

Pekka Tamminen

# Lync Server 2010 -käyttöönotto

Metropolia Ammattikorkeakoulu  
Insinööri (AMK)  
Tietotekniikka  
Insinöörityö  
21.4.2012

Tekijä Otsikko	Pekka Tamminen Lync Server 2010 -käyttöönotto
Sivumäärä Aika	35 sivua + 3 liitettä 21.4.2012
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaajat	järjestelmäasiantuntija Juha Kemiläinen tietohallintopäällikkö Markku Aalto yliopettaja Janne Salonen
<p>Tämän insinööriyön tarkoituksena oli suunnitella, toteuttaa ja valvoa Lync Server 2010 -järjestelmän käyttöönotto Vahanen-yhtiölle. Työ koostui käyttöönoton suunnittelusta, toteuttamisesta, Lync-järjestelmän määrittelystä ja asentamisesta.</p> <p>Työn alussa tutustutaan Lync Server 2010:n komponentteihin, jotka ovat hyödyllisiä varsinkin Lync-järjestelmän ylläpitäjille. Tämän jälkeen kerrotaan Lync-infrastruktuurin luonnista Vahanen-yhtiölle ja yrityksen tarpeista kyseistä järjestelmää koskien. Seuraavaksi työssä esitellään Lync-järjestelmän asennusdokumentaatio. Lopuksi esitellään yhteenveto käyttöönoton onnistumisesta.</p> <p>Työn tuloksena Vahanen-yhtiö sai järjestelmän, joka tukee yrityksen viestintää, tiedonkulkua ja toimintatapoja.</p>	
Avainsanat	Lync 2010, Microsoft, yhdistetty viestintä, pikaviestintä

Author Title	Pekka Tamminen Lync Server 2010 deployment
Number of Pages Date	35 pages + 3 appendices 21 Apr 2012
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructors	System Specialist Juha Kemiläinen IT Manager Markku Aalto Principal Lecturer Janne Salonen
<p>The purpose of this Bachelor's thesis was to design, deploy and supervise the deployment of Lync Server 2010 to Vahanen Group. The study includes the planning and execution of deployment, as well as defining and actually installing of the Lync Server 2010.</p> <p>At the beginning of this study the components of Lync Server 2010 which are valuable to the system administrators of Lync Server 2010 are presented. The study proceeds by presenting the creation of the infrastructure of Lync and the company's needs for the system. Next, the report of the deployment procedure is presented. The study ends with a summary of the success of deployment.</p> <p>As a result of this study, Vahanen Group got a system which supports the company's communication, flow of information and procedures.</p>	
Keywords	Lync 2010, Microsoft, Unified communications, instant messaging

## Sisällys

1	Johdanto	1
2	Lync Server 2010	1
2.1	Aktiivihakemisto	2
2.2	Planning Tool	2
2.3	Topology Builder	2
2.4	Control Panel	3
2.5	Management Shell	3
2.6	Best Practices Analyzer	4
2.7	Lync-asiakasohjelmat	4
3	Käyttöönotto	5
3.1	Infrastrukturi	5
3.2	Käyttöönoton suunnittelu ja seuranta	6
3.3	Topologian suunnittelu	6
3.4	Työasema-asennukset	9
4	Järjestelmän asennus	9
4.1	Lync Server 2010 Front End -palvelimen asennus	9
4.1.1	Active Directoryn valmistelu	13
4.1.2	Topologian asennus ja julkaisu	16
4.2	Lync Server 2010 Edge -palvelimen asennus	19
4.3	Lync Server 2010 Reverse proxy	26
4.4	Lync Server 2010 Mobility ja Autodiscover	29
4.5	Ylläpidolliset toimet ja palomuurimääritykset	33
5	Yhteenveto	34
	Lähteet	36
	Liitteet	
	Liite 1. Lync Server 2010 -palomuurimääritykset	
	Liite 2. Kuvien lisääminen aktiivihakemistoon	
	Liite 3. Käyttäjien tuominen/poistaminen Lync-järjestelmään	

## 1 Johdanto

Vahanen-yhtiö on yksi Suomen suurimmista rakennus- ja kiinteistöalan asiantuntijaorganisaatioista, jonka palveluksessa työskentelee nykyään noin 400 asiantuntijaa 15 eri toimipisteessä. Yritys tarjoaa rakennesuunnittelua, arkkitehtuuria, erikoisasiantuntijapalveluita, talotekniikkaa, kiinteistöjohtamista, taloyhtiöpalveluita, ympäristöpalveluita ja kansainvälisiä palveluita. Asiantuntijoiden suuri määrä ja organisaation laajuus tuovat haasteita perinteiseen viestintään ja yhteydenpitoon.

Tämä insinöörytyö sai alkunsa vuoden 2011 kesänä, jolloin Vahanen-yhtiön tietohallintopäällikkö Markku Aallolle ehdotin insinöörytyön aloittamista vuoden 2012 tammikuussa. Yhteistuumin päätimme Lync Server 2010:n olevan varsin hyvä työn kohde. Lync Server 2010 oli jo itselleni tuttu Metropolia Ammattikorkeakoulun Ammatillisesti suuntaavaprojekti -kurssilta, jossa valitsin työkseni tällöin juuri ilmestyneen Lync Server 2010 -järjestelmän. Tämä työ käsitteli yksinkertaisimman Lync-käyttöönoton.

Tässä insinöörytyössä esitellään Lync Server 2010 -käyttöönottoon Vahanen-yhtiölle käsiteltäviä vaiheita, asennuksen dokumentaatiota ja yhteenvedon lopputuloksista. Lisäksi työssä tutustutaan Lync Server 2010:n yleisimpiin tarvittaviin työkaluihin ja ohjelmiin. Tavoitteena oli tehdä Vahanen-yhtiölle järjestelmä, joka tukee viestintää ja tiedonkulkua, tehostaa toimintatapoja, vähentää tietohallinnon työkuormaa ja tuo kustannussäästöjä.

## 2 Lync Server 2010

Lync Server 2010 on Microsoftin työkalu yhdistettyyn viestintään. Lync Server 2010 tunnettiin aikaisemmin nimellä Microsoft Office Communicator. Lynciä voisi verrata helposti Microsoft Messenger- ja Skype-sovelluksiin, mutta Lync on suunnattu suoraan yrityksille.

Ominaisuuksia, joita Lync Server 2010 tarjoaa, ovat esimerkiksi pikaviestit, puhelut, videopuhelut, näytön jakaminen, PowerPoint-esityksen näyttö, äänestykset, valkotaulu, puhelu- ja videokonferenssit. Lisäksi Lync-järjestelmän pystyy integroimaan suoraan puhelinverkkoon, jolloin Lyncistä voisi soittaa suoraan esimerkiksi kännykkäliittymään.

## 2.1 Aktiivihakemisto

Aktiivihakemisto (Active Directory) on Microsoftin käyttämä hakemistopalvelu. Aktiivihakemisto on tärkeä osa Windows-ympäristöä: se autentikoi käyttäjät ja sillä hallitaan muun muassa käyttäjiä, ryhmiä ja tietokoneita. Aktiivihakemiston yksi keskeisistä käsitteistä on toimialue, johon kaikki verkon Windows-tietokoneet pääasiassa kuuluvat.

Aktiivihakemistoa hallitaan Active Directory Users and Computers -nimisen työkalun avulla.

## 2.2 Planning Tool

Planning Tool on Microsoftin julkaisema työkalu Lync Server 2010 -topologian suunnitteluun. Työkalulla määritellään halutut komponentit omaan Lync-infrastruktuuriin, kuten halutaanko mahdollistaa ulkoisten käyttäjien ja liittoutumien käyttö Lyncissä, halutaanko ottaa käyttöön puhelinoperaattori tuki (PSTN) käyttöön, halutaanko julkaista monitorointi-, arkisto- tai erillinen tietokantapalvelin infrastruktuuriin.

Työkalu julkaisee lopuksi valmiin infrastruktuurin, johon täytyy määrittää IP-osoitteet ja täydelliset toimialuenimet. Työkalu julkaisee myös palomuuriasetukset ja DNS-nimet, joita infrastruktuuri vaatii. Lisäksi topologian pystyy viemään suoraan Topology Builderissa käytettävään tiedostomuotoon, ja näin mahdollistaa topologian viemisen Lynciin.

## 2.3 Topology Builder

Topology Builder on Lync-topologian hallintatyökalu. Tällä työkalulla voidaan lisätä tarvittaessa esimerkiksi monitorointi-, edge- tai arkistointipalvelimen infrastruktuuriin. Tällä hallinnoidaan myös Lyncin SIP-toimialueita ja verkkosoitteita, joita Lync käyttää.

Haluttujen muutosten jälkeen topologia julkaistaan ja on tällöin käytettävissä. Topologian muuttaminen ei aiheuta katkoksia käytössä, ellei muuteta kriittisiä asetuksia, jotka voivat aiheuttaa yhteysongelmia käyttäjillä.

## 2.4 Control Panel

Lync Server 2010 -palvelinta voidaan hallita Lync Server 2010 Control Panel -ohjelmalla. Ohjelman hallintamahdollisuuksiin kuuluu

- käyttäjien hallinta
- topologian ominaisuuksien ja tilojen seuranta
- tiedostopäätteiden sääntöjen hallinta, tiedostojen jaossa
- puheluiden reitityksien ja ominaisuuksia (Enterprise voice)
- soittoryhmien hallinta
- puhelin- ja videoneuvotteluiden asetusten hallinta
- asiakasohjelmien- ja laitteiden hallinta
- ulkopuolisten käyttäjien pääsyn hallinta
- liittoutumien (federation) hallinta
- monitoroinnin ja arkistoinnin määrytykset
- verkkoasetukset, kuten tiedonsiirron määrät eri aliverkoissa.

## 2.5 Management Shell

Lync Server 2010 Management Shell on edistyksellisempi työkalu Lync-järjestelmän hallintaan. Management Shell -työkalulla onnistuu käyttäjien lisääminen Lync-järjestelmään erittäin helposti. Työkalusta löytyy paljon mahdollisuuksia joita Lync Server 2010 Control Panel ei tarjoa, kuten esimerkiksi "Set-CsClientPolicy", joka mahdollistaa muun muassa, saako käyttäjä käyttää omaa kuvaa Lync-järjestelmässä. Kaiken kaikkiaan Lync-järjestelmän PowerShell-kirjasto sisältää noin 550 komentoa.

## 2.6 Best Practices Analyzer

Microsoft Lync Server 2010 Best Practices Analyzer on työkalu Lync Server 2010 -topologian validointiin. Best Practices Analyzer kerää Lync Server 2010 -topologian määrittäykset ja selvittää, onko määrittäykset tehty Microsoftin ohjeiden mukaan. [9.]

Työkalu palauttaa listan ongelmista, kuten määrittäyksiä optimoinnista, ei tuetuista vaihtoehtoista, puuttuvista päivityksistä tai määrittäyksistä, joita Microsoft ei suosittele. [9.]

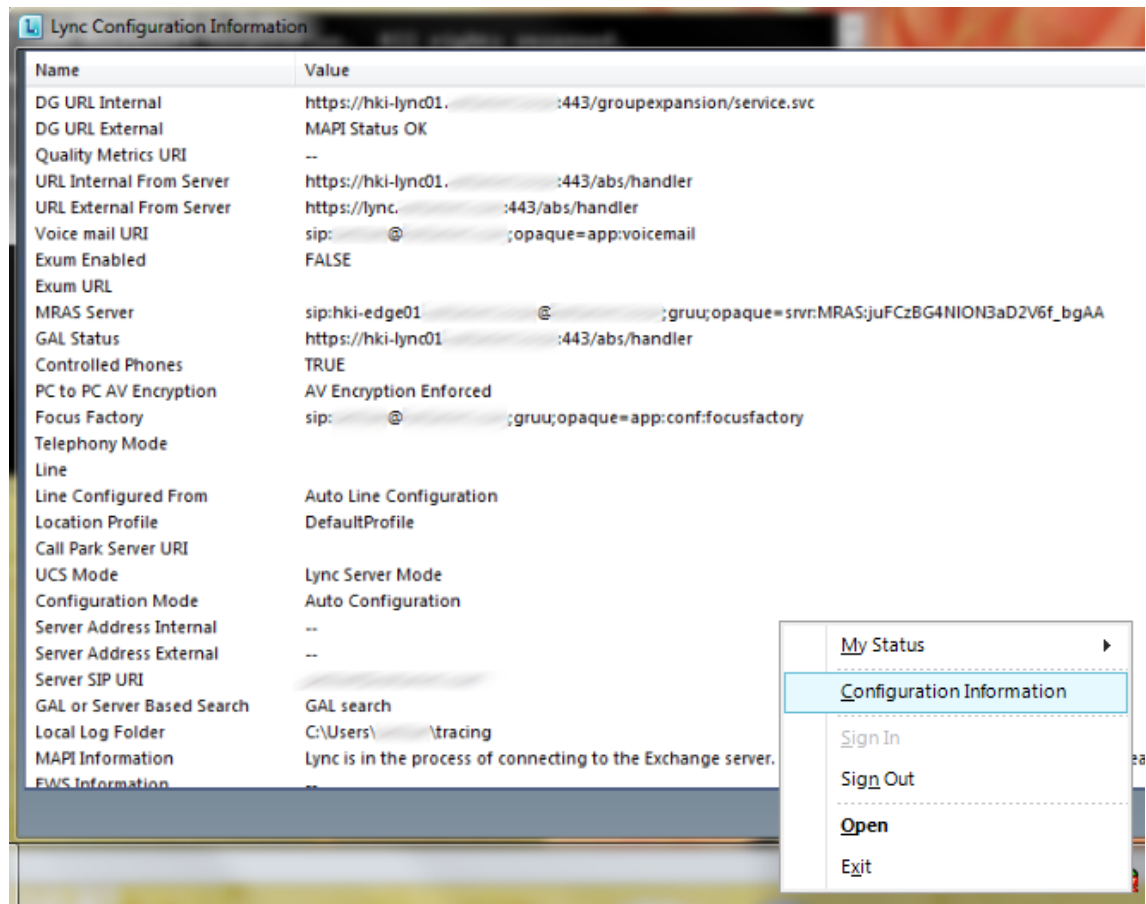
## 2.7 Lync-asiakasohjelmat

Lync-järjestelmässä toimivat seuraavat asiakasohjelmat:

- Lync 2010 (erilliset 32-, ja 64 bittiset asiakasohjelmat)
- Lync 2010 Attendee
- Lync 2010 Attendant
- Lync for Mac
- Communicator for Mac
- Lync Web App
- Lync 2010 Phone Edition (iOS, Android, Symbian^3 Belle).

