Deployment guide:

Configuring a highly available Microsoft® Lync Server® 2013 environment on Dell™ architecture

Principled Technologies®

DELL

Microsoft

A Principled Technologies deployment guide commissioned by Dell Inc.

TABLE OF CONTENTS

Table of contents **2**

Introduction **4**

About the components **4**

About the Dell PowerEdge M1000e blade enclosure 4

About the Dell PowerEdge M620 server nodes 5

About the Intel Xeon processor E5 family 5

About the Dell EqualLogic PS-M4110 blade array 5

About Microsoft Windows Server 2012 6

About Microsoft Lync Server 2013 6

We show you how – Installing Lync Server 2013 on Dell architecture **7**

Existing infrastructure 7

Installing the hardware 7

Networking overview 8

Configuring the PowerConnect modules 9

Isolating the Live Migration network 11

Configuring the PS-M4110 networking 11

Configuring the PowerEdge M620 blade servers 12

Configuring the PS-M4110 storage 14

Configuring the volumes in the OS 17

Creating the failover cluster 17

Configuring the failover cluster 18

Creating the VMs 20

Creating the Lync Server file shares 21

Preparing the Active Directory for Lync 22

Preparing the primary Front End VM 25

Building the topology 26

Installing the configuration to the primary Front End VM 29

Adding the secondary Front End VM to the topology 32

Updating the primary Front End VM 33

Installing the configuration to the secondary Front End VM 34

Designating the secondary Front End pool as a backup 35

Adding the backup SRV 37

Commands for manual failover 38

Summing it all up **39**

Appendix A – Installing the hardware and configuring the networking **40**

Installing the hardware 40

Configuring the PowerConnect M8024-k 10GbE modules 41

Configuring the PS-M4110 networking 41

Appendix B – Configuring the M620 blades **43**

Installing Windows Server 2012 Datacenter Edition on the M620s 43
Creating a network for Live Migration 43
Joining the M620s to the domain 43
Adding the MPIO feature 44
Appendix C – Configuring the storage 45
Configuring the PS-M4110 RAID policy 45
Finding the initiator IQN 45
Creating volumes on the PS-M4110 45
Providing multiple IQNs access to a volume 46
Connecting the M620s to the volumes 46
Preparing the volumes for cluster shared storage 46
Appendix D – Creating the failover cluster and building the VMs 48
Creating the failover cluster 48
Configuring the failover cluster 48
Installing Dell EqualLogic Host Integration Tools 4.5.0 49
Configuring MPIO settings 50
Installing the Hyper-V roles 50
Creating a virtual switch 50
Creating the VMs 51
Installing Windows Server 2012 Datacenter Edition on the VMs ... 51
Joining the VMs to the domain 52
Appendix E – Preparing the Active Directory and VMs for Lync Server 2013 53
Preparing the Active Directory 53
Providing Lync permissions to the Domain Admin 54
Configuring the DNS 54
Creating the Lync Server file shares 55
Preparing the primary Front End VM 55
Appendix F – Installing Lync Server 2013 Standard Edition 57
Building the topology 57
Installing the configuration to the primary Front End VM 58
Adding the secondary Front End pool 59
Updating the primary Front End VM 60
Installing the configuration to the secondary Front End VM 61
Designating the secondary Front End pool as a backup 62
Updating the Front End VMs 63
Adding the backup SRV 63
About Principled Technologies 64

INTRODUCTION

When considering a highly available solution for your business' communications needs, choosing a Dell architecture solution over a traditional hardware combination of servers, networking, and storage can save your IT administrator lots of configuration and management time. A Dell converged infrastructure solution can offer small businesses and remote offices performance, scalability, and streamlined management. These features keep important communications workloads running for your business.

In this guide, we take you through the simple, straightforward process of setting up a highly available Microsoft Lync Server 2013 environment on a Dell solution consisting of the following hardware:

- 1 Dell PowerEdge™ M1000e blade enclosure
- 2 Dell PowerEdge M620 blade servers
- 1 Dell EqualLogic™ PS-M4110 blade storage array
- 4 Dell PowerConnect™ M8024-k 10GbE switch modules

We set up this environment in our labs, and we provide each step we took along with any best practices we recommend. First, read more about the components of the Dell solution. Then, continue on for an overview of how to configure a Microsoft Lync Server 2013 environment (for detailed steps, see the corresponding appendices).

ABOUT THE COMPONENTS

About the Dell PowerEdge M1000e blade enclosure

The Dell PowerEdge M1000e blade chassis and its supported fabric interconnects are designed for dense computing situations. Features of the PowerEdge M1000e include:

- **Management.** Reduces administrative demand by providing a secure centralized management interface for the chassis and blades within, using proven Web (SSL-encrypted) and CLI (SSH/Telnet) technologies.
- **Simplified configuration.** The Chassis Management Controller allows administrators to control up to nine enclosures and 144 server blades, including BIOS/firmware change management and updates, thermal monitoring, and power threshold configuration.
- **Flexible I/O.** Six interconnect sockets with the capability to support three fully redundant fabrics, a passive midplane with more than 8 Tbps in I/O bandwidth capacity, and FlexIO support provide a number of connectivity options for your servers.
- **Reliability and efficiency.** Six power supplies and nine fans, all hot-swappable, allowing for no-downtime maintenance of key chassis

components. All components are tuned for maximum power efficiency to reduce datacenter power consumption.

For more information about the Dell PowerEdge M1000e Blade Enclosure, visit www.dell.com/us/enterprise/p/poweredge-m1000e/pd.

About the Dell PowerEdge M620 server nodes

The Dell PowerEdge M620 has features optimized for performance, density, and energy efficiency.

- **Processors.** The Dell PowerEdge M620 is powered by two Intel® Xeon® E5-2600-series processors, which incorporate the very latest in processor technology from Intel. The powerful processors provide the performance you need for your essential mainstream tasks. The Intel Xeon E5-2600-series processor gives you up to eight cores per processor or up to 16 cores per server.
- **Memory.** The Dell PowerEdge M620 holds up to 768GB DDR3 RAM (up to 1600 MHz) across 24 DIMM slots per server node.
- **Management.** The Dell PowerEdge M620, like all late-model Dell servers, comes with the Dell Lifecycle Controller. This tool simplifies server management by providing a single interface for management functions and by storing critical system information in the system itself. There are no CDs or USB keys to monitor for drivers or firmware.

About the Intel Xeon processor E5 family

The new Intel Xeon processor E5 family, which comes standard in new Dell PowerEdge servers, incorporates innovative technology and features to meet the computing demands of the present and future. The Intel Xeon processor E5 family delivers intelligent and adaptive performance using such features as Intel Turbo Boost Technology 2.0, Intel Advanced Vector Extension, Intel Integrated I/O, and Intel Data Direct I/O Technology. These new processors also feature Intel Trusted Execution Technology (Intel TXT) and utilize Intel Advance Encryption Standard New Instructions (Intel AES-NI) to help keep your data safe.

For more information about the Intel Xeon processor E5 family, visit www.intel.com.

