OULUN AMMATTIKORKEAKOULU

Topias Päkkilä

Windows Server Update Services -palvelun käyttöönotto

Windows Server Update Services -palvelun käyttöönotto

Topias Päkkilä
Opinnäytetyö
Syksy 2014
Tietojenkäsittelyn koulutusohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma, järjestelmäasiantuntemus

Tekijä: Topias Päkkilä
Opinnäytetyön nimi: Windows Server Update Services -palvelun käyttöönotto
Työn ohjaaja: Jukka Kaisto
Työn valmistumislukukausi- ja vuosi: Syksy 2014 Sivumäärä: 37

Tämän opinnäytetyön aiheena oli Windows Server Update Service -palvelun käyttöönotto Oulun ammattikorkeakoulun liiketalouden yksikön järjestelmätukilaboratoriossa. Aihe löytyi opinnäytetyönohjaajalta. Tietoperustana oli Microsoftin Technet-portaali sekä alan kirjallinen materiaali.

Työssä käytiin läpi, mitä ovat riskit, uhat ja haavoittuvuudet. Lisäksi vastattiin kysymyksiin mitä ovat erilaiset päivitykset, mitä päivitysohjelmistovaihtoehtoja Microsoft tarjoaa ja mitä eri ominaisuuksia päivitysohjelmat pitivät sisällään. Päivitysvaihtoehdoista käytiin läpi Microsoft Update, Microsoft System Center Configration Manager, Microsoft Intune ja Windows Server Update Service. Windows Update- ja WSUS-ohjelma on tarkoitettu Microsoftin tuotteiden ja käyttöjärjestelmien päivitykseen. SCCM- ja Intune-ohjelmalla voidaan päivittää ja jakaa myös muiden valmistajien ohjelmia.

Opinnäytetyön tavoitteena oli asentaa ja ottaa käyttöön Windows Server Update Services -päivityspalvelu. Asennus piti sisällään WSUS-palvelun asennuksen, SQL-palvelimen asennuksen sekä ryhmäkäytänteiden asettamisen toimialueeseen. Työssä tarkasteltiin WSUS-palvelun tuottamia päivitysraportteja ja Microsoft Baseline Security Analyzer -ohjelman raportointia.

Työn lopputuloksena voitiin todeta, että Windows Update -palvelun kautta tietokoneiden päivitys oli hallitsematonta ja tuli suorittaa manuaalisesti. Windows Server Update Service -palvelun kautta päivitykset saatiin asennettua työasemille keskitetysti. Ryhmäkäytänteiden avulla päivitykset saatiin asentumaan automaattisesti tiettyyn kellonaikaan tiettynä päivänä.

Asiasanat: Windows Server Update Services, Ryhmäkäytänteet, Päivitykset

ABSTRACT

Oulu University of Applied Sciences
Degree programme in Business Information Systems

Author: Topias Päkkilä
Title of thesis: Implementing a Windows Server Update Services
Supervisor(s): Jukka Kaisto
Term and year when the thesis was submitted: Autumn 2014 Number of pages: 37

The subject of this thesis was to implement a Windows Server Update Services (WSUS) server in the computer laboratory of Oulu University of Applied Sciences, School of Business and Information Management. This laboratory is intended for computer system expertise students. The source for the theoretical background of this thesis was collected from Microsoft Technet portal and written material.

This thesis determines what the risks, threats and vulnerabilities are for companies. In addition answers were provided to questions such as what kind of different updates there are, what different update programs Windows offers and what their features are. This thesis covers Wisndows Update, Microsoft System Center Configuration Manager, Microsoft Intune and Windows Server Update Services programs. Windows Update and WSUS programs are for updating Microsoft's own programs and operating system. With SCCM and Microsoft Intune you are able to update and deploy different manufacturer's programs.

The goal of this study was to install and implement the WSUS service. The process included the installation of both WSUS service and Structured Query Language server (SQL). Group Policy Objects were taken into use in the domain. This thesis studies the security reports generated by WSUS program and Microsoft Baseline Security Analyzer program.

The result of this study was that in a situation where updating computers was uncontrollable and performed manually, it could now be done automatically and centrally via WSUS service. Due to the fact that the Group Policy Objects were used, the updates were installed automatically on a specific time and on a specific day.

Keywords: Windows Server Update Service, Group Policy Object, Updates

SISÄLLYS

1 JOHDANTO

Heti, kun tietokone yhdistetään Internetiin, se tulee alttiiksi hakkereiden hyökkäyksille. Hakkerit käyttävät hyväksi käyttöjärjestelmien ja ohjelmistojen haavoittuvuuksia. Haavoittuvuuksia päivitetään ohjelmistojen jakamilla korjauspäivityksillä. Microsoft tarjoaa useita ohjelmistoja päivityksien asennukseen, ja riippuen siitä, tarvitseeko päivityksiä asentaa muutamalle tietokoneelle vai useille kymmenille tai sadoille tietokoneille, on ylläpitäjän syytä harkita eri vaihtoehtoja. Jos koneita on useita kymmeniä, on niiden hallinta haastavaa Windows Update -palvelun kautta. Windows Server Update Service lataa päivitykset paikalliselle koneelle ja jakaa päivityksiä sisäverkon kautta halutuille työasemille. Tämä säästää kaistan käyttöä ja siitä muodostuvia kuluja. Päivitysten jaosta tulee hallittua, sillä järjestelmän ylläpitäjä päättää, mitä päivityksiä jaetaan millekin tietokoneelle. Päivitysten asennuksesta ja jaosta saadaan täysin automatisoitua.

Työn tavoitteena oli pystyttää Windows Server Update Service -palvelu Oulun Ammattikorkeakoulun Liiketalouden yksikön järjestelmäasiantuntijaopiskelijoiden käyttämään tietokonelaboratorioon. Työssä asennettiin kaksi palvelinta, joista toiseen asennettiin WSUS-rooli ja toiseen SQL-palvelin. Aihe työhön saatiin opinnäytetyön ohjaajalta.

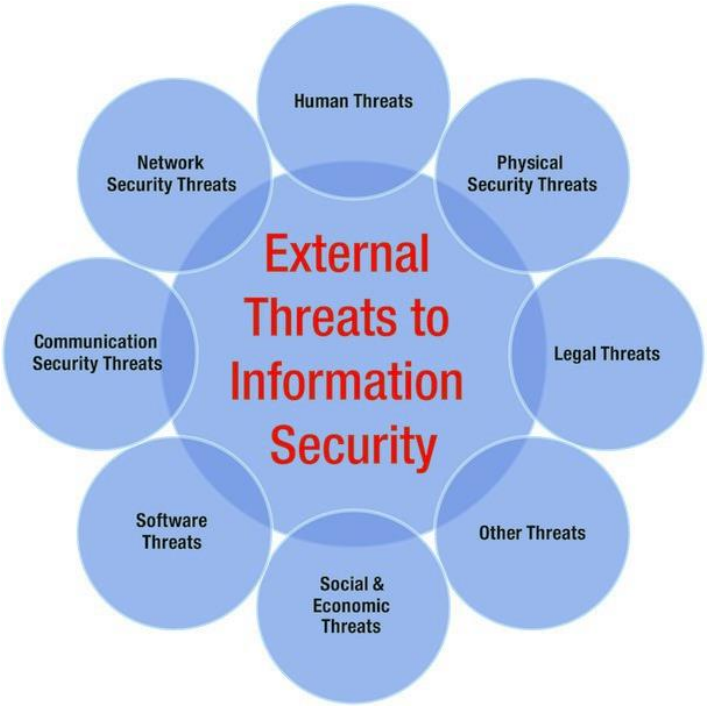
Kohde toimialueen tietokoneet olivat kaikki virtuaalisia työasemia. Työstä rajattiin pois normaalit työasemat ja palvelimet. WSUS-palvelu hakee päivityksiä vain Windows 8.1 -käyttöjärjestelmälle, Microsoft Office -ohjelmistolle sekä Windows Defender -ohjelmalle.

2 UHAT, RISKIT JA RISKIENHALLINTA

Uhka on toimintaa, jossa kohteeseen pyritään vaikuttamaan negatiivisesti, jotta se saataisiin toimimaan uhkaajan haluamalla tavalla. Vahingollisuutensa takia uhka pyritään estämään ja torjumaan. Sen torjuminen ei kuitenkaan tarkoita, että vahingolta vältyttäisiin. Kuviossa 1 osoitetaan ulkoisia uhkia yritykselle. Niitä ovat esimerkiksi verkkouhat, sovellusuhat ja ihmisen toteuttamat uhat. Verkkouhista (network security threats) mainittakoon SQL-injektio, jossa käyttäjän suorittamia komentoja SQL-kantaan ei osata suodattaa, jolloin hakkeri voi saada käyttöön koko SQL-tietokannan. Verkkouhkiin kuuluu myös palvelunestohyökkäys, jossa palvelin tai verkkolaite ylikuormitetaan. Lisäksi verkkolaitteissa olevia oletussalasanoja voidaan hyödyntää ja näin ottaa laitteet käyttöön.

Sovellusuhat (software threats) pitävät sisällään muun muassa troijalaiset ja virukset, sekä käyttöjärjestelmän tietoturva-aukot (näitä avattu sivulta 10 alkaen). Ihmisten toteuttamia (Human threats) uhkia ovat hakkereiden toteuttamat hyökkäykset ja järjestelmänvalvojan heikon salasanan hyödyntäminen. Yritykset ovat tietenkin alttiita luonnonuhille (natural threats). Maanjäristykset, hurrikaanit ja tulvat eivät niinkään kosketa Suomea, mutta isossa mittakaavassa ovat todellisia uhkia. Muita uhkia voivat olla tietokoneen laitteiston, kuten kovalevyn tai prosessorin, rikkoutuminen. (Limnéll, Majewski, Salminen 2014, 111-113; Rao, Nayak 2014, kappale 3; F-secure, hakupäivä 28.11.2014)

Ulkoisten uhkien lisäksi yrityksen toimintaan vaikuttavat sisäiset uhat. Sisäisen uhan lähteenä ovat tyypillisesti tyytymättömät työntekijät tai yrityksen kumppanit. Yleensä ongelmana ovat liian suuret käyttöoikeudet, tai se, että ne saa usein liian helposti hankittua. Vahinkoa järjestelmään voi tulla myös haittaohjelmasta tietämättömän työntekijän kautta. Vuonna 2013 neljätoista prosenttia kyberhyökkäyksistä tuli yrityksen sisältä, mikä on merkittävästi enemmän kuin edeltävinä vuosina. (Limnéll, Majewski, Salminen 2014, 105.)



KUVIO 1. Ulkoiset uhat (Rao, Nayak, 2014, kappale 3)

Täydellistä turvaa uhkia vastaan on mahdotonta saavuttaa, ja hyökkäyksen tekijän työ on aina helpompaa kuin sen, joka yrittää puolustautua uhkia ja hyökkäyksiä vastaan. Hyökkääjän täytyy löytää vain yksi hyödynnettävissä oleva heikkous järjestelmässä, kun taas puolustautujan on pyrittävä suojautumaan kaikkia mahdollisia uhkia vastaan pitäen samalla kustannukset kohtuullisina. Tietoturvaan investointi on kannattavaa, sillä vaikka sen ylläpito voi olla kallista, tietoturvauhan toteutuessa siitä aiheutuvat kustannukset voivat olla moninkertaiset tietoturvan ylläpitoon verrattuna. Tietoturvan pettäessä vahingot eivät ole välttämättä ainoastaan rahallisia, vaan esimerkiksi yritysten tietokoneilla sijaitsevaa dataa voi vuotaa ulkopuolisten käyttöön. (Rhodes-Ousley 2013, kappale 1.)

