäisessä testissä huomattu DC:llä tapahtuva todentaminen ja toinen tapahtumista on kirjauduttavalta koneelta kerätty tapahtuma.

Neljännessä testissä testattiin Audit policy changea. Muutettiin DC:lla määritettyjä Audit policy -asetuksia ottamalla Account logon -asetuksista failure-tapahtumien keräys pois. Tästä kertyi tapahtuma, joista voidaan nähdä asetuksien muuttaminen. Myös asetuksen palauttamisesta muodostui samankaltainen tapahtuma, josta kävi ilmi asetuksen muuttaminen. Seuraavana tapahtumat ovat Syslog-muodossa.

```
Mar 21 12:54:04 logtest1.logad.lab.cygate.fi MSWinEvent-
Log,1,Security,11282,Sat Mar 21 12:54:04 2015,4719,Microsoft-Windows-
Security-Auditing,N/A,N/A,Success Au-
dit,logtest1.logad.lab.cygate.fi,Audit Policy Change,,System audit po-
licy was changed. Subject: Security ID: S-1-5-18 Account Name: LOG-
TEST1$ Account Domain: LOGAD Logon ID: 0x3E7 Audit Policy Change: Cat-
egory: Account Logon Subcategory: Credential Validation Subcategory
GUID: {0CCE923F-69AE-11D9-BED3-505054503030} Changes: Failure re-
moved,344612

Mar 21 13:04:05 logtest1.logad.lab.cygate.fi MSWinEvent-
Log,1,Security,12576,Sat Mar 21 13:04:05 2015,4719,Microsoft-Windows-
Security-Auditing,N/A,N/A,Success Au-
dit,logtest1.logad.lab.cygate.fi,Audit Policy Change,,System audit
policy was changed. Subject: Security ID: S-1-5-18 Account Name: LOG-
TEST1$ Account Domain: LOGAD Logon ID: 0x3E7 Audit Policy Change: Cat-
egory: Account Logon Subcategory: Credential Validation Subcategory
GUID: {0CCE923F-69AE-11D9-BED3-505054503030} Changes: Failure add-
ed,345733
```

Viidennessä testissä testattiin Audit privilege use -tapahtumien valvontaa. Aiemmin on määritetty, että valvotaan vain epäonnistumisia. Testi1:n käyttäjälle on määritetty Domain user -oikeudet, joten on yritetty päästä katsomaan Local security policies -asetuksia. Asetuksiin on näillä oikeuksilla pääsy estetty. Tästä muodostui seuraava tapahtuma. Muita tähän liittyviä tapahtumia ei muodostunut.

```
Mar 21 10:56:55 logtest2.logad.lab.cygate.fi MSWinEventLog,3,Security,1504,Sat Mar 21 10:56:55 2015,4673,Microsoft-Windows-Security-Auditing,N/A,N/A,Failure Audit,logtest2.logad.lab.cygate.fi,Sensitive Privilege Use,,A privileged service was called. Subject: Security ID: S-1-5-21-3782078238-118341055-997336219-1110 Account Name: testi1 Account Domain: LOGAD Logon ID: 0x35CF91 Service: Server: Security Service Name: - Process: Process ID: 0xa64 Process Name: C:\Windows\System32\mmc.exe Service Request Information: Privileges: SeCreateGlobalPrivilege,2241
```

Viimeisessä testissä testattiin Audit system events -tapahtumien valvontaa. Event viewerista poistettiin kaikki Security-tapahtumat. Tästä muodostui yksi tapahtuma, mistä selviää tapahtuma.

```
Mar 21 13:28:50 logtest2.logad.lab.cygate.fi MSWinEventLog,1,Security,3405,Sat Mar 21 13:28:50 2015,1102,Microsoft-Windows-Eventlog,N/A,N/A,Information,logtest2.logad.lab.cygate.fi,Log clear,,The audit log was cleared. Subject: Security ID: S-1-5-21-3782078238-118341055-997336219-1111 Account Name: testi2 Domain Name: LOGAD Logon ID: 0x3DA9B2,2589
```

6 Yhteenveto

Työ eteni alusta alkaen sujuvasti ja suunnitelmien mukaisesti. Työ on rajattu varsin tarkasti ja työ oli laajuudeltaan sopiva käytettävään aikaan nähden.