About the Dell EqualLogic PS-M4110 blade array

The Dell EqualLogic PS-M4110 is an enterprise-class storage array designed to install directly into a blade chassis. Simple integration with Dell PowerEdge M-series servers and switches in the PowerEdge M1000e chassis allows for a full-featured, single-chassis solution without external dependencies. The PS-M4410 features a full suite of

enterprise-class management tools and features, including EqualLogic array firmware, SAN Headquarters, and Host Integration Tools.

About Microsoft Windows Server 2012

Windows Server® 2012, the latest release of this server OS from Microsoft®, includes many new features and enhancements. According to Microsoft, Windows Server 2012 focuses on four core areas:

- **Beyond virtualization.** Windows Server 2012 provides a robust and dynamic virtualization platform through Hyper-V®, and includes new features that provide flexible options for delivering cloud services.
- **The power of many servers, the simplicity of one.** Windows Server 2012 offers features that allow for high availability and ease of management for multiple-server infrastructures.
- **Every app, any cloud.** Windows Server 2012 delivers a scalable and flexible Web and application platform by providing a consistent and open set of tools and frameworks that apply to applications on premises, in the cloud, or in a hybrid environment.
- **Modern work style, enabled.** Microsoft Windows Server 2012 empowers users and IT staff with remote access to data, applications, and simpler management tools while strengthening security and compliance.

About Microsoft Lync Server 2013

Microsoft Lync Server 2013 is a unified communications platform that lets users communicate securely and stay connected with colleagues and customers, from virtually wherever they chose to work.

Lync connects people on Windows 8 and other operating systems including mobile devices, as part of their everyday productivity experience. Lync provides a consistent, single-client experience for presence, instant messaging, voice, video, and meetings. Users can switch among devices as they choose based on their needs. Lync offers familiar and consistent user experience across PC, phone, browser, and tablets.

To learn more about Microsoft Lync Server 2013, visit office.microsoft.com/en-us/lync/.

WE SHOW YOU HOW – INSTALLING LYNC SERVER 2013 ON DELL ARCHITECTURE

This guide walks you through deploying virtualized instances of Microsoft Lync Server 2013 onto a Windows Server 2012 Hyper-V® Failover Cluster. We recommend this configuration as it takes advantage of both guest-level and application-level high availability features. This guide is intended for a business with approximately 500-1000 users that uses Lync Server 2013 Standard Edition. For more information on sizing and capacity planning, see http://technet.microsoft.com/en-us/library/gg615015.aspx.

We first show you how to create a Hyper-V® Failover Cluster on two Dell PowerEdge M620 nodes running Windows Server 2012, using the Dell EqualLogic PS-M4110 blade storage to host the shared data. We then detail how to configure a highly available Lync Server 2013 Standard Edition environment consisting of three virtual machines: a pair of Lync Server 2013 Standard Edition Front End VMs, and a file server to handle quorum witness and topology information. Under this configuration, in the event that the server node hosting the primary Lync Server 2013 Front End VM goes offline, the secondary Front End VM will provide automatic failover of voice features without interruption to any participants, and any non-voice features can either be failed over manually on the application level, or will resume function as soon as the downed VM reboots on the other server node via Windows Server 2012 and Hyper-V failover clustering.

Existing infrastructure

This guide assumes a pre-existing infrastructure that contains an Active Directory® Domain Controller, DNS server, and an Active Directory Certificate Authority. Further information can be found at the following links:

- Active Directory Domain Services: technet.microsoft.com/en-us/library/hh831484.aspx
- Active Directory Certificate Services: technet.microsoft.com/en-us/library/hh831740.aspx
- Certificate requirements: technet.microsoft.com/en-us/library/gg398066.aspx

Installing the hardware

Before beginning this section, install the blade enclosure into a rack near sufficient 240V power outlets. Additionally, each Dell PowerEdge M620 will need a mezzanine NIC card (an Intel X520 10GbE in our tests). For detailed steps, see Appendix A.

Provide a DHCP-enabled network connection to both Chassis Management Controller (CMC) modules on the back of the enclosure. If not using DHCP, provide the CMC with a static IP address using the front control panel.

1. Ensure that the mezzanine cards to be used for iSCSI traffic are installed into Slot B on each Dell PowerEdge M620 blade server, and insert the blades into the front of the enclosure. We placed the blade servers into slots 1 and 2.
2. Insert the Dell EqualLogic PS-M4110 blade storage into slots 3 and 4 on the front of the enclosure.
3. Insert two of the Dell PowerConnect M8024-k 10Gb Ethernet switch modules into slots A1 and A2 on the back of the enclosure.
4. Insert the remaining two Dell PowerConnect M8024-k 10Gb Ethernet switch modules into slots B1 and B2 on the back of the enclosure.
5. Provide domain-connected 10Gb network connections to port 20 (or an available port other than ports 17 and 18) on the M8024-k modules in slots A1 and A2.
6. Provide two 10Gb connections between the M8024-k modules in A1 and A2, using ports 17 and 18 on each. It is a best practice to cross the cables, i.e., connect port 17 in slot A1 to port 18 in slot A2, and vice versa.
7. Repeat step 6 for the M8024-k modules in slots B1 and B2.
8. Power on the enclosure.

Networking overview

This deployment requires three networks. The first is a domain-connected network, which connects to the external Active Directory domain controller and other existing infrastructure. The second is a Live Migration network, which comprises only the two clustered servers and allows VMs to move from one node to another with no downtime. The third is an iSCSI network, which connects to the PS-M4110 storage array and allows the storage to be shared across the servers. It is a best practice to isolate traffic from these networks. In our setup, we had two dual-port NICs in each blade: one of these is integrated and corresponds with fabric A, and the other is a mezzanine card configured to correspond with fabric B. We assigned a port from the integrated NIC for the domain-connected network, and the other port for Live Migration traffic. We isolated these networks by using different subnets and configuring tagged VLAN traffic for the Live Migration network. We used the mezzanine cards and fabric B for a dedicated iSCSI network. Figure 1 shows the sample IP scheme we used.

Server	NIC	IP Address	Traffic type	VLAN ID
ServerNode1	1	192.168.1.51	Domain	0 (untagged)
	2	192.168.20.51	Live Migration	20
	3	192.168.10.51	iSCSI	0
	4	192.168.10.53	iSCSI	0
ServerNode2	1	192.168.1.52	Domain	0
	2	192.168.20.52	Live Migration	20
	3	192.168.10.52	iSCSI	0
	4	192.168.10.54	iSCSI	0
ADServer	1	192.168.1.1	Domain	0
Cluster1	1	192.168.1.70	Domain	0
PS-M4110 Group	1	192.168.10.60	iSCSI	0
PS-M4110 Member	1	192.168.10.61	iSCSI	0
First Front End VM	1	192.168.1.11	Domain	0
Second Front End VM	1	192.168.1.12	Domain	0
File Server VM	1	192.168.1.15	Domain	0

Figure 1: Network configuration for failover clustering.