Lync 2010 -asiakasohjelman käyttämiä asetuksia pystyy seuraavaan painamalla CTRL-näppäintä pohjassa ja oikealla hiirennäppäimellä Lync-kuvaketta Windows-käyttöjärjestelmän ilmoitusalueella. Tämä on erityisen hyödyllistä tietoa varsinkin vian-selvitysvaiheissa.





Kuvio 1. Lync 2010 -asiakaspäätteen asetukset.

### 3 Käyttöönotto

#### 3.1 Infrastrukturi

Vahanen-yhtiön IT-ympäristö koostuu toimialueesta, jonka keskipisteenä on Leppävaaran toimipisteen palvelinkeskus. Lisäksi yhtiön sisäverkko ulottuu Kannelmäkeen, Hämeenlinnaan, Lahteen, Turkuun, Poriin, Lappeenrantaan, Jyväskylään, Viroon, Romaniinaan, Intiaan ja Arabiemiraatteihin.

Yrityksen ratkaisut ovat pääasiassa Microsoft-pohjaisia, joten integroituminen Lync Server 2010 -järjestelmään on hyvä. Yrityksestä löytyy jo valmiiksi Microsoftin Aktiivihakemisto ja sertifiikaattipalvelin, joten näiden asennuksia ei tässä työssä käsitellä.

### 3.2 Käyttöönoton suunnittelu ja seuranta

Insinööriyön käyttöönoton aluksi tein projektisuunnitelman, joka sisältää projektin tavoitteet ja tehtävät, rajaukset ja liittymät, osittelun ja vaiheistukset, aikataulut ja resurssisuunnitelmat, budjetin ja kustannusohjauksen, muutosten hallinnan, dokumentaation määritykset, projektin riskien hallinnan, projektin etenemisen seurannan ja projektin päättämisen.

Ensimmäinen projektin ohjausryhmä pidettiin 5.1.2012 tietohallintopäällikkö Markku Aallon ja järjestelmäasiantuntija Juha Kemiläisen kanssa. Ohjausryhmässä käytiin läpi projektin tavoitteet, projektin seuranta, työtehtävät, infrastruktuuri ja tarvittavat materiaalit.

Ensimmäiset testikäyttäjät Lync-järjestelmä sai helmikuun alussa, jolloin kaikista yksinkertaisin Lync-järjestelmä oli asennettu. Asennus jatkui ulkoisten yhteyksien osalta. Lisäksi keräsin uusia testikäyttäjiä järjestelmälle.

Maaliskuussa asennukset olivat pääasiassa kunnossa, joten suunnittelin käyttöönotolle aikataulutuksen, ohjeistukset ja tiedotteen yksikön päälliköille tulevasta käyttöönotosta. Puolesta välissä kuukautta käyttäjät saivat oman tiedotteen ja ohjeistukset intranet-järjestelmään. Huhtikuun alussa kaikilla käyttäjille oli asentunut Lync-asiakaspääte.

### 3.3 Topologian suunnittelu

Planning tool for Microsoft Lync Server 2010 on työkalu, joka auttaa suunnittelemaan Lync Server 2010 -topologian. Planning tool havainnollistaa ja määrittelee topologian komponentit, täydelliset toimialuenimet (FDQN), IP-osoitteet, palomuuriasetukset ja muuta. Planning tool -työkalulla voi suunnitella erilaisia topologioita ja vertailla näiden sovellutuksia omaan infrastruktuuriin. Tämä pystyy myös hyödyntämään luotua topologiaa viemällä sen XML-tiedostossa Topology Builderiin. [1: s.100.]

Yrityksen vaatimukset järjestelmälle olivat, että tämä toimii sekä sisä- että ulkoverkossa. Lisäksi jatkossa olisi mahdollisuus myös mobiililaitteilta mahdollisuus päästä Lync-yhteyteen. Enterprise Voice-, arkistointi- ja monitorointipalveluiden ei katsottu olevan tarpeellisia tässä vaiheessa. Yrityksen toivomuksena oli, että Microsoft Exchange Server

2010 Outlook Web Accessin käyttämää Microsoft Threat Management Gateway -palvelinta pystyisi hyödyntämään Lync Server 2010 Reverse Proxyna.

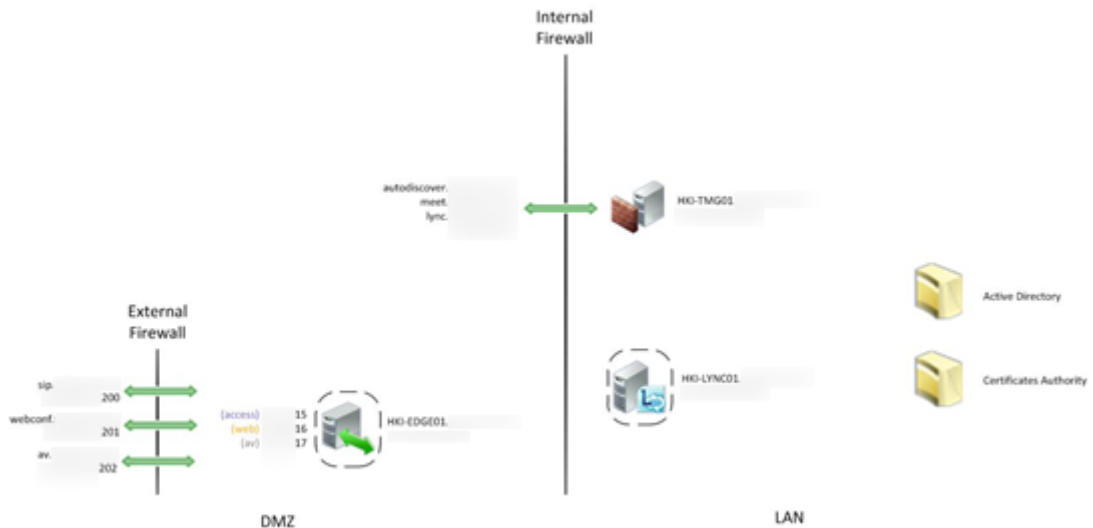
Lync Edge serverin voi julkaista joko 1 tai 3 IP-osoitteella. Näiden edut ja haitat on esitetty Taulukossa 1.

Taulukko 1. Lync Edge Serverin vertailu julkaisemalla yhdellä tai kolmella IP-osoitteella [2.]

	<b>Hyödyt</b>	<b>Haitat</b>
<b>Yksi täydellistä toimialuenuimeä &amp; IP-osoitetta</b>	<p>Vähentää julkisten sertifikaattien tarvetta.</p> <p>Vähentää julkisten DNS-nimien tarvetta.</p> <p>Kustannussäästöt ostettaessa sertifikaatteja ja IP-osoitteiden hankinnassa</p>	Joutuu standardi porttien sijasta käyttämään portteja, jotka saattaa aiheuttaa yhteysongelmia verkoissa, jotka estävät ei standardit portit.
<b>Kolme täydellistä toimialuenuimeä &amp; IP-osoitetta</b>	Mahdollisuus käyttää standardi portteja (443,https), vähentää palveluun kohdistuvia ongelmia verkossa.	<p>Lisää julkisten sertifikaattien tarvetta.</p> <p>Lisää julkisten DNS-nimien tarvetta.</p> <p>Lisää julkisten IP-osoitteiden tarvetta.</p>

Ensimmäisessä projektin ohjausryhmässä päätettiin käyttää kolmen IP-osoitteen vaihtoehtoa. Lisäksi mietittiin vaihtoehtoa sertifikaatin hankinnalle. Sertifikaatin tulisi tukea SAN-nimien käyttöä sertifikaateissa; näin yhden sertifikaatin tilaaminen voisi riittää. Kuitenkin tulimme tulokseen, että tilaisimme sertifikaatin, joka kattaa kaikki toimialueen alinimet (wildcard).

Vaatimusten perusteella suunnittelin Lync Server 2010 -topologian, Planning tool for Microsoft Lync Server 2010 -työkalua hyödyntäen. Topologia on esitetty kuvassa 1.



Kuvio 2. Suunniteltu topologia Vahanen-yhtiöille.

Topologia sisältää Lync Front End-, Lync Edge-, Certification Authority-, Active Directory ja Threat Management Gateway palvelimet. Lync Edge -serverillä on 2 verkkokorttia, ja 3 IP-osoitetta DMZ-verkkoalueella.

Taulukko 2. Lync Server 2010 -topologian verkko-osoitteet

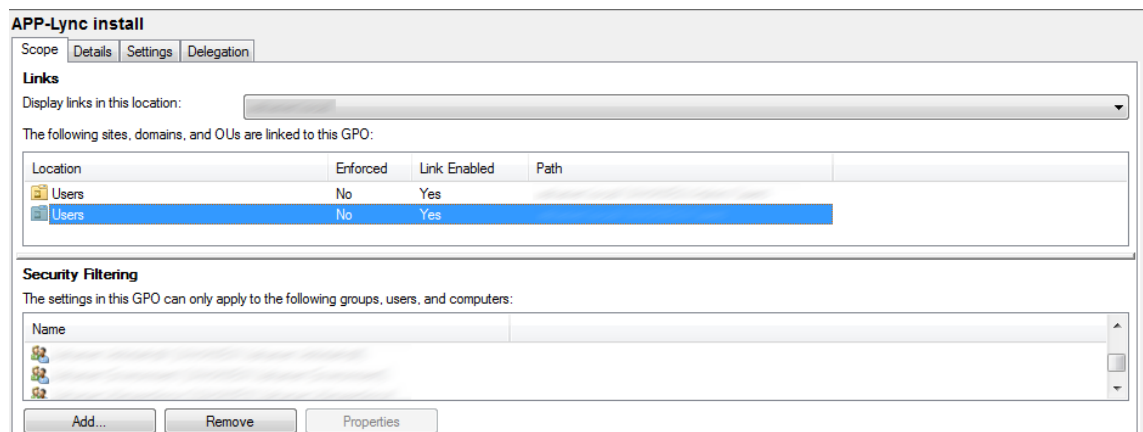
Julkinen IP	Sisäinen IP	Verkkonimi
xxx.xxx.xxx.200	xxx.xxx.xxx.15	sip.yritys.domain
xxx.xxx.xxx.201	xxx.xxx.xxx.16	webconf.yritys.domain
xxx.xxx.xxx.202	xxx.xxx.xxx.17	av.yritys.domain
xxx.xxx.xxx.203	xxx.xxx.xxx.104	lync.yritys.domain
xxx.xxx.xxx.203	xxx.xxx.xxx.104	meet.yritys.domain
xxx.xxx.xxx.203	xxx.xxx.xxx.104	dialin.yritys.domain

xxx.xxx.xxx.203	xxx.xxx.xxx.104	lyncover.yritys.domain
-----------------	-----------------	------------------------

Topologia esitettiin projektinohjaajille, jotka hyväksyivät kyseiset määritykset, joten muutoksia ei tarvinnut enää tässä vaiheessa tehdä.

### 3.4 Työasema-asennukset

Työasema-asennukset suoritettiin yksiköittäin kahden päivän välein käyttäjille. Tämän ansiosta tarvittaviin yhteydenottoihin pystyttiin vastaamaan, eivätkä työt kerääntyneet yhdelle päivälle. Asennus tapahtui Group Policy -työkalun avulla lisäämällä käyttöönottoaiheessa olevan yksikön ryhmä kyseiseen Group Policyyn.



Kuvio 3. Työasema-asennukset Group Policy -työkalussa.

