

Tommy Lindholm

Microsoft System Center 2012 Configuration Manager

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikka
Insinööriyö
Päivämäärä 19.04.2013

| | |
|--|---|
| Tekijä(t) Otsikko Sivumäärä Aika | Tommy Lindholm Microsoft System Center 2012 Configuration Manager 41 sivua + 1 liite 15.9.2010 |
| Tutkinto | Insinööri (AMK) |
| Koulutusohjelma | Tietotekniikka |
| Suuntautumisvaihtoehto | Tietoverkot |
| Ohjaaja(t) | Lehtori Tapio Wikström |
| <p>Tässä opinnäytetyössä käsitellään Microsoft System Center Configuration Manager 2012 – ohjelmistoa. Opinnäytetyön alussa tehdään yleiskatsaus Configuration Manager – ohjelmistoon ja sen suomiin mahdollisuuksiin. Käytännönsuudessa tutustutaan ohjelmiston asennukseen, käyttöjärjestelmän levitykseen ja ohjelmistokirjaston rakentamiseen.</p> <p>Työ toteutettiin VMWare-virtualisointialustalla, minne luotiin kaksi palvelinta ja kolme työasemaa. Palvelimien käyttöjärjestelmiksi asennettiin Windows Server 2008 R2. Palvelimet jaettiin Domain Controlleriin ja Configuration Manageriin.</p> <p>Configuration Manager palvelimelle asennettiin SQL-tietokanta, jonne koko ympäristö ohjattiin. Configuration Managerilla luotiin käyttöjärjestelmälevykuvat Windows 7 Enterprisesta, jotka asennettiin kahdelle työasemalle verkon yli. Yksi työasema oli asennettuna valmiiksi, joka toimi ympäristön testauspisteinä.</p> <p>Tämän opinnäytetyön tarkoituksena on saada yleiskäsitys Configuration Managerista ja sen monipuolisuudesta ympäristöstä riippuen.</p> | |
| Avainsanat | Configuration Manager, käyttöönotto, tutkimus |

| | |
|---|--|
| Author(s) Title | Tommy Lindholm Microsoft System Center 2012 Configuration Manager |
| Number of Pages Date | 41 pages + 1 appendices 19 Apr 2010 |
| Degree | Bachelor of Engineering |
| Degree Programme | Information Technology |
| Specialisation option | Computer Networks |
| Instructor(s) | Tapio Wikström, Senior Lecturer |
| <p>This thesis addresses the Microsoft System Center Configuration Manager 2012 software. The study begins with the overview of the Configuration Manager 2012 software and possibilities it brings. The practical section introduces the software's installation, the distribution of operating systems and the construction of the software library.</p> <p>The work was carried out on a VMWare virtualization platform, onto which were created two servers and three workstations. Windows Server 2008 R2 was installed for the server's operating system. The servers were divided into a Domain Controller and a Configuration Manager.</p> <p>The SQL database was installed upon the Configuration Manager server where the whole environment was directed. A Windows 7 Enterprise operating system image was created with Configuration Manager which was installed onto two workstations over the network. One workstation was preinstalled which served as an environmental testing point. The purpose of this thesis is to obtain an overview of the Configuration Manager and its versatility depending on the environment.</p> | |
| Keywords | Configuration Manager, Implementation, Research |

Sisällys

Lyhenteet

| | | |
|-------|---|----|
| 1 | Johdanto | 1 |
| 2 | Yleiskatsaus Configuration Manager -ohjelmistoon | 1 |
| 2.1 | Toimipistehierarkkia (Site Hierarchy) | 2 |
| 2.2 | Toimipisteen järjestelmät (Site systems) | 3 |
| 2.3 | Löytötyypit (Discovery types) | 4 |
| 2.4 | Asiakkasohjelma (Clients) | 5 |
| 2.5 | Kokoelmat (Collections) | 5 |
| 2.6 | Ohjelmistopäivityspalvelut (Software update services) | 6 |
| 2.6.1 | Windows-päivityspalvelut (Windows software update services) | 7 |
| 2.6.2 | Päivitysten synkronointi (Software Synchronization) | 7 |
| 2.6.3 | Ohjelmistopäivitysten graafinen hallintakonsoli | 8 |
| 2.7 | Mobiililaitteiden hallinta (Mobile device management) | 9 |
| 2.8 | Raportointi (Reporting) | 9 |
| 2.9 | Käyttöjärjestelmän levittäminen (Operating system deployment) | 10 |
| 2.10 | Turvallisuus ja valtuutukset | 12 |
| 2.11 | Varmuuskopiointi, palautus ja niiden ylläpito | 15 |
| 3 | Suunnitelma | 16 |
| 3.1 | Alkuasetelma | 16 |
| 3.2 | Hahmotelma | 17 |
| 4 | Toteutus | 17 |
| 4.1 | Toimialue | 18 |
| 4.2 | Configuration Manager -palvelin | 18 |
| 4.3 | Resurssien löytäminen ja järjestely Configuration Managerissa | 19 |
| 4.4 | Rajojen ja rajaryhmien määrittäminen | 22 |
| 4.5 | Laitteistokokoelman luonti | 25 |
| 4.6 | Clienttien asennus ja hallinto | 25 |
| 4.7 | Käyttöjärjestelmän luonti ja asennus | 28 |
| 4.8 | Ohjelmistojen levittämisen käyttöönotto | 31 |

5 Yhteenveto

33

Lähteet

35

Lyhenteet

| | |
|------|--|
| ADDS | Active Directory Domain Services on AD:n palvelinrooli , jolla voidaan toteuttaa skaalautuva, turvallinen hallittava infrastruktuuri |
| APT | Advanced persistent threat. Usein verrataan ryhmäksi, kuten ulkopuolinen valtio, jolla on valmiudet ja aiomukset kohdistettuun hyökkäykseen tehokkaasti tiettyä yksikköä kohtaan. Termiä käytetään usein verkkouhkia määriteltäessä. |
| b | bitti, pienin mahdollinen informaation yksikkö. Bitillä on kaksi mahdollista arvoa, joita kuvaavat yleensä ykkönen ja nolla. (Käytä tyyliä Lyhenneluettelon kohta.) |
| B | tavu, kahdeksan bitin muodostama informaation yksikkö. |
| BIOS | Basic Input-Output Systemin tarkoitus on alustaa ja varmistaa järjestelmän laitteistokomponentit. BIOS lataa käyttöjärjestelmän muistiin käynnistettäväksi. |
| DC | Domain controller on toimialueen ylläpitoon tarkoitettu serverirooli. Pääsääntöisesti DC on vastuussa toimialueen turvallisuudesta ja käyttäjäautentikoinnista. |
| DHCP | Dynamic Host Configuration Protocol on verkkoprotokolla, jolla hallinnoidaan verkkolaitteita, jotta ne kykenevät kommunikoimaan IP-verkossa. |
| DNS | Domain Name Services, eli verkon nimipalvelujärjestelmä, joka muuttaa verkkotunnuksia IP-osoitteeksi |

| | |
|-----------|--|
| FSP | Fallback status pointilla seurataan käyttäjien käyttöönottoa Windows-käyttöjärjestelmässä ja tunnistetaan nämä käyttäjät tietokoneilla, jotka eivät ole hallinnoitavissa. |
| IIS | Internet information services on joukko laajennusmoduuli ominaisuuksia, jotka on suunniteltu Microsoft Windows-käyttöjärjestelmille. |
| LDAP | Lightweight Directory Access Protocol on hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla. LDAP:in yleisin käyttötarkoitus on käyttäjätunnistus ja käyttöoikeuksien tarkistaminen. |
| Metatieto | on tietoa tiedosta eli kuvailevaa ja määrittävää tietoa jostakin tietovarannosta tai sisältöyksiköstä. |
| OSD | Operating system deployment sallii käyttäjän tehdä käyttöjärjestelmistä levykuvia ja asentaa niitä kohde tietokoneeseen. Myös tehtävien järjestely on mahdollista. |
| RAID | Redundant Array of Independent Disks (RAID) on tekniikka, jolla tietokoneiden vikasietoisuutta ja/tai nopeutta kasvatetaan käyttämällä useita erillisiä kiintolevyjä, jotka yhdistetään yhdeksi logiseksi levyksi. RAID-tekniikkaa käytetään etenkin siellä, missä levyjen vasteajat tai virheettömyys ovat tärkeitä, kuten levy- ja tietokantapalvelimissa. |
| SQL | Structured Query Language on tietokantaohjelmointikieli, joka on suunniteltu relaatiotietokanta ohjelmistojen hallintaan |
| SSRS | SQL Server Reporting Services on serveripohjainen raportointiohjelmisto, jota hallinoidaan selainkäyttöliittymällä |
| Sysprep | Microsoftin työkalu jolla valmistellaan käyttöjärjestelmäkäyttöönottoon. |

1 Johdanto

System Center 2012 on Microsoftin rakentama hallintajärjestelmä, jonka tarkoituksena on helpottaa tietotekniikkaympäristön hallittavuutta. System Center on Microsoftin tuotteiden muodostama kokonaisuus, josta puhutaan perheenä. Perheeseen kuuluvat Configuration Manager, Endpoint Protection, Virtual Machine Manager, Orchestrator, Operation manager, Service manager, App Controller ja Data Protection Manager.

Tässä opinnäytetyössä perehdytään Configuration Manageriin eli asetusten hallintaan. Configuration Manager ohjelman tarkoituksena on ylläpitää yrityksen sisäistä määräystenmukaisuutta ja hallintaa. Yrityksen työntekijöille voidaan mahdollistaa pääsy vain tarvittaviin ohjelmistoihin ja laitteistoihin, joka parantaa yritysturvallisuutta.

Configuration Manager lisää tehokkuutta käyttöjärjestelmien levittämisessä, samalla vähentäen kustannuksia ohjelmistojen jakamisessa, laitehallinnassa, turvallisuudessa ja työpöydän virtualisoinnissa. [1, s. 1-4.]

Työssä tutustutaan Configuration Manageriin ja sen suomiin mahdollisuuksiin pien- tai suuryrityksessä. Opinnäytetyön käytännön osuudessa tehdään pieni ympäristö, jossa pudotetaan käyttöjärjestelmä käyttäjälle ja luodaan kirjasto halutuista ohjelmistoista. Toteutus kuvastaa pienen yrityksen toteutusta. [1, s. 1; 2, s. 1; 23. 24.]

2 Yleiskatsaus Configuration Manager -ohjelmistoon

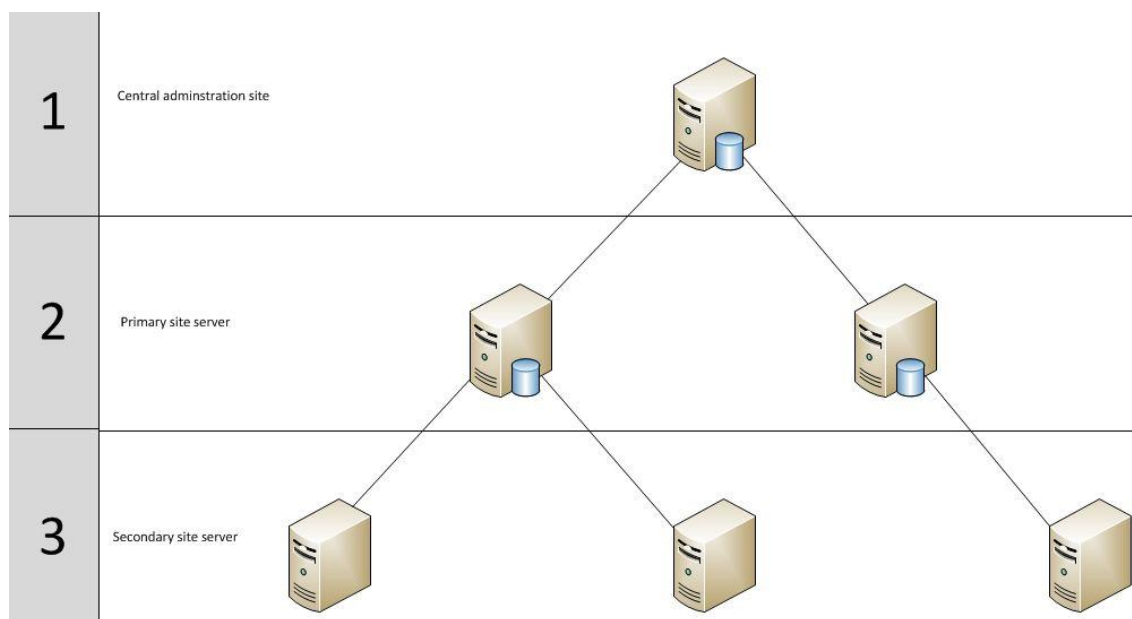
Configuration Manager on ohjelmistoratkaisu, joka antaa yrityksen ympäristön ylläpitäjille toiminnallisuutta konfiguraatioiden, päivitysten, ohjelmistojen ja käyttöjärjestelmien hallinnassa. Configuration Managerin selkeällä graafisella käyttöliittymällä saadaan inventoitua ympäristön eri käyttöjärjestelmät, laitteistot ja ohjelmistot.