Palvelimien lokienvalvonta-asetukset saatiin selvitettyä Windows-palvelimelta sekä Linux-palvelimelta. Linux-palvelimen osalta selvitettiin vain nykyiset asetukset ja niiden todettiin olevan vaatimusten mukaiset. Windows-palvelimen osalta selvisi asetuksien olevan myös vaatimuksien mukaiset, joten muutoksia niiden osaltakaan ei tarvinnut tehdä. Audit policyn toimintaa selvitettäessä selvisi, että eräät asetukset muodostavat runsaita määriä lokitapahtumia, joka tuottaa nk. kohinaa eli peittää tärkeät tapahtumat alleen. Selvityksessä todettiin, että näitä asetuksia ei valvota. Asetukset dokumentoitiin, jotta ne voidaan ottaa käyttöönottoprosessiin mukaan.

Työn tekemistä hidasti jonkin verran testiympäristön perustaminen, koska alustavaa suunnitelmaa ei saatu toteutettua muutamien ongelmien vuoksi. Sen vuoksi perustettiin kaikki tarvittavat komponentit suoraan testiympäristöön, joilla pystyttiin välttämään näitä ongelmia.

Testiympäristössä saatiin tarvittavat testaukset suoritettua ja niiden tuloksia voidaan pitää onnistuneina. Muutama testi jäi tekemättä, koska se olisi vaatinut aikaa asetuksien selvittämiseen, jotta halutut tapahtumat olisi saatu muodostettua. Tällä ei ole mielestäni suurta vaikutusta itse työhön, koska tarkoitus oli tutustua lokitapahtumiin alhaisella tasolla. Testit olivat verrattain yksinkertaisia, mutta ovat usein toistuvia ja yleisiä.

Lähteet

1 Karen, Kent & Murugiah, Souppaya. 2006. Guide to Computer Security Log Management. Verkkodokumentti. <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>. Luettu 14.1.2015

2 Chuvakin, Anton A., Schmidt, Kevin J. & Phillips Christopher. 2012. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Syngress.

3 Syslog. Verkkodokumentti. <http://en.wikipedia.org/wiki/Syslog#Facility_levels>. Luettu 10.1.2015

4 An Introduction to Syslog. Rainer Gerhards. 2004. Verkkodokumentti. <http://www.monitorware.com/common/en/seminarsonline/syslog-intro-v1.pdf>. Luettu 17.1.2015

5 Event logging. MSDN Microsoft. <http://msdn.microsoft.com/en-us/library/windows/desktop/aa363652%28v=vs.85%29.aspx>. Luettu 18.1.2015

6 Audit Policy. TechNet. <https://technet.microsoft.com/en-us/library/cc766468%28v=ws.10%29.aspx>. Luettu 23.1.2014.

7 Advanced audit policy configuration. TechNet. <https://technet.microsoft.com/en-us/library/jj852202%28v=ws.10%29.aspx>. Luettu 24.1.2014.

8 Installing Active Directory, DNS and DHCP to Create a Windows Server 2012 Domain Controller. Youtube. <https://www.youtube.com/watch?v=0WyBxwJD_c0>. Katsottu 22.2.2015.

9 Known Issues for Installing and Removing AD DS. TechNet. Päivitetty 30.11.2011. <https://technet.microsoft.com/en-us/library/cc754463%28v=ws.10%29.aspx>. Luettu 26.2.2015.

Syslog-konfiguraatio

```
# Log all kernel messages to the console.

# Logging much else clutters up the screen.
#kern.*             /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none   /var/log/messages

# The authpriv file has restricted access.
authpriv.*          /var/log/secure

# Log all the mail messages in one place.
mail.*              /var/log/maillog

# Log cron stuff
cron.*              /var/log/cron

# Everybody gets emergency messages
*.emerg             *

# Save news errors of level crit and higher in a special file.
uucp,news.crit      /var/log/spooler

# Save boot messages also to boot.log
local7.*            /var/log/boot.log

#Forward logs to collector
*.info              @x.x.x.x

#nco events
local0.error        @x.x.x.x
```

Nxlog konfiguraatio

```
## This is a sample configuration file. See the nxlog reference manual about the
## configuration options. It should be installed locally and is also available
##  online  at  http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html
## Please set the ROOT to the folder your nxlog was installed into,
## otherwise it will not start.

#define ROOT C:\Program Files\nxlog
define ROOT C:\Program Files (x86)\nxlog

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log

<Extension syslog>
    Module      xm_syslog
    SnareDelimiter ,
</Extension>

<Input internal>
    Module      im_internal
</Input>

<Input eventlog>
    Module      im_msvistalog
# For windows 2003 and earlier use the following:
#   Module      im_mseventlog
</Input>

<Output out>
    Module      om_tcp
    Host        10.206.2.29
```

```
    Port        514
    Exec        to_syslog_snare();
</Output>

<Route 1>
    Path        eventlog, internal => out
</Route>.
```