## 4 Järjestelmän asennus

### 4.1 Lync Server 2010 Front End -palvelimen asennus

Laitteistosuosituksia Lync Server 2010 -järjestelmälle on esitetty taulukossa 3.

Taulukko 3. Lync Server 2010 laitteistovaatimukset [3.]

	<b>Suositus/vaatus</b>
<b>Prosessori</b>	64-bittinen kaksi- tai neliydinprosessori, 2,0 GHz tai enemmän.
<b>Muisti</b>	16 GB
<b>Kovalevy</b>	Vähintään 72 GB vapaata tilaa kovalevyllä 10 000 RPM kierrosnopeudella.
<b>Verkko</b>	1 verkkokortti 1 Gbps nopeudella. 2 verkkokorttia suositeltu.
<b>Käyttöjärjestelmä</b>	Windows 2008 x64 SP2, Windows 2008 R2

Lync Front End -palvelinta varten loin VMware vSphere -alustalle Microsoft Windows Server 2008 R2 -palvelimen, johon on lisätty 120 GB kovalevy, 3 GB muistia, 2 vCPU ja 1 verkkokortti. Muisti on suosituksia vähäisempi, koska suositukset on tehty paljon isommille infrastruktuureille.

Lync Server 2010 -järjestelmän ohjelmisto edellytykset ovat Windows PowerShell 2.0 komentoriympäristö, Microsoft .NET Framework 3.5 SP1, Windows Installer 4.5, Windows Media Format Runtime, Message Queuing, IIS ja tietokanta palvelin. Lisäksi Lync Server 2010 Control Panel vaatii toimiakseen Microsoft Silverlight 4 -lisäosan. IIS:n vaatimat moduulit ovat [4.]

- Static Content
- Default Document
- HTTP Errors
- ASP.NET
- .NET Extensibility
- Internet Server API (ISAPI) Extensions

- ISAPI Filters
- HTTP Logging
- Logging Tools
- Tracing
- Windows Authentication
- Request Filtering
- Static Content Compression
- IIS Management Console
- IIS Management ScrIPts and Tools
- Anonymous Authentication
- Client Certificate Mapping Authentication.

Ohjelmistot, jotka asentuvat automaattisesti Lync Server 2010 asentaessa ovat [4.]

- Microsoft Visual C++ 2008 Redistributable
- Microsoft Visual J# version 2.0 Redistributable
- URL Rewrite Module version 2.0 Redistributable
- SQL Server 2008 Express SP1
- SQL Server 2008 Native Client.

Lync Front End -palvelimelle asennettiin vaadittavat IIS, Microsoft .NET Framework 3.5 SP1 palvelut, Message Queuing. Lisäksi Active Directoryn valmistelua varten joutui asentamaan Remote Server Administration Tools (RSAT) -työkalun, joka mahdollistaa Domain Controllerille tehtävät muutokset. Nämä kaikki pystyy asentamaan PowerShell-komennolla seuraavasti:

```
Import-module Servermanager

Add-WindowsFeature MSMQ-Server,MSMQ-Directory,NET-
Framework,RSAT-ADDS,web-server,Web-Static-Content,Web-Default-
Doc,Web-Http-Errors,Web-Http-Redirect,Web-Asp-Net,Web-Net-
Ext,Web-ISAPI-Ext,Web-ISAPI-Filter,Web-Http-Logging,Web-Log-
Libraries,Web-Http-Tracing,Web-Windows-Auth,Web-Client-
Auth,Web-Filtering,Web-Stat-Compression,Web-Mgmt-Console,Web-
```

```
ScrIPTing-Tools -Restart
```

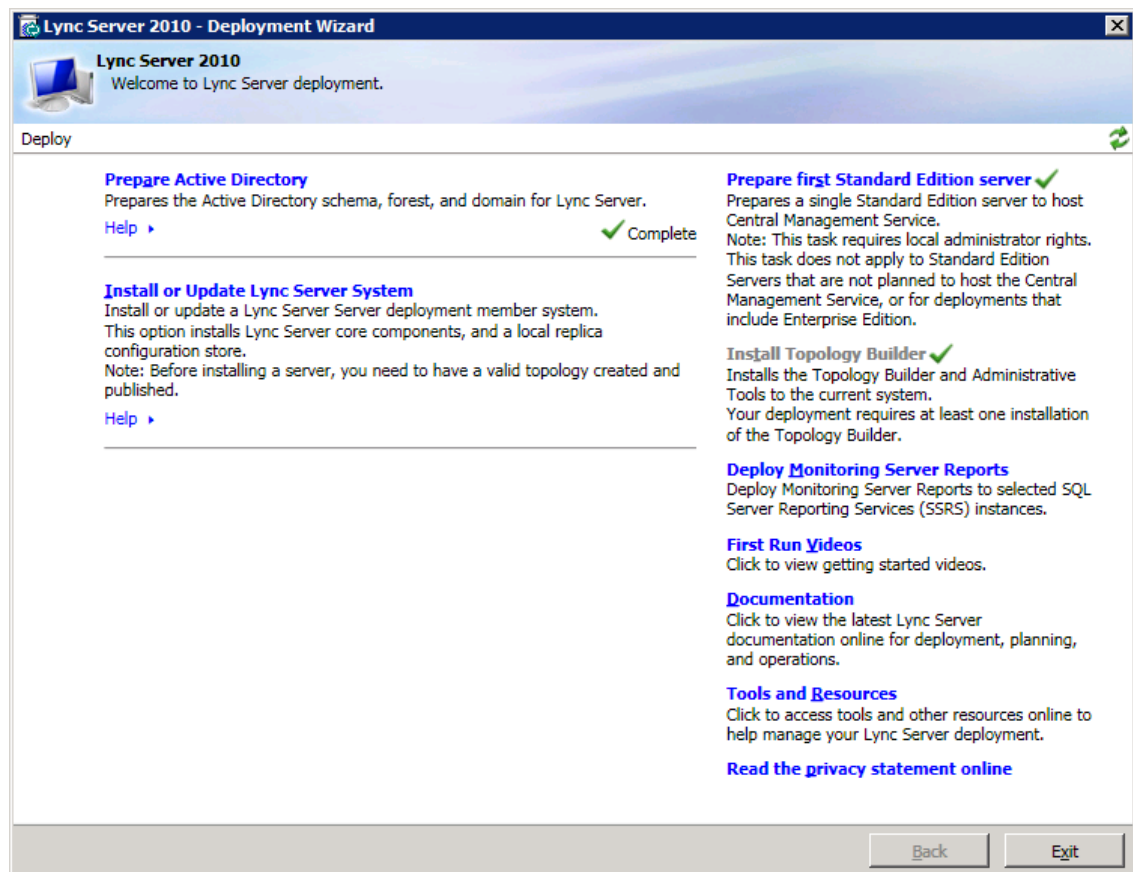
Tämän jälkeen asennettiin Lync Server 2010 -asennusmedialta Asennus pyytää hyväksymään Microsoft Visual C++ 2008 Redistributable -ohjelmiston. Lisäksi asennus pyytää käyttäjältä Lyncin asennuspolkua sekä hyväksymään lisenssi sopimuksen.



Kuvio 4. Lync Server 2010:n asennus.

Asennuksen jälkeen Lync Server 2010 Deployment Wizard avautuu. Deployment Wizard on esitetty kuviossa 3.





Kuvio 5. Lync Server 2010:n asennus.

Luotiin verkkojako nimeltä LyncShare, jolle määrättiin NTFS kirjoitus ja lukuoikeus kaikille.

#### 4.1.1 Active Directoryn valmistelu

Ennen kuin Lync Server 2010 julkaistaan, pitää Active Directory Domain Services (AD DS) valmistella. Valmistelu pitää sisällään Lyncin vaatimat schan luokka- ja attribuutilaajennukset ja ryhmien ja käyttäjien luonnit Active Directoryyn. [1: s.107]

Valmistelu alkaa painamalla Lync Server 2010 Deployment Wizardissa Prepare Active Directory -kohtaa. Ennen aloittamista on syytä kuitenkin ottaa varmuuskopio schan master domain controllerista. Lisäksi mahdollisiin schan laajennuksien ongelmiin on hyvä varautua tekemällä seuraavat asiat ennen valmistelua:

1. Katkaistaan master domain controllerin yhteys verkosta.
2. Sjärjestelmän tilan varmuuskopio master domain controllerista.
3. Suoritettiin vaihe yksi, eli scheman laajennus.
4. Kun scheman laajennus on valmis, yhdistetään domain controller takaisin verkkoon, ja varmistetaan että replikointi on aktiivinen ja toiminnassa.
5. Jos scheman laajennus menee jostain syystä pieleen, pystytään tila palauttamaan ennalleen varmuuskopiosta.

Vaiheessa kaksi tarkastetaan että scheman laajennus on replikoitunut kaikkiin palvelimiin, johon Active Directory Domain Services on asennettu. Tarkastus tapahtuu seuraavalla tavalla:

1. Avataan ADSI Edit käynnistä-valikon järjestelmätyökaluista, tai vaihtoehtoisesti adsiedit.msc.
2. ADSI Edit työkalun Action valikosta valitaan Connect to.
3. Connection Settings ikkunasta Select a well known Naming Context alavetovälikosta valitaan Schema, paina OK.
4. Etsitään scheman sisällöstä CN=ms-RTC-SIP-SchemaVersion objekti. Jos rangeUpper attribuutin arvo on 1100 ja rangeLower attribuutin arvo on 14, on replikointi onnistunut.
5. Tarkistetaan kaikki ne palvelimet, joihin Active Directory Domain Services on asennettu.
6. Jos replikointi ei ole valmis, odotetaan noin 15 minuuttia replikoinnin valmistumista.

Vaiheessa kolme asennus luo universaalit ryhmät Lync Server 2010 varten.

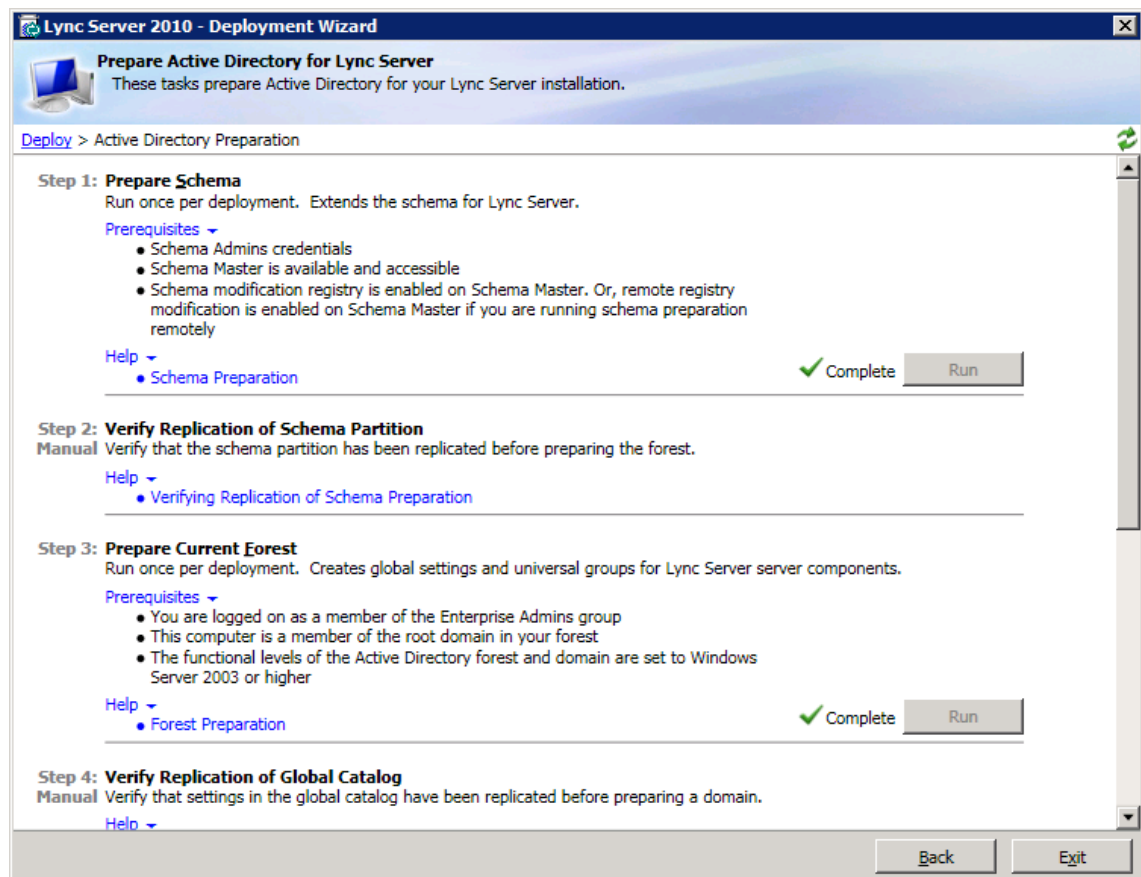
1. Suoritetaan vaihe kolme.
2. Suoritetaan komento Get-CsAdForest Lync Server Management Shell työkalussa. Jos vastaus komentoon on LC\_FORESTSETTINGS\_STATE\_READY, on luonti onnistunut.
3. Tarkistetaan tämän jälkeen, onko Active Directory Users and Computers Users haaran alle asentunut CsAdministrator ryhmä ja muita Cs-alkuisia ryhmiä. Jos

ryhmät löytyvät, on vaihe kolme onnistunut, muuten käynnistetään replikointi manuaalisesti tai odotetaan noin 15 minuuttia.