Suurten yritysten haasteeksi kasvaa oman henkilökunnan liikkuvuus globaalisesti. Kannettavat tietokoneet, matkapuhelimet ja tabletit saatetaan liittää useisiin tuntemattomiin verkkoihin, jotka altistavat ne haittaohjelmille. Hallitsemalla

tietoisuutta oman ympäristön sisällöstä, vähennetään riskejä ja samalla parannetaan tuottavuutta ja tietoturvaa. [1, s. 37; 2; 3; 4.]

2.1 Toimipistehierarkkia (Site Hierarchy)

Jokaisessa verkkoympäristössä on vähintään yksi päätoimipiste (Primary Site). Jos ympäristö sisältää usean päätoimipisteen, on silloin oltava olemassa keskustoimipiste (Central Administration Site, CAS). Keskustoimipisteen ainoa tehtävä on hallinoida kaikkia toimipisteitä ja helpottaa niiden välistä liikennettä. Usean päätoimipisteen yhdistäminen voidaan toteuttaa vain keskustoimipisteen avulla. Päätoimipisteelle sijoitetaan asiakkaat, joita halutaan hallinoida käyttäen Configuration Manageria hyväksi. Yksi päätoimipiste voi ylläpitää 100 000 asiakasta, jonka jälkeen on suositeltavaa luoda toinen päätoimipiste asiakaskannan lisäykselle. Ympäristö saattaa sisältää myös toissijaisia toimipisteitä (Secondary Sites), jotka toimivat päätoimipisteen alaisuudessa jakaen ympäristön kuormituksen hierarkkialle lähetetyistä asiakastiedoista. Tarvittaessa toissijaisille toimipisteille voidaan jakaa vastuuta sisällön jakamisesta muille toimipisteille. Kuvassa 1 näkyy hierarkkian jakautuminen ympäristössä. [1, s. 43; 3; 4.]



Kuva 1. Hierarkkia laskeutuu puumallin mukaisesti kuten kuvassa on esitetty.

2.2 Toimipisteen järjestelmät (Site systems)

Riippuen toimipistetyypistä jokainen palvelin voi ylläpitää useita erilaisia rooleja. Seuraavat roolit (Roles) on vaadittavia toimipisteen toiminnallisuuden ylläpitämiseksi. Jokainen tietokone – palvelin tai työasema, joka isännöi toimipistejärjestelmärooleja, kutsutaan toimipistejärjestelmäpalvelimeksi. Näitä palvelinrooleja ovat muun muassa [1, s. 46; 3; 4.]:

- Component server: Vaaditaan kaikissa palvelimissa, jotka toteuttavat Configuration Managerin toiminnallisuuksia.
- Site database server: Palvelin, jolle on asennettu SQL-tietokanta palvelut ajamaan Configuration Managerin toimipisteen tietokantaa.
- Site server: Configuration Managerin oletusrooli, joka vaaditaan keskus-, pää- ja sivutoimipisteellä.

Lisänä oletusarvoisille rooleille voidaan asentaa omavalintaisia rooleja tukemaan muita valmiuksia. Näitä omavalintaisia rooleja ovat seuraavat [3; 4.]:

- Application catalog web service point: Välittää tietoa ohjelmistokirjastosta ohjelmistoluetteloverkkosivustolle.
- Application catalog website point: Esittää saatavissa olevia ohjelmistoja käyttäjille.
- Asset intelligence synchronization point: Sallii inventoida ja hallita ohjelmistolisenssejä yrityksessä.
- Distribution point: Rooli mahdollistaa asiakkaiden pääsyn asennettaviin sovelluksiin .
- Management point: Hallinointipiste helpottaa kommunikointia asiakkaan ja toimipiste palvelimen välillä. Hallinointipiste varastoi menettelytapa datan asiakkaalle ja vastaanottaa tilannepäivitykset inventaarioineen.

- Mobile device enrollment proxy point: Sallii mobiililaitteiden rekisteröinnin Configuration Manageria käyttäen
- Fallback status point: Rooli määrittelee vaihtoehdoisen paikan, jonne asiakaskoneet voivat ilmoittaa tilatietoja, jos yhteys hallinnointipisteeseen katkeaa.
- Reporting services point: Tämän roolin avulla sopeutetaan raportointipalvelut SQL-tietokannan oman raportointipalvelujen kanssa.
- Software update point: Ohjelmistopäivityspiste tarjoaa ohjelmistojen päivitysten hallintaa Configuration Manager asiakkaille WSUS:en kanssa.

2.3 Löytötyypit (Discovery types)

Configuration Manager mahdollistaa useita menetelmiä etsiä verkossa ja ympäristössä sijaitsevia resursseja ja niiden tietoja. Menetelmät voidaan rekursiivisesti kohdistaa tiettyihin LDAP-polkuihin, jolloin tarkoituksena on löytää halutut resurssit. Menetelmät ovat seuraavat [1, s. 49; 1 s. 419; 10; 11.]:

- Active Directory Forrest: Löytää metsät, toimialueet, AD-toimipisteet ja IP-aliverkot. Lisänä menetelmä automaattisesti luo AD- ja IP- aliverkkorajat löydettyä.
- Active Directory Group Discovery: Löytää AD:n ryhmät ja niihin kuuluvat jäsenyydet.
- Active Directory User Discovery: Löytää käyttäjätiedot AD:sta.
- Network Discovery: Löytää kaikki laitteet, joita toimialueessa on kuten tietokoneet, tulostimet ja verkkolaitteet. Löytömenetelmää ei suositella käytettäväksi sen aiheuttaman suuren liikennemäärän ja resurssikuormituksen takia.
- Heartbeat: Tämä löytömenetelmä on ainoa, joka on oletuksena asetettu käytössä olevaksi. Asiakaskoneet lähettävät tasaisen aikavälein tietoa olemassa

olostaan Configuration Managerille. Näin Configuration Manager tietää, mitä käyttäjiä tai koneita ei tule poistaa tietokannasta.

- Delta Discovery: Tunnistaa löytömenetelmän jälkeen tehdyt muutokset AD:ssa käyttäen vähemmän resursseja kuin täysi järjestelmän löytömenetelmä. Delta Discovery löytää uusia resursseja, mutta ei havaitse poistettuja resursseja.

2.4 Asiakasohjelma (Clients)

Asiakasohjelmat toimivat hallituissa järjestelmissä kuten käyttöjärjestelmissä ja palvelimissa. Client tarkistaa ja ylläpitää ympäristönsä ajantasaisuutta sille määritellyn intervallin mukaisesti Configuration Manager -palvelimelta. Tarkistuksia ovat muun muassa tietokoneen sisältö, turvallisuuspäivitykset, virtatilan hallinta, sovellustenhallintaa, sovellusten asennus ja poisto, uudelleen asennusta ja tietokoneen asetusten hallintaa. [1, s. 419-488; 12; 13.]

2.5 Kokoelmat (Collections)

Kokoelmat edustavat loogisia ryhmyksiä resursseista, käyttäjistä ja laitteistoista. Kokoelmilla voidaan asentaa ohjelmistopäivityksiä, hallita sovelluksia, virranhallintaa ja asiakasryhmien asetuksia. Kokoelmat jaetaan kahteen eri luokkaan, laitteistoihin ja käyttäjiin. Laitteistot koostuvat tietokoneista ja mobiililaitteista. Käyttäjät koostuvat käyttäjänimistä ja AD-käyttäjärhymistä.

Kokoelmat ovat Configuration Managerin yksi tärkeimmistä ominaisuuksista, mutta samalla väärin käytettynä vaarallisin. Muokatessa olemassa olevan kokoelman sääntöjä on mahdollista kasvattaa laitteistojen ja käyttäjien määrää kokoelmassa huomattavasti. Jos kokoelman tehtävänä on asentaa pakolla ohjelmistoja tai käyttöjärjestelmiä, voivat seuraukset olla hyvin haitallisia.

Kokoelmat sisältävät yhden tai useamman säännön, jotka määrittelevät kokoelman jäsenyyden Configuration Managerissa. Sääntöjä on yhteensä neljä. Nämä neljä sääntöä ovat nimeltään Direct Rule, Query Rule, Include Rule ja Exclude Rule.

Direct Rule -jäsenyys sallii valita käyttäjät tai tietokoneet, joita halutaan valita kokoelmaan. Tämä mahdollistaa hallinnoinnin kokoelmiin kuuluvista resursseista. Tämä jäsenyys ei muutu ilman, että resurssi poistetaan Configuration Managerista. Resurssin on oltava löydetty Configuration Managerissa ennen kuin niitä voidaan lisätä kokoelmiin.

Query Rule päivittävät dynaamisesti jäsenyyttä kokoelmassa perustuen sille asetetun aikataulun mukaisesti. Suoraan sääntöön verrattuna tiedustelu päivittää kantaansa, jos uusia laitteita lisätään kokoelmaan.

Include Rule sallii lisätä muita käyttäjiä kokoelmista toisiin kokoelmiin Configuration Managerissa. Jäsenyys periytyy kokoelmaan aikataulun mukaan muutosten tapahduttua uudessa kokoelmassa.

Exclude Rule jättää ulkopuolelle kokoelmien käyttäjät Configuration Managerista. Syy poissulkemiselle voi olla päivitysten asennuksen laiminlyöminen tai clientin rikkoutuminen työasemassa, joka saattaa olla turvallisuusriski. Poissulkeva sääntö on aina etusijalla sääntöhierarkiassa ja estää sen perusteella kokoelmat muista säännöistä täysin. [1, s. 628-635; 14.]

2.6 Ohjelmistopäivityspalvelut (Software update services)

Ohjelmistojen ja käyttöjärjestelmien päivityksissä on otettava huomioon monia asioita, jotka ovat riippuvaisia ympäristöstä ja käyttäjä vaatimuksista. Onnistunut päivitys tarvitsee suunnittelua ja valmistelua.

On selvitettävä, mitä halutaan päivittää ja mitä ei. Joissakin ympäristöissä saattaa olla sovelluksia, jotka eivät tue uusimpia järjestelmäpäivityksiä. Tästä johtuen ympäristön päivittäminen on aina suositeltavaa suorittaa testiympäristössä, jotta vältetään turhilta ongelmilta. Jos testiympäristön toteuttaminen ei ole mahdollista, tulee ottaa selvää päivitysten vaikutuksista muihin sovelluksiin.

Usein käyttöjärjestelmäpäivitykset vaativat uudelleenkäynnistyksen. Tämän takia päivitykset tulisi suorittaa vaiheittain, jolloin se ei vaikuta yrityksen työn jatkuvuuteen.

Vaikka päivitykset toteutettaisiin kiireettömämpään aikaan, tulisi niistä ilmoittaa aina ympäristön ylläpito henkilökunnalle. [1, s. 670-672; 7; 8; 9.]

2.6.1 Windows-päivityspalvelut (Windows software update services)

Windows software update services eli WSUS on Microsoftin oma palvelimille tarkoitettu ohjelma, jonka tarkoitus on jakaa päivityksiä järjestelmille. WSUS käyttää hyväkseen agenttia skannatakseen sovellettavuutta ja myöhemmin päivitysten asennusta, joita WSUS toimittaa. WSUS-ohjelman yhtenä ongelmana on ohjelman rajoittuvuus suurissa ympäristöissä. Tämän ongelman korjaa Configuration Managerin laaja ympäristön hallinta. [1, s. 673. 2; s. 167-180; 7; 8; 9.]

2.6.2 Päivitysten synkronointi (Software Synchronization)

Ohjelmistopäivitysten synkronisointi Configuration Managerissa on prosessi, jossa haetaan ohjelmistopäivityksen metatietoa Microsoft-päivityksistä halutun kriteerin mukaan. Päivitysten synkronisointi oman ympäristön ulkopuolelta suoritetaan vai sille määrätyn ohjelmistopäivityspisteen kautta. Synkronisoinnissa palvelimet hakevat Microsoftilta uusimmat päivitykset ja delegoi ne halutulla tavalla sille asetetun aikataulun mukaisesti.

Metatieto jokaisen päivityksen kohdalla määrittelee, mihin tuotteeseen tai tuotteisiin se on soveltuva. Tuote voi olla esimerkiksi tietty versio käyttöjärjestelmästä tai sovelluksesta. Jokainen päivitys määritellään luokituksella, joka helpottaa erityyppisten päivitysten organisointia. Configuration Manager sallii synkronoitaviksi seuraavat päivitysluokat. [1, s. 674-685; 7; 8; 9.]

- Kriittiset päivitykset: Yleinen kriittinen päivitys, joka ei ole turvallisuuteen liittyvä.
- Määritelmäpäivitys: Tarkentaa päivityksiä viruksista tai määritelmistä.
- Ominaisuuspäivitys: Määrittelee uusia tuote ominaisuuksia.
- Turvallisuuspäivitys: Tuotekohtaiset turvallisuuspäivitykset.

- Palvelupäivitys: Kumulatiivisia korjaustiedostoja sovelluksille. Nämä päivitykset sisältävät turvallisuuspäivitykset, kriittisetpäivitykset ja ohjelmistopäivitykset.
- Työkalut: Määrittää apuohjelman tai ominaisuuden, joka helpottaa täydentämään muita tehtäviä.
- Päivitykset: Määrittelee päivityksen tietylle sovellukselle tai tiedostolle, joka on asennettu.