Kuten uhkat, myös riskit ovat jatkuvasti läsnä yritysten toiminnassa. Riski on negatiivinen tapahtuma, joka tulee mahdollisesti toteutumaan tulevaisuudessa. Riskiä ei voida siis täysin torjua, vaan torjumisen sijaan siihen tulisi suhtautua kysymällä, mitä voidaan tehdä, jotta riskin mahdollisuus toteutua olisi mahdollisimman pieni. Riskien välttäminen on mahdollista riskitietoisuudella, jossa lasketaan erilaisten riskien todennäköisyys ja niiden mahdollinen vaikutus. (Limnéll ym 2014, 108-109.)

Riskienhallinnalla yritys kohdentaa resurssit kohteisiin, joissa riskin toteutumisen mahdollisuus on kaikkein suurin. Rousku mainitsee kirjassaan, että ilman riskienhallintaa osa investoinneista kohdentuu väärään paikkaan, koska riskejä ei ole osattu arvioida oikein. (Rousku 2014, 61.) Oikein koostettu riskienhallinnan prosessi sisältää suunnittelun, riskien tunnistamisen, analysoinnin ja seuraamisen vaiheet sekä lisäksi raportoinnin ja dokumentaation (Limnéll ym 2014, 110).

3 HAAVOITTUVUUDET

Haavoittuvuus tarkoittaa järjestelmässä olevaa väärinkäytön mahdollistavaa vikaa. Haavoittuvaista järjestelmää väärinkäytettäessään hakkeri voi saada esimerkiksi pääkäyttäjän oikeudet ilman käyttäjätunnusta ja salasanaa. Hakkeri voi näin muokata, poistaa tai ladata tiedostoja. Haavoittuvuus myös mahdollistaa haitta- tai vakoiluohjelman upottamisen tietokoneeseen. Kun järjestelmässä tai ohjelmassa havaitaan haavoittuvuus, sitä korjataan toimittajan julkaisemilla päivityksillä. Esimerkiksi Microsoft julkaisee kerran kuussa päivityspaketin, joka tunnetaan epävirallisesti nimellä Patch Tuesday. Kaikki julkaisijat eivät kuitenkaan julkaise päivityksiä heti haavoittuvuuksien tullessa ilmi, vaan päivityksien viive vaihtelee niiden vaatimien korjausaikojen mukaan. (Rousku 2014, 53.)

TAULUKKO 1. Haavoittuvuudet

Haavoittuvuus	Kuvaus
Nollapäivähaavoittuvuus	Haavoittuvuuksia, jotka ovat ohjelman tekijän tiedossa, mutta niihin ei ole olemassa korjausta. Ohjelman tekijä pyrkii tiedottamaan keinoista, joilla uhka voidaan minimoida. (Rousku 2014, 53 – 54)
Takaovi	Koodiin jätetty aukko, jota ohjelman tekijä tai hakkeri voi käyttää hyväksi, esimerkiksi ohittamalla normaalit tietoturvakäytänteet. (Silberschatz, Galvin, Gagne, 2013, kappale 14.2.1).

Haavoittuvuus	Kuvaus
Troijalainen	Troijalainen yrittää esiintyä hyödyllisenä ohjelmana, kuten päivityksenä, suorittaen taustalla ei-haluttuja toimia. Voi esimerkiksi poistaa tai kopioida tiedostoja hakkerin haluamaan kohteeseen. (F-secure hakupäivä 2.12.2014)
Variaatio troijalaisesta	Haittaohjelma, joka emuloi sisäänkirjautumista. Ensimmäisen kirjautumisen yhteydessä kirjaantuminen epäonnistuu. Todellisuudessa hakkerin haittaohjelma on kopioinut tunnukset. (Silberschatz ym, 2013, kappale 14.2.1.)
Spyware	Useimmiten Shareware- ja Freeware-ohjelmien mukana kulkeutuva haittaohjelma. Kaappaa tietokoneilta käyttäjän tietoja. Näyttää myös mainoksia tietokoneella. Spyware-haittaohjelmaa hyödyntäen lähetetään arviolta 90 % maailman spam-viesteistä. (Silberschatz ym, 2013, kappale 14.2.1.)
Virus	Haittaohjelma, joka lisää ohjelmaan tai tiedostoon omaa koodiansa, koettaen samalla monistaa itseään.

4 PÄIVITYSTYYPIT

Tässä opinnäytetyössä käydään läpi neljä eri päivityksille tarkoitettua ohjelmistoa. Yrityskäytössä Windows Update -ohjelmisto, joka on osa Windows-käyttöjärjestelmää, on usein riittämätön. Isoilla yrityksillä on tarve keskitetylle päivitysten jaolle sisäverkon kautta. Windows Update -ohjelma ja Windows Server Update Service -ohjelmisto tarjoaa ratkaisun Microsoftin ohjelmien, käyttöjärjestelmien ja kolmansien osapuolien ajureiden päivitykseen. System Center Configuration Manager -ohjelmistolla voidaan ylläpitää Windows-käyttöjärjestelmien lisäksi Mac OS X-, ja Linux-käyttöjärjestelmiä sekä mobiililaitteita. Windows Intune tukee Windows –käyttöjärjestelmiä sekä (Technet 2014a, hakupäivä 11.12.2014)

4.1 Mitä ovat päivitykset, Hotfixit ja Servicepack

TAULUKKO 2. Päivityksien kuvaus

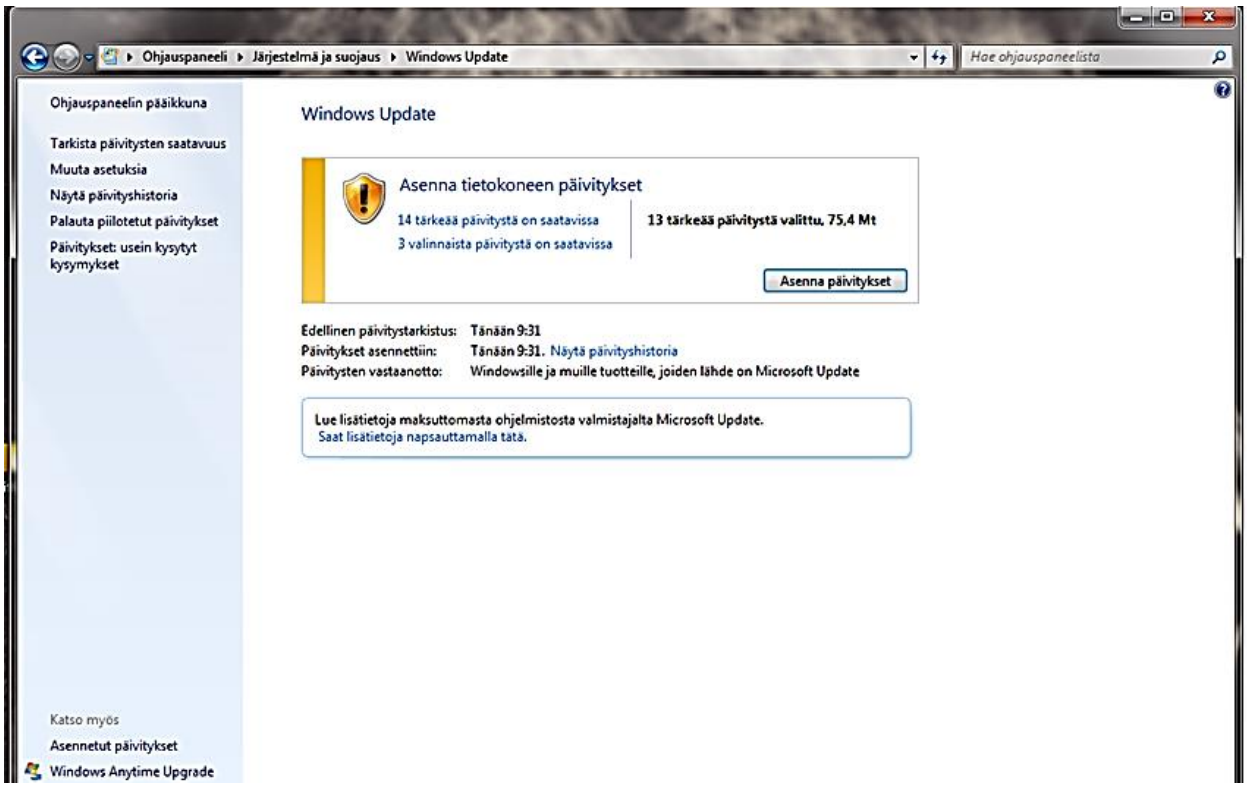
Päivitys	Kuvaus
Kriittinen päivitys asiakkaan pyynnöstä (Critical-on-Demand):	Päivitys, jonka asiakas pyytää, koska kokee ongelmien heikentävän yrityksen kykyä toimia normaalisti.
Kriittinen päivitys (Critical update):	Päivitys, jolla korjataan tietty kriittinen ongelma, joka ei kuitenkaan ole tietoturvaongelma.
Hotfix:	Kumulatiivinen yhden tai useamman tiedoston päivityspaketti, jolla korjataan ongelmia tuotteessa. Hotfix-päivitys vaikuttaa kaikkiin korjausta vaativiin tiedostoihin ja sijanteihin. Hotfix-päivitystä ei aina jaeta yrityksen ulkopuolelle, vaan se on asiakaskohtainen.

Tietoturvapäivitys (Security update):	Laajasti jaettu päivitys, joka korvaa tietoturvaan liittyviä haavoittuvuuksia tietylle tuotteelle. Haavoittuvuudet Microsoft on jakanut ryhmiin kriittinen, tärkeä, kohtuullinen ja matala.
Service Pack	Testattu, kumulatiivinen paketti, joka pitää sisällään hotfix-päivityksiä, tietoturvapäivityksiä, kriittisiä päivityksiä ja normaaleja päivityksiä. Voi myös sisältää muita korjauksia, joita on huomattu tuotteen julkaisun jälkeen.
Ohjelmapäivitys (Software Update):	Mikä tahansa päivitys, joka on julkaistu parantamaan tai korjaamaan ohjelmia.
Update Rollup	Testattu, kumulatiivinen paketti helposti jaettavissa olevia päivityksiä, joka kattaa yleensä tietyn osa-alueen, kuten tietoturvan tai tuotteen komponentin, esimerkiksi Internet Information Services -palvelun (IIS).
Päivitys (Upgrade):	Ohjelmistopaketti, joka korvaa aikaisemmin asennetun version tuotteesta uudella versiolla, säilyttäen kuitenkin asiakkaan tiedostot ja asetukset. (Carpenter, 2012, kappale 15).
Tunnistetiedostojen päivitys (Definition Update)	Päivityksiä virus- tai muihin tunnistetiedostoihin.

4.2 Windows Update

Windows Update on Windows-käyttöjärjestelmän mukana tuleva päivitysohjelma, joka etsii päivityksiä Windows Update -sivustolta. Ohjelma etsii päivitykset automaattisesti, mikäli asetus on asetettu päälle. Windows Update-ohjelman käytöstä kysytään ensikerran käyttöjärjestelmän asennuksen yhteydessä. Ohjelma tutkii Microsoft-ohjelmistojen versioita, tietokoneen merkkiä ja mallia ja asentaa päivityksiä tietojen perusteella. Microsoftin verkkosivulla kuitenkin huomautetaan, että monia päivityksiä ei asenneta automaattisesti, vaikka ne on koneelle ladattu. (Microsoft 2014a, hakupäivä 30.9.2014.)