Vaiheessa viisi asennus määrittää käyttöoikeuslistat universaaleille ryhmille.

1. Suoritetaan vaihe viisi.
2. Suoritetaan komento Get-CsAdDomain Lync Server Management Shell työkalussa. Jos vastaus komentoon on LC\_DOMAINSETTINGS\_STATE\_READY, on luonti onnistunut.

Vaiheessa kuusi lisätään Lync-pääkäyttäjät CsAdministrator- ja RTCUniversalServerAdmins-ryhmään.



Kuvio 6. Lync Server 2010 Deployment Wizard, Prepare Active Directory.

#### 4.1.2 Topologian asennus ja julkaisu

Seuraavaksi asennettiin Topology Builder, Lync Server 2010 Deployment Wizard -työkalusta. Tämän jälkeen suoritettiin Prepare first Standard Edition server -kohta. Tämä asentaa tarvittavat SQL-sovellukset ja tietokannat palvelimelle.

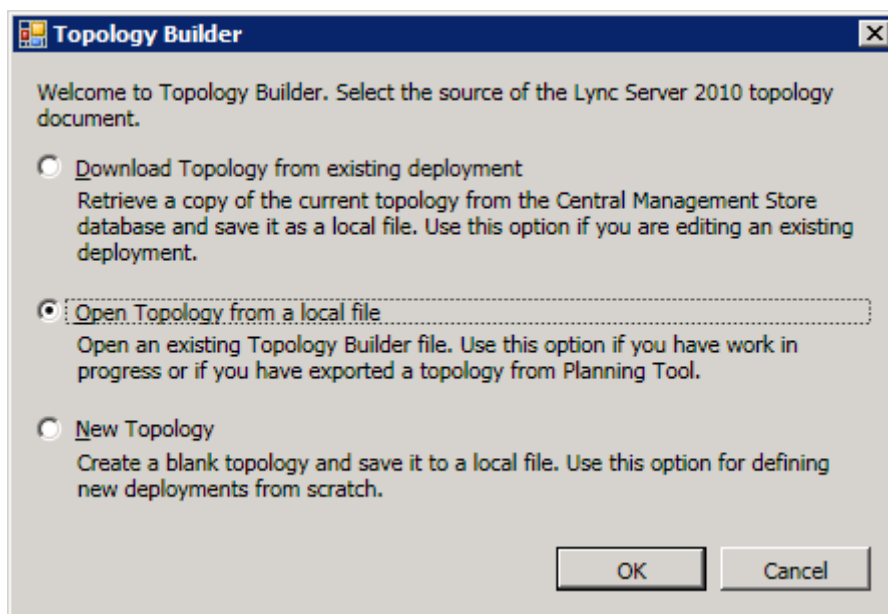
Lisättiin tarvittavat DNS-nimet DNS-serverille:

Taulukko 4. Lync Server 2010 -topologian DNS-nimet

<b>Nimi</b>	<b>IP-osoite</b>
meet.yritys.local	xxx.xxx.xxx.101
dialin.yritys.local	xxx.xxx.xxx.101
lyncadmin.yritys.local	xxx.xxx.xxx.101
meet.yritys.domain	xxx.xxx.xxx.101
dialin.yritys.domain	xxx.xxx.xxx.101
lync.yritys.domain	xxx.xxx.xxx.104
sip.yritys.domain	xxx.xxx.xxx.103
webconf.yritys.domain	xxx.xxx.xxx.103
av.yritys.domain	xxx.xxx.xxx.103
_sipinternaltls._tcp.yritys.local	xxx.xxx.xxx.101:5061
_sipinternaltls._tcp.yritys.domain	xxx.xxx.xxx.101:5061

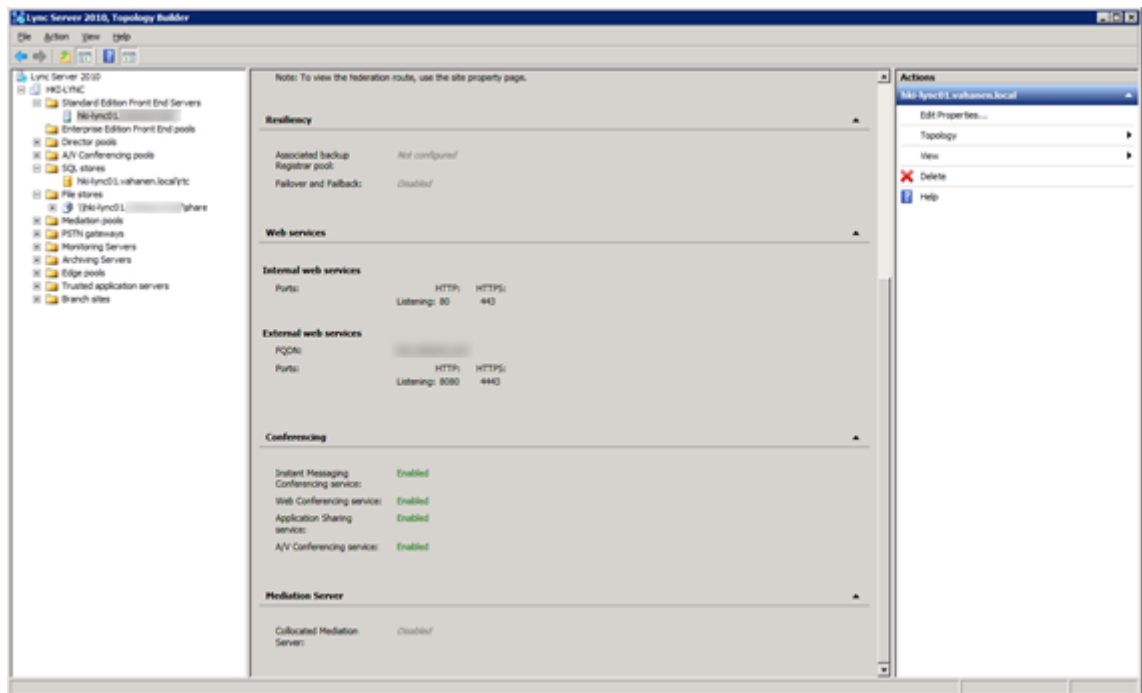
_sipfederationtls._tcp.yritys.domain	xxx.xxx.xxx.15:5061
_sip._tls.yritys.domain	xxx.xxx.xxx.15:443

Topologian määrittäminen tapahtui Lync Server Topology Builder -työkalulla. Käynnistäessä työkalua valittiin topologia valmiiksi tehdystä topologiasta, joka oli tehty Planning Tool -työkalulla.



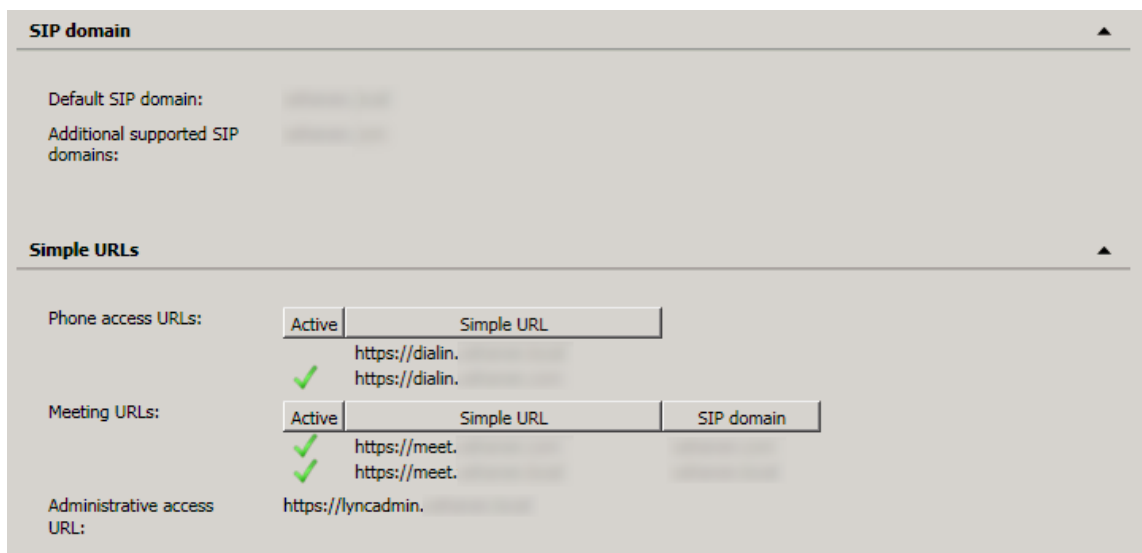
Kuvio 7. Lync Server 2010 Deployment Wizard, Prepare Active Directory.

Standard Edition Front End Server -haaran alta varmistettiin, että SQL store ja File share kohdat olivat määritysten mukaiset. Lisäksi External web services täydellinen toimialueenimi kenttä vaihdettiin osoittamaan lync.yritys.domain -osoitteeseen. Tämä on TMG-palvelimelle osoittava DNS-tietue.



Kuvio 8. Lync Server 2010 Topology Builder.

Lisäksi lisättiin sallittuihin SIP-toimialueihin yritys.domain, ja kyseiseen toimialueeseen myös puhelin- ja kokousosoitteet.

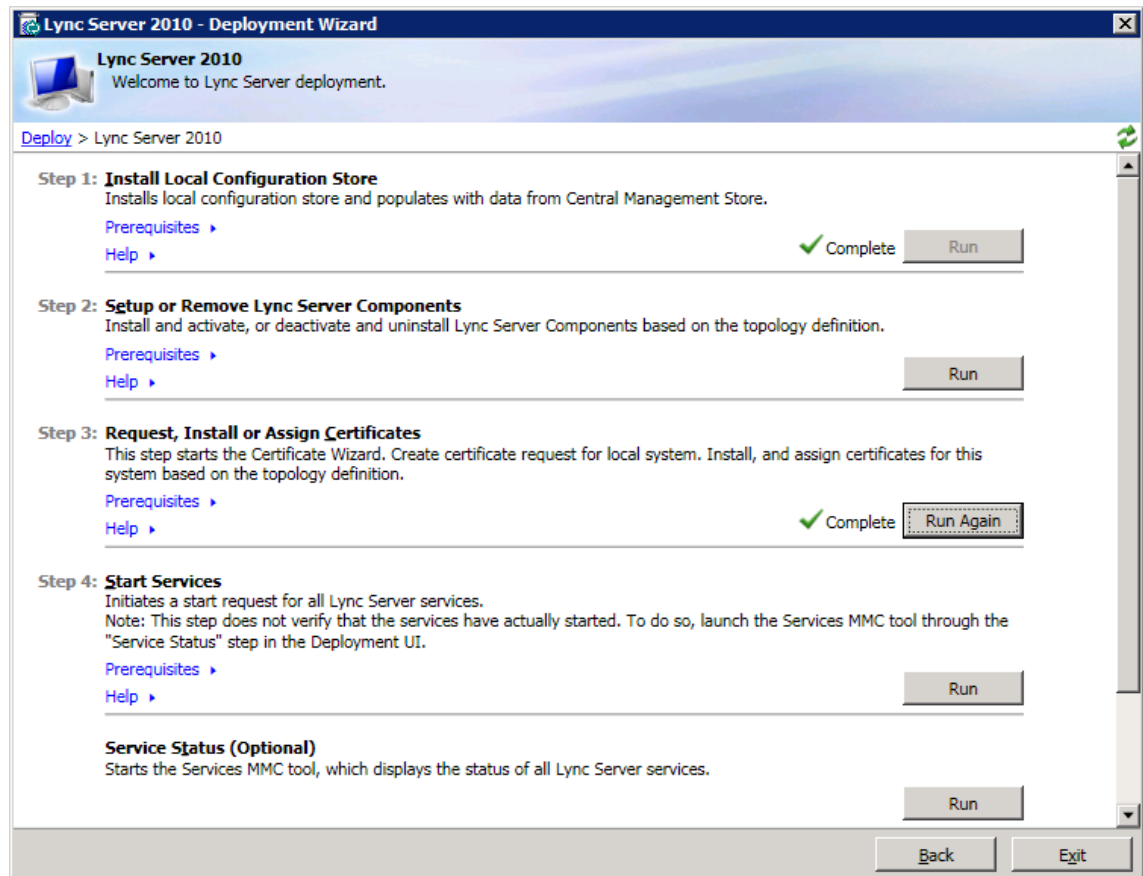


Kuvio 9. Lync Server 2010 Topology Builder Simple URLs.