2.6.3 Ohjelmistopäivitysten graafinen hallintakonsoli

Graafisen konsolin tarkoitus on yksinkertaistaa ja vähentää ylläpitäjän työmäärää. Jokainen ympäristön päivitys on listattuna näkyville konsolissa tarkasti määriteltynä. Päivitykset on listattu yksilöllisin identifiointi tunnuksin jotka helpottavat ohjelman seuranta päivitysprosessissa. Jokainen prosessi on värikoodattu tilan mukaisesti

- Vihreä: Normaali
- Harmaa: Vanhentunut
- Punainen: Pätemätön
- Keltainen: Korvattu
- Sininen: Metatieto pelkästään filter.

Päivityksiä voidaan tutkia itsessään myös tarkemmin niiden omien asetusten kautta. Täältä löydetään tietoa muun muassa tarkistuspäivistä, ylhäälläoloajoista, ympäristössä vallitsevan tärkeysjärjestysasteen, ohitetut päivitykset ja turvallisuuden. Päivitystietoja voidaan muuttaa samanaikaisesti useampaa kerrallaan. Konsolissa on mukana myös suodatin-tekniikoita, jotka rajoittavat päivityksiä sen mukaan, mitä käyttäjä haluaa nähdä. [1, s. 692-696; 7; 8; 9.]

2.7 Mobiililaitteiden hallinta (Mobile device management)

Mobiililaitteiden määrän kasvu yritysmaailmassa tuo mukanaan uusia riskejä ja hyötyjä. Salliessamme liikkuvien laitteiden pääsyn yrityksen toimialueelle kasvattaa se tehokkuutta ja säästää aikaa päivittäisessä työssä. Nämä vapaudet kuitenkin tuottavat haasteen riskien ja tietoturvan hallinnassa. Arkaluonteinen yritystieto saattaa olla saatavilla matkapuhelimissa, jotka voivat olla henkilöiden yksityisiä puhelimia. Jos yritykset eivät hanki omaa puhelinta työntekijöilleen, on käytettävä tekniikoita, joilla saadaan yrityksen ja käyttäjän henkilökohtainen tieto eristettyä toisistaan.

Matkapuhelinten laaja käytettävyys ja liikkuvuus luovat haasteen. Käyttäjät kantavat matkapuhelimiaan aina mukanaan kaikkialle. Sen todennäköisyys hävitä tai tulla varastetuksi on huomattavasti suurempi kuin kannettavien tietokoneiden. Tämän takia yrityspuhelimille tulisi toteuttaa seuraavia vaihtoehtoja.

- "Sandbox": Yritystieto on eristetty muusta ympäristöstä kansiolla, joka on kryptattu ja suojattu salasanalla tai muilla autentikointimenetelmällä. Tällä tavalla jos laite häivää, voidaan tarvittaessa yritystieto pyyhkiä etäisesti.
- Matkapuhelimeen laitetaan vahva salasana, joka estää ulkopuolisen pääsyn laitteelle. Pyyhintäpalvelu tuhoaa tiedot, jos salasana on annettu väärin tarpeeksi useasti.
- Sovellusten lataamisen salliminen kaupoista on suuri riski. On suotavaa estää pääsy sovelluskaappoihin kokonaan.

System Centerissä käytetään hyväksi Mobile Device Manageria, jolla voidaan hallinnoida laitteistoja ja ohjelmistoja matkapuhelimissa. [1, s. 751-784; 15; 16.]

2.8 Raportointi (Reporting)

Raportit mahdollistavat tiedon analysoinnin Configuration Managerista. Perinteisten hakumetodien lisäksi Configuration Managerissa on mahdollista toteuttaa omia mukautettuja hakuja, joiden perusteella voidaan toteuttaa haluttuja raportteja. Configuration Manager antaa työvälineet, joilla voidaan käyttää kehittyneitä raportointiominaisuuksia SQL Server Reporting Servicessä, eli SSRS:ssä.

SSRS tarjoaa suuren määrän työkaluja ja palveluja, joilla voidaan luoda, asentaa ja hallita raportteja. Palvelu on palvelin pohjainen raportointialusta, joka mahdollistaa kattavat toiminnallisuusmahdollisuudet erilaisille tietolähteille. Raportointi helpottaa ylläpitäjiä keräämään, järjestelemään ja esittämään tietoa. Raportoinnissa on tietoja käyttäjistä, laitteistosta, ohjelmistoluetteloista, ohjelmistopäivityksistä, sovelluksista, toimipisteiden tilasta ja muista Configuration Manager operaatioista yrityksessä. [1, s. 871-884; 17; 18.]

2.9 Käyttöjärjestelmän levittäminen (Operating system deployment)

Uusien käyttöjärjestelmien asentaminen yrityksissä voi tulla kalliiksi, jos sitä ei suunnitella hyvin. Suunnittelemalla käyttöjärjestelmien asentamiset voidaan mahdollistaa tehokas työajan käyttö ja ehkäistä muun muassa mahdolliset tietohäviöt. Configuration Manager käyttää Operating system deploymentia eli OSD:tä hyväkseen käyttöjärjestelmien yksittäis- ja massalevityksessä. OSD on automatisoitu järjestelmä, levykuvan luontivaiheesta asennusvaiheeseen asti. Ennen käyttöjärjestelmän asennusta voidaan järjestelmä mukauttaa haluttuun tilaan osioimalla, formatoimalla tai biossia päivittämällä. Asennuksen jälkeen voidaan suorittaa ohjelmistopäivityksiä tai sovellusten asentamista.

Aikataulutetusti automatisoidut asennukset voidaan rajoittaa haluttujen kriteerien mukaisesti kuten laitteiston, sijainnin, kohdekäyttäjän tai järjestelmäroolien mukaan. OSD on integroitu Configuration Manageriin, jonka takia se voi käyttää hyväkseen ohjelmistoasennusta, päivittämistä ja raportointia yhdestä hallintakonsolista. [1, s. 959-962; 2, s. 247-258; 19; 20.]

Configuration Managerilla voidaan suorittaa seuraavat asennusskenaariot. [1, s. 963-964. 20.]

- Uusi tietokone: Tässä skenaariossa luodaan uusi käyttöjärjestelmä ja oletetaan, että kohdekoneella sijaitseva tieto on yhdentekevää ja asennuksen yhteydessä alustetaan levy, jonne käyttöjärjestelmä tullaan asentamaan.
- Virkistys: tässä skenaariossa asennetaan uusi käyttöjärjestelmä vanhan päälle säilyttäen käyttökelpoiset käyttäjätiedot sekä asennetaan valtuutetut

sovellukset, jotka virkistävät käyttöjärjestelmää. Toimenpiteeseen johtavat yleisimmät syyt ovat uudempaan käyttöjärjestelmään päivitys, käyttöjärjestelmän rikkonaisuus tai jos käyttöjärjestelmä ei vastaa nykyisiä standardeja.

- Korvaava: tämä skenaario on samankaltainen kuin virkistys, mutta siihen liittyy fyysisen järjestelmän vaihtaminen tai korvaaminen uudella. Koska käyttäjä tiedot sijaitsevat vanhassa järjestelmässä, täytyy ne siirtää uuteen, jonka OSD tekee.
- OEM, original equipment manufacturer: tässä skenaariossa luodaan uusi käyttöjärjestelmä alusta alkaen, kuten uusi tietokone skenaariossa. Levykuva kuitenkin saadaan toimialueen ulkopuolelta toiselta osapuolelta, joka on laitevalmistaja tai kauppias. Uudelleenkäynnistyksen yhteydessä OSD ottaa asennetun käyttöjärjestelmän haltuun.

Vaikka OSD on täysin integroitu Configuratoin Manageriin, käyttää se hyväkseen useita erillisiä työkaluja. OSD käyttää näitä erillisiä työkaluja perustaessaan uutta käyttöönnottoa ja vianmäärityksessä. Esiteltävät työkalut ovat Sysprep, WAIK, WDS ja PXE.

Sysprep on yksi yleinen työkalu, jota käytetään automoidun asennuksen valmisteluun. Levykuvia tehdessä sysprep poistaa useita yksilöllisyystunnisteita. Uudelleenkäynnistyksen yhteydessä ajetaan kevyt asennusvaihe, jossa luodaan uusi ja yksilöllinen tunnistus järjestelmälle. Tämä mahdollistaa uuden tuoteavaimen syötön, laitteiston havaitsemisen ja ajurien asennusprosessin. OSD automatisoi täysin kevytasennuksen käyttäen hyväksi rakennetiedostoa, jonka nimi vaihtelee käyttöjärjestelmän standardien mukaisesti. Tiedosto sisältää tuoteavaimen, yrityksen nimen, verkkotietoa ja toimialuevaltuuksia. [1, s. 965. 25.]

Windows Automated Installation Toolkit, eli WAIK on kokoelma työkaluja ja dokumentaatioita, jotka on suunniteltu Windows-käyttöjärjestelmän asentamiseen. WAIK on tarkoitettu erittäin kustomoiduille ympäristöille. WAIK tarjoaa erittäin joustavia mahdollisuuksia ympäristövaihtelevuuksien kannalta. Yritysten välillä on kuitenkin otettava huomioon liiketoiminnan tarpeet ja resurssit. [1, s. 966-967; 26.]

Windows Deployment Services, eli WDS mahdollistaa etäkäyttöjärjestelmän asennuksen. WDS:n tarkoituksena on toimia esiasennuspalvelimena Windows-levykuvien jakamisessa sekä asentamisessa. [20.]

Preboot execution environment, eli PXE mahdollistaa tietokoneen käynnistämisen verkosta haluttua käynnistyslevykuvaa käyttäen. Tätä ominaisuutta voidaan hyödyntää käyttöjärjestelmän levykuvan levittämisessä verkon yli tyhjälle laitteelle. [20.]

2.10 Turvallisuus ja valtuutukset

Tiedosta on tullut yksi tärkeimmistä omaisuuksista yrityksissä nykypäivänä. Avain seikkoja tehokkaan järjestelmän hallinnoimiseen ovat tiedon eheyden varmistaminen, luottamuksellisuus ja saatavuus. Oikean turvallisuusrakenteen ja ylläpidollisten valtuutusten jakaminen vaatii tarkan ymmärryksen teknisistä asioista. On otettava huomioon yrityksen säännöstyksset, menettelytavat ja tekniset mahdollisuudet.

Tietoturvallisuuden tavoite on turvata tiedon luottamuksellisuus, eheys, seuranta ja palveluiden saatavuus. Yrityksen on kyettävä säilyttämään itsellään kolmannen osapuolen tietoa turvallisesti, jotta pystytään välttymään tabudellisista menetyksistä asiakasmenetyksen suhteen. Tehokkaan turvallisuusjärjestelmän on pystyttävä suojaamaan tietoa ja järjestelmää ulkopuoliselta muokkaukselta. On tärkeää pitää kirjaa toimialueessa tai järjestelmässä tapahtuvista käyttäjä toiminnoista. Tietoturvan rikkoutuessa on olemassa tarkat lokit tapahtuneesta ja paikasta.

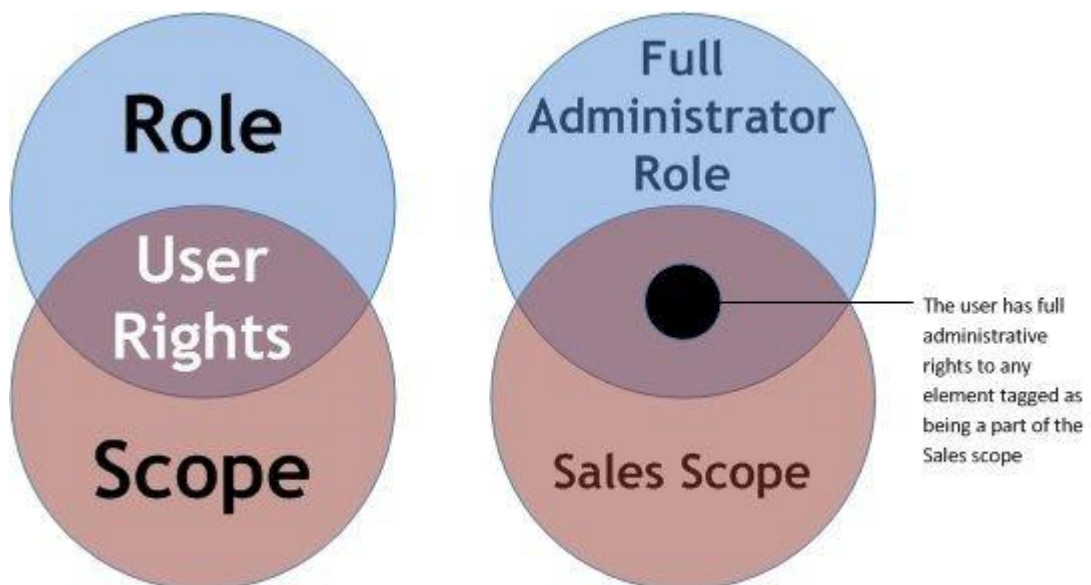
Turvallisuusratkaisut

Configuration Manager ohjelmistona voi olla merkittävä ympäristön turvallisuuden kannalta. Configuration Managerilla voidaan määrätä käyttöjärjestelmiä päivityksiin tai kieltää niiden asentaminen, joka on yleinen riski tietoturvallisuudessa. Configuration Manager voi tuoda keskitettyä hallintaa Windows-palomuurimenettelyissä ja käyttöjärjestelmäturvauksessa haittaohjelmia vastaan. [1, s. 1065-1116.]