Configuring the PowerConnect modules

1. Use Internet Explorer to access the CMC. The default username is `root` and the default password is `calvin`. Note that you may want to modify the default credentials for security reasons.
2. Access the I/O Module GUI for the M8024-k module in A1 and log in with the same credentials.
3. Under System→Stack Management→Stack Port Summary, edit ports 0/17 and 0/18 so that they are used for stacking instead of Ethernet (Figure 2).

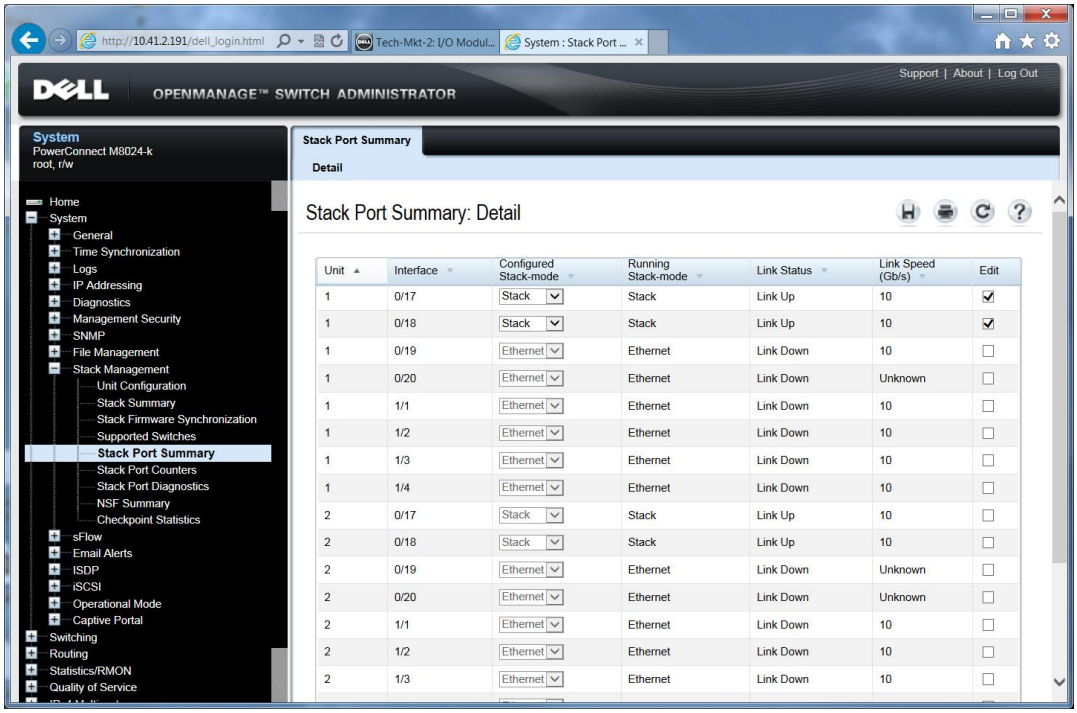

Figure 2: Configuring the M8024-k stacking ports.

4. After clicking Apply, click Save. This will allow these settings to persist in the event of a switch reboot.
5. Repeat steps 2 through 4 for the M8024-k module in A2. The switches will now be stacked and will function as one unit.
6. Repeat steps 2 through 5 for the M8024-k modules in B1 and B2.

Isolating the Live Migration network

1. Access the I/O Module GUI for the M8024-k in slot A1, and navigate to Switching→VLAN→Port Settings.
2. For Unit 1, Port Te1/0/1, use the Port VLAN Mode drop-down menu to select Trunk (see Figure 3). Click Apply.

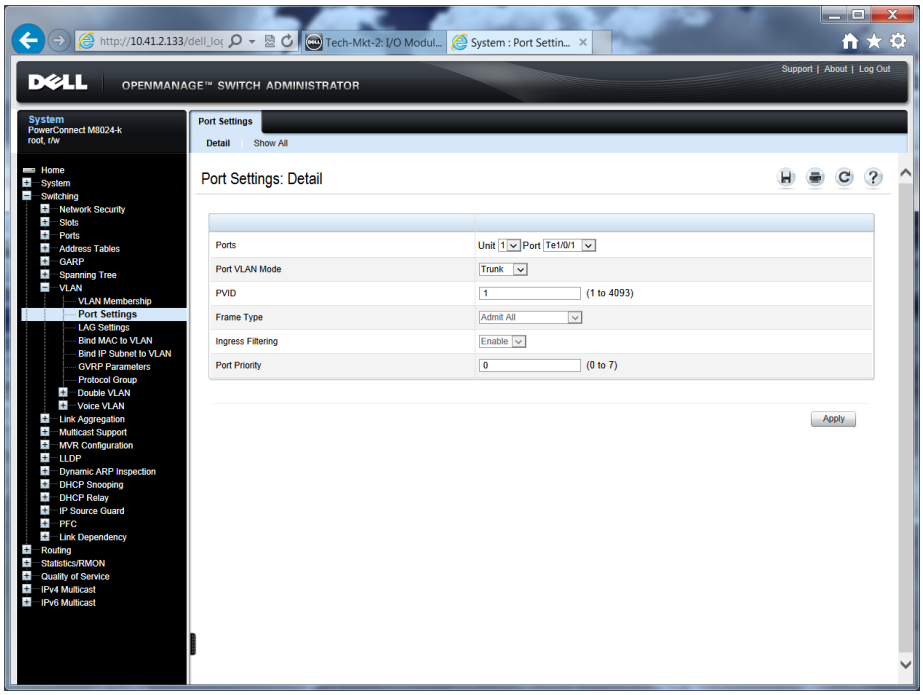

Figure 3: Configuring the M8024-k ports for VLAN traffic.

3. Click Save.
4. For Unit 1, Port Te1/0/2, use the Port VLAN Mode drop-down menu to select Trunk. Click Apply.
5. Click Save.

Configuring the PS-M4110 networking

1. From the CMC, select SLOT-03, and click Configure Array.
2. Enter member and group networking information and credentials (Figure 4). Use Fabric B.