Kun asetukset saatiin muutettua oikeaksi, julkaistiin topologia. Jatkettiin asennusta Deployment Wizard -työkalussa painamalla Install or Update Lync Server System -linkkiä. Suoritettiin asennuksen vaihe 1 ja 2. Vaiheessa 3 suoritettiin sertifikaatin asen-

nus. Sertifikaatti pyydettiin toimialueen Certification Authority -palvelimelta, ja tämän jälkeen asetettiin sertifikaatti Lync Front End -palvelimelle. Käynnistettiin Lync Serverin palvelut ja Front End -palvelin oli käyttökunnossa.

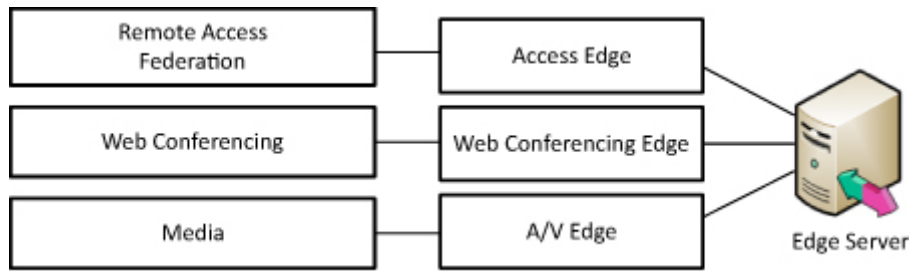
Lyncin valkotaulut, äänestykset ja muut eivät välttämättä toimi, jos sertifikaatti on esimerkiksi Microsoft IIS -järjestelmässä luotu tai sertifikaatti on itse allekirjoitettu. Harmaiden hiuksien välttämiseksi kannattaa asentaa CA-palvelin infrastruktuuriin.



Kuvio 10. Lync Server 2010 Deployment Wizard - Install or Update Lync Server System.

#### 4.2 Lync Server 2010 Edge -palvelimen asennus

Tarjotakseen käyttäjille kirjautumisen etänä liittoutumien ja julkisten pikaviestinohjelmistojen yhteyden, täytyy olla asennettuna Edge-palvelin osana infrastruktuuria. Jos liittoutuminen (federation) on otettu käyttöön, voidaan Lync-infrastruktuuriin tuoda käyttäjiä liittoutuneista toimialueista, joissa on yhtäläillä liittoutuminen käytössä Edge-palvelimessa. [2.]



Kuvio 11. Lync Server 2010 Edge -palvelin.

Asennettiin vastaavanlainen virtuaalikone kuin Lync Front End palvelimelle, mutta sillä erolla, että Edge-palvelimelle tuli kaksi verkkokorttia ja Windows Server 2008 R2:ta ei ole liitetty toimialueeseen. Edge serverissä on 1 IP-osoite sisäisessä verkkokortissa, 3 IP-osoitetta DMZ-verkkoalueella ja näiden lisäksi 3 julkista IP-osoitetta.

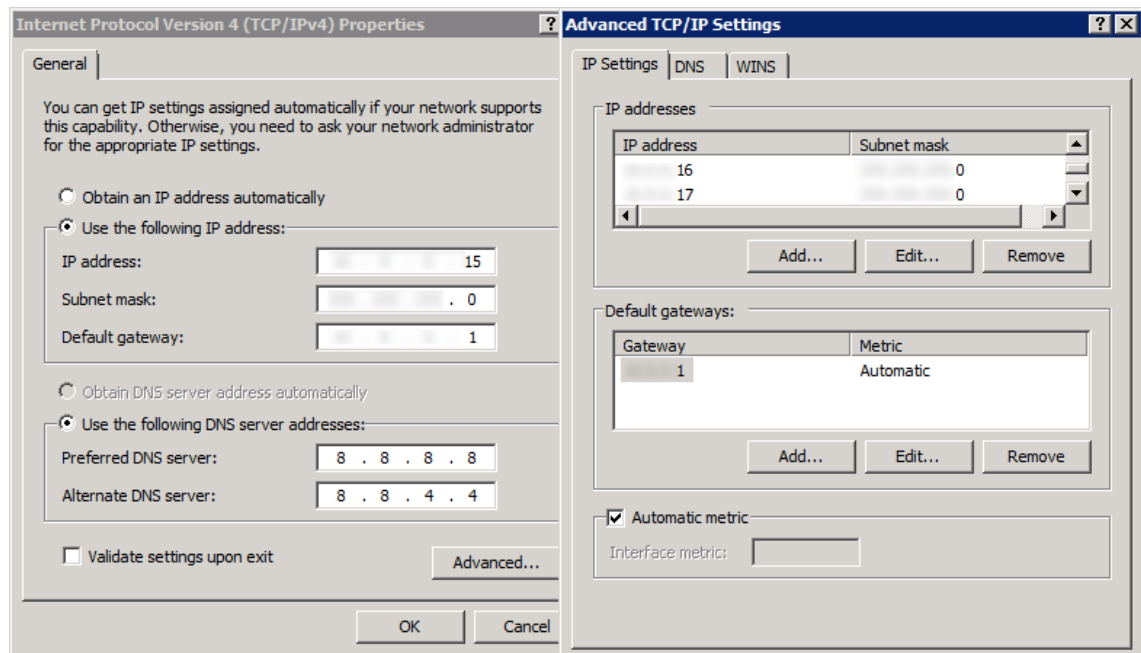
Taulukko 5. Lync Server 2010 Edge -palvelimen verkkotopologia.

Nimi	Julkinen IP	DMZ IP
sip.yritys.domain	xxx.xxx.xxx.200	xxx.xxx.xxx.15
webconf.yritys.domain	xxx.xxx.xxx.201	xxx.xxx.xxx.16
av.yritys.domain	xxx.xxx.xxx.202	xxx.xxx.xxx.17

Palvelimen sisäiselle verkkokortille määriteltiin staattiset verkkoasetukset, jossa IP-osoite on xxx.xxx.xxx.103. Sisäiselle verkkokortille ei määritellä yhdyskäytävää tai nimipalvelimia.

Palvelimen DMZ-verkon verkkokortille määriteltiin taulukon 5 mukaiset IP-osoitteet. Verkkokortin asetukset on esitetty kuviossa 12.





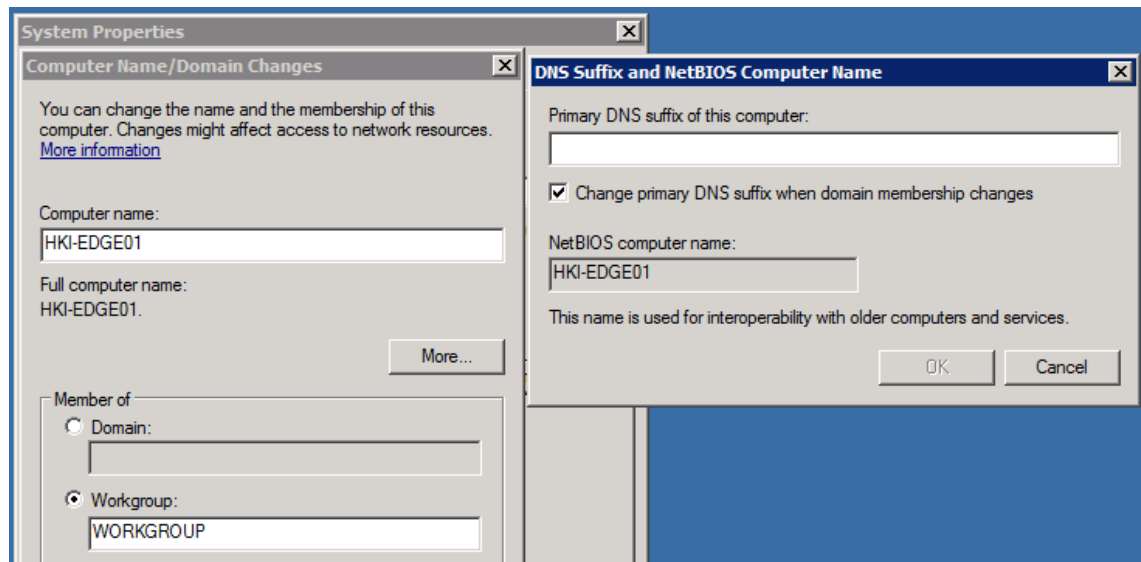
Kuvio 12. Edge-palvelimen verkkokortin asetukset.

Verkkokorttien asetusten jälkeen lisättiin "C:\Windows\System32\drivers\etc\hosts" -tiedostoon seuraavanlaiset tiedot:

```
xxx.xxx.xxx.xxx HKI-CA01.yritys.local
xxx.xxx.xxx.101 HKI-LYNC01.yritys.local
```

Tämän tiedoston muutokset kertovat palvelimelle kyseisten DNS-nimien IP-osoitteet, koska Edge-palvelimen sisäverkon verkkokortilla ei ole määrättyjä DNS-palvelimia.

Tämän jälkeen vaihdettiin Edge-palvelimen DNS-pääte osoittamaan yritys.local toimi-alueeseen. Tämä on esitetty kuviossa 13. Kyseinen muutos vaati koneen käynnistämisen uudelleen.



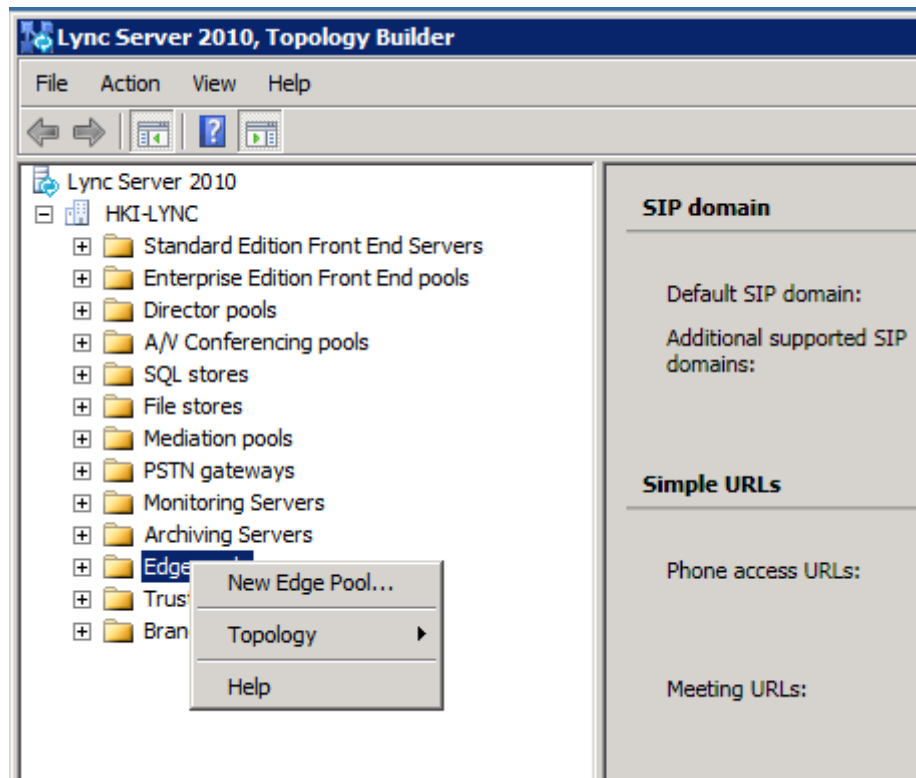
Kuvio 13. DNS-päätteen asetukset

DNS-päätteen asennuksen jälkeen asennettiin Microsoft .NET Framework 3.5 SP1, jonka voi suorittaa kirjoittamalla seuraavanlaiset komennot PowerShell-tulkkiin.

```
Import-module Servermanager
Add-WindowsFeature NET-Framework
```