Hyvin hallinnoitussa ympäristössä ei ole myöskään liikaa oikeutettuja käyttäjiä. Näitä voidaan karsia automatisoidulla päivitysten, ohjelmistojen ja käyttöjärjestelmien asennuksella.

Roolipohjainen ylläpito

Roolipohjainen ylläpito on yksi tärkeimmistä ominaisuuksista koko Configuration Managerissa. Sillä voidaan hallinoida ylläpidollisia oikeuksia tehokkaasti käyttäjille, rajaamalla tarpeet työnkuvan mukaisiksi kuten kuvassa 2 näkee. Täysoikeutettu ylläpitäjä voi ajaa ja levittää mitä tahansa koodia Configuration Manager -ympäristössä, kerätä käyttäjien tiedostoja mistä vaan ja ottaa käyttöjärjestelmät hallintaansa. Näillä oikeuksilla ylläpitäjä voi käytännössä tehdä mitä vaan ympäristössä. Tämän takia rooleja määritellään ylläpito käyttäjille tehtävien tarpeiden mukaisesti antaen vähimmäismäärän oikeuksia, jotta voidaan toteuttaa vastuutehtävät ja hallita väärinkäytöstä. [1, s. 1068. 27.]



Kuva 2. Roolien rajaaminen

Turvallisuusroolit: sisältävät joukon oikeuksia, jotka sallivat käyttäjän suorittaa tiettyjä tehtäviä. Configuration Managerin mukana tulee valmiiksi tehtyjä oletus rooleja, jotka edustavat tyypillisiä työvastualueita tietotekniikkaylläpitäjille, joilla on tarve päästä Configuration Manageriin käsiksi. Tarvittaessa ylläpitäjät voivat luoda myös uusia rooleja organisaation omien tarpeittensa mukaan. [1, s. 1070; 27.]

Turvallisuuslaajuus (Security Scope)

Security scopet määrittelevät rajat, joita kukin käyttäjä voi suorittaa rooliin määrittelyistä toiminnallisuuksista. Oikeuksia voidaan rajoittaa tarkentamalla jokaista turvallisuus objektia, jotka kohdistuvat käyttäjän rooleihin. [1, s. 1074; 27.]

Infrastruktuurin turvaaminen

Tehokas hallinto ja seuranta voi suuresti parantaa toimialueen turvallisuutta. Hallinointityökalujen eheyden vaarantaminen on huomioitava riski. Advanced persistent threat, eli APT:n kaltaisten ryhmien tarkoituksena on verkon kautta varastaa arvokasta yritystietoa ja yrityssalaisuuksia sotilaallisen tai ekonominen etuisuuden edistämiseksi. Nämä ryhmät yrittävät usein vaikuttaa domain controllereihin päästäkseen käsiksi koko järjestelmään. Ennen kuin aloitetaan infrastruktuurikomponenttien yksittäistä suunnittelua, tulisi ottaa huomioon kokonaisuuden turvallisuus ja koskemattomuus ulkopuolisilta.

Huomioitavia asioita ovat fyysinen turvallisuus ja laitteistojen valinta. Valitaan mahdollisimman turvallinen sijainti ja saatavilla olevat laitteistot toimipistejärjestelmille. Toimipistepalvelimet ja -tietokannat tulisi sijoittaa turvallisissa tietokeskuksissa. Käyttöjärjestelmät on pidettävä johdonmukaisesti ajan tasalla muiden järjestelmävaatimusten kanssa. Kehittyvä turvallisuus ja teknologiatietoisuus näkyvät nykyajan modernien käyttöjärjestelmäsuunnittelussa.

Tavallinen periaate järjestelmän turvaamisessa on vähentää mahdollisia heikkouksia poistamalla tarpeettomat palvelut, tilit, sovellukset, verkkojaot ja avonaiset verkkoportit. Toimialueita laatiessa on otettava huomioon niiden määrä. Mitä vähemmän toimialueita on, sitä helpompaa on hallinoida toimialueturvallisuutta. Ylimääräisten toimialueiden turvaaminen kasvattavat palvelinten, tietokantojen ja sisäisten kommunikaatiolinkkien määrää.

Verkkohyökkäyksiä voidaan vähentää huomattavasti rajoittamalla käyttäjien pääsy vain tarvittaville palvelimille. Toimialuepalvelimet ja Tietokantapalvelimet ovat tärkeimmät alueet ympäristössä. Jos käyttäjät voivat luoda verkkoyhteyksiä näille palvelimille, on se huomioitava suurena riskinä. Palvelinroolien erittely toisistaan vähentää tarvetta palveluille ja porteille järjestelmässä vähentäen hyökkäysaluetta. Palvelimet, jotka tarvitsevat IIS -palveluita, tulisi eristää niistä, jotka sitä eivät tarvitse, koska ne

kasvattavat suuresti hyökkäysalaa. FSP:in, eli Fallback Status Pointin on määriteltävä ottamaan vastaan autentikoimatonta käyttäjätietoa, jonka takia se on eristettävä muista toimialueista. On pyrittävä välttämään rooleja, jotka isännöivät toisia sovelluksia toimialue järjestelminä, erityisesti ohjelmistoja, jotka pohjautuvat IIS tai tietokantapalvelimille.

Palvelinten sijoittelussa tulisi ottaa huomioon kaikkien toimialuejärjestelmien sijoittaminen paikkaan, joka on mahdollisimman turvallinen fyysisesti ja verkko pääsyjen suhteen. Fyysisesti hyökkääjä voi asentaa ylläpitotyöasemaan laitteistoja, jotka voivat kompromisoida koko järjestelmän. Verkkoliikenne tulisi rajoittaa vain Configuration Managerin toimenpiteille ja palvelinten perustoiminnoille.

Ohjelmistoturvallisuuden kannalta antivirusohjelmat ovat perinteinen tapa suojautua ohjelmistokohtaisia hyökkäyksiä vastaan. Tällaisten ohjelmien perustoimintaperiaate on verrata prosesseja ja tiedostoja omaan tietokantaansa tunnetuista haittaohjelmista tai reagoida outoon käyttäytymiseen koneessa. Tällä tavalla voidaan turvautua tehokkaasti laajalti levitettyyn haittaohjelmaan. Tehokas menetelmä suojata korkea-arvoiset resurssit on sallia vain tarvittavien ohjelmien toiminta ja kieltää muut oletusarvona.

Toimialue palvelimella on erilaisia käyttöoikeus ryhmiä luotu oletusarvoisesti ja ylläpitäjien tulisi suunnitella ne uudestaan oman ympäristönsä tarpeiden mukaisiksi. On otettava huomioon, kenellä on tarpeet mihinkin toimipaikkaan. Configuration Manager käyttää digitaalista sertifikaattitunnistautumista verkkoliikenteessä ja arkaluontoisten tiedostojen siirrossa. [1, s. 1089-1116.]

2.11 Varmuuskopiointi, palautus ja niiden ylläpito

Terveellisen järjestelmän takana on hyvin suunniteltu varmuuskopiointi ja palautusprosessi. Kaikilla tuotantojärjestelmillä tulisi olla laadittu palautus ja varmuuskopiointimenettelyt, jotta voidaan ylläpitää tiedon eheyttä. Jokaisen toimipaikan tulisi asettaa palvelimet ajamaan automatisoitua varmuuskopiointi menetelmää koko toimialueelle mukaanlukien tietokantaa, tiedostoja, rekisteriavaimia ja järjestelmän rakenneinformaatiota. On tietosuojaeheyden kannalta suositeltavaa käyttää omaa varmuuskopiointipalvelinta ulkoistetun kolmannen osapuolen sijaan. Varmuuskopiointi suoritetaan oletuksena paikalliselle levyille juurihakemistoon. On

suositeltavaa käyttää erillistä RAID -levyjärjestelmää, jonne aikataulutetusti ajetaan varmuuskopiot toimipaikoista ja käyttöjärjestelmä levykuvista. [1, s. 1125; 21; 22.]

3 Suunnitelma

Kaikkien järjestelmien toteuttamisessa tärkein vaihe on itse suunnittelu. Suunnitteluvaiheessa käydään läpi, millainen ympäristö on olemassa, mitkä ovat yrityksen tarpeet ja missä tilassa ympäristön tulisi olla toteutuksen jälkeen. Jotta voidaan saada Configuration Managerista kaikki hyöty irti, on tiedossa oltava yrityksen tavoitteet, nykyinen ympäristö ja tietotekniikkaan liittyvät hidasteet. Opinnäytetyön käytännön osuus toteutetaan Metropolia Ammattikorkeakoulun laboratorioympäristössä. Käytän viittä virtuaalikonetta, joista kaksi toimii palvelimena. Palvelimiksi asennettiin Server 2008 R2. Yhteen koneista asennan Windows 7 Enterprise-käyttöjärjestelmän, joka toimii ympäristön toiminnallisuuksien testaajana. Kaksi virtuaalikonetta jätetään tyhjiksi ja niihin asennetaan käyttöjärjestelmät verkon yli Configuration Managerilla.

3.1 Alkuasetelma

Opinnäytetyö aloitetaan tyhjältä pöydältä, eli minkäänlaista valmista pohjaa ympäristöstä tai ohjelmistoista ei ole. VMWarella luodaan virtuaalikytkin Test_SCCM2012 toimialuetta varten, jonka tarkoituksena on hallinnoida ympäristön sisäistä liikennettä ja ohjata ulkoverkkoon tarkoitettu liikenne NAT-palvelimelle. Jokaiselle laitteelle ympäristössä luodaan oma virtuaalinen verkkokortti. NAT-palvelimen tehtävä on ohjata liikennettä toimialueelta ulkoverkkoon hyväksikäyttäen toimialueen virtuaalikytkimessä olevaa verkkokorttia ja ulkoverkon kytkimeen kiinnitettyä verkkokorttia.

Palvelimien määrä pidetään mahdollisimman pienenä, jotta ympäristö pysyisi yksinkertaisena. Palvelimia luodaan kaksi, jotka nimetään niiden tarkoitusten mukaisesti DC:ksi ja SCCM:ksi. Koska suurin osa palveluista asennetaan SCCM-palvelimelle, annetaan sille huomattavasti enemmän konetehoja.

Luodaan yksi virtuaalikone, jossa on valmiiksi asennettu Windows 7-käyttöjärjestelmä ja kaksi tyhjää konetta. Tyhjiin koneisiin käyttöjärjestelmät asennetaan Configuration

Manageria hyväksikäyttäen työn edettyä siihen pisteeseen. Valmiin käyttöjärjestelmän tarkoitus työssä on ympäristön toimintojen testaus. Koneen tarkoituksena on testata käyttäjien oikeuksia sisäänkirjautuessa, clientin asennusta ja ohjelmistokirjaston toimivuutta.

Palvelimet ja testikone päivitetään täysin. Configuration Manager -koneelle on erikseen haettava Microsoftin sivuilta server 2008 SP2 -päivitys, joka ei automaattisesti päivity Windowsin päivitysohjelmiston kautta.

3.2 Hahmotelma

Ennen käytännönsuuden aloittamista tutustuin ammattikirjallisuuden kautta toteutusvaiheeseen. Ennen toteutuksen aloittamista hahmotin tietokoneella työjärjestyksen, jonka mukaan lähtisin rakentamaan käytännönsuutta. (Lite1)

DC-palvelimen rakentaminen aloitetaan erottelemalla laitteistot ja käyttäjät tehtävien mukaisesti. Laitteistot eritellään palvelimiin ja työasemiin. Luotavat käyttäjät jaetaan toimialue- ja palvelutilikäyttäjiiin. Toimialuekäyttäjinä pidetään yritykselle keksittyjä työntekijöitä. Heidät voidaan jakaa alikansioihin halutulla tavalla, jos toimipaikkoja olisi useita. Palvelutilikäyttäjien tarkoituksena on ajaa erilaisia palvelutehtäviä ohelmistoille, jotka toimivat toimialueessa. Rooleiksi palvelimelle asennetaan vain ADDS ja DNS.

SCCM-palvelimen rakentaminen aloitetaan luomalla kansio "Sources", johon tallennetaan kaikki lähdemateriaalit. Tähän kansioon tulee päivitykset, ohjelmat ja käynnistyskuvakkeet. Kansiolle annetaan lukuoikeus kaikille käyttäjille, mutta kirjoitusoikeus annetaan vain ylläpitäjille. Configuration Manager -palvelimelle asennetaan rooleiksi Application Server, DHCP, File Services, IIS, WDS ja WSUS. Samalle palvelimelle asennetaan SQL-tietokanta. Pienen ympäristön takia verkon resurssien etsintäprosessi ei tuota kuormitusta verkkoliikenteelle. Verkon uudelleen löytäminen suoritetaan kuitenkin vain automatisoidusti seitsämän päivän välein.

4 Toteutus

Toteutus voidaan aloittaa, kun palvelimet on rakennettu suunnitelman mukaisesti. Toteutus aloitetaan ympäristön rakentamisella. Aloitetaan rakentamalla toimialue,

jonka jälkeen siirrytään Configuration Managerin toteuttamiseen. Lopuksi suoritetaan käyttöjärjestelmien ja ohjelmistojen asennukset työasemille.