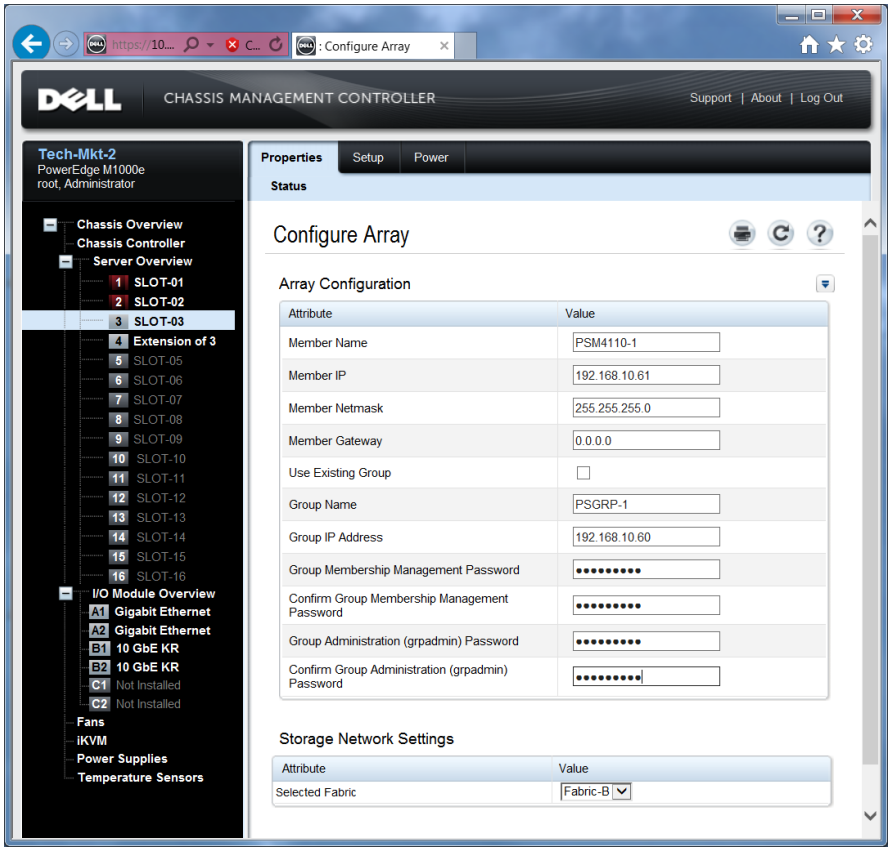

Figure 4: Configuring the PS-M4110 networking.

Note: With this configuration, the iSCSI subnet will also be used for management of the PS-M4110. To separate management and iSCSI network traffic, it is possible to set up management access through the CMC to Ethernet port 1 on the PS-M4110. Further information can be found in Setting up a Dedicated Management Port (page 46) in the Dell EqualLogic PS-M4110 Blade Storage Arrays Installation Guide.[1]

3. Click Apply.

Configuring the PowerEdge M620 blade servers

For more detailed steps, see Appendix B.

1. Connect a monitor, mouse, and keyboard to the KVM module on the back or the front of the M1000e.
2. Press the Ctrl key twice rapidly to access the KVM menu and select the desired blade.

[1] Access to the guide requires an EqualLogic support account (this comes included with your Dell EqualLogic array). The direct link to this page is https://eqlsupport.dell.com/support/download_file.aspx?id=1648&langtype=1033

3. Attach an external DVD drive with the Windows Server 2012 installation media to the desired blade.
4. Power on the blade server, and install Windows Server 2012 Datacenter Edition with a GUI. Repeat for the other blade server.
5. Assign static IP addresses to the blade server NICs. In our setup, we used the first port on the onboard NIC for domain-connected network traffic and the second port for Live Migration. Ensure that the ports used for Live Migration have a VLAN ID and are on a separate subnet from the domain. We used both ports on the mezzanine card for iSCSI.
6. Join the M620 blades to the domain.
7. Add the MPIO feature to both blades.

Configuring the PS-M4110 storage

For more detailed steps, see Appendix C.

1. From one of the M620 blades, use Internet Explorer® to navigate to the group IP address. Log in with the credentials supplied earlier.
2. Under Members, right-click the PS-M4110 to access the initial configuration wizard.
3. Configure the PS-M4110 with a RAID policy and initial RAID capacity appropriate to your organization (Figure 5).

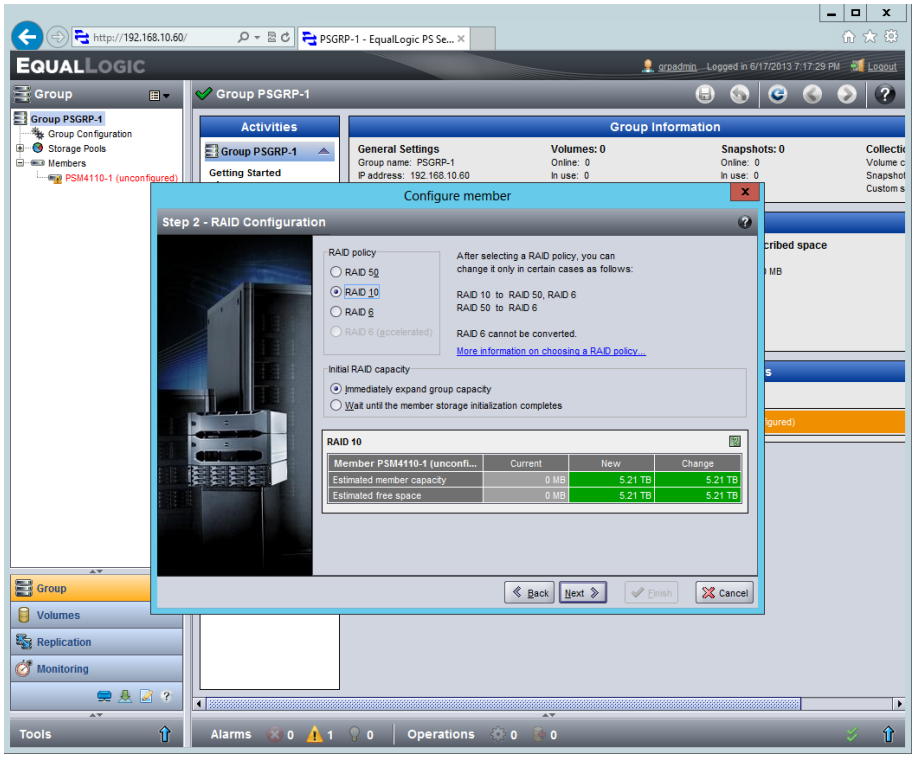

Figure 5: Configuring the PS-M4110 RAID policy.

4. Create volumes based on your organizational needs (Figure 6). For this guide, you will require at least two volumes: one for Quorum and one for storing the VMs' virtual hard drives. In our setup, we created these volumes with the following sizes:
    - Quorum, 10 GB
    - VHDs, 2 TB