Windows Update luokittelee päivitykset kolmeen eri ryhmään: tärkeä, suositeltu ja valinnainen. Tärkeisiin päivityksiin kuuluu suojauspäivityksiä, kriittisiä päivityksiä ja luotettavuutta parantavia ominaisuuksia. Suositeltuihin päivityksiin kuuluvat ohjelmistopäivitykset sekä uudet ominaisuudet tai olemassa olevien ominaisuuksien parantaminen. Valinnaisiin päivityksiin taas kuuluvat päivitykset tai ohjelmistot, jotka on mahdollista asentaa manuaalisesti. Näihin kuuluu muun muassa Microsoftin omat kokeiluohjelmistot tai Microsoftin kumppaneiden valinnaiset laiteohjaimet. (Microsoft 2014a, hakupäivä 30.9.2014.)



KUVIO 2. Windows Update

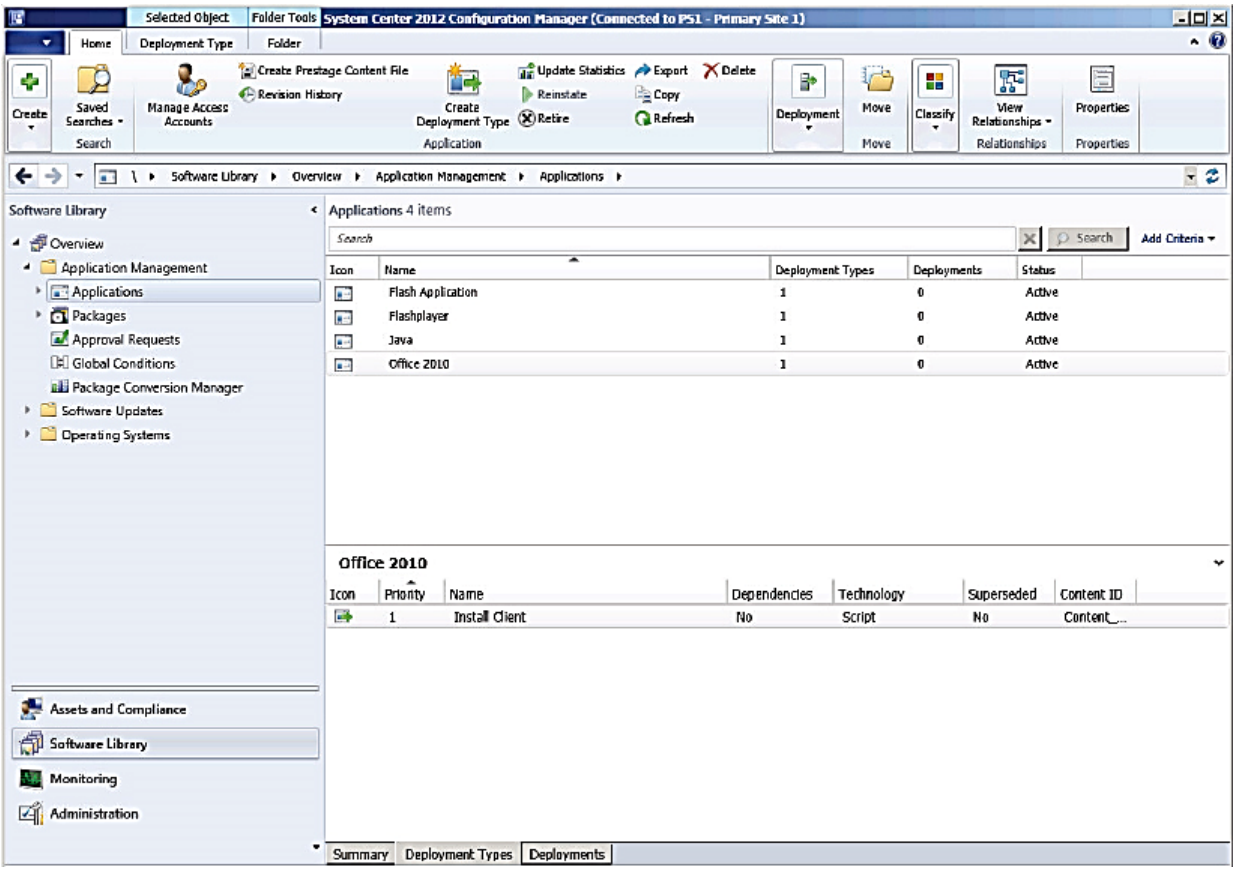
Windows Update on riittävä kotikäyttäjän ja pienen yrityksen käyttöön, mutta isommissa yrityksissä se ei riitä. Isoissa yrityksissä on vaikea pitää kirjaa siitä, mitkä koneet ovat päivitysten suhteen ajan tasalla, ja lisäksi useiden yksittäisten tietokoneiden ladatessa ulkoverkosta päivityksiä kaistanvaraus on suurta. (Morimoto, Noel, Yardeni, Droubi, Abbate, Amaris 2012, kappale 13.)

4.3 System Center Configuration Manager

System Center Configuration Manager -ohjelmisto tarjoaa huomattavasti suuremman määrän ominaisuuksia Windows Update -ohjelmaan verrattuna, ja se onkin tarkoitettu isoille yrityksille, joilla on tarvetta jakaa päivityksiä niin sovelluksille kuin käyttöjärjestelmillekin.

SCCM-sovellus käyttää aktiivihakemistoa (Active Directory), jonka kautta se hakee käyttäjät ja tietokoneet, joille palveluita jaetaan. Lisäksi se käyttää aktiivihakemistoa autentikointiin. (Technet, 2014b, hakupäivä 16.10.2014.)

SCCM-ohjelma tarjoaa mahdollisuuden lähes minkä tahansa ohjelman jakeluun sen kautta. Ohjelman kautta voi jakaa muun muassa Java-, Flashplayer- ja Office-ohjelmiston. Samalla onnistuu myös kuviossa 3 näkyvä sovellusten päivitys. Älypuhelimille on mahdollista jakaa sovelluksia ja päivityksiä siinä missä normaaleille tietokoneillekin. SCCM-ohjelma tukee Android-, iOS- ja Windows Phone- mobiilikäyttöjärjestelmiä (Rachui, Agerlund, Martinez, Daalmans 2012, kappale 1.)



KUVIO 3. Configuration Manager Features (Rachui, Agerlund, Martinez, Daalmans 2012, kappale 1)

Inventaariolistan kautta voi selata yrityksen käytössä olevien tietokoneiden kokoonpanoa koneen valmistajasta prosessorin tyyppiin ja muistin määrään. Sovellusinventaarion kautta taas nähdään käytössä olevien sovellusten versiot ja seurataan niiden käyttöä. Sen avulla voidaan seurata, mitä ohjelmia käytetään paljon ja mille asennetuille ohjelmille ei ole enää käyttöä, tai kuka käyttäjä käyttää mitäkin sovellusta juuri sillä hetkellä.

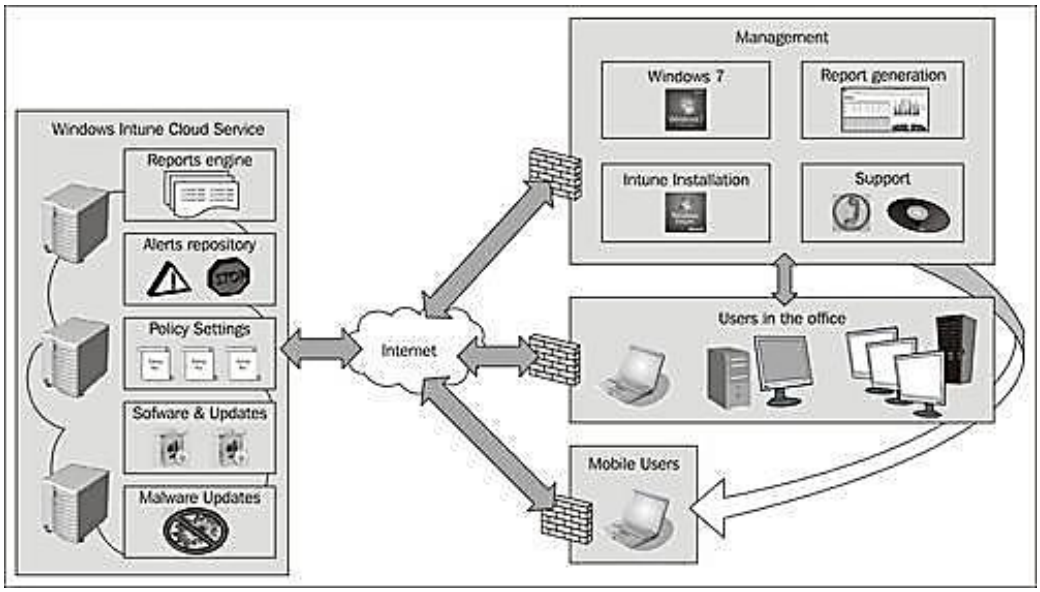
Käyttöjärjestelmät voidaan jakaa tietokoneille SCCM-ohjelman kautta. Vanhempi versio tuki vain työasemille jakoa, mutta uuden version myötä myös palvelinkoneille voidaan jakaa palvelinkäyttöjärjestelmä käyttäen siitä otettua kuvaa. (Rachui, Agerlund, Martinez, Daalmans 2012, kappale 1.)

Ohjelma tukee Wake-On-Lan -ominaisuutta ohjelmistojen jakelussa, tarkoittaen sitä, että koneen ollessa kiinni on Wake-On-Lan -ominaisuutta hyödyntäen mahdollista käynnistää suljettuna oleva tietokone vastaanottamaan ohjelmistojakelun. (Rachui, Agerlund, Martinez, Daalmans 2012, kappale 1.)

4.4 Windows Intune -palvelu

Windows Intune -palvelu on Microsoftin pilvipalveluna tarjoama SAAS-sovellus (Software As A Service), jolla voidaan jakaa päivityksiä ja sovelluksia verkon yli. Se on tarkoitettu pienille ja keskisuurille yrityksille, sekä yrityksille, joilla on tarvetta käyttää tietokoneita yrityksen ulkopuolelta. Tietokoneille, joiden halutaan käyttävän Intune-palvelua, on asennettava asiakasohjelma, jotta tietokone osaa yhdistää itsensä Intune-palveluun. Asiakaskoneen ollessa yhdistettynä ohjelmistoon ei sen tarvitse olla yrityksen toimialueessa saadakseen jaettavat sovellukset tai päivitykset. (Overton 2012, kappale 3).

Ylläpitäjällä ei ole tarvetta olla yhteydessä asiakastietokoneisiin, vaan riittää, että ylläpitäjä huolehtii Intune-palvelu ryhmäkäytänteistä, raporteista ja hälytyksistä. Kuvio 4 näyttää ratkaisun, jossa käyttöjärjestelmän ja Intune-ohjelmiston asentaa järjestelmänvalvoja päivityksien- ja ohjelmistojenjakelun tullessa pilvipalvelun kautta. (Overton 2012, kappale 3.)