4.1 Toimialue

DC-palvelin korotetaan palvelimesta toimialueen hallintakoneeksi Dcpromo-komennolla, joka avaa Active Directory Domain Servicesin ohjatun asennuksen. Asennuksessa luodaan uusi toimialue, jolle annetaan nimeksi opinnäytetyön mukaisesti "inssi" ja verkkotunnisteeksi ".fi" -päätte. Toimialueen asennuksen jälkeen päivitetään AD-tietokannan malli Configuration Managerin mallin mukaiseksi. Toimenpide lisää tarvittavat luokka- ja attribuuttimääritykset ympäristöön. Tämä tapahtuu automaattisesti asennuslevyllä sijaitsevan extadsch.exe -ohjelman avulla. Luodaan toimialuepalvelimelle järjestelmän hallintasäiliö, jota toimipaikkapalvelin ja hallinnointipiste käyttävät tallentaakseen julkaistua tietoa rajoista tai sertifiikaateista.

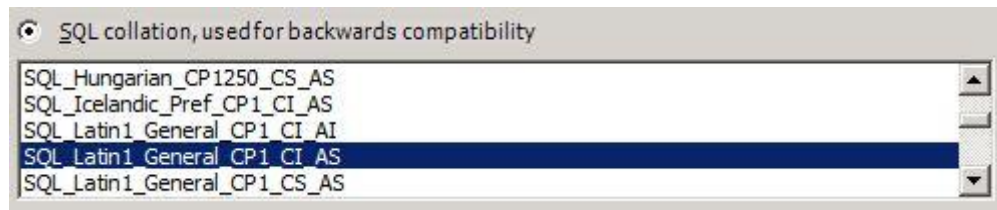
Tehdään toimialueelle hallinnointikäyttäjäkunta ja annetaan heille rajoitetut oikeudet, jotka mukautetaan tehtävien mukaisiksi. Nimeäminen hallinnointitunnuksille luodaan yhtenäiseksi asettamalla toimialuetunnus nimen eteen ja tehtävä lyhennettynä perään. Tämä käytäntö helpottaa tunnuksien erottamisen muista henkilökäyttäjätunnuksista.

- inssi_JD -tunnuksen tehtävä on liittää uudet työasemat toimialueeseen.
- inssi_CP -tunnuksen tehtävä on ajaa clientti työasemaan.
- inssi_SQL -tunnuksen tehtävä on hallinoida tietokantapalveluja.
- inssi_NA -tunnuksen tehtävä on mahdollistaa pääsy SCCM järjestelmän verkko resursseihin.

4.2 Configuration Manager -palvelin

Palvelimelle asennetaan ensimmäisenä tietokantaohjelmisto SQL 2008 R2. Asennuksessa on huomioitava Configuration Managerin erityiset vaatimukset tietokannasta. Poikkeuksellisia vaatimuksia, joiden kanssa tulee olla tarkkana, on kollaatio. Sen on oltava SQL_Latin1_General_CP1_CI_AS kuten kuvassa 3. Palvelimelle

avataan sisäisen liikenteen (TCP) portit 1433 & 433 ja ulkoisen liikenteen (UDP) portti 1434. Ilman näitä Configuration Manager ei pysty kommunikoimaan tietokannan kanssa.



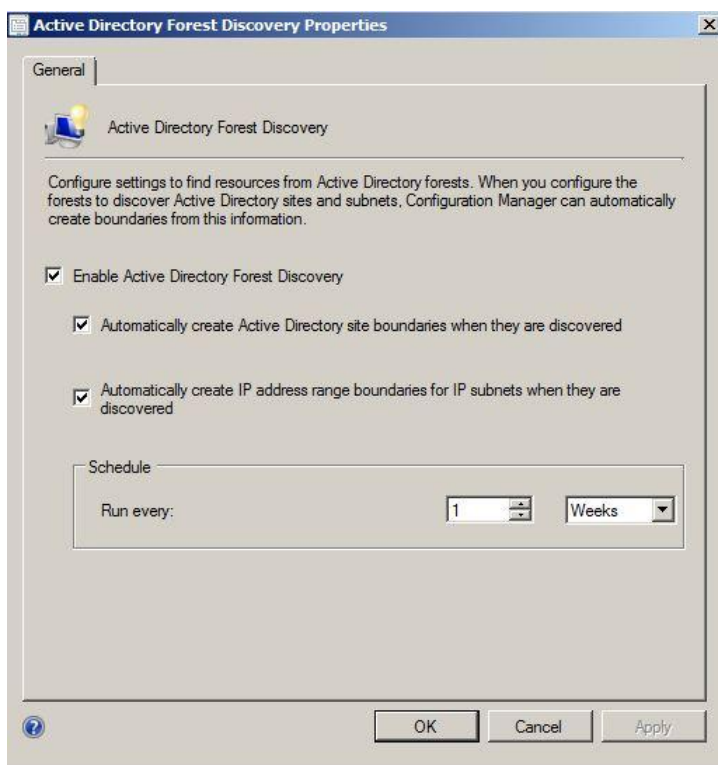
Kuva 3. Oikean kollaation valinta.

Asennetaan palvelimelle Configuration Managerin ensisijainen toimipaikka. Ennen asentamista on ladattava palvelimelle asennusta edellyttävät tiedostot. Asennuslevyltä löytyy ohjelma, joka automaattisesti hakee verkosta tarvittavat tiedostot koneelle. Asennuksessa valitaan kieleksi englanti. Toimipaikkatunnukseksi laitetaan CM1 ja nimeksi SCCMinssi. Asennuksessa annetaan samalla palvelimella olevan tietokannan tiedot. Lopuksi annetaan asennusta valmistelevan tarkistusohjelman ajaa toimintonsa. Kun kaikki tarkistuskohdat ovat vihreänä, voidaan aloittaa asennus. Tarkistuksessa saattaa ilmetä varoituksia asentamattomista ohjelmistoista, mutta ne korjataan jälkikäteen.

Asennusta kannattaa seurata lokitiedostostoista, jotka löytyvät oletusarvoisesti "ProgramFiles/Microsoft Configuration Manager/Logs". Jos asennuksessa ilmenee ongelmia, löydetään niille syyt lokerista.

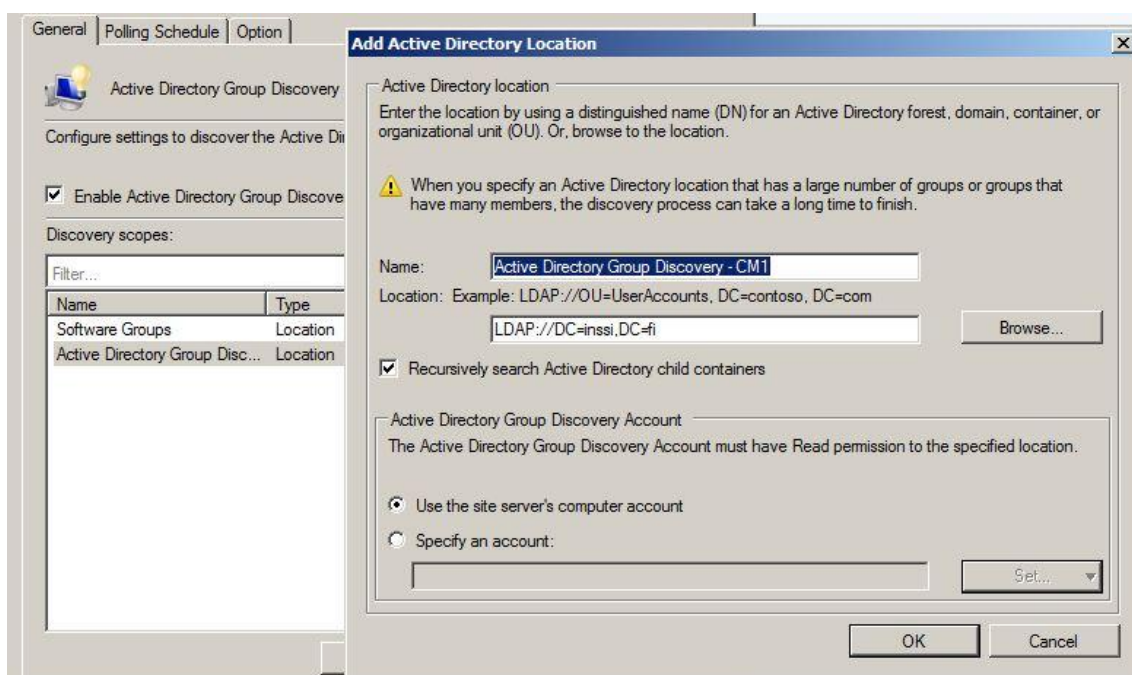
4.3 Resurssien löytäminen ja järjestely Configuration Managerissa

Configuration Manager löytää verkon, sekä koneiden ja käyttäjien hallintaan tarvittavia resursseja. Löydettyä uusia resursseja jaetaan ne muiden toimipisteiden välillä. Koska kaikkia resursseja ei tarvitse löytää, tulee ne rajoittaa oman ympäristön mukaisesti. Haut kannattaa ajoittaa päivittämään kantansa uusien tai vanhentuneiden resurssien varalta kuten kuvassa 4 näkyy.



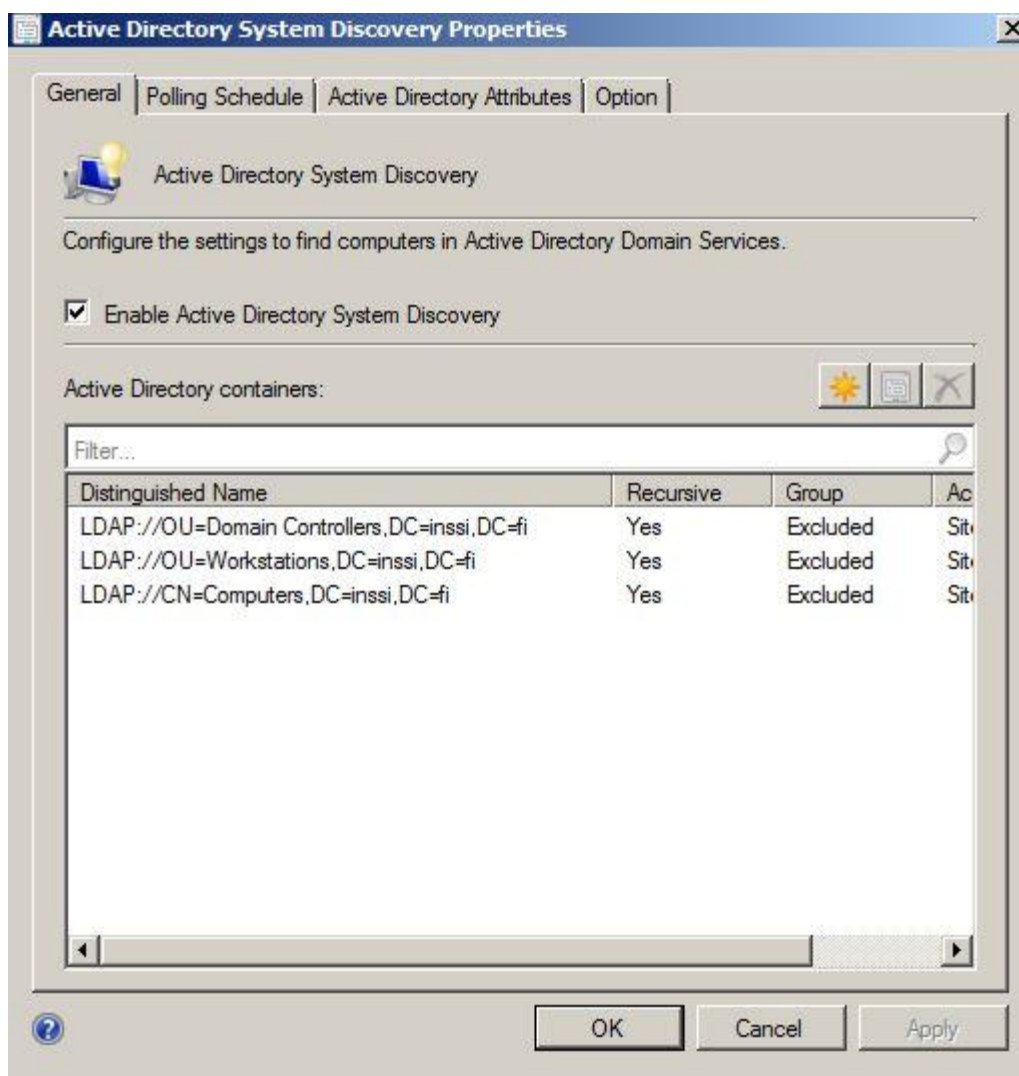
Kuva 4. Verkon löyto.

Active Directory Forest Discovery: Mahdollistetaan verkon löytö ja asetetaan se suoritettavaksi viikon välein.



Kuva 5. Haula tunnistetaan ryhmien jäsenyys työasemille ja käyttäjille.