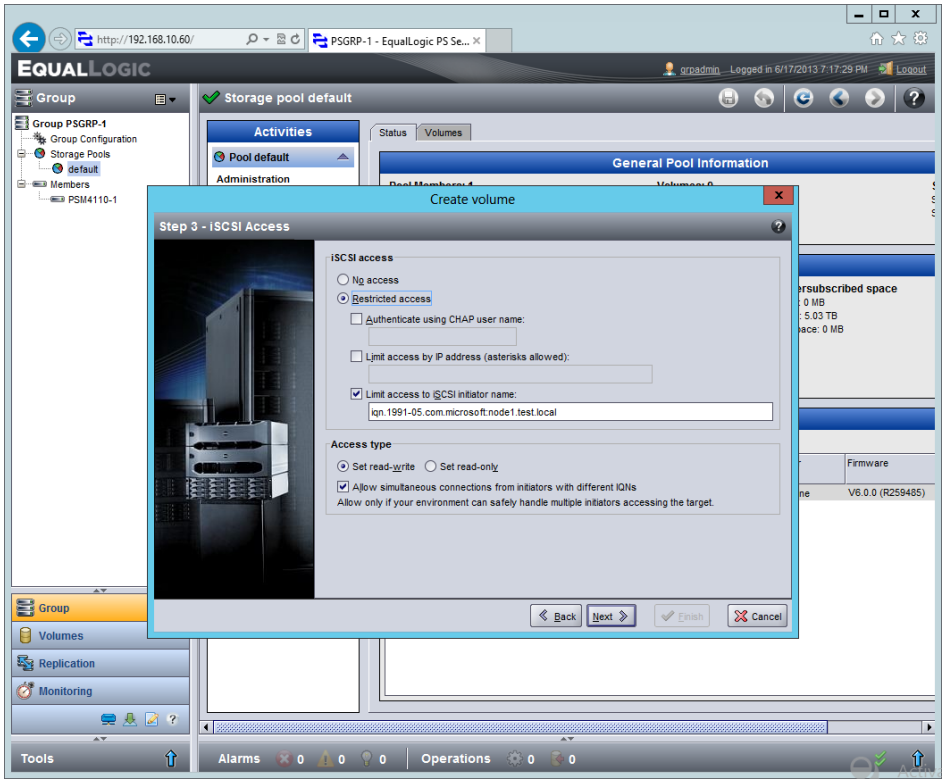

Figure 6: Creating a volume on the PS-M4110.

5. Provide access to each volume for both host server (Dell PowerEdge M620) IQNs (Figures 7 and 8).

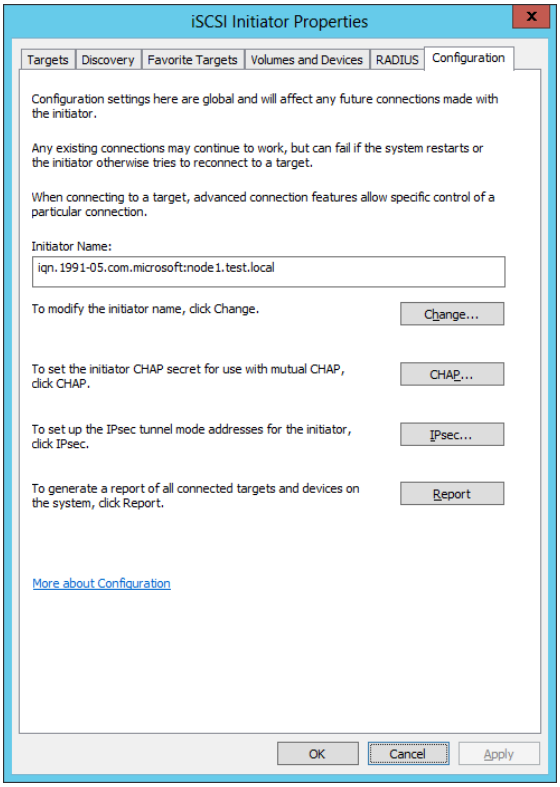

Figure 7: Finding the IQN.

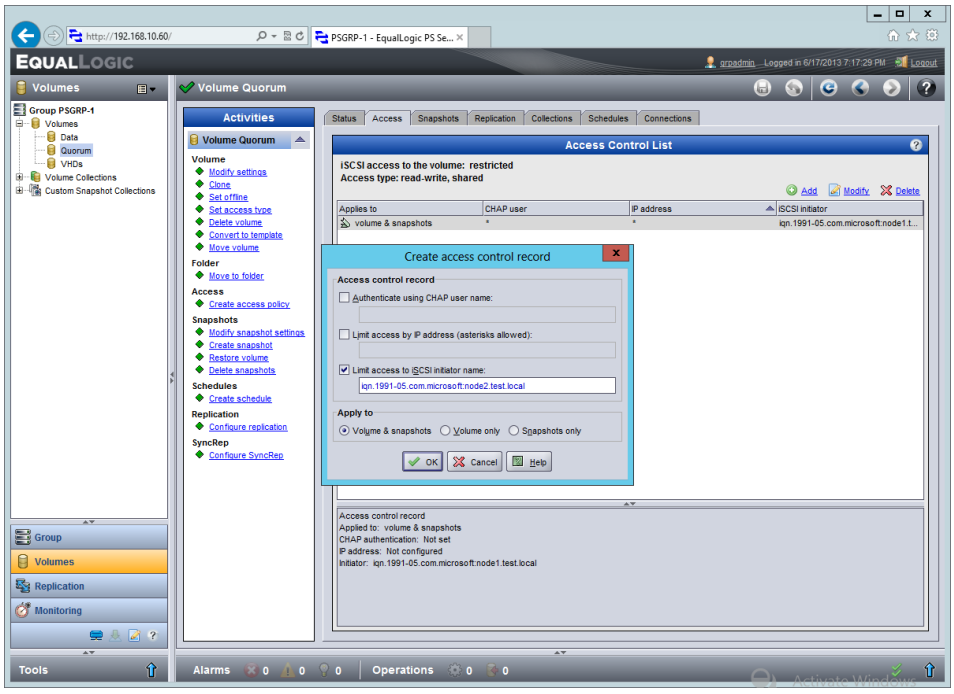

Figure 8: Providing multiple IQNs access to a volume.

Configuring the volumes in the OS

1. Use iSCSI Initiator to connect each M620 to the volumes. Ensure that multi-pathing is enabled.
2. Use Disk Management to bring the disks online and initialize them to create MBR partitions.
3. Create volumes on the disks but do not assign drive letters (Figure 9).

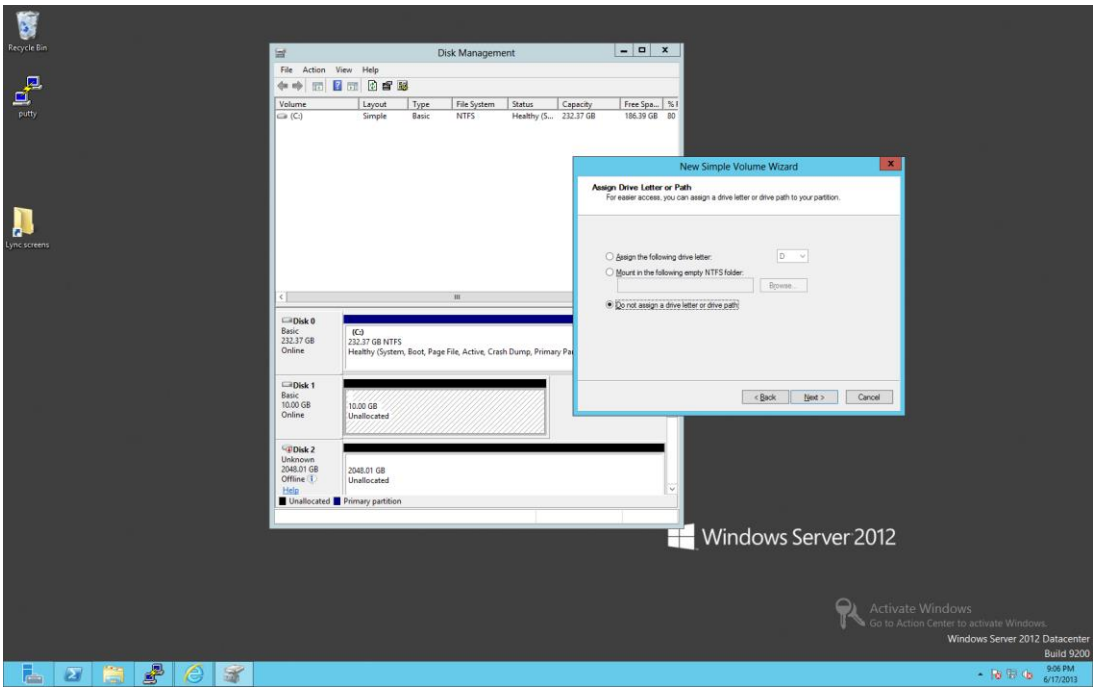

Figure 9: Preparing the volumes for cluster shared storage.