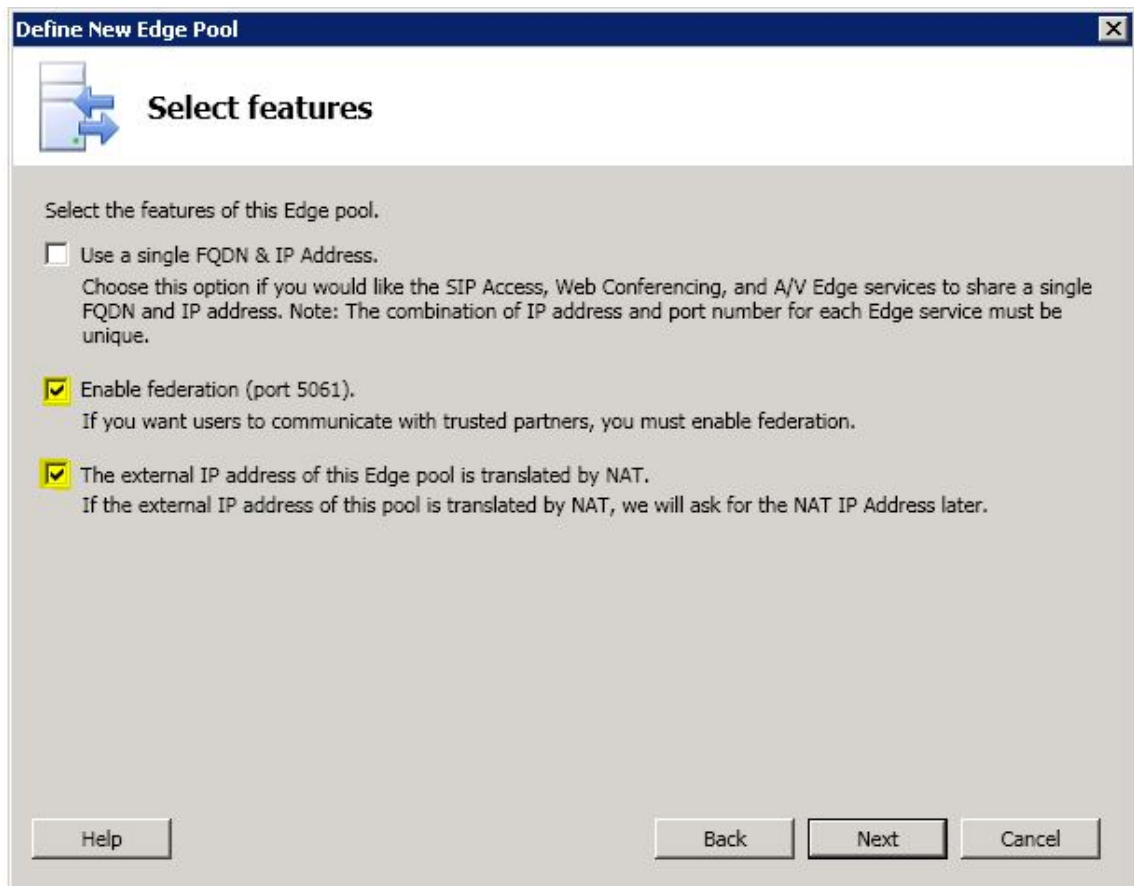
Tämän jälkeen suoritettiin Lync Server 2010:n asennus asennusmedialta kuten luvussa 4.1. Rutiinin jälkeen Edge-palvelimella löytyy myös Microsoft Lync Server 2010 Deployment Wizard -työkalu.

Seuraavaksi lisättiin Edge-palvelin Lync-topologiaan Front End -palvelimen Topology Builder -työkalulla. Valittiin Topology Builderin Edge Pools kohta oikealla hiiren klikkauksella, jonka jälkeen valittiin New Edge Pool -kohta.



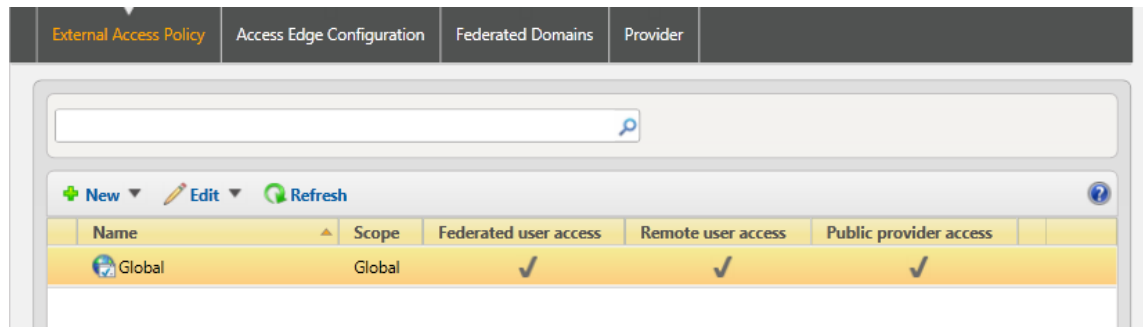
Kuvio 14. Lync Server 2010 Topology Builder – New Edge Pool.

Edge-palvelimen täydellinen toimialuennimeksi määritettiin HKI-EDGE01.yritys.local. Valittiin käyttämään liittoutumaa, 3 IP-osoitetta ja että Edge-palvelimen DMZ-verkon IP-osoitteet ovat julkiseen verkkoon NAT-käännettyt.



Kuvio 15. New Edge Pool - Features.

Seuraavassa vaiheessa määritettiin ulkoiset täydelliset toimialuenimet, jotka on esitetty taulukossa 5. Palvelut laitettiin käyttämään porttia 443, joka on tunnetummin HTTPS. Seuraavassa vaiheessa määriteltiin Edge-palvelimen sisäinen IP-osoite xxx.xxx.xxx.102. Tämän jälkeen määriteltiin tämän DMZ-verkon IP-osoitteet, jotka on esitetty taulukossa 5. Tämän jälkeen määriteltiin Access Edgen käyttämä public IP-osoite xxx.xxx.xxx.200. Näiden vaiheiden jälkeen julkaistiin topologia, joka sisältää myös Edge-palvelimen. Jotta ulkoiset yhteydet ja liittoutumat toimivat, on ne hyväksyttävä Lyncin hallintapaneelista.



Kuvio 16. Hallintapaneelin ulkoisen pääsyn asetukset.

Viimeisenä viedään topologian asetukset Front End -palvelimelta Edge-palvelimelle. Tämä tapahtui seuraavanlaisella komennolla Lync Server Management Shellissä:

```
Export-CsConfiguration -FileName C:\Topology_vienti.zip
```

Lync Edge -palvelimen Deployment Wizardista valittiin "Install or Update Lync Server System". Ensimmäisessä asennusvaiheessa valittiin keskitetyn hallinnan palvelimen tiedot kerättäväksi juuri luodusta Topology\_vienti.zip -tiedostosta.

Seuraavaksi suoritettiin vaihe kaksi, jonka asennustoimi oli automatisoitu.

Kolmannessa vaiheessa tuotiin Edge-palvelimelle sertifikaatit. Sisäisen sertifikaatin tuonti tapahtuu seuraavalla rutiinilla:

- Siirryttiin osoitteeseen: HKI-CA01.yritys.local/certsrv (CA-palvelin).
- Valittiin Download a CA Certificate, Certificate Chain, or CRL.
- Valittiin Download CA Certificate.
- Avattiin sertifikaatti hallintapaneeli paikallisessa koneessa.
- Ladattiin sertifikaatti Trusted Root Certification Authorities polun alle.
- Lähetettiin sisäisen sertifikaatin pyyntö Certificate Wizard kohdassa.

Ulkoisen palvelun sertifikaatin tulee olla ulkoiselta luotetulta varmentajalta pyydetty. Jotta palvelua päästiin testaamaan ennen varsinaista sertifikaatin hankintaan, hankin testi sertifikaatin VeriSign-palveluntarjoajalta. Muita palveluntarjoajia, jotka tarjoavat testisertifikaatteja, ovat muun muassa Thawte.

Ulkoisen sertifikaatin pyyntöä tehdessä on hyvä huomioida myös Reverse Proxy - palvelimessa käytettävät DNS-nimet, kun lisätään sertifikaatin SAN-nimiä (Subject Alternative Name). Julkisen sertifikaatin varmentajan tulee tällöin tukea useita SAN-nimiä.

### 4.3 Lync Server 2010 Reverse proxy

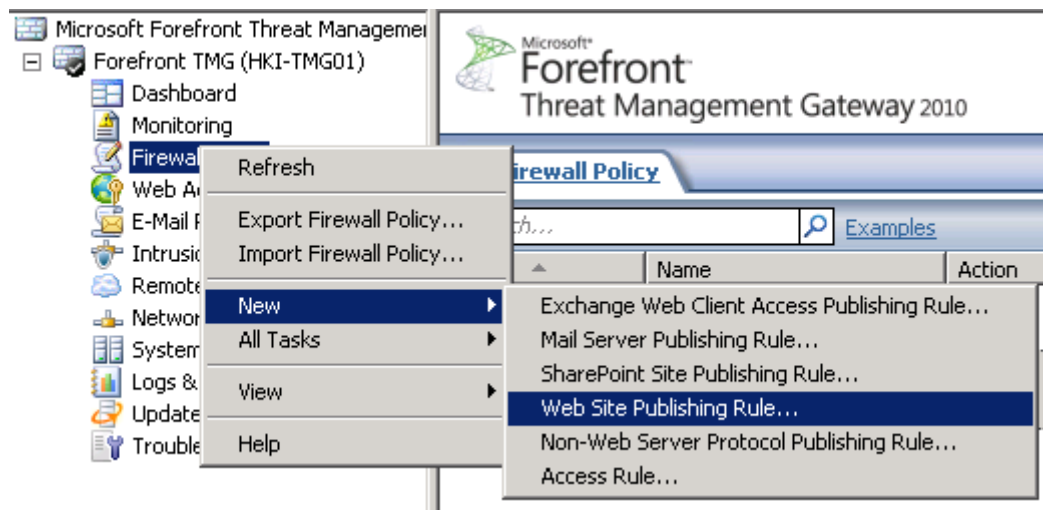
Reverse proxy -palvelin on välttämätön Lync Server 2010 -infrastruktuurissa, jos ulkoisten käyttäjien tarvitsee päästä käsiksi Lync Server 2010 web-palveluihin. Reverse proxy mahdollistaa seuraavat palvelut Lync-infrastruktuurissa: [6.]

- ulkoisten käyttäjien pääsyn lataamaan neuvotteluiden sisältöä
- ulkoisten käyttäjien pääsyn laajentamaan jakeluryhmiä
- ulkoisten käyttäjien pääsyn osoitekirjan tietoihin
- pääsyn Microsoft Lync Web App -ohjelmaan
- pääsyn Dial-in-konferenssiasetukset-sivulle
- pääsyn Lync paikkatieto palveluun
- ulkoisten laitteiden päivityksen
- verkko-osoitteiden automaattisen selvityksen mobiilisovelluksille.

Microsoft Forefront Threat Management Gateway on verkon turva ja suojaohjelmisto. Ennen Forefront TMG -ohjelmistoa tämä tunnettiin nimellä ISA Server (Microsoft Internet Security and Acceleration Server). Forefront TMG voi toimia reitittimenä, VPN-,

NAT- ja proxy-serverinä. Lisäksi tämä pystyy toimimaan palomuurina ja verkon kiihdyttäjänä. [7.]

Palvelimen käyttöönotto alkoi lisäämällä TMG-palvelimelle yksi kiinteä IP-osoite (xxx.xxx.xxx.104) lisää. Seuraavaksi aloin luoda Forefront TMG -hallintatyökalulla uutta verkkosivun julkaisua ja verkon kuuntelijaa.



Kuvio 17. Uusi verkkosivun julkaisun sääntö

Ensimmäisessä verkkosivun julkaisuvaiheessa määriteltiin verkkosivun julkaisulle nimi "Lync Web Publishing Rule". Tätä seurasi määrittäminen, hyväksytäänkö verkkoliikenne verkkosivun julkaisulle vai ei. Valitsin hyväksytään kohdan, koska olin luomassa sivuston kuuntelijaa, johon on tarkoitus päästä.

Kolmannessa vaiheessa valittiin, julkaistaanko yksi verkkosivu, useita vai palvelinfarmi. Valitsin kohdan yksi verkkosivu. Seuraavassa vaiheessa määriteltiin, käytetäänkö yhteydessä SSL-salausta vai ei. Koska kirjautumiset on pidettävä salassa, on ehdottomasti valittava SSL-vaihtoehto.

Viidennessä vaiheessa määritettiin sisäisen sivuston (Lync Server 2010 Front End -palvelin) täydellinen toimialue nimi "hki-lync01.yritys.local". Seuraavassa vaiheessa määriteltiin halutut verkkosivut, jotka julkaistaan palvelimelta. Halusimme, että kaikki Lyncin ulkoisen verkon palvelut julkaistaan, joten määrittäminen Path-kenttään on "/\*".

**New Web Publishing Rule Wizard**

**Internal Publishing Details**  
Specify the internal path and publishing options of the published Web site. You can publish the entire Web site, or limit access to a specified folder.

Enter the name of the file or folder you want to publish. To include all files and subfolders within a folder use /\*. Example: folder/\*.

Path (optional):

Based on your selection, the following Web site will be published:

Web site:

Forward the original host header instead of the actual one specified in the Internal site name field on the previous page

< Back   Next >   Cancel

Kuvio 18. Julkaistavat verkkosivut palvelimelta.

Seuraavassa kohdassa määriteltiin julkinen osoite, joka johtaa julkaistulle sivulle. Tämä Lync infrastruktuurissa on "External Web Services" -kenttä julkaistussa topologiassa, tämä infrastruktuurissamme on "lync.yritys.domain".

Seuraavassa kohdassa aloitettiin -luoda uutta verkkosivun kuuntelijaa. Asennus alkoi määrittelemällä kuuntelijalle nimi "Lync Web Listener". Tätä seurasivat vaihtoehdot, käytetäänkö SSL-yhteyttä tietokoneen välisessä yhteydessä. Tähän valitsin SSL-vaihtoehdon.