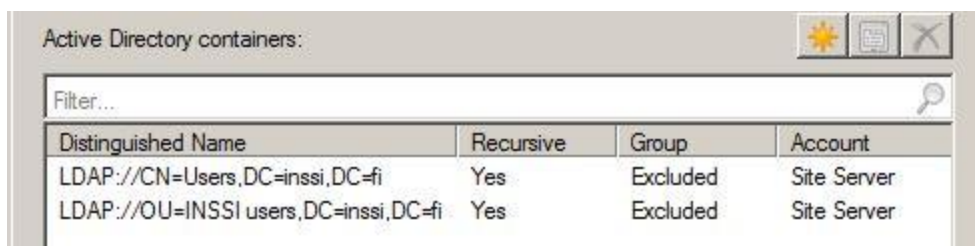
Active Directory Group Discovery: Mahdollistetaan haku, josta tunnistetaan ryhmien jäsenyys työasemille ja käyttäjille. Annetaan haulle nimi ja toimialueen osoite kuten kuvassa 5 on tehty. Ajoitetaan täydellinen verkon uudelleen tarkistus seitsämän päivän välein ja delta discovery viiden minuutin intervallilla. Koneille laitetaan rajoittavaksi tekijäksi kolmenkymmenen päivän yhteysvaatimus toimialueeseen ja yhdeksänkymmenen päivän vaatimus salanan vaihdolle.



Kuva 6. Mahdollistetaan toimialueessa olevien tietokoneressurssien tunnistamisen.

Active Directory System Discovery: Mahdollistetaan haku, joka tunnistaa toimialueessa olevat tietokoneressurssit, jonka avulla voidaan asentaa clientti löydetyille koneelle. Luodaan erilliset haut Domain Controllers, Workstation ja Computers OU:lle Active

Directory:stä, kuten kuvasta 6 on tehty. Ajoitetaan täydellinen verkon uudelleentarkistus seitsemän päivän välein ja delta discovery viiden minuutin intervallilla. Koneille laitetaan rajoittavaksi tekijäksi kolmenkymmenen päivän yhteysvaatimus toimialueeseen ja yhdeksänkymmenen päivän vaatimus salanan vaihdolle.



The screenshot shows a window titled "Active Directory containers:" with a search filter field and a table of results. The table has four columns: Distinguished Name, Recursive, Group, and Account. Two rows are visible, both with "Yes" in the Recursive column and "Excluded" in the Group column.

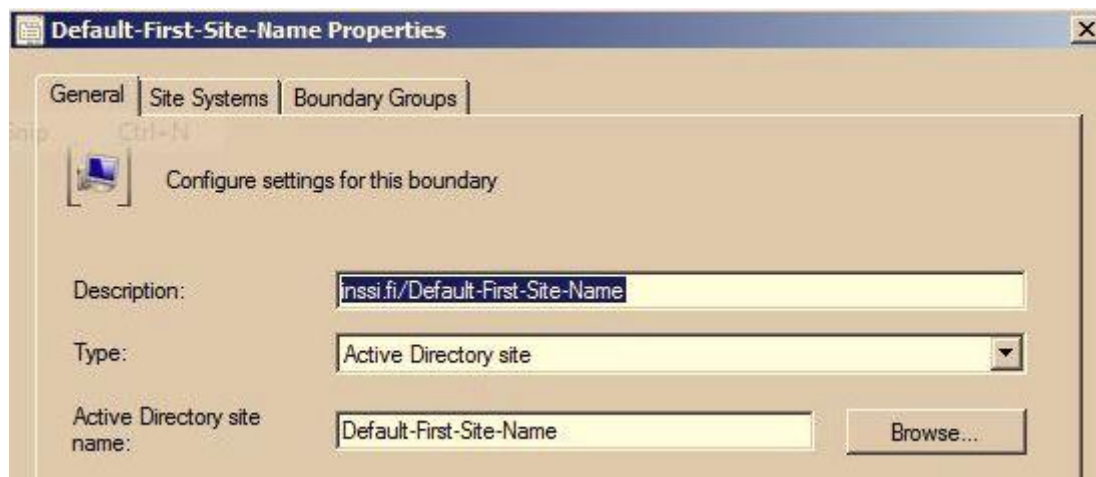
| Distinguished Name | Recursive | Group | Account |
|--------------------------------------|-----------|----------|-------------|
| LDAP://CN=Users,DC=inssi,DC=fi | Yes | Excluded | Site Server |
| LDAP://OU=INSSI users,DC=inssi,DC=fi | Yes | Excluded | Site Server |

kuva 7. Haulla tunnistettavat käyttäjätilit ja niiden määritteitä.

Active Directory User Discovery: Mahdollistetaan haku, joka tunnistaa käyttäjätilit ja niihin liittyvät määritteet. Luodaan erilliset haut Users ja INSSI_users OU -kansioille kuten kuvassa 7. Ajoitetaan täydellinen verkon uudelleen tarkistus seitsemän päivän välein ja delta discovery viiden minuutin intervallilla.

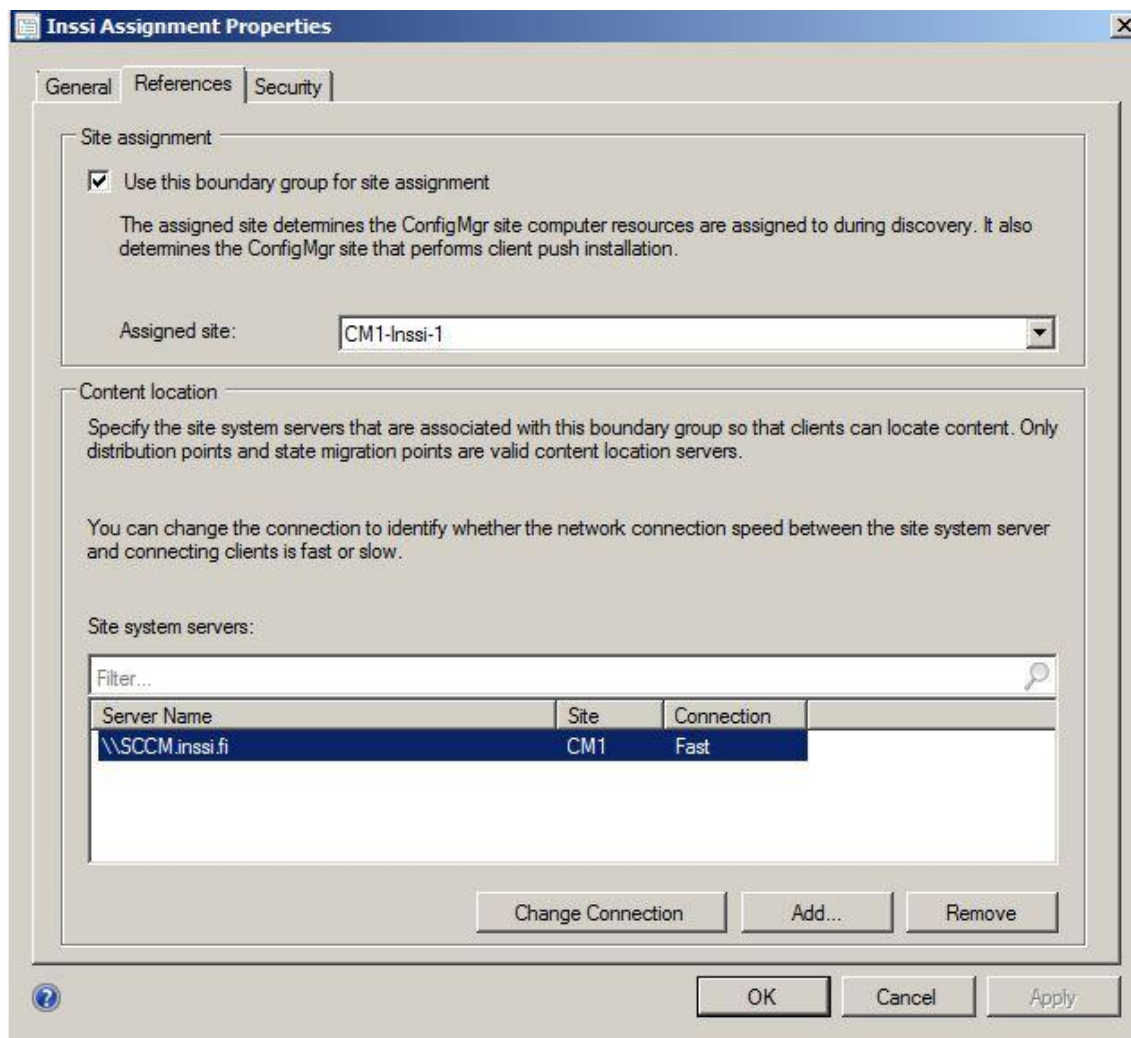
4.4 Rajojen ja rajaryhmien määrittäminen

Rajat ovat IP-osoite aliverkkoja tai alueita. Rajojen määrittäminen on helppoa, koska Active Directory Forest Discovery on luonut ne jo toimialueen mukaisesti käytettäväksi. Luodaan raja toimialueen oletusarvoisesta rajoituksesta, joka näkyy kuvassa 8.



Kuva 8. Oletusrajaryhmän muokkaaminen oman ympäristön mukaisesti.

Luodaan rajaryhmä selkeyden vuoksi, ja koska tietyt optiot vaativat sitä. Rajaryhmiä voidaan ajatella globaalissa yrityksessä maantieteellisinä rajoina. Kohdistetaan ryhmän toimipaikka toimeksiantona Configuration Managerin CM1:lle kuten kuvassa 9.



Kuva 9. Rajaryhmän luominen toimipaikalle.

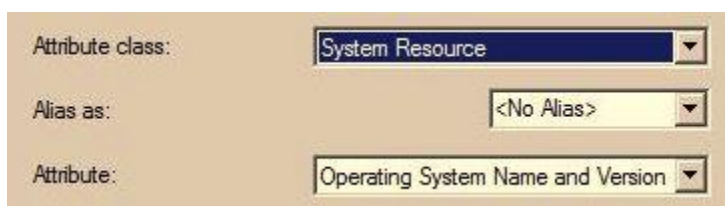
Palvelimelle asennetaan seuraavat järjestelmän toimipaikka roolit: DHCP, Application Server, File Services, Web Server (IIS), WDS, WSUS. Varmistetaan scope-asetuksista, että PXEclientti on asetettu portille 60, joka näkyy kuvassa 10. Muuten saattaa ilmetä yhteensopivuusongelmia.

| | | | |
|---------------------------|----------|----------------------------|------|
| 003 Router | Standard | 192.168.0.254 | None |
| 066 Boot Server Host Name | Standard | 192.168.0.2 | None |
| 067 Bootfile Name | Standard | smsboot\x64\wdsnbp.com | None |
| 006 DNS Servers | Standard | 192.168.0.1, 10.95.254.253 | None |
| 015 DNS Domain Name | Standard | inssi.fi | None |
| 060 PXEClient | Standard | PXEClient | None |

Kuva 10. PXE clientin portin varmistus.

4.5 Laitteistokokoelman luonti

74Luodaan kaksi laitteistokokoelmaan - yksi työasemille ja toinen palvelimille. Asetetaan kokoelmalle jäsenyysääntö tietokantaan nimettynä tarkoituksensa mukaisesti ja asetetaan inkrementaalinen päivittäminen päälle. Inkrementaalinen päivitys määrääjoin arvioi uusia resursseja ja lisää pätevät kokoelmaan. Tietokantahaun attribute class -kohtaan valitaan System Resource, eli järjestelmäresurssi ja sen attribuutiksi valitaan Operating System Name and Version, joka näkyy kuvassa 11. Tämä tarkoittaa käyttöjärjestelmän nimeä ja versiota.



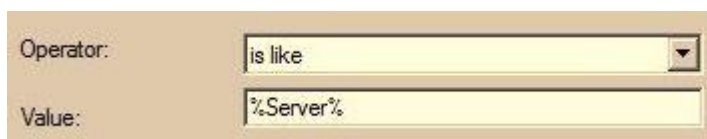
Attribute class: System Resource

Alias as: <No Alias>

Attribute: Operating System Name and Version

Kuva 11. Jäsenyyden valinta.

Nyt on asetettu, mitä halutaan etsiä, jonka jälkeen annetaan etsinnälle arvo. Operator-kohtaan valitaan: is like (on yhtäkuin). Value-kohtaan asetetaan %Server%-palvelin tai työasema. Kuvassa 12 näkyy palvelinten haku.



Operator: is like

Value: %Server%

Kuva 12. Palvelinten haku tietokannasta.

4.6 Clienttien asennus ja hallinto

Ennen clientin rakentamista asennetaan toimipaikalle tarvittavat roolit. Valitaan asennettaviksi rooleiksi Application Catalog Web Service Point, Application Catalog Website Point, Asset Intelligence Synchronization Point ja Software Update Point. Roolit asennetaan oletusarvoin, paitsi Website Pointille osoitetaan toimipaikkapalvelimen osoite kuten kuvassa 13.

Site system server:

Specify the settings for the IIS website. The website must already exist on this server.

IIS website:

Web application name:

Client connections

Specify the NetBIOS name used in the Application Catalog URL for client computers on the intranet.