4. Once the volumes are configured on one M620, bringing them online on the second M620 will carry the settings over.

Creating the failover cluster

For more detailed steps, see Appendix D.

1. Use Server Manager to install the Failover Cluster feature on both M620s, and restart them.
2. From one of the M620s, which we will refer to as a node, open Failover Cluster Manager and validate the configuration (Figure 10). In the report, ensure that the iSCSI volumes show up under List Potential Cluster Disks.

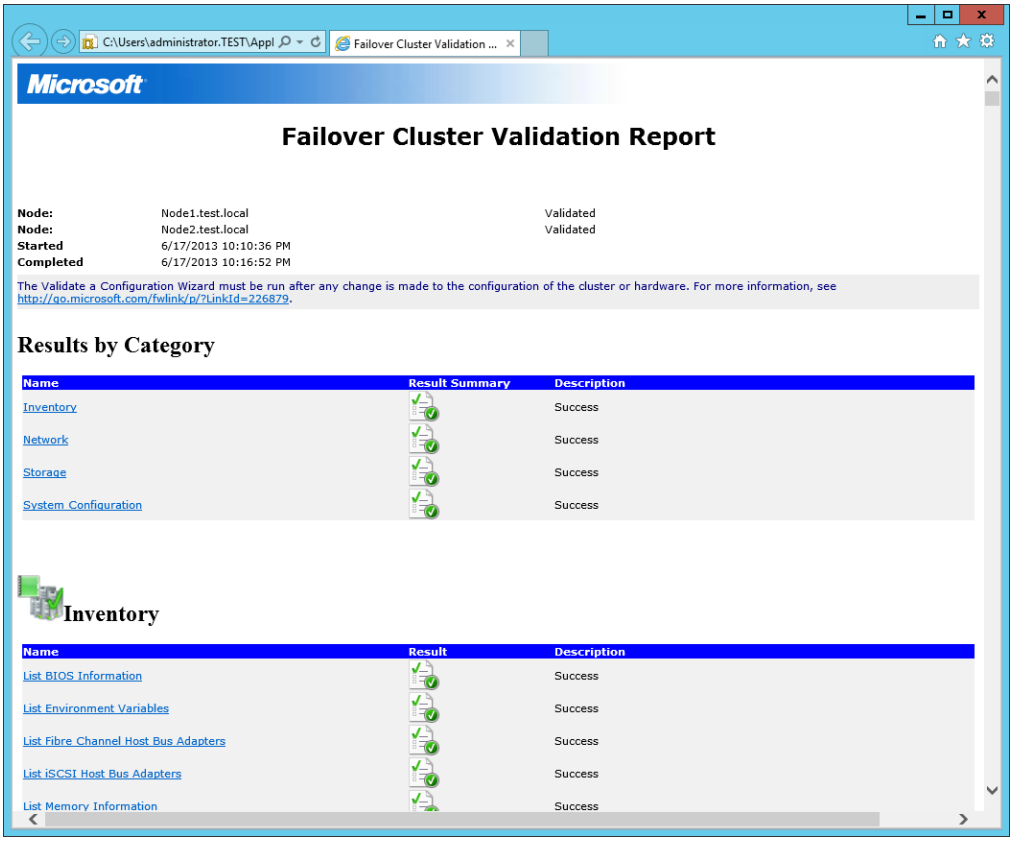

Figure 10: Successful cluster validation check.

3. Create the cluster, adding all available storage.
4. Download and install Update for Windows Server 2012 (KB2803748), a hotfix to prevent Microsoft Management Console crashes in Failover Cluster Manager from http://www.microsoft.com/en-us/download/details.aspx?id=36468.
5. Restart both nodes.

Configuring the failover cluster

1. Verify the network properties for each network in Failover Cluster Manager, and ensure that the iSCSI network is not used for cluster traffic.
2. Use the Live Migration settings to assign the appropriate network you will use for this purpose.
3. Set the Quorum disk to be used as the disk witness for quorum. This may have been set automatically. If not, use the following steps:
   a. Click More Actions→Configure Cluster Quorum Settings.
   b. Click Next.

c. Select Advanced quorum configuration and witness selection, and click Next.

d. Select All nodes, and click Next.

e. Leave the Allow cluster to dynamically manage the assignment of node votes checkbox checked, and click Next.

f. Select Configure a disk witness, and click Next.

g. Select the disk to be used for quorum, and click Next.

h. Click Next.

i. Click Finish.