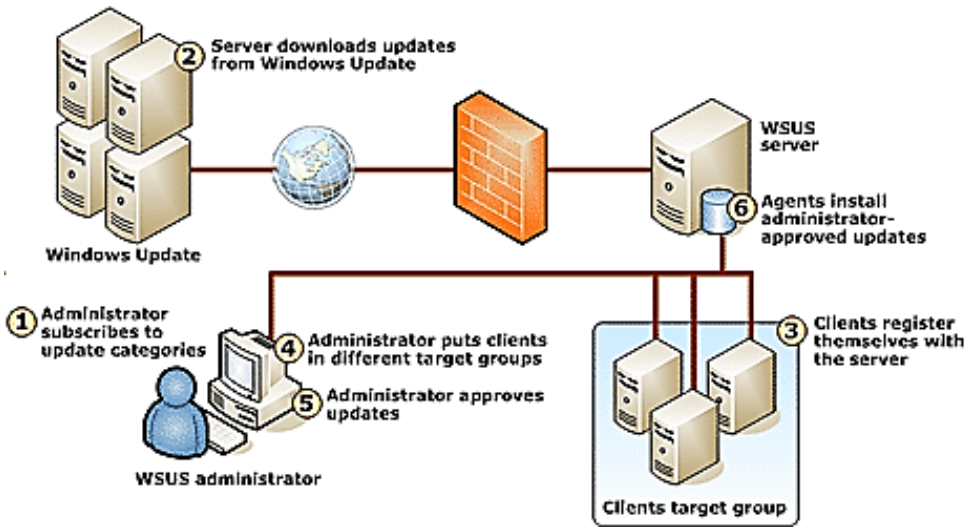
KUVIO 4. Windows Intune (Overton, 2012, kappale 3)

Intune-ohjelma vaatii Windows-käyttöjärjestelmistä business-version toimiakseen. Lisenssit Intune-ohjelmistoon ostetaan vastaten koneiden määrää. Ohjelmiston kautta jaettujen ohjelmien tulee tukea hiljaista asennusta (silent install) toimiakseen. Ohjelmien täytyy myös sijaita Intune-pilvipalvelun tallennustilassa. (Technet 2014c, hakupäivä 28.10.2014.)

4.5 Windows Server Update Services

Windows Server Update Services on Windows-palvelimille asennettava rooli. Alun perin se oli Microsoftin verkkosivuilta ladattava sovellus, mutta nykyään se on integroitu osaksi palvelinkäyttöjärjestelmää. Se kehitettiin helpottamaan päivityksien hallittavuutta tilanteessa, jossa jokainen kone piti manuaalisesti päivittää Windows Update -sivuston kautta. (Morimoto ym 2012, kappale 13.)

Päivitykset ladataan paikalliselle palvelimelle, jossa WSUS-rooli on asennettuna, Windows Update -palvelun kautta, jonka jälkeen päivitykset jaetaan keskitetysti sisäverkon kautta työasemille (kuvio 6). Tämä vähentää yrityksen verkon käyttöä tilanteessa, jossa useat yksittäiset tietokoneet lataisivat päivityksiä ulkoverkosta Windows Update -sivuston kautta. Päivitykset voi ajastaa latautumaan palvelimelle haluttuun kellonaikaan. (Morimoto ym 2012, kappale 13.)



KUVIO 5. Windows Server Update Services (Technet, 2014d, hakupäivä 26.11.2014)

WSUS-palvelu käyttää SQL-tietokantaa tallentaakseen metadataa päivityksistä ja tietokoneista. Metadatan avulla päätellään, onko päivitys tietokoneille tarpeellinen. WSUS-ohjelmiston raportit tulevat SQL-tietokannasta. Raportointiohjelma luo raportin tilanteesta, jossa työasema on viimeksi

ollut yhteydessä tietokantaan. Palvelinrooli antaa valittavaksi joko Windows Server -käyttöjärjestelmässä olevan sisäisen tietokannan (Windows Interal Database) tai ulkoisen tietokannan, kuten esimerkiksi Microsoft SQL Server. (Technet, 2014e, hakupäivä 26.11.2014.)

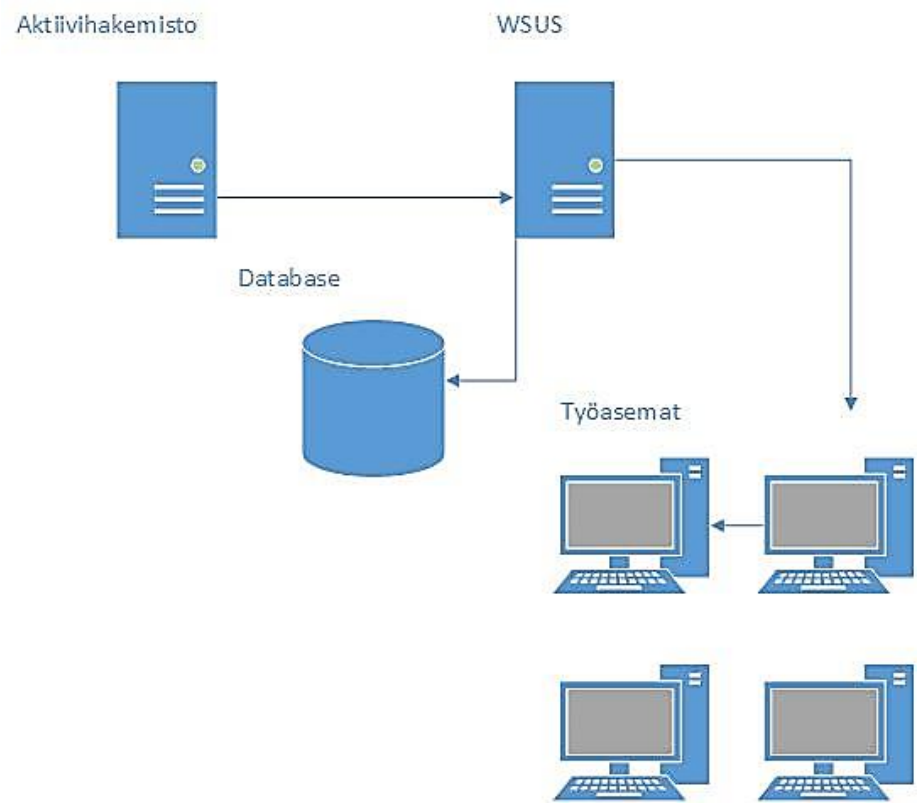
Ryhmäkäytänteiden kautta saadaan työasemat yhdistettyä WSUS-palveluun ja säädettyä työasemien päivityksiin liittyviä asetuksia. Ryhmäkäytänteillä luodaan sääntöjä muun muassa siitä, kuinka useasti työasema tarkistaa päivityksiä, minä päivänä ja mihin kellon aikaan päivityksiä asennetaan ja käynnistetäänkö tietokone uudelleen, kun päivitykset ovat asennettu. (Technet 2014f, hakupäivä 26.11.2014.)

WSUS-rooli tarjoaa Server Clean Up Wizard -ohjelman, jolla voidaan poistaa vanhoja työasemia tai palvelimia, jotka eivät ole käytössä, sekä vanhoja päivityksiä ja päivitystiedostoja palvelimelta. Email-notifications -toiminto lähettää sähköpostiin status-raportteja ja tietoja muun muassa siitä, milloin uusia päivityksiä on synkronoitu. (Panek, 2013, kappale 11.)

5 WINDOWS SERVER UPDATE SERVICES –PALVELUN KÄYTTÖÖNOTTO

Esivalmisteluina asennettiin kaksi erillistä palvelinta. Palvelimet olivat virtuaalisia. Palvelimia käytettiin Mcrosoft Hyper-V -virtualisointialustalla. Windows Server Update Services asennettiin toiselle ja SQL-palvelin toiselle palvelimelle. Molemmat palvelut olivat kiinni samassa toimialueessa. WSUS-ohjelmisto tarjoaa mahdollisuuden käyttää Windows-palvelimissa olevaa sisäistä Windows Interal Database -tietokantaa, mutta tässä opinnnäytetyössä käytettiin erillistä Microsoft SQL Server 2012 -tietokantaa. Palvelimille annettiin RAM-muistia 4 GB. Laitevaatimuksissa WSUS-ohjelmistolle vaadittiin tyypillisessä 500–3000 asiakasta sisältävässä asennuksessa minimissään 2 GB RAM-muistia ja 30GB kovalevytilaa. (Technet 2014g, hakupäivä 12.11.2014).

5.1 SQL-palvelimen asennus



KUVIO 6. Käyttäjätunnuksien selvennys

Kuviolla 6 selvennetään tietokannan ja aktiivihakemiston käyttäjätunnuksia. Toimialueen aktiivihakemistoon on luotu käyttäjätunnus. Tämä käyttäjätunnus on lisätty SQL-palvelimen käyttäjiin (Login). SQL-palvelimelta tunnukselle lisättiin roolit dbcreator, security admin ja public.

SQL-asennuksen yhteydessä SQL-instanssiksi nimettiin WSUSSQL ja SQL-palveluiden oletuskäyttäjätunnukset seuraavista rooleista vaihdettiin: SQL server Database Engine Account, SQL Server admin, Analysis Service Configuration account, Reporting Services Configuration account. Microsoft SQL Server Management Studion kautta SQL-palvelimelle laitettiin Max Degree of Parallelism arvoksi 1.

Palvelimelta avattiin palomuurista TCP-portit 1433, 60706 ja UDP-portti 1434. Palomuurisääntö pätee, kun tietokone on yhdistetty toimialueessa. Portit 1433 ja 1434 ovat SQL-serverin oletusportteja. Portti 60706 on satunnaislukuna generoitu portti, jota asiakas käyttää ollessaan yhteydessä SQL-palvelimeen. Asiakas avaa portin 60706 ja on yhteydessä palvelimeen TCP-portin 1433 kautta.

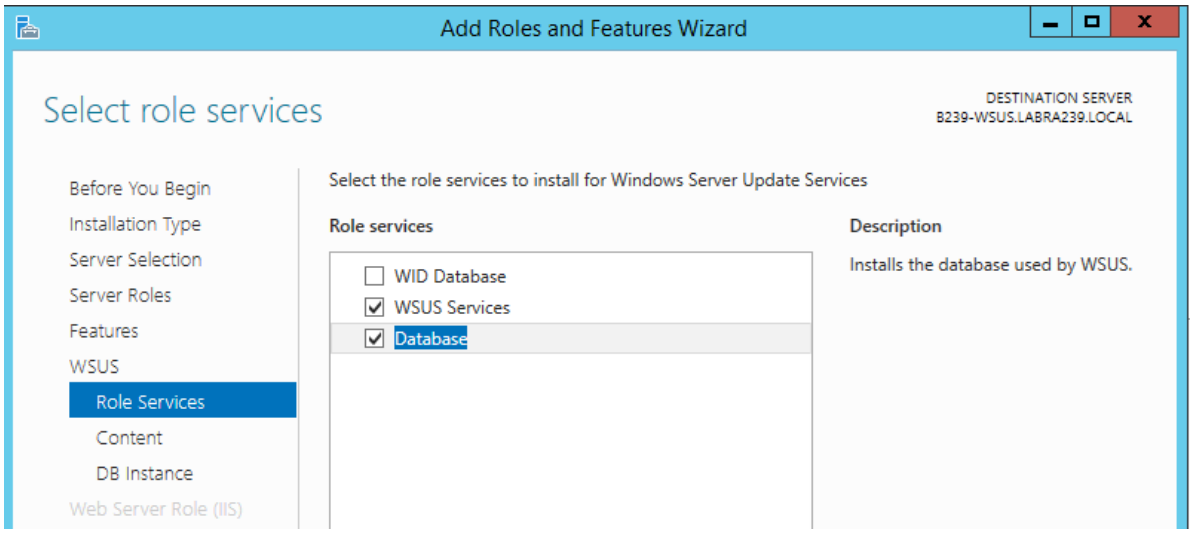
5.2 Windows Server Update Services -palvelimen asennus

WSUS-palvelimelle luotiin uusi datalevy päivityksille. Levy otettiin käyttöön levyhallinnassa. Levy luotiin, koska päivitykset vievät kovalevytilaa, eikä niiden tallennusta voi siis suositella käyttöjärjestelmän kanssa samaan osioon kiintolevyllä.