NetBIOS name:

Kuva 13. Website Pointille valitaan toimipistepalvelin

Clienttien ominaisuuksia hallinnoidaan oletusarvoisesti Default Client Settings objektin kautta. Muutetaan oletusarvoisia asetuksia seuraavanlaisiksi.

Clientti lähettää kartoituksen mahdollisista laitteistomuutoksista, päivitysten puutteista ja suoritukseen kykenevistä ohjelmistoista päivittäin. Mahdollisista menettelymuutoksista suoritetaan kysely palvelimelle puolen tunnin välein, kuten kuvasta 14 näkyy. Clientille määritetään palvelimen osoite, minne sen tulee kommunikoida.

Default Settings

Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.

Specify how client computers retrieve policy

Device Settings

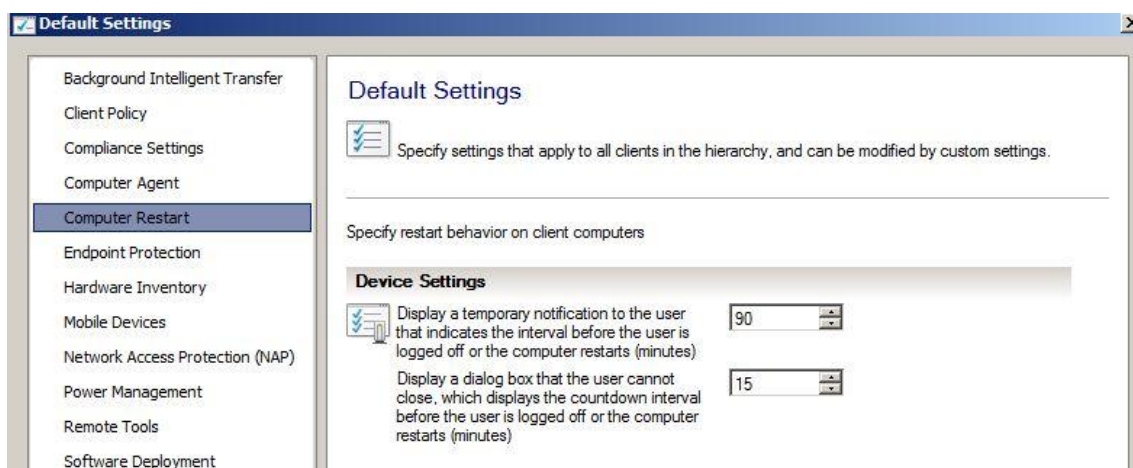
Client policy polling interval (minutes)

Enable user policy polling on clients

Enable user policy requests from Internet clients

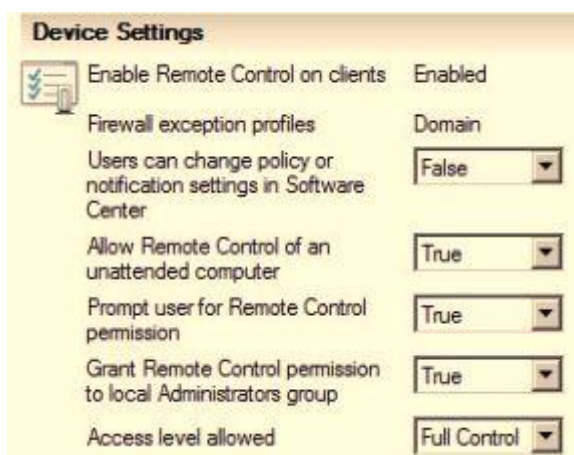
Kuva 14. Clientin ja palvelimen välinen eheyden tarkistaminen.

Clientille annetaan valtuudet sammuttaa tai käynnistää uudestaan työasema. Puolitoista tuntia ennen sulkemista annetaan käyttäjälle ilmoitus tapahtumasta ja viittätoista minuuttia ennen ilmestyy lähtölaskenta, jota ei ole mahdollista sulkea. Mikä näkyy kuvassa 15.



Kuva 15. Mahdollistetaan työasemien virranhallinta.

Luodaan kaksi mukautusta, jotka määrittelevät omat käytännöt palvelimille ja työasemille. Kuvan 16 mukaisesti palvelin-clientille luodaan asetus, joka sallii toimialueen sisäisen etäyhteydenoton luomalla sen palomuurin poikkeuksen.



kuva 16. Palvelimen etäyhteyden salliminen.

Työasemille luodaan sama etäyhteys-määritelmä kuin palvelimille, mutta lisätään seuraavat optiot. Sallitaan laitteiston virranhallinta clientille ja estetään käyttäjää muuttamasta tätä. Asetetaan pakollisten ohjelmistojen tarkistus toteutumaan päivittäiseksi.

Luodaan oma client-paketti laitteistokokoelmalle, jotta ei sekoiteta oletusarvoisia asetuksia. Tehdään uusi client-paketti, joka laitetaan saamaan lähdetiedostonsa aina lähdekansioista. Lähdekansioiksi viitataan toimipaikkaa \\sccm\sms_CM1\client. Jaetaan uusi paketti laitteistokokoelmalle.

Sijoitetaan luodut clientit laitteistokokoelmiin tehtävien mukaisesti. Clientin asennuspaketti on noin 160 Mb, joten on huomioitava mahdollinen viive sijoituksissa.

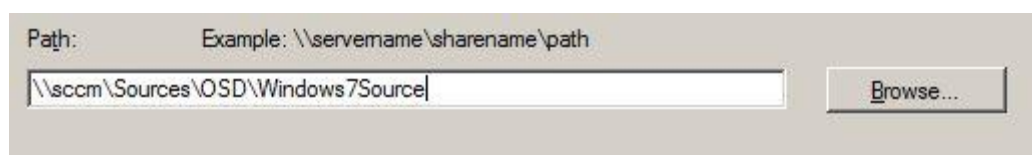


Kuva 17. Palvelinkokoelman valinta.

Valitaan kokoelma ja suoritetaan clientin asennus, kuten kuvasta 17 näkee. Kirjaututtaessa sisään valmiiksi asennetulle työasemalle tarkistetaan asennuksen toteutuminen ohjauspaneelista.

4.7 Käyttöjärjestelmän luonti ja asennus

Liitetään SCCM-koneeseen Windows 7 x64 Enterprise -käyttöjärjestelmän asennuslevy, josta kopioidaan kaikki materiaali koneelle Sources/OSD/Windows7Source -kansioon. Lisätään kansio Configuration Managerin käyttöjärjestelmän lähdeasennussegmenttiin viitaten siihen verkko-osoitteella kuten kuvassa 18. Lähde nimetään toimialueen ja arkkitehtuurin mukaisesti.



Kuva 18. Asennuslevykansion verkko-osoite

Kun käyttöjärjestelmän asennuspaketti on luotu, jaetaan se laitteistokokoelmalle.

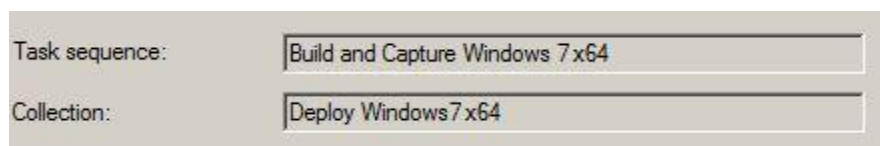
Muokataan x86 -arkkitehtuurille tarkoitettua käynnistyslevykuvaa siten, että se sijoitetaan PXE -palvelupisteeltä. Kun muutos on tehty, jaetaan se laitteistokokoelmalle. x64 -arkkitehtuurin levykuvaketta ei voida käyttää, koska sillä ei voida tehdä alemman arkkitehtuuritason sijoituksia, kun puolestaan vanhemmalla voidaan tehdä uudempi.

Luodaan task sequence (MIKÄ)käyttöjärjestelmän rakentamiselle ja kaappaamiselle.

- Asetetaan käynnistyslevyksi sijoittamamme kuvake, mutta asennetaan x64 -arkkitehtuurinen käyttöjärjestelmä.
- Liitetään tuleva työasema työryhmään nimeltä workgroup.
- Asennetaan luomamme clientti .
- Asennetaan kaikki päivitykset.
- Kaapataan kuvake ja osoitetaan se kansioon \\sccm\sources\osd\Windows7.

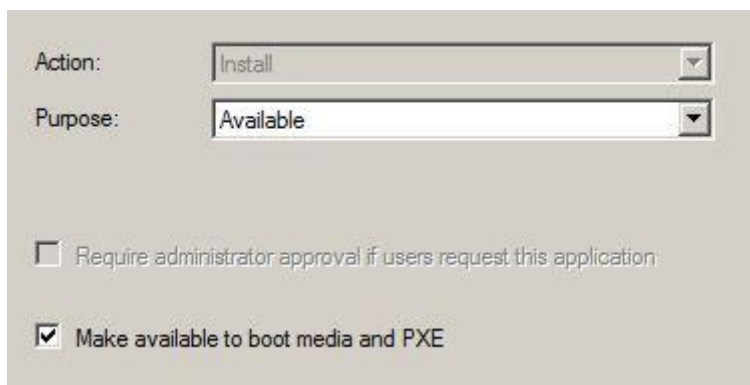
Tuodaan tyhjä virtuaalikone Configuration Managerin tietokantaan manuaalisesti. Annetaan koneelle haluttu nimi ja ilmoitetaan sen MAC-osoite, jotta Configuration Manager voi tunnistaa koneen. Lisätään kone sille luotuun kokoelmaan "Deploy Windows 7 x64".

Sijoitetaan luotu Task sequence osoittamalla se äsken luotuun kokoelmaan kuten kuvassa 19.



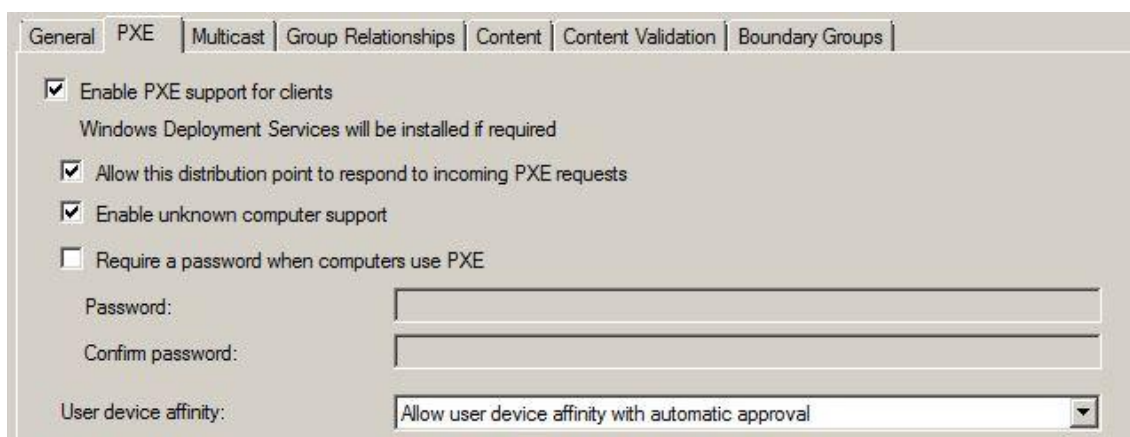
Kuva 19. Task sequencen osoitus.

Valitaan tarkoituksiksi saatavilla ja varmistetaan, että PXE-saatavuus on valittuna kuten kuvassa 20.



Kuva 20. PXE:n varmistus.

Asetetaan jakelupisteestä PXE -tuki päälle. Sallitaan palvelimelta PXE -pyyntöihin vastaaminen ja tuki tuntemattomille tietokoneille. Ei laiteta salasana vaatimuksia, koska eivät ole tarpeellisia tässä ympäristössä kuten kuvassa 21.



Kuva 21. Jakelupisteen PXE -tuen aktivointi.

Aloitetaan uuden koneen asennus käynnistämällä tietokone. Koneen kysyessä verkkokäynnistystä painetaan F12 -näppäintä, joka hyväksyy sen. Kuvassa 22 näytetään näppäinpyyntö verkkokäynnistykselle.



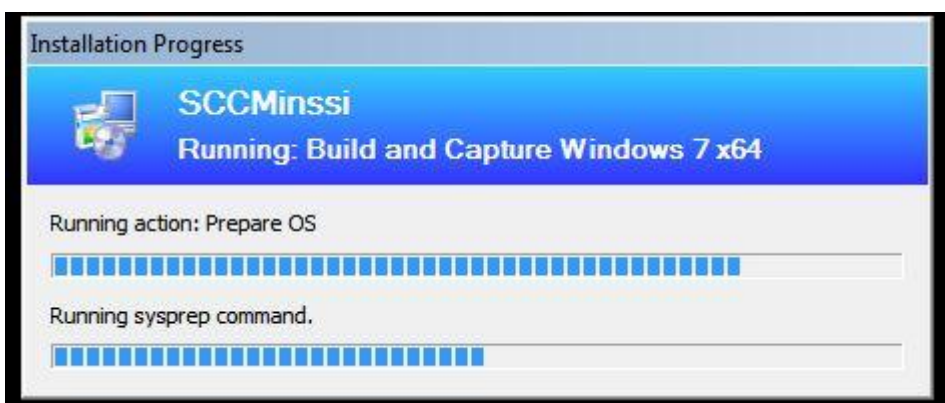
Kuva 22. PXE -käynnistyksen hyväksyttäminen.