4. Make the disk designated for VHDs into a Cluster Shared Volume.

5. Install Dell Host Integration Tools 4.5.0 onto both blades. Enable all features during installation.

6. Adjust the MPIO settings in Auto-Snapshot Manager to remove any subnets not being used for iSCSI (Figure 11).

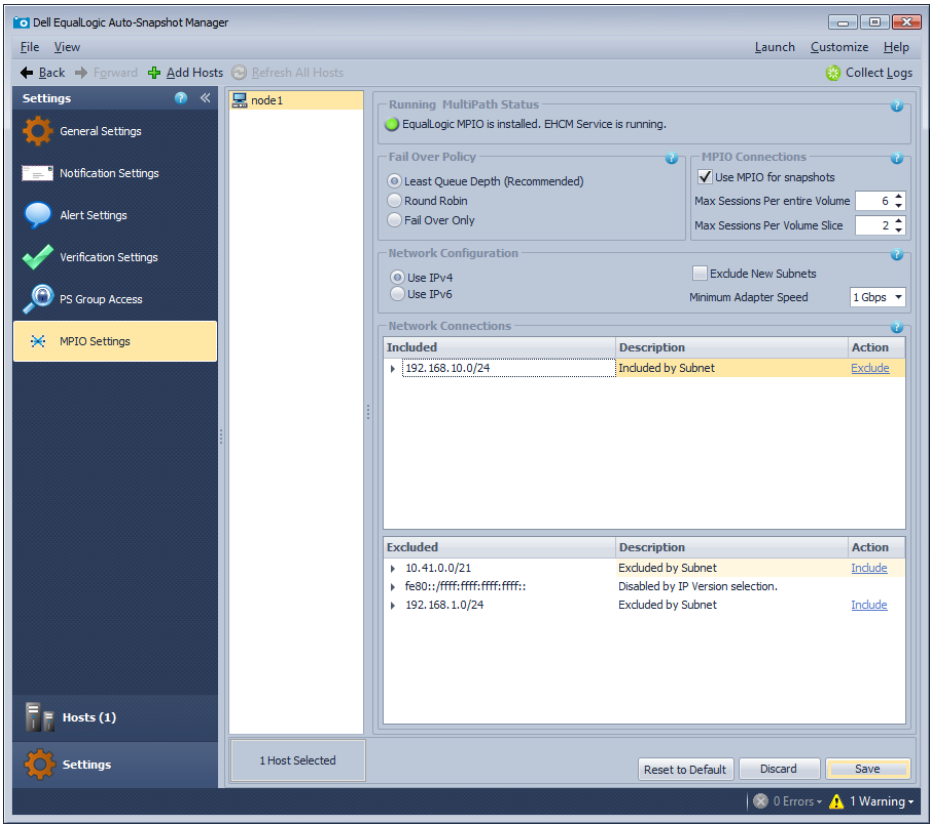

Figure 11: Excluding subnets from iSCSI traffic.

Creating the VMs

1. Install the Hyper-V role on both nodes. Do not configure a virtual switch or live migration. Set the default stores to use the VHDs' cluster shared volume. The default path for shared cluster storage is C:\ClusterStorage.
2. Create an external virtual switch on each node using a domain-connected NIC adapter (Figure 12). These switches must have exactly the same name between nodes.

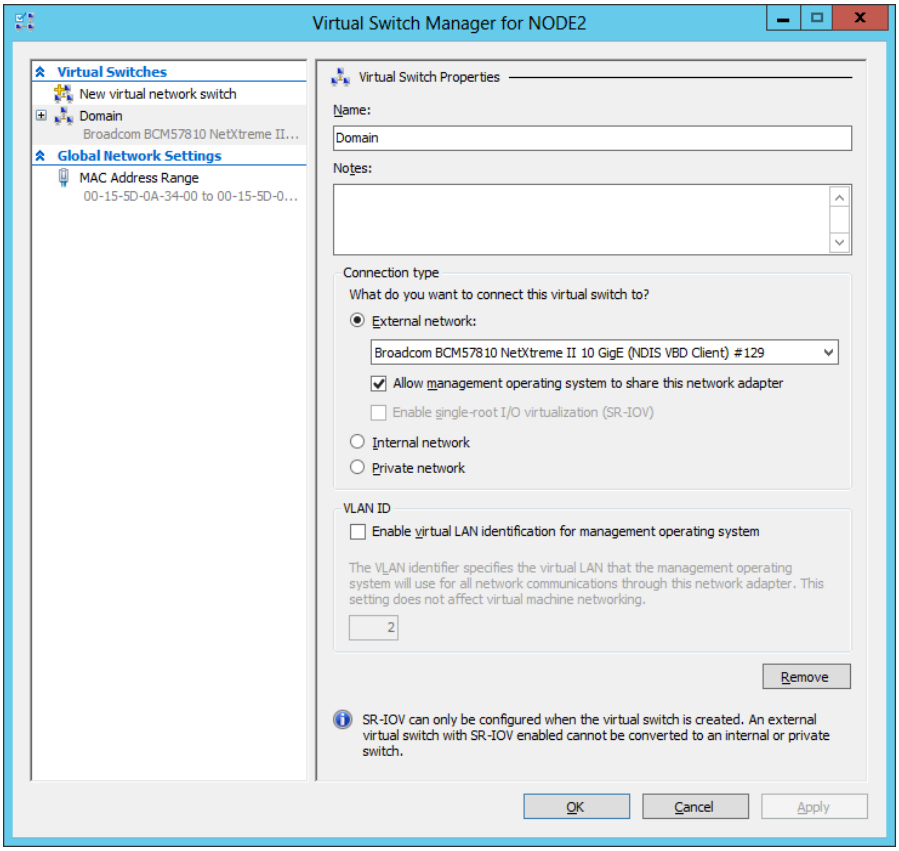

Figure 12: Creating the virtual switches.

3. Use Failover Cluster Manager to create three VMs (Figure 13; you can find further information on Lync Server 2013 hardware requirements at technet.microsoft.com/en-us/library/gg398438.aspx):
    - LSFE01 on Node 1. This will be the primary Front End.
    - LSFE02 on Node 2. This will be the backup Front End.
    - LSFS on any node. This will be the file server and quorum witness.

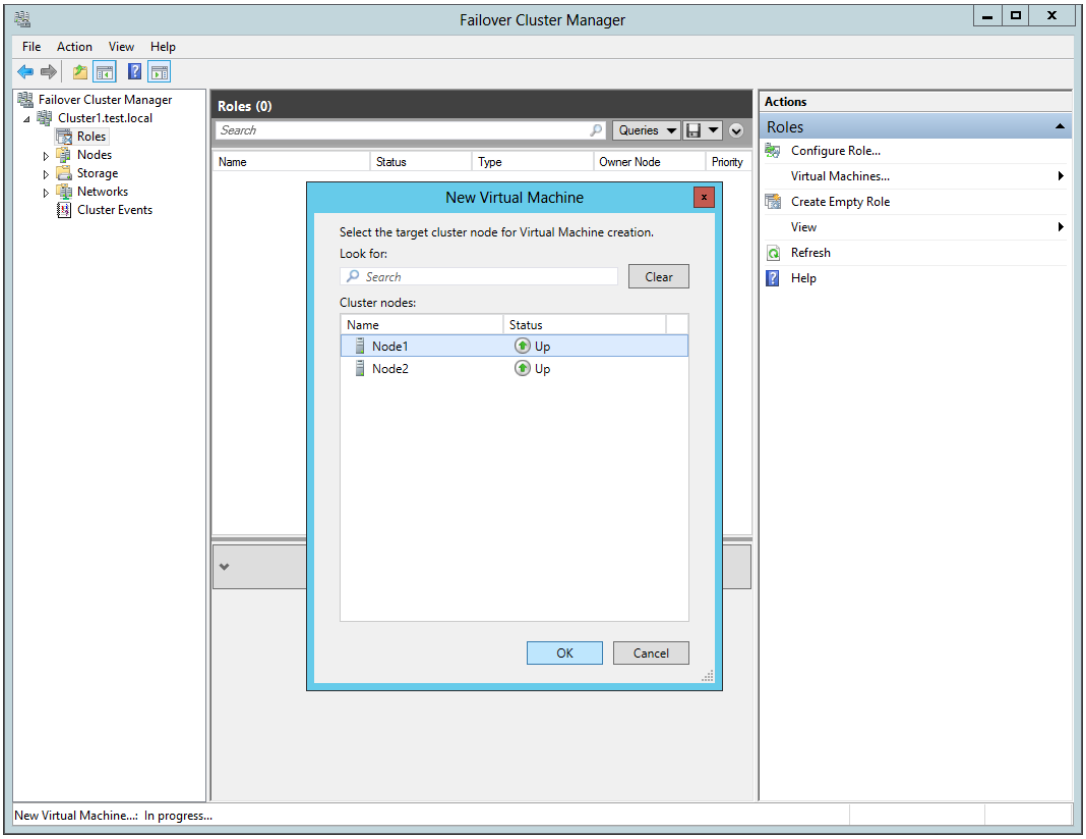

Figure 13: Creating a VM in Failover Cluster Manager.