Rooli asennetaan järjestelmänvalvojan tunnuksilla. Roolin asennuksen yhteydessä tunnus lisätään automaattisesti WSUS-palvelimen käyttäjäryhmään WSUS administrators. Tunnuksesta tulee SQL-tietokannan omistaja. Roolia asennettaessa käyttäjätunnus on sama, kuin SQL-palvelimelle lisätty käyttäjätunnus.

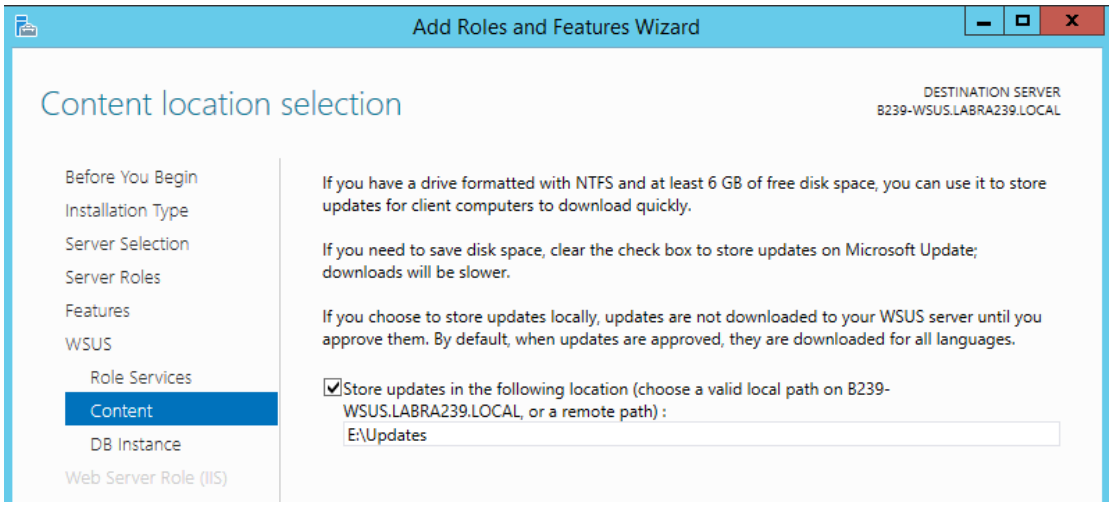
Asennus suoritettiin Server Managerin kautta roolin asennuksesta ja eteni normaalisti. Valittiin rooli, jonka jälkeen valittiin asennettavat ominaisuudet (feature). Tarvittavat ominaisuudet tulivat automaattisesti, kun rooli oli valittu.

Tietokanta-kohdassa oli valittavissa WID (Windows Interal Database) tai ulkoinen tietokanta (Database). Opinnäytetyössä käytettiin Microsoft SQL Server 2012 -ohjelmistoa, eli valitaan ulkoinen tietokanta (Kuvio 7).



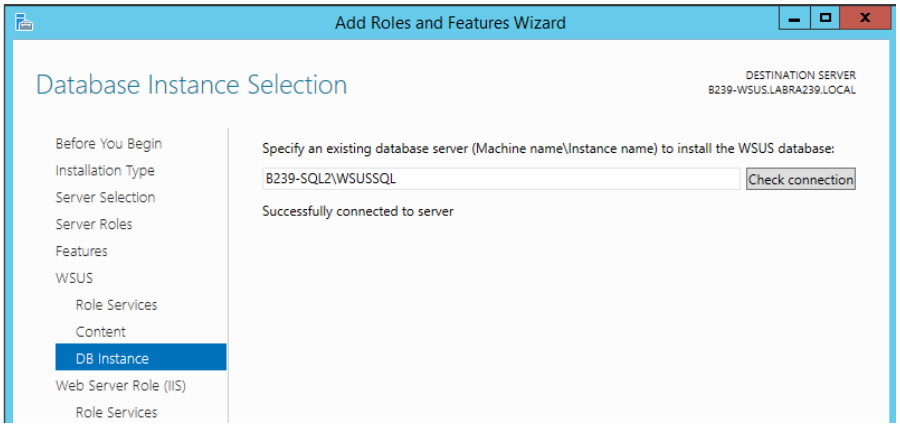
KUVIO 7. WSUS-tietokannan valinta

Päivityksille oli tehty erillinen virtuaalinen kovalevy. Tyypilliselle asennukselle (500–3000) kovalevytilaa suositeltiin 30GB (kuvio 8).



KUVIO 8. Päivitysten sijainti

Asennuksen yhteydessä yhdistettiin WSUS-palvelin tietokantaan. On huomioitava, että asennusta suorittavan käyttäjätunnuksen on pystyttävä kirjautumaan tietokantaan. Tämän jälkeen tarkennettiin WSUS-ohjelmalle SQL-palvelin ja SQL-palvelimen instanssi (kuvio 9).



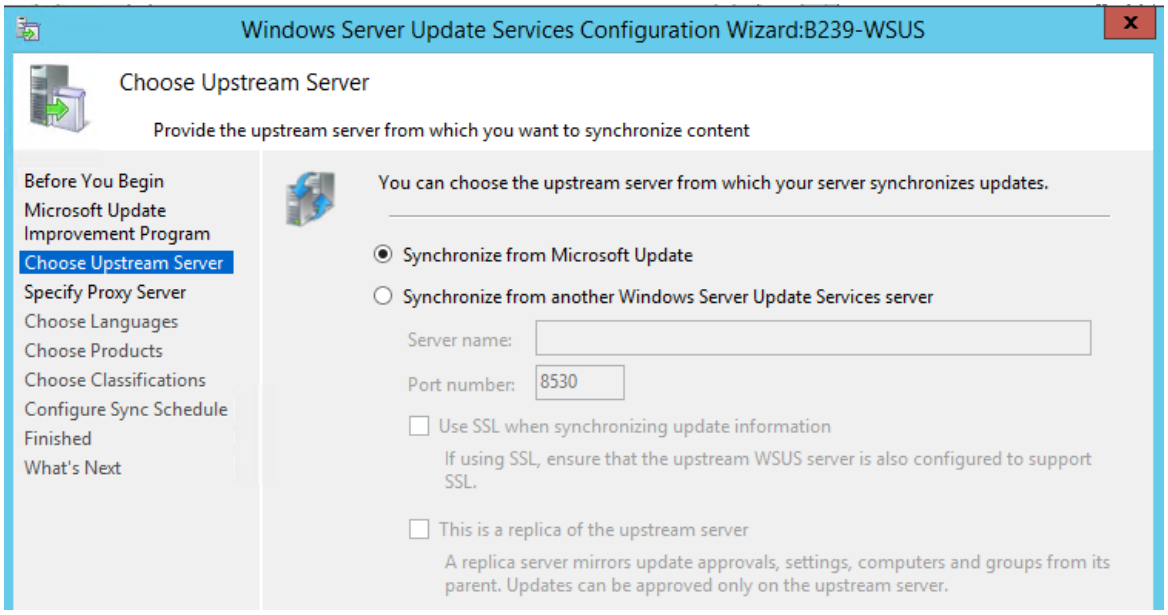
KUVIO 9. SQL-palvelimen- ja instanssin tarkentaminen

Valittiin vielä ominaisuudet Internet Information Service (IIS) -roolille. Tässä tapauksessa valittiin oletuksena olevat valinnat, jonka jälkeen suoritettiin asennuksen jälkeiset toimet (Post installation).

5.3 WSUS-palvelun konfigurointi

Roolin asennuksen jälkeen suoritettiin Windows Server Update Service -ohjelmiston käyttöönotto-asetukset. Asetukset asetettiin WSUS Configuration Wizardin kautta. Asetukset on mahdollista asettaa myöhemmin WSUS-konsolin kautta.

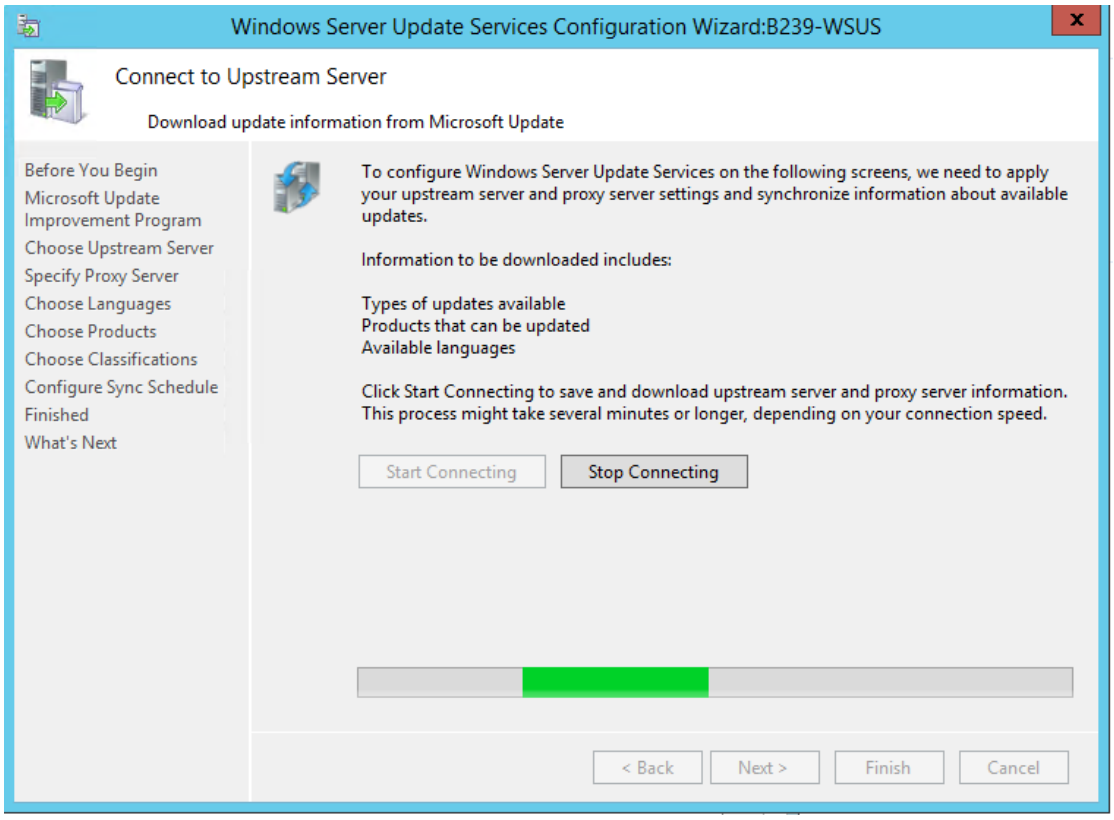
Valittiin, haetaanko päivitykset Windows Update -sivustolta, vai haetaanko ne toiselta WSUS-palvelimelta. Jos yritys on isompi, on mahdollista, että yksi WSUS-palvelin lataa päivitykset paikallisesti kovalevylle. Tähän palvelimeen on taas ketjutettu useampi WSUS-palvelin, jotka lataavat päivitykset tältä palvelimelta, jakaen päivityksiä eteenpäin (kuvio 10).