Valitaan levykuva ja aloitetaan asennus. Kuvassa 23 nähdään, miltä asennusprosessi näyttää.



Kuva 23. Käyttöjärjestelmän asennus.

Asennuksen jälkeen otetaan automaattisesti sysprep:illä talteen levykuva käyttöjärjestelmästä, joka näkyy kuvasta 24.



Kuva 24. Käyttöjärjestelmän syspreppaaminen.

Lopuksi koneelle asentuu clientti, jonka jälkeen käyttöjärjestelmä on valmis.

4.8 Ohjelmistojen levittämisen käyttöönotto

Luodaan sovelluksille oma alikansio sources -kansion alle. Kansion sisään luodaan ohjelmien mukaiset alikansiot. Ladataan .msi -asennuspaketit Firefoxista ja 7zip-ohjelmistoista ja sijoitetaan ne kansioihinsa.

Configuration Managerista aloitetaan ohjelmiston luomisprosessi. Laitetaan tyypiksi natiivi ja sijainniksi Firefoxin .msi -asennustiedosto. Yleisiin tietoihin asetetaan ohjelmiston nimi ja asennuspaketin mukainen versionumero, joka nähdään kuvasta 25. Ohjelman luomisen jälkeen muutetaan sen käyttöönotto -ominaisuuksia. Vaihdetaan

kategoriavaatimukseksi käyttäjä. Lisätään vaatimus, joka sallii operaation suoritettavaksi Windows7 -käyttöjärjestelmissä.

Name: Mozilla Firefox (En-us)

Administrator comments:

Manufacturer: Mozilla

Software version: 17.0.4

Optional reference:

Administrative categories: Select...

Date published: 10. 4.2013

Allow this application to be installed from the Install Application task sequence action instead of deploying it manually

Kuva 25. Mozilla Firefox -tietojen asettelu

Sijoitetaan Firefox distribution pointille. Asetuksiin laitetaan ohjelmiston asennettavaksi vapaaehtoisena ja käyttäjälle näkyväksi ohjelmistokeskuksessa. Toteutetaan samat toteutukset 7zip -ohjelmiston kanssa.

Kirjaudutaan sisään työasemalle ja haetaan käynnistä-valikosta Software Center. Ohjelmistokirjastoon aukeaa ohjelmat, jotka juuri luotiin ja nähdään kuvassa 26. Asennetaan molemmat ja käyttöjärjestelmä on saatu haluttuun loppupisteeseen.

| NAME | TYPE | PUBLISHER | AVAILABLE AFTER | STATUS |
|--|------------------|-----------|-----------------|-----------|
| 7-Zip | Application | 7-Zip.org | 3/4/2013 | Available |
| 7-Zip 9.20 (x64 edition) | Application | | 3/4/2013 | Available |
| Deploy Windows 7 ent. x64 - New Computer | Operating System | | 3/19/2013 | Available |
| Deploy Windows 7 ent. x64 - Refresh | Operating System | | 3/19/2013 | Installed |
| Mozilla Firefox (en-US)-copy | Application | Mozilla | 3/20/2013 | Available |
| Win7 testi asennus | Operating System | | 3/19/2013 | Available |

Kuva 26. Software Centerissä valittavissa olevat ohjelmistot.

5 Yhteenveto

Tämän opinnäytetyön lähtökohtana oli tutustua System Center Configuration Manager 2012 -ohjelmistoon. Työn alussa käytiin läpi ohjelmiston ominaisuuksia yleisesti, jonka jälkeen esitetään toteutusympäristö ja suunnitelma. Suunnitelmassa käydään läpi toteutettavia asioita ennen itse Configuration Managerin asennusta. Lopuksi toteutetaan ohjelmiston asennus, jonka avulla asennetaan tyhjille työasemille käyttöjärjestelmät.

Työn käytännön osuuden alkutilanteen ja lopputuloksen väliin on mahtunut paljon virheitä ja ongelmia. Itse ympäristö tehtiin alusta alkaen kolme kertaa.

Alusta lähtien Microsoftin Routing and Remote Access (RRAS) -palvelinta ei saatu reitittämään ympäristöä ulkoverkkoon, jonka seurauksena kaikki päivitykset ja sovellukset jouduttiin siirtämään manuaalisesti. Tämä tuotti huomattavan paljon ylimääräistä työtä ja ongelmia, joiden ratkaisemiseen kului useita kymmeniä tunteja.

Ensimmäisellä kerralla ympäristö oli rakennettu liian monimutkaiseksi suhteessa sen käyttötarkoitusta varten. Ympäristön toiminnot oli jaettu monelle eri palvelimelle. Suurimmaksi ongelmaksi syntyi tietokantapalvelimen erottaminen Configuration Managerista. Virheilmoitukset viittasivat jatkuvasti palvelinten välisiin kommunikointiongelmiiin. Ammatilaisten kirjoituksissa ohjeistettiin välttämään ohjelmistojen erottamista ellei ole välttämätöntä. Näin parhaaksi aloittaa kaiken alusta.

Toisella kerralla ympäristö yksinkertaistettiin kahdeksi palvelimeksi, ja reitittävä palvelin vaihdettiin linux-pohjaiseksi. DC -palvelimelle asennettiin ADDS- ja DNS- palvelut. SCCM -koneelle annettiin tarpeeksi tilaa ja tehoa, jotta se kykenisi ajamaan kaikki loput toiminnot. Työ edistyi ongelmitta, kunnes rakennuksen palvelinhuoneessa hajosi ilmastointi, ja kaikki laitteet jouduttiin sammuttamaan nopeasti. Tämän jälkeen alkoi ympäristössä ilmetä ongelmia, joille ei saatu ratkaisua. Näin parhaaksi aloittaa kaiken alusta.

Kolmannella kerralla toteutin kaiken samalla tavalla kuin toisella kerralla. Ainoana ongelmana ilmeni distribution pointin hajoaminen, mutta se korjaantui uudelleenasennuksella. Itse koen, että työn aikana koetut ongelmat ja niiden selvittäminen on opettanut Configuration Managerin käytössä eniten.

On saatu haluttu lopputulos käytännön osuudesta ja voidaan abittaa Metropolin laboratorioympäristön toteutuksen suunnittelu.

Lähteet

- 1 Kerrie, Meyler. Byron, Holt. Marcus, Oh. Jason, Sandys. Greg, Ramsey. 2012. System Center 2012 Configuration Manager Unleashed. Indianapolis, IN, USA: Sams Publishing.
- 2 Kent, Agerlund. 2012. System Center 2012 Configuration Manager Mastering the Fundamentals. UK: Deployment Artists.
- 3 Microsoft TechNet, System Center Configuration Manager TecCenter, Configuration Manager, Documentation Library for System Center 2012 Configuration Manager, Getting Started with System Center 2012 Configuration Manager, Fundamentals of Configuration Manager. Saatavissa: <http://technet.microsoft.com/library/gg682106.aspx>.
- 4 Microsoft TechNet, System Center Configuration Manager TecCenter, Configuration Manager, Site Administration for System Center 2012 Configuration Manager, Planning for Configuration Manager Sites and Hierarchy. Saatavissa: <http://technet.microsoft.com/library/gg682075.aspx>.
- 5 Microsoft TechNet, System Center Configuration Manager TecCenter, Configuration Manager, Documentation Library for System Center 2012 Configuration Manager, Getting Started with System Center 2012 Configuration Manager, Supported Configurations for Configuration Manager. Saatavissa: <http://technet.microsoft.com/library/gg682077.aspx>.
- 6 Microsoft TechNet, System Center Configuration Manager TecCenter, Deploying Software and Operating Systems in System Center 2012 Configuration Manager, Application Management in Configuration Manager. Saatavissa: <http://technet.microsoft.com/library/gg699373.aspx>.
- 7 Microsoft TechNet, System Center Configuration Manager TecCenter, Software Updates in Configuration Manager, Configuring Software Updates in Configuration Manager: Saatavissa: <http://technet.microsoft.com/en-us/library/gg712312.aspx>.
- 8 Microsoft TechNet, System Center Configuration Manager TecCenter, Software Updates in Configuration Manager, Planning for Software Updates in Configuration Manager. Saatavissa: <http://technet.microsoft.com/en-us/library/gg712696.aspx>.
- 9 Microsoft TechNet, TechNet Video, Screencasts, SCCM 2012 SP1 and the new way handling Software Updates explained. Saatavissa: <http://technet.microsoft.com/en-us/video/sccm-2012-sp1-and-the-new-way-handling-software-updates-explained.aspx>.

- 10 PrajwalDesai, SCCM, Deploying SCCM 2012 Part 7. Saatavissa: <http://prajwalDesai.com/deploying-sccm-2012-part-7-configuring-discovery-and-boundaries/>.
- 11 Windows-noob, server noob, SCCM 2012, Configuration Manager 2012, Configuration Manager 2012 – Beta 2, LAB - Part 3. Additional Configuration. Saatavissa: <http://www.windows-noob.com/forums/index.php?/topic/3840-using-sccm-2012-beta-2-in-a-lab-part-3-additional-configuration/>.
- 12 Microsoft TechNet, Deploying Clients for System Center 2012 Configuration Manager, Technical Reference for Client Deployment in Configuration Manager, About Client Settings in Configuration Manager. Saatavissa: <http://technet.microsoft.com/en-us/library/gg682067.aspx>.
- 13 Microsoft TechNet, Deploying Clients for System Center 2012 Configuration Manager, Configuring Client Deployment in Configuration Manager, How to Install Clients on Windows-Based Computers in Configuration Manager. Saatavissa: <http://technet.microsoft.com/en-us/library/gg712298.aspx>.
- 14 Microsoft TechNet, Assets and Compliance in System Center 2012 Configuration Manager, Collections in Configuration Manager, Introduction to Collections in Configuration Manager. Saatavissa: <http://technet.microsoft.com/en-us/library/gg682177.aspx>.
- 15 Microsoft TechNet Magazine, Issues, 2011, July, System Center Managing Mobile Devices. Saatavissa: <http://technet.microsoft.com/en-us/magazine/hh316170.aspx>.
- 16 Microsoft TechNet, Deploying Clients for System Center 2012 Configuration Manager, Planning for Client Deployment in Configuration Manager, Determine How to Manage Mobile Devices in Configuration Manager. Saatavissa: <http://technet.microsoft.com/en-us/library/gg682022.aspx>.
- 17 Windows-noob, server noob, SCCM 2012, Configuration Manager 2012, Adding the Reporting Services Point role. Saatavissa: <http://www.windows-noob.com/forums/index.php?/topic/4550-using-sccm-2012-rc-in-a-lab-part-11-adding-the-reporting-services-point-role/>.
- 18 Microsoft TechNet, Site Administration for System Center 2012 Configuration Manager, Reporting in Configuration Manager, Introduction to Reporting in Configuration Manager. Saatavissa: <http://technet.microsoft.com/en-us/library/gg682105.aspx>.
- 19 Windows-noob, server noob, SCCM 2012, Configuration Manager 2012, Deploying Windows 8 Consumer Preview using Configuration Manager 2012 RC2. Saatavissa: <http://www.windows-noob.com/forums/index.php?/topic/5124-using-sccm-2012-rc-in-a-lab>

part-15-deploying-windows-8-consumer-preview-using-configuration-manager-2012-rc2/.

- 20 Microsoft TechNet, Deploying Software and Operating Systems in System Center 2012 Configuration Manager, Operating System Deployment in Configuration Manager, Introduction to Operating System Deployment in Configuration Manager. Saatavissa: <http://technet.microsoft.com/en-us/library/gg682108.aspx>.
- 21 Microsoft TechNet, Site Administration for System Center 2012 Configuration Manager, Operations and Maintenance for Site Administration in Configuration Manager, Backup and Recovery in Configuration Manager. Saatavissa: <http://technet.microsoft.com/en-us/library/gg712697.aspx>.
- 22 DamianFlynn, ConfigMgr, SCCM 2012 DataBase Recovery. Saatavissa: <http://www.damianflynn.com/2012/08/22/sccm-2012-database-recovery/>.
- 23 Microsoft TechNet, TechNet Library, System Center, System Center Technical Documentation Library. Saatavissa: <http://technet.microsoft.com/en-us/library/cc507089.aspx>.
- 24 Microsoft TechNet, TechNet Library, Introduction to Configuration Manager. Saatavissa: <http://technet.microsoft.com/fi-FI/library/gg682140.aspx>.
- 25 Microsoft TechNet, Library, Deployment Tools Technical Reference, Sysprep Technical Reference, What is Sysprep?. Saatavissa: [http://technet.microsoft.com/en-us/library/cc721940\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc721940(v=ws.10).aspx).
- 26 Microsoft TechNet, Library, Windows Automated Installation Kit (Windows AIK), Windows Automated Installation Kit (Windows AIK) User's Guide. Saatavissa: [http://technet.microsoft.com/en-us/library/cc749528\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc749528(v=ws.10).aspx).
- 27 TechRepublic, blogs, data center, Microsoft SCCM 2012: Understand role-based access control. Saatavissa: <http://www.techrepublic.com/blog/networking/microsoft-sccm-2012-understand-role-based-access-control/5748>.

6 Liitteet



Liite 1. Suunnitelma.