Tämän jälkeen määriteltiin, mitä kuuntelija kuuntelee. Tämän työn tapauksessa kuunnellaan sisäistä IP-osoitetta xxx.xxx.xxx.104, joka lisättiin tämän luvun alussa. Seuraavaksi määriteltiin SSL-sertifikaatti kuuntelijalle. Vein Lync Edge-palvelimen sertifikaatin

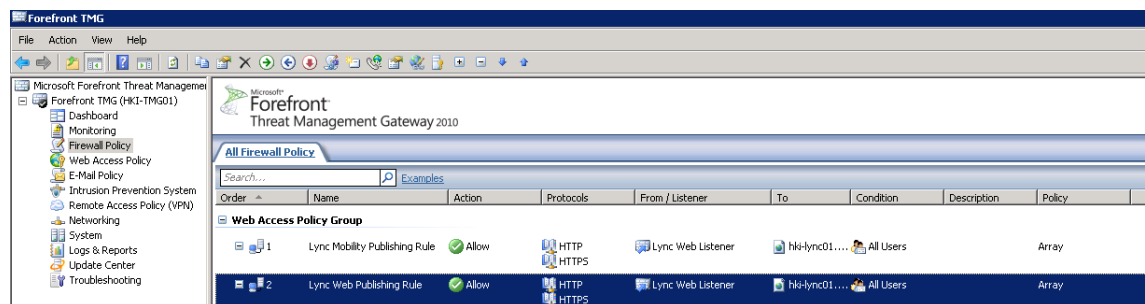


ja toin sen paikallisen koneen henkilökohtaisiin sertifiikaatteihin. Tämän jälkeen valitsin sertifiikaatin ja määritin tämän kyseiselle kuuntelijalle.

Autentikointiasetus -kohdassa valittiin, ei autentikointia, koska Lync Server 2010 Front End -palvelimen IIS-järjestelmä suorittaa autentikoinnin joka tapauksessa. Tämän jälkeen verkkosivun kuuntelijan asetukset oli määritelty.

Sivuston julkaisun asennus jatkui määrittämällä autentikoinnin TMG ja Front End palvelimen välille. Tähän vastasin ”No delegation, but client may authenticate directly”. Tämä oli asennuksen viimeinen kohta.

Tämän jälkeen käytiin vielä muuttamassa kuuntelija hyväksymään tietokoneen yhteydenpyynnöt http-portista. Lisäksi verkkosivun kuuntelija muutettiin siltaamaan http-yhteydet 8080-porttiin ja SSL-yhteydet 4443-porttiin. Lisäksi luotiin meet ja dialin verkko-osoitteet julkisiin osoitteisiin.



Kuvio 19. TMG-palomuorisäännöt.

#### 4.4 Lync Server 2010 Mobility ja Autodiscover

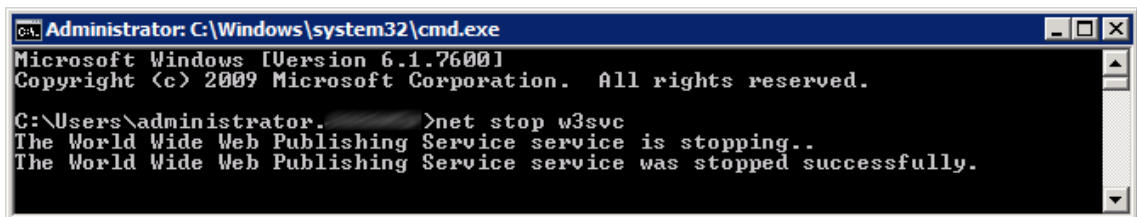
Lync Mobility -palvelu mahdollistaa Lync-palveluiden käytön mobiililaitteissa. Käyttöönottamisen jälkeen käyttäjät pystyvät käyttämään tuettuja Apple iOS-, Android-, Windows Phone- ja Symbian-laitteita pikaviestien lähettämiseen, vastaanottamiseen, yhteystietojen ja tilatietojen katsomiseen. [5.]

Lync Mobility -palvelu vaatii Lync Server 2010-ohjelmiston päivityksen (Cumulative Update 4). Tämä mahdollistaa Mobility- palvelun käytön Lync-ympäristössä. Asennuspa-

ketti löytyy <http://www.microsoft.com/download/en/details.aspx?id=11551> -osoitteesta.

Aluksi luotiin sisäinen DNS-nimi (CNAME), jota Lync 2010 Mobility -palvelu vaatii. Tämä on "lynccdiscoverinternal", joka ohjaa Lync Front End -palvelimelle.

Asennus alkoi Front End -palvelimen Lync Server Management Shellissä, jonne ajettiin komento "*Stop-CsWindowsService*". Tämä sammuttaa Lyncin palvelut. Seuraavaksi sammutettiin IIS-järjestelmän verkkosivujen julkaisupalvelut komennolla "*net stop w3svc*".



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\administrator.>net stop w3svc
The World Wide Web Publishing Service service is stopping..
The World Wide Web Publishing Service service was stopped successfully.
```

Kuvio 20. IIS-järjestelmän julkaisupalveluiden sammuttaminen.

Seuraavaksi käynnistettiin Lync Server 2010 -päivityspaketti, josta valittiin Asenna Päivitykset. Tämä päivitti tarvittavat päivitykset palvelimelle. Tämän jälkeen sammutettiin uudestaan Lync-palvelut Lync Server Management Shellissä komennolla *Stop-CsWindowsService* ja käynnistettiin IIS-järjestelmän verkkosivujen julkaisupalvelu komennolla "*net start w3svc*".

Seuraavaksi ajettiin "*Install-CsDatabase -Update -ConfiguredDatabases -SqlServerFqdn hki-lync01.yritys.local -ExcludeCollocatedStores*" -komento, jotta tausta-SQL-kanta päivittyisi tukemaan uutta päivitystä.

```

Administrator: Lync Server Management Shell
SqlMajorVersion : 10
SqlMinorVersion : 0
SqlBuildNo : 2531
SQL version is acceptable: 10.0.2531.0
Default database data file path is C:\Program Files\Microsoft SQL Server\MSSQL10
.RTC\MSSQL\Data
Default database data file path is C:\Program Files\Microsoft SQL Server\MSSQL10
.RTC\MSSQL\Data
Default database log file path is C:\Program Files\Microsoft SQL Server\MSSQL10.
RTC\MSSQL\Data
Opened database lis
Setting security in lis
Failed to set DbOwner to sa
.RTCUniversalServerAdmins has a Win32_Account instance of SIDType 2
Refreshing existing .\RTCUniversalServerAdmins SQL login
Refreshing existing .\RTCUniversalServerAdmins db user in lis
Adding .\RTCUniversalServerAdmins SQL login
Adding .\RTCUniversalServerAdmins db user in lis
Adding user .\RTCUniversalServerAdmins to role AdminRole
Successfully added logins and db users to the specified database roles in lis

Exit code: SUCCESS (0)

PS C:\Users\administrator >

```

Kuvio 21. SQL-palvelimen päivitys.

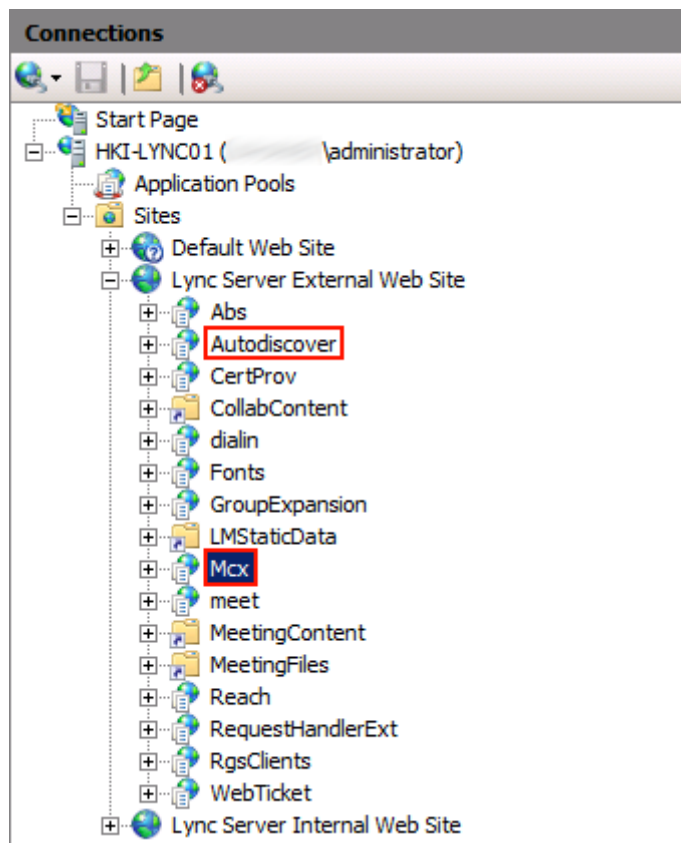
Käynnistetään Lyncin palvelut Lync Server Management Shellissä komennolla *Start-CsWindowsService*.

Konfiguroitiin Mobility-palvelun vaatimat kuuntelevat portit komennolla *"Set-CsWebServer -Identity hki-lync01.yritys.local -McxSipPrimaryListeningPort 5086 -McxSipExternalListeningPort 5087"*. Tämän jälkeen julkaistaan muutokset topologiaan komennolla *"Enable-CsTopology -verbose"*.

Mobility- ja Autodiscover -palveluiden asennus vaatii Dynamic Content Compression IIS-moduulin asentuaakseen. Tämän asennus onnistui komennolla *"Import-Module ServerManager | Add-WindowsFeature Web-Server, Web-Dyn-Compression"*.

Jos käytetään IIS versiota 7.0, täytyy asentaa ASP.NET hotfix ennen Mobility-palvelun asentamista. [5.]

Mobility- ja Autodiscover -palveluiden asennuspaketit ladattiin Front End -palvelimelle. Ladattu MsxStandalone.msi -asennuspaketti vietiin C:\ProgramData\Microsoft\Lync Server\Deployment\cache\4.0.7577.0\setup\ -nimisen kansion alle. Palveluiden asennus suoritettiin komennolla *" cd "C:\Program Files\Microsoft Lync Server 2010\Deployment" & .\Bootstrapper.exe"*. Tämän jälkeen Autodiscover- ja Mobility -palveluiden asentuminen varmistettiin IIS-järjestelmässä.



Kuvio 22. Mobility ja Autodiscover -palvelut IIS-järjestelmässä.

Jotta käyttäjät pystyisivät hyödyntämään Autodiscover -palvelua, tulee myös päivittää sertifikaatit koskemaan osoitteita `lyncdiscover.yritys.domain` ja `lyncdiscoverinternal.yritys.local`.

Lisäksi Lync Reverse Proxy -palvelimelle lisättiin "Lync Mobility Publishing Rule" -niminen verkkosivun julkaisu. Tämän asennus tehtiin samalla tavalla kuin luvussa 4.3 poikkeuksena julkaistavien verkkonimien kohdalla (`lyncdiscover.yritys.domain`). Lisäksi tämä käyttää samaa kuuntelijaa kuin kyseisen luvun "Lync Web Publishing Rule".

Viimeisenä Mobility -palvelun asennuksena suoritettiin Push-ilmoitus -palvelu. Push-palvelu lähettää mobiililaitteille ilmoituksia uusista viesteistä ja ilmoituksista, vaikka mobiililaitteen sovellus olisi ei-aktiivinen. [5]

```
New-CsHostingProvider -Identity "LyncOnline" -Enabled $true -
ProxyFqdn "sipfed.online.lync.com" -VerificationLevel
UseSourceVerification
```