KUVIO 10. Mistä päivitykset haetaan?

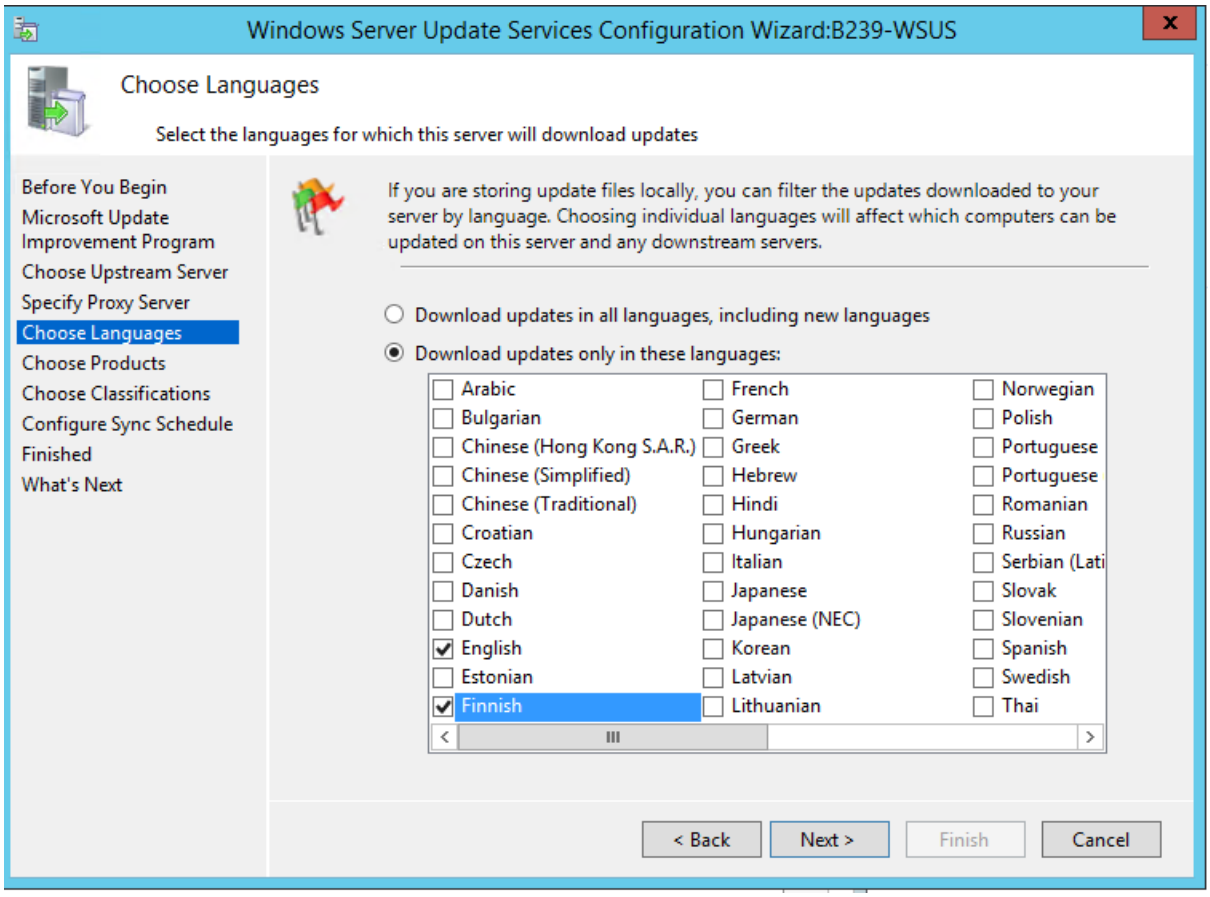
Tässä opinnäytetyössä ei käytetä välityspalvelinta (proxy server), joten kohta ohitettiin.

WSUS-palvelin yhdistettiin Windows Update -palveluun (kuvio 11).



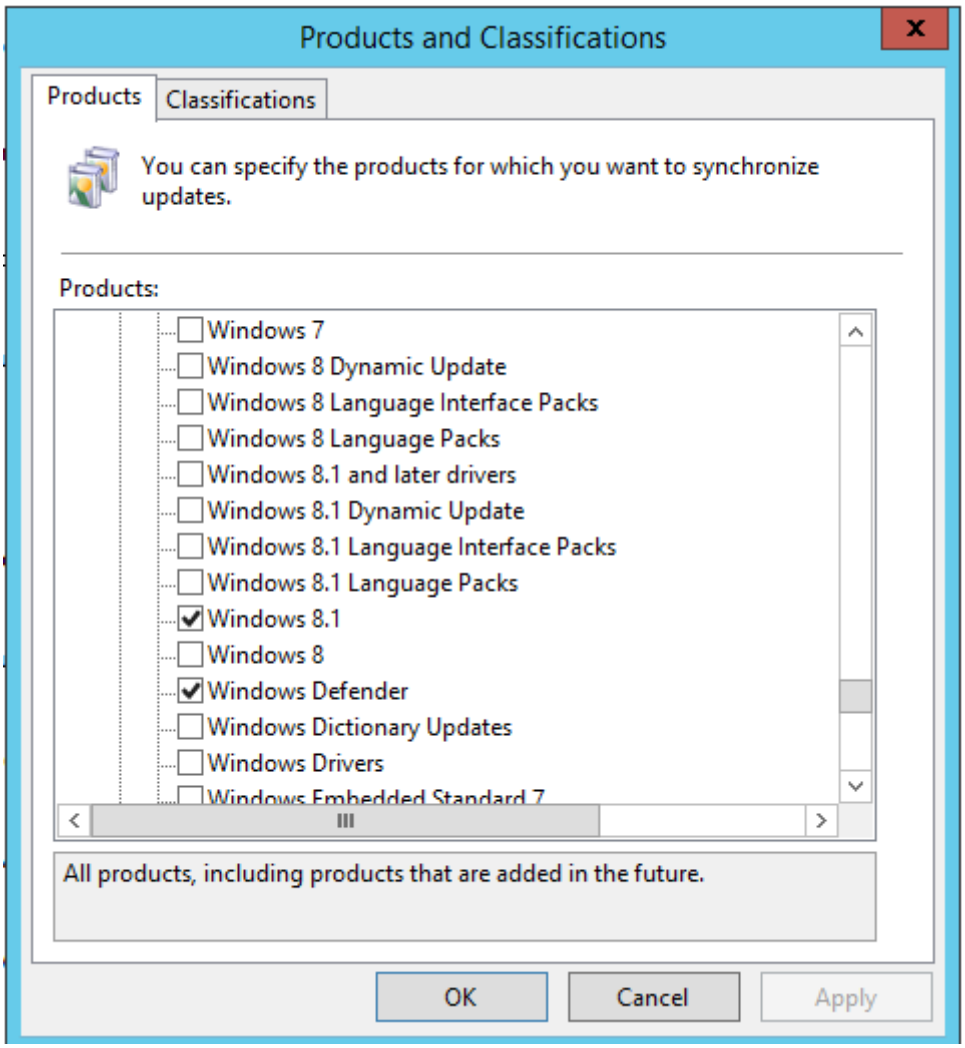
KUVIO 11. Synkronointi Windows Update -palveluun

Valittiin, mille kielille päivityksiä haetaan. Kun päivitykset ladataan tietokoneelle paikallisesti kovalevylle, on huomioitava, että mitä enemmän kielipaketteja on valittuna käyttöön, sitä enemmän kovalevytilaa käytetään. Opinnäytetyössä päivityksiä ladattiin suomen ja englannin kielille (kuvio 12).



KUVIO 12. Kielipakettien valinta

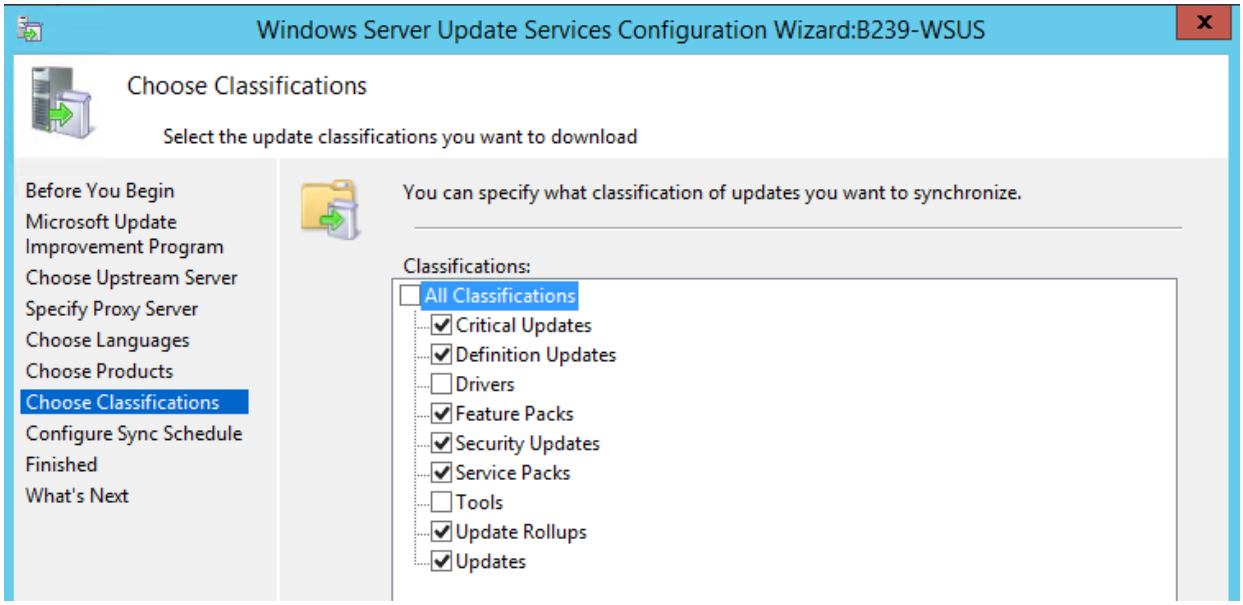
WSUS-ohjelmiston kautta on mahdollista ladata päivityksiä Microsoftin käyttöjärjestelmille, ohjelmille ja kolmansien osapuolien ajureille. Tässä opinnäytetyössä haettiin päivityksiä Office 2013 -ohjelmistolle, Windows 8.1 -käyttöjärjestelmälle ja Windows Defeder –ohjelmistolle (kuvio 13). Windows Defender on tarkoitettu torjumaan haittaohjelmia (Microsoft, hakupäivä 2.12.2014b).



KUVIO 13. Mille ohjelmistolle tai käyttöjärjestelmille päivityksiä haetaan

.

Valittiin, mitä päivityksiä haetaan (kuvio 14). Tästä opinnäytetyöstä rajattiin pois ajurit ja työkalut. Päivityksien termeistä kerrotaan opinnäytetyön sivuilla 11–12.

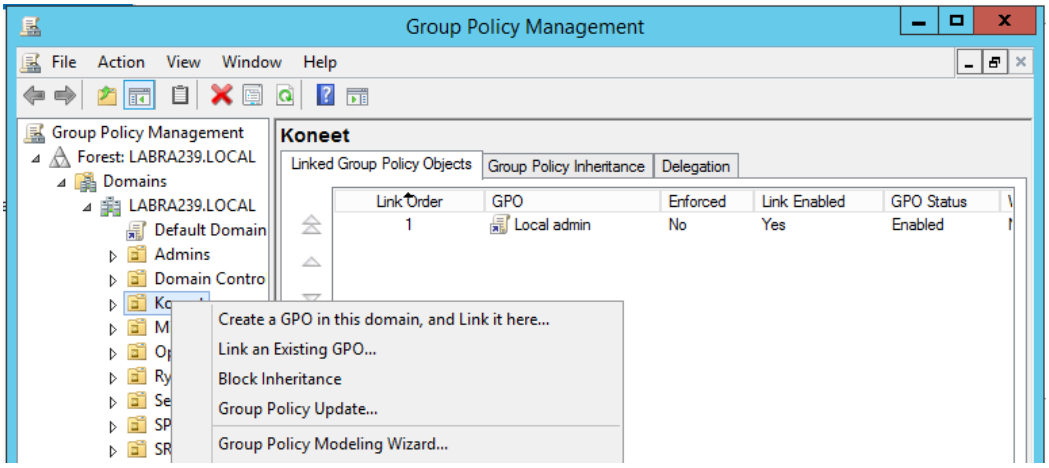


KUVIO 14. Päivityksien valinta

5.4 Ryhmäkäytänteet

Ryhmäkäytänteitä on mahdollista asettaa työasemille joko paikallisesti tai aktiivihakemiston kautta. Paikallisesti asennettavia ryhmäkäytänteitä käytetään lähinnä silloin, kun aktiivihakemistoa ei ole. Paikalliset ryhmäkäytänteet koskevat kaikkia käyttäjiä, mukaan lukien järjestelmänvalvojia. Tässä opinnäytetyössä tietokoneet ovat yhteydessä toimialueen aktiivihakemistoon. Aktiivihakemistossa on luotuna organisaatioyksikkö, johon tietokoneet, joiden halutaan käyttävän WSUS-ohjelmaa, on lisätty. Ryhmäkäytänteiden ollessa asetettuna organisaatioyksikölle koskee se kaikkia tietokoneita tai käyttäjiä jotka ovat lisättynä kyseiseen organisaatioyksikköön. Ryhmäkäytänteitä on sekä tietokonekohtaisia että käyttäjäkohtaisia. Tietokonekohtaisia asetuksia voivat olla esimerkiksi paikallisen palomuurin asetukset. Käyttäjäkohtaisiin asetuksiin voi kuulua esimerkiksi, ohjauspaneelin sisältö käyttäjälle. (Moskowitz 2013, kappale 1.) Tässä opinnäytetyössä ryhmäkäytänne on tietokonekohtainen ja koskee tietokoneiden päivitysasetuksia.

Ryhmäkäytänne lisättiin Group Policy Managerin kautta organisaatioyksikölle, jolle sääntöjen halutaan tulevan. Palvelimelle lisättiin WSUS-niminen käytänne (kuvio 15).



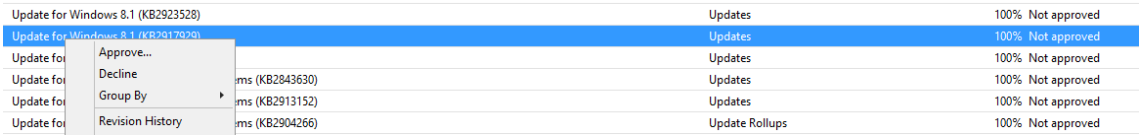
KUVIO 15. Ryhmäkäytänteen lisääminen

Tarvittavat ryhmäkäytänteet löytyvät Group Policy Management -konsolista sijannista: Computer Configuration\Policies\Administrative\Templates\Windows Components\Windows Update.

Ryhmäkäytänteet ovat opinnäytetyössä tietokonekohtaisia, ja ne säädettiin koskemaan päivityskäyttäytymistä. Tietokoneet näyttävät päivitysten ollessa asennettavana oletuksena tietokoneen sammutusvalikossa Install Updates and Shutdown -valinnan. Tietokoneet käynnistyvät automaattisesti valmiustilasta, jos päivityksiä on ajastettu asennettaviksi. Käyttäjille annetaan 45 minuuttia aikaa tallentaa tallentamattomat työt ennen tärkeiden päivityksien asennusta. Päivitykset asennetaan automaattisesti joka perjantaiyö. Työasemat tarkistavat päivityksiä joka 20. tunti WSUS-palvelimelta. Vaikka tietokoneet ovat yhteydessä WSUS-palvelimeen, tietokoneet tarkistavat tietoja ajoittain myös Windows Update -palvelusta. Kaikki käyttäjät pystyvät asentamaan päivityksiä. Päivitykset, jotka eivät vaadi uudelleen käynnistystä tai keskeytä palvelua, asennetaan heti. Jos päivityksiä on lykätty, ehdotetaan tietokoneen uudelleenkäynnistystä 30 minuutin kuluttua. Tietokoneen ajastetun uudelleenkäynnistyksen koittaessa tietokone odottaa 15 minuuttia ennen pakotetun uudelleenkäynnistyksen aloittamista. Mikäli asennukset lykkääntyivät ajastetussa asennuksessa edellisellä kerralla, odottaa tietokone uudelleenkäynnistyksen jälkeen 30 minuuttia ennen kuin aloittaa päivityksien asennuksen. Tietokoneet on määritetty lisättäväksi Tietokoneet-ryhmään WSUS-palvelussa. Päivitysten täytyy olla Microsoftin allekirjoittamia, jotta ne hyväksyttäisiin asennettavaksi.

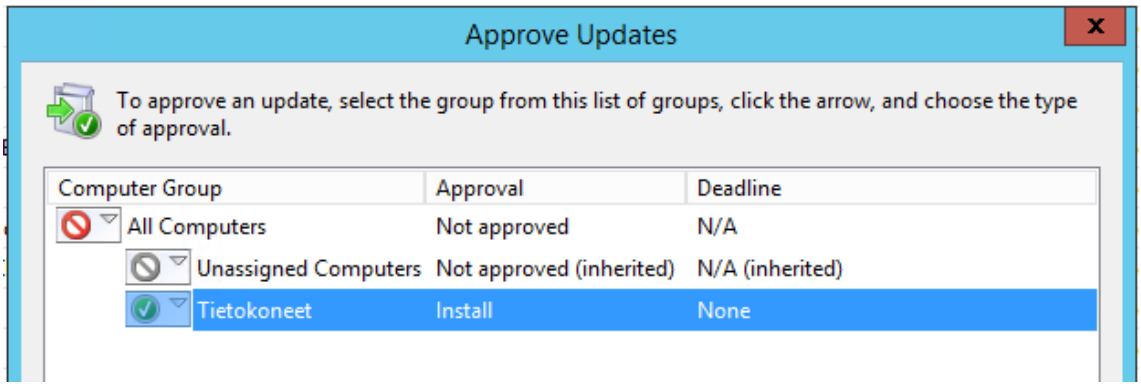
6 WINDOWS SERVER UPDATE SERVICES –PALVELUN KÄYTTÖ

Windows Server Update Services -palvelun kautta asetettiin kriittiset päivitykset ja tietoturvapäivitykset sekä tunnistetiedostot hyväksyttäväksi automaattisesti. Muut päivitykset on hyväksyttävä erikseen (kuvio 16).



KUVIO 16. Päivitysten hyväksyntä

Ohjelmistoon lisättiin Tietokoneet-ryhmä, johon aktiivihakemiston kautta liittyneet koneet sijoitettiin. Ryhmien kautta olisi mahdollista asettaa päivitykset testattavaksi yksittäiselle testitietokoneelle, jotta päivityksiä asennettaessa usealle koneelle ei tulisi odottamattomia ongelmia, mutta tarvetta sille ei tässä työssä koettu. Asennusta hyväksyttäessä valittiin ryhmä, jolle päivitysten haluttiin asentuvan (kuvio 17).



KUVIO 17. Hyväksyntä tietylle ryhmälle

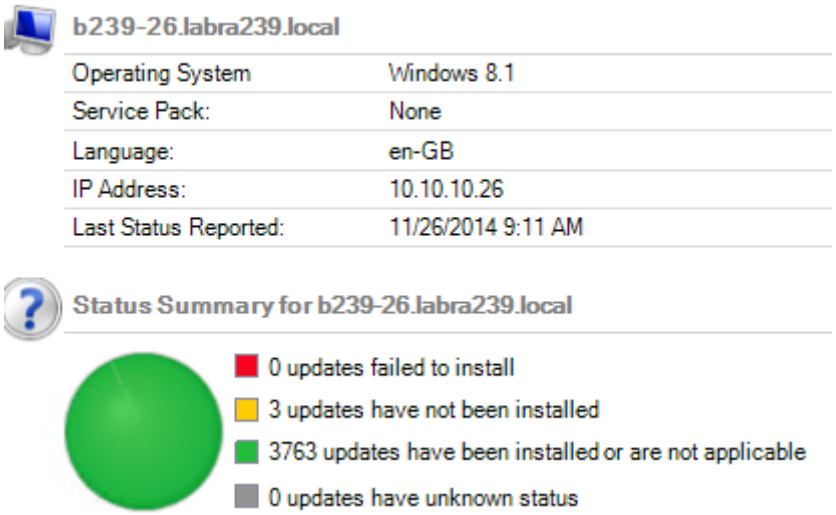
7 RAPORTOINTI

Opinnäytetyössä tarkasteltiin kahden eri ohjelman päivityksistä saatavia raportteja. Windows Server Update Services -sovelluksella tutkittiin ohjelman sisällä tapahtuvaa raportointia, ja lisäksi tarkasteltiin Microsoft Baseline Security Analyzer -ohjelman tuottamaa raporttia.

7.1 Windows Server Update Services -raportointi

Windows Server Update Services -ohjelma tarjoaa raportteja sekä yksittäisistä päivityksistä että yksittäisistä tietokoneista. Ohjelman kautta voidaan havaita, kuinka moni kone tarvitsee päivitystä, onko päivitys onnistunut ja kuinka monelle koneelle päivitys on asennettu. WSUS-ohjelmiston raportointi pohjautuu siihen, milloin tietokone on viimeksi ollut yhteydessä WSUS-palveluun.

Kuviossa 18 kuvatussa raportissa näkyy valitun tietokoneen päivitysten tila, mistä huomataan, että kolmea päivitystä ei ole asennettu. Tämä tarkoittaa sitä, että kolme päivitystä on hyväksytty asennettavaksi, mutta ne ovat tarpeettomia. Tietokone on siis asentamattomista päivityksistä huolimatta ajan tasalla.