```
New-CsAllowedDomain -Identity push.lync.com
Set-CsPushNotificationConfiguration -
EnableApplePushNotificationService $true -
EnableMicrosoftPushNotificationService $true
```

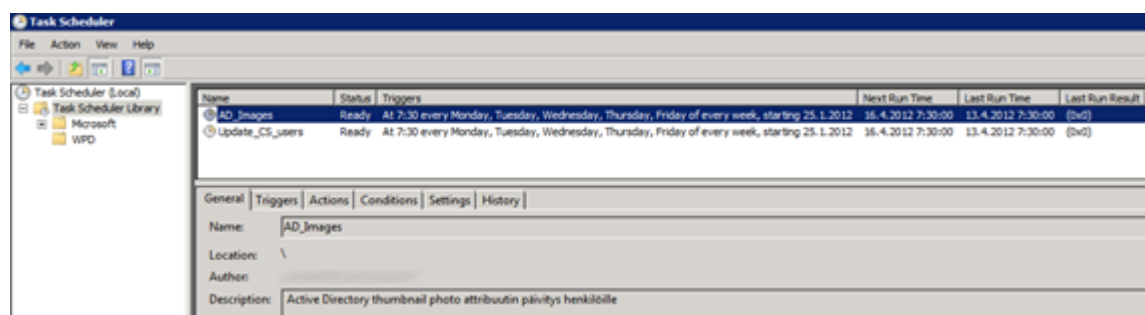
#### 4.5 Ylläpidolliset toimet ja palomuurimääritykset

Lähtökohtaisesti palomuurimäärityksissä käytettiin ajatusta ”salli pakolliset portit estä muut”. Tarvittavat palomuuuri määritykset on esitetty Liitteessä 1.

Ylläpidollisia toimia, joita Lync Server 2010 -järjestelmään on tehty:

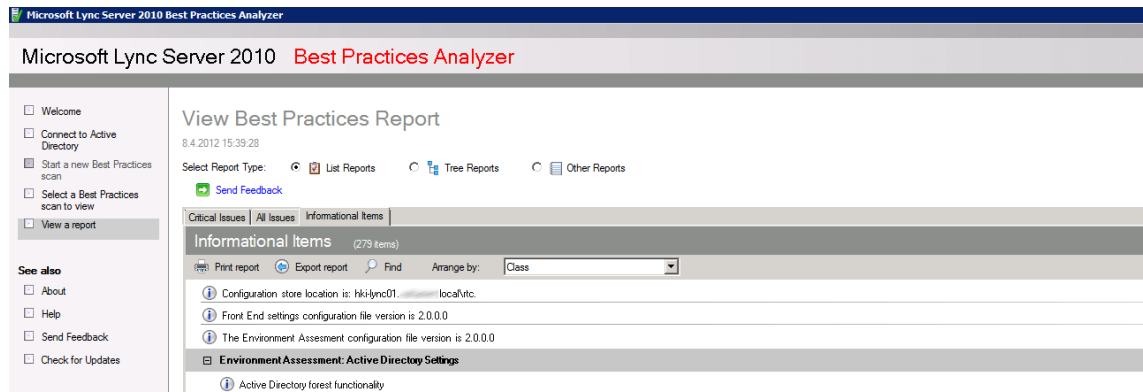
- käyttäjien lisääminen Lync-järjestelmään automaattisesti
- käyttäjien poistaminen Lync-järjestelmästä, kun käyttäjä disabloidaan
- sääntöjen asettaminen käyttäjille automaattisesti
- kuvien lisääminen aktiivihakemistoon.

Kaikki toimet suorituvat ajastettuina toimina (Task Scheduler) kello 7.30, joka arkipäivä. Toimien PowerShell-skriptit on esitetty liitteissä.



Kuvio 23. Ajastettut toimet Lync-järjestelmään.

Lisäksi järjestelmä validointiin Microsoft Lync Server 2010 Best Practices Analyzer -työkalun avulla. Ohjelma varoitti, että Lync Server 2010 -järjestelmän muistia että prosessoreita on liian vähän verrattuna suosituksiin. Lisäksi ohjelma havaitsi, että palvelin pyörii VMwaren päällä.



Kuvio 24. Lync Server 2010 -järjestelmän validointi.

## 5 Yhteenveto

Tässä insinööriyössä suunniteltiin, toteutettiin ja valvottiin Lync Server 2010:n käyttöönotto Vahanen-yhtiölle.

Projekti alkoi selvittämällä hieman taustoja, joita Lync-järjestelmältä halutaan. Tämän jälkeen työstin projektisuunnitelman, joka sisälsi sen kaikki ominaispiirteet. Seuraavassa vaiheessa pidettiin projektin ohjausryhmä, jossa käytiin projektisuunnitelma läpi. Lisäksi ohjausryhmässä päätettiin käyttöönoton kannalta kriittisiä määrittämiä.

Työssä asennettiin Lync Server 2010 Front End-, Lync Server 2010 Edge -palvelimet ja lisäksi konfigurointiin Forefront TMG palvelin ja Lync Server 2010 Mobility-palvelu Lync-infrastruktuuriin. Asennuksien yhteydessä tuli monenlaisia ongelmia vastaan, mutta kaikista näistä kuitenkin selvisin, kiitokset hyvälle Microsoftin laatimille ohjeille Lync-käyttöönottoon, kollegalleni ja Wireshark-ohjelmalle.

Asennuksien jälkeen luotiin ohjeistukset, tiedotteet ja käyttöönottoaikataulut yksikön päälliköille ja myöhemmin käyttäjille. Käyttöönotto sujui hyvin, ja ovensuukyselyiden perusteella myös käyttäjät ovat pääosin tyytyväisiä järjestelmään.

Loppujen lopuksi työ saatiin valmiiksi. Aikaa käyttöönottoon kului yhteensä noin 4 kuukautta. Kuitenkin oppimiskokemus tästä työstä on ollut valtaisa. Käyttöönottoprojektin suunnittelu, seuranta ja johtaminen on ollut erittäin haastava tehtävä. Pelkästään oppitunneilla kyseisiä asioita ei voi oppia. Lisäksi kommunikointi eri tasojen välillä käyttöö-

ottoprojekteissa ja hankkeissa on erittäin tärkeää. Myös Lync-järjestelmän tietoisuus on noussut huimasti.

Kehityskohteita järjestelmälle löytyy monia, kuten esimerkiksi puhelinoperaattori tuen tuomisen järjestelmään, integroimalla videoneuvottelulaitteita suoraan Lync-järjestelmään ja monitorointi- tai arkistointipalveluiden tuominen infrastruktuuriin. Joka tapauksessa Vahanen-yhtiö sai työkalun, joka tehostaa yrityksen viestintää, tiedonkulkua ja toimitapoja. Lisäksi tämä tuo kustannussäästöjä.

## Lähteet

- 1 10534A Planning and Designing a Microsoft Lync Server 2010 Solution. Microsoft Corporation, 2011.
- 2 Microsoft Lync Server 2010 Edge Server Deployment Guide. Microsoft Corporation, 2012.
- 3 Microsoft Lync Server 2010 Standard Edition Deployment Guide. Microsoft Corporation, 2012.
- 4 Microsoft Lync Server 2010 Planning Guide. Microsoft Corporation, 2012.
- 5 Microsoft Lync Server 2010 Mobility Guide. Microsoft Corporation, 2012.
- 6 Set Up Reverse Proxy Servers. Microsoft Corporation, 2011. [verkkodokumentti]. [Viitattu 8.4.2012]. Saatavissa: <http://technet.microsoft.com/en-us/library/gg398069.aspx>.
- 7 Microsoft Forefront Threat Management Gateway. [verkkodokumentti]. [Viitattu 8.4.2012]. Saatavissa: [http://en.wikipedia.org/wiki/Threat\\_Management\\_Gateway](http://en.wikipedia.org/wiki/Threat_Management_Gateway).
- 8 Lync 2010 – Reverse Proxy. [verkkodokumentti]. [Viitattu 20.2.2012]. Saatavissa: <http://www.darylhunter.me/blog/2011/11/lync-2010-reverse-proxy-part-3.html>.
- 9 Overview of Best Practices Analyser. [verkkodokumentti]. [Viitattu 14.4.2012]. Saatavissa <http://technet.microsoft.com/en-us/library/gg591349.aspx>.



## Lync Server 2010 - palomuurimääritykset

### Firewall Report

This report lists the source and destination ports and IP addresses for both External and Internal interfaces.

Note: The settings provided by this tool are based on available best practices and the information you provide. You bear the risk of using the settings. Microsoft gives no express warranties, guarantees or conditions.

Edge Role	Source IPAddresses	Source Port	Destination IP Address	Destination Port	Transport	Application	Comments
<b>External Firewall Ports Settings</b>							
<b>External Interface</b>							
Access	15	Any	Any	80	TCP	HTTP	
Access	15	Any	Any	53	UDP	DNS	
Access	Any	Any	15	443	TCP	SIP (TLS)	Client to server SIP traffic for external user access
Access	Any	Any	15	5061	TCP	SIP (MTLS)	For federated and public IM connectivity using SIP
Access	15	Any	Any	5061	TCP	SIP (MTLS)	For federated and public IM connectivity using SIP
Web Conferencing	Any	Any	16	443	TCP	PSOM (TLS)	
A/V	17	50000 - 59999	Any	Any	TCP	RTP	Required only for desktop sharing and/or federation with partners running Office Communications Server 2007 or Office Communications Server 2007 R2.  Also required for application sharing and/or file transfer with Lync Server 2010 federated users using A/V sessions with Windows Live Messenger.
A/V	17	50000 - 59999	Any	Any	UDP	RTP	Required only for federation with partners still running Office Communications Server 2007.

Edge Role	Source IPAddresses	Source Port	Destination IP Address	Destination Port	Transport	Application	Comments
A/V	Any	Any	17	50000 - 59999	TCP	RTP	Required only for federation with partners still running Office Communications Server 2007.
A/V	Any	Any	17	50000 - 59999	UDP	RTP	Required only for federation with partners still running Office Communications Server 2007.
A/V	17	Any	Any	3478	UDP	STUN/MSTURN	3478 outbound is used to determine the version of Edge server Lync Server 2010 is communicating with and also for media traffic from Edge server to Edge server.  Required for federation with Office Communications Server 2007 R2, and also if multiple Edge pools are deployed within a company.
A/V	Any	Any	17	3478	UDP	STUN/MSTURN	
A/V	Any	Any	17	443	TCP	STUN/MSTURN	
<b>Reverse Proxy</b>							
N/A	Any	Any		80	TCP	HTTP	Optional: Can be used to redirect http traffic to https.
N/A	Any	Any		443	TCP	HTTPS	
<b>Internal Firewall Ports Settings</b>							
<b>Internal Interface</b>							
Access	103	Any	101	5061	TCP	SIP (MTLS)	Destination will be the Next Hop server(s). In the case of the reference architecture, it's the IPAddresses of the two pool front ends.

Edge Role	Source IPAddresses	Source Port	Destination IP Address	Destination Port	Transport	Application	Comments
Access	101	Any	103	5061	TCP	SIP (MTLS)	Source will be the Next Hop server(s). In the case of the reference architecture, it's the IPAddresses of the two pool front ends.
Access	101	Any	103	4443	TCP	HTTPS	Used by the replication agent for CMS database replication, include all front end servers.
Web Conferencing	Any	Any	103	8057	TCP	PSOM (MTLS)	
A/V	101	Any	103	5062	TCP	SIP (MTLS)	Include all front end servers using this particular A/V authentication service.
A/V	Any	Any	103	3478	UDP	STUN/MSTURN	
A/V	Any	Any	103	443	TCP	STUN/MSTURN	
<b>Reverse Proxy</b>							

## Kuvien lisääminen aktiivihakemistoon

```
# ThumbnailPhoto-attribuutti
# Z-aseamalla sijaitsee käyttäjien kuvat "*sAMAccountname*.jpg"
# Pekka Tamminen

Import-module ActiveDirectory

Write-Host "Listing all users in AD!"
$alist = "username`n"
$userlist = Get-ADUser -Filter * -Properties * | Select-Object -
Property SamAccountName | Sort-Object -Property SamAccountName
$userlist | ForEach-Object {
    $arec = $_.SamAccountName
    $aline = ($arec -join "`t") + "`n"
    $alist += $aline
}
$alist | Out-File ADUsers.csv
$userlist = Import-Csv ADUsers.csv

$cryptoServiceProvider = [System.Security.Cryptography.MD5CryptoServiceProvider];
$hashAlgorithm = new-object $cryptoServiceProvider

if(Test-Path -path Z:\){
    foreach ($account in $userlist) {
        if($account -ne ""){
            $result = get-aduser $account.username -Properties thumbnailphoto;
            $username = $result.sAMAccountName

            if(Test-Path Z:\$username.jpg){
                if ($result.thumbnailphoto) {

                    if([String]::Join("", $hashAlgorithm.ComputeHash($result.thumbnailphoto)) -ne [String]::Join("", $hashAlgorithm.ComputeHash((Get-Content Z:\$username.jpg -Encoding byte)))){
```

```
$photo = [byte[]](Get-Content Z:\$username.jpg -Encoding byte)
Set-ADUser $username -Replace @{thumbnailPhoto=$photo}

    Write-Host $username " - Photo replaced!"
} else {

    Write-Host $username " - Photo already exists!"
}

} else {

    $photo =
[byte[]](Get-Content Z:\$username.jpg -Encoding byte)
Set-ADUser
$username -Replace @{thumbnailPhoto=$photo}
Write-Host
$username " - Picture added!"
}
}
}
}
```

## Käyttäjien tuominen/poistaminen Lync-järjestelmään

```
# Tuo käyttäjät aktiivihakemiston ryhmästä LyncUsers
# Pekka Tamminen

Import-Module Lync

Get-CsAdUser -LdapFilter "(memberof:1.2.840.113556.1.4.1941:=CN=LyncUsers,OU=Groups,DC=yritys,DC=local)" | ?{$_ .UserAccountControl -eq "NormalAccount" -and $_.Enabled -ne $true} | Enable-CsUser -RegistrarPool "hki-lync01.yritys.local" -SipAddressType sAMAccountName -SipDomain yritys.local

Get-CsAdUser -LdapFilter "(memberof:1.2.840.113556.1.4.1941:=CN=LyncUsers,OU=Groups,DC=yritys,DC=local)" | ?{$_ .UserAccountControl -eq "NormalAccount" -and $_.Enabled -ne $true} | Grant-CSCClientPolicy -PolicyName Yritys

Get-CsAdUser | ?{$_ .UserAccountControl -match "AccountDisabled" -and $_.Enabled -eq $true} | Disable-CsUser
```