KUVIO 18. WSUS-raportointi

7.2 Microsoft Baseline Security Analyzer

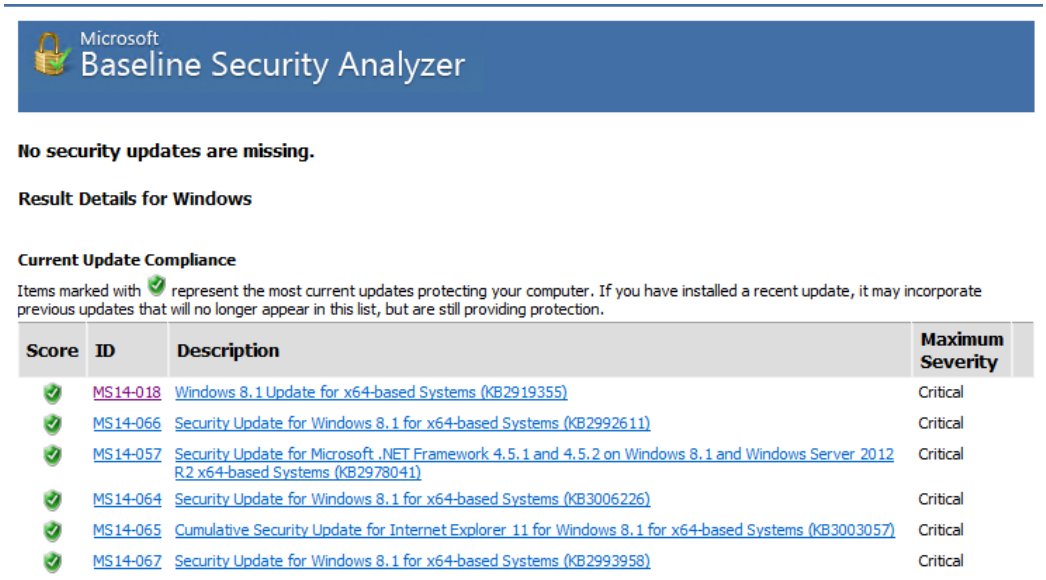
Microsoft Baseline Security Analyzer -ohjelman avulla voidaan tarkistaa tietokoneiden heikot salasanat ja ilman salasanaa olevat käyttäjätunnukset, Internet Information Services -roolin oletustietoturvan, SQL-palvelinohjelmiston version, pääkäyttäjän salasanan, sekä sen, käyttääkö SQL yhdistettyä autentikointia, eli voiko SQL-palvelimelle kirjautua sekä SQL-käyttäjätunnuksella että Windows -käyttäjätunnuksella. Lisäksi ohjelmalla tarkistetaan tietokoneiden päivitysten tila. MBSA-ohjelmalla voi tutkia paikallista tietokonetta tai tutkia tietokoneita etänä. Yksittäistä tietokonetta voidaan etsiä tietokoneen nimen tai IP-osoitteen avulla. Useita tietokoneita voi etsiä IP-osoitesarjan tai toimialueen nimen avulla. (Microsoft 2014c, hakupäivä 26.11.2014.)

MBSA-ohjelma vaatii, että File and Print sharing - ja Remote Registery -palvelut ovat päällä skannattaessa etäkoneita. Kohdekoneilla täytyy myös olla päivitysagentti (Update Agent) asennettuna ja automaattisen päivityspalvelun pitää olla päällä. MBSA-ohjelma käyttää TCP-portteja 135, 139 ja 455 ja UDP-portteja 137 ja 138 kommunikointiin etätietokoneiden välillä. Skannattavalla koneella tulee näiden porttien olla auki palomuurista. (Technet 2014h, hakupäivä 26.11.2014.)

Raportoinnissa MBSA-ohjelma käyttää sekä WSUS-palvelua, johon työasema on yhteydessä, että Windows Update -palvelua. Molempien palveluiden tuloksia verrataan keskenään, ja mikäli WSUS-palvelussa on hyväksymättömiä päivityksiä, merkitään ne raporttiin sinisellä tähdellä.

Skannattavat tietokoneet olivat etätietokoneita. Skannausta suorittavan käyttäjän oli oltava toimialueen järjestelmänvalvoja.

Kuviossa 19 on skannattu yksittäinen toimialueen tietokone. MBSA näytti kaikkiaan 36 viimeksi asennettua päivitystä kohdekoneelta. Tietokone oli raportin mukaan ajan tasalla.



Microsoft
Baseline Security Analyzer

No security updates are missing.

Result Details for Windows

Current Update Compliance

Items marked with represent the most current updates protecting your computer. If you have installed a recent update, it may incorporate previous updates that will no longer appear in this list, but are still providing protection.

Score	ID	Description	Maximum Severity
	MS14-018	Windows 8.1 Update for x64-based Systems (KB2919355)	Critical
	MS14-066	Security Update for Windows 8.1 for x64-based Systems (KB2992611)	Critical
	MS14-057	Security Update for Microsoft .NET Framework 4.5.1 and 4.5.2 on Windows 8.1 and Windows Server 2012 R2 x64-based Systems (KB2978041)	Critical
	MS14-064	Security Update for Windows 8.1 for x64-based Systems (KB3006226)	Critical
	MS14-065	Cumulative Security Update for Internet Explorer 11 for Windows 8.1 for x64-based Systems (KB3003057)	Critical
	MS14-067	Security Update for Windows 8.1 for x64-based Systems (KB2993958)	Critical

KUVIO 19. Microsoft Baseline Security Analyzer –raportti

8 JOHTOPÄÄTÖKSET

Ennen Windows Server Update Service -ohjelman asennusta ja käyttöönottoa päivitykset oli asennettava manuaalisesti Windows Update -palvelun kautta. Windows Update -ohjelman päivitykset oli helppo lykätä myöhemmäksi, jolloin päivitykset jäivät usein asentamatta. WSUS-palvelun avulla päivitykset saatiin automaattisesti jaettua työasemille. Palvelu jakaa automaattisesti vain kriittiset ja tärkeät päivitykset. Muut päivitykset järjestelmänvalvoja hyväksyy jaettavaksi WSUS-konsolissa.

Käyttöönoton jälkeen saatiin kriittiset ja tärkeät päivitykset jaettua automaattisesti asennettavaksi työasemille. Tietokoneet asentavat päivitykset ennalta määrättynä ajankohtana ryhmäkäytänteiden avulla. WSUS-palvelun käyttöönoton myötä tietokoneiden päivitys oli helposti hallittavissa ja asennukset voitiin suorittaa keskitetysti.

WSUS-palvelun raporteista on mahdollista tarkistaa, ovatko työasemien päivitykset ajan tasalla. On tosin huomattava, että raportit ovat tilanteesta, jossa tietokone on viimeksi ollut yhteydessä WSUS-palveluun. Myös yksittäisistä päivityksistä on saatavilla raportteja, joista voi tarkastella, mille koneille kyseinen päivitys on asennettu. Microsoft Baseline Security Analyzer -ohjelman ja WSUS-palvelun raportit erosivat toisistaan. Jos haluaa olla täysin varma, että tietokoneet ovat ajan tasalla, on hyvä käyttää molempia ohjelmia päivitysten tarkasteluun.

..

9 POHDINTA

Windows Server Update Service -palvelun käyttöönotosta järjestelmätukitietokonelaboratorioon sovittiin opinnäytetyön ohjaajan kanssa toukokuussa 2014. Työn aloitusajankohta oli syksyllä 2014. Työn tekemistä helpotti tuttu ympäristö: iso osa käymistäni kursseista on pidetty samassa laboratoriossa.

Opinnäytetyön tavoitteena oli asentaa ja ottaa käyttöön WSUS-palvelu ja SQL-palvelin. Palvelimet ja työasemat olivat kaikki virtuaalisia, mutta tämä ei vaikuttanut työn kulkuun. Ryhmäkäytänteet tulivat erilliseltä palvelimelta, jossa oli asennettuna aktiivihakemisto. Tämä palvelin oli asennettu valmiiksi ja ollut käytössä jo aiemmin.

Työ saatiin valmiiksi ajallaan, mutta työn olisi voinut aloittaa aikaisemminkin. Alun vaikeutena oli lähteiden löytäminen, mutta kun lähestymistapaa vaihdettiin, saatiin teoriaosuuden kirjoittaminens hyvin alkuun. Työ sujui ilman suuria ongelmia. Pohdintaa aiheuttivat käyttäjätunnukset ja ryhmäkäytänteet. Käyttäjätunnuksille tuli antaa tarvittavat käyttäjäoikeudet sekä WSUS-palvelimelle että SQL-tietokantaan. Päivitysten lataus ja asennus ryhmäkäytänteistä ajoitettiin aikaan, jolloin siitä ei ole haittaa tietokonelaboratorion opiskelijoille. Pohdittiin myös, voiko asennuksien jälkeistä automaattista uudelleen käynnistystä suorittaa, koska opiskelijoiden tunnukset voivat olla tietokoneella auki, joissa on töitä kesken.

LÄHTEET

Abbate, A. Amaris C. Droubi, O. Morimoto, R. Noel, M. & Yardeni, G. 2012. Windows Server 2012 Unleashed. Sams

Agerlund, K. Daalmans, P. Martinez, S. & Rachui, S. 2012. Mastering System Center 2012 Configuration Manager. Sybex.

Carpenter, T. 2012. Microsoft Windows Operating System: Essentials. Sybex.

F-secure 2014. Terminology. Hakupäivä 1.10.2014,
https://www.f-secure.com/en/web/labs_global/terminology

Gagne, G. Galvin, P. & Silberschatz, A. 2013. Operating System Concepts Essentials, Second Edition. John Wiley & Sons.

Limnéll, J. Majewski, K & Salminen M. 2014. Kyberturvallisuus. Jyväskylä: Docendo.

Microsoft 2014a. Tietoja automaattisista päivityksistä. Hakupäivä 30.9.2014,
http://windows.microsoft.com/fi-fi/windows/understanding-windows-automatic-updating#1TC=windows-7

Microsoft 2014b. Windows Defender. Hakupäivä 2.12.2014,
http://windows.microsoft.com/fi-fi/windows7/products/features/windows-defender

Microsoft 2014c. Microsoft Free Security Tools – Microsoft Baseline Security Analyzer. Hakupäivä 26.11.2014,
http://blogs.microsoft.com/cybertrust/2012/10/22/microsoft-free-security-tools-microsoft-baseline-security-analyzer/

Moskowitz, J. 2013, Group Policy: Fundamentals, Security, and the Managed Desktop, 2nd Edition. Sybex.

Overton, D. 2012. Microsoft Windows Intune 2.0: Quickstart Administration. Packt Publishing.

Panek, W. 2013. MCSA Windows Server 2012 Complete Study Guide.Sybex.

Rao, U. & Nayk, U. 2014. The InfoSec Handbook. Apress.

Rhodes-Ousley, M. 2013. Information Security The Complete Refrence, Second Edition. McGraw-Hill.

Rousku, K. 2014. Kyberturvaopas: tietoturvaa kotona ja työpaikalla

Technet 2014a. Manage SUSE Linux Using System Center Configuration Manager 2012 SP1. Hakupäivä 11.12.2014,
http://blogs.technet.com/b/meacoex/archive/2013/02/13/manage-suse-linux-with-system-center-2012-sp1.aspx

Technet 2014b. Introduction to Configuration Manager. Hakupäivä 16.10.2014,
http://technet.microsoft.com/fi-fi/library/gg682140.aspx

Technet 2014c. Prepare for software deployment with Microsoft Intune. Hakupäivä 28.10.2014,
http://technet.microsoft.com/en-us/library/dn646955.aspx

Technet, 2014d. WSUS overview. Hakupäivä 26.11.2014,
http://technet.microsoft.com/en-us/library/cc539281.aspx

Technet, 2014e. Overview of WSUS updates. Hakupäivä 26.11.2014,
http://technet.microsoft.com/en-us/library/dd939871%28v=ws.10%29.aspx

Technet, 2014f. Configure Automatic Updates by Using Group Policy. Hakupäivä 26.11.2014,
http://technet.microsoft.com/en-us/library/cc720539%28v=ws.10%29.aspx

Technet, 2014g Determine WSUS Capasity Requirements. Hakupäivä 12.11.2014,
http://technet.microsoft.com/en-us/library/cc708483%28v=ws.10%29.aspx

Technet, 2014h. Microsoft Baseline Security Analyzer FAQ. Hakupäivä 26.11.2014, http://technet.microsoft.com/en-us/security/cc184922