4. Install Windows Server 2012 Datacenter Edition with a GUI on each VM.
5. Connect the virtual switch to each VM.
6. Connect the VMs to the domain.

Creating the Lync Server file shares

On the file server VM, create two directories (one for each Front End) on the C:\ drive and allow read and write access to the following groups (Figure 14):

- RTCComponentUniversalServices
- RTCHSUniversalServices
- RTCUniversalConfigReplicator
- RTCUniversalServerAdmins

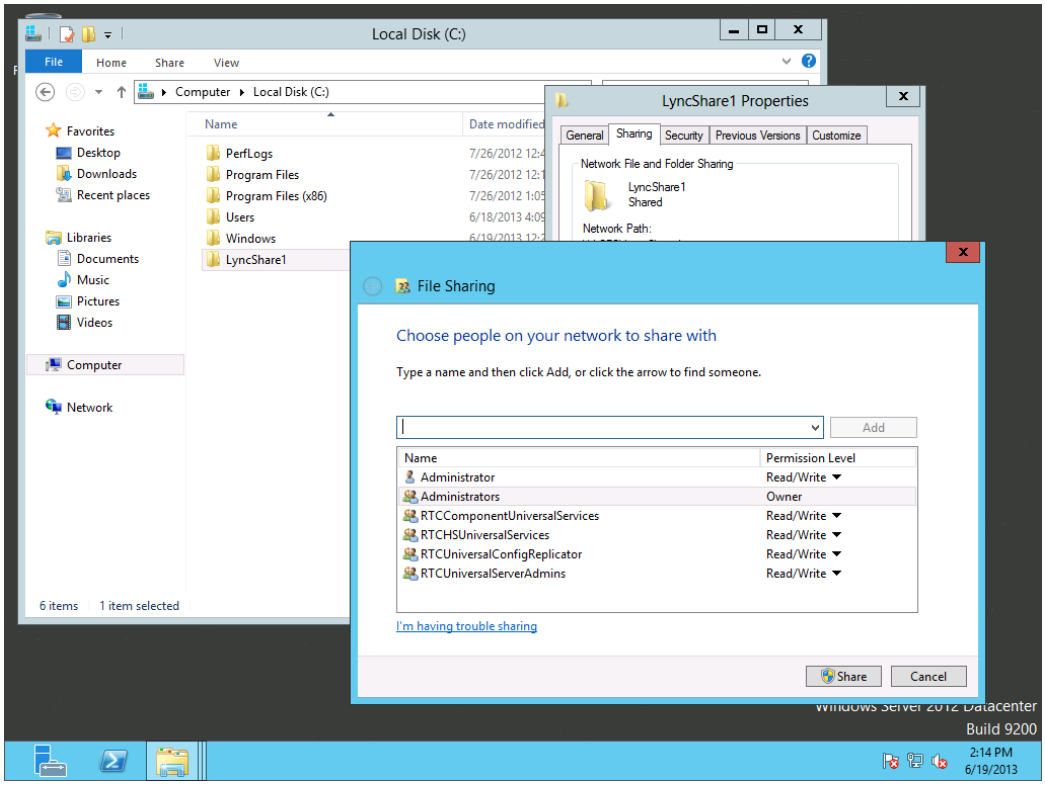

Figure 14: Creating the first file share. Repeat for LyncShare2.

Preparing the Active Directory for Lync

For more detailed steps, see Appendix E.

1. Use the Lync Server 2013 setup GUI to prepare the schema, forest, and domain (Figure 15).

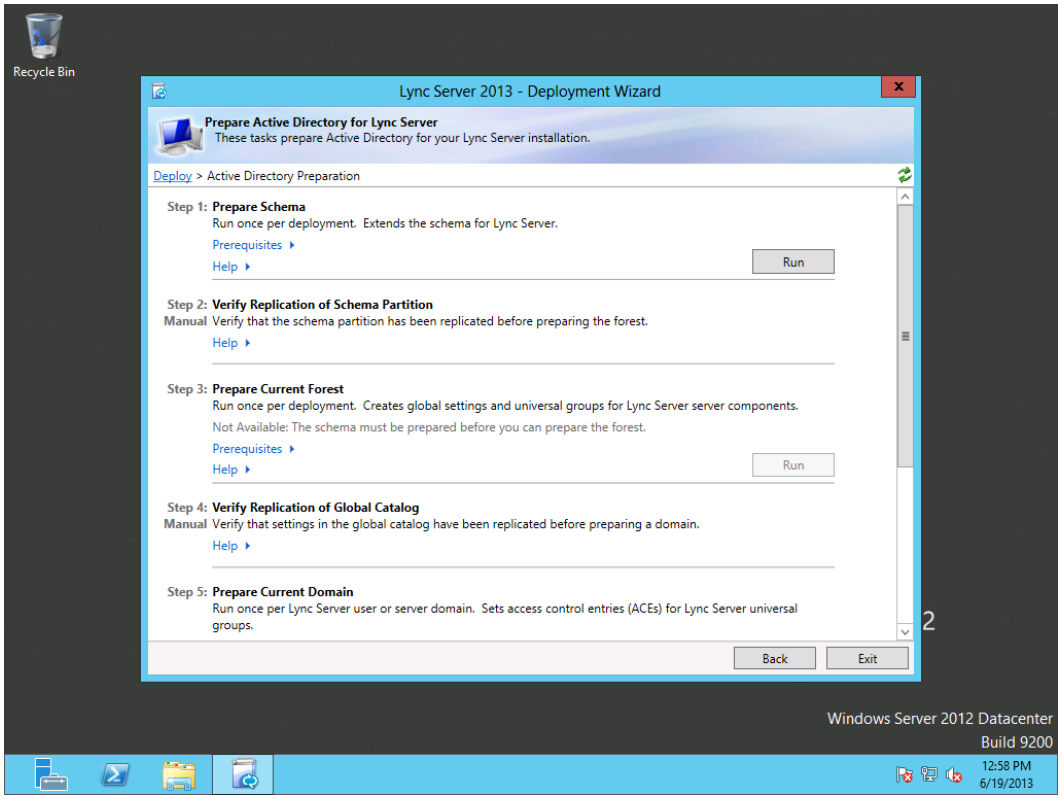

Figure 15: Preparing the Active Directory for Lync.

2. Use Active Directory Users and Computers to make the user account you plan to use for managing Lync a member of the CSAdministrator and RTCUniversalServerAdmins groups.
3. Using DNS Manager, create a new Service Location record with the following properties (Figure 16; Use your own Front End FQDN):
    - Service: `_sipinternaltls`
    - Protocol: `_tcp`
    - Port Number: `5061`
    - Host offering this service: `LSFE01.test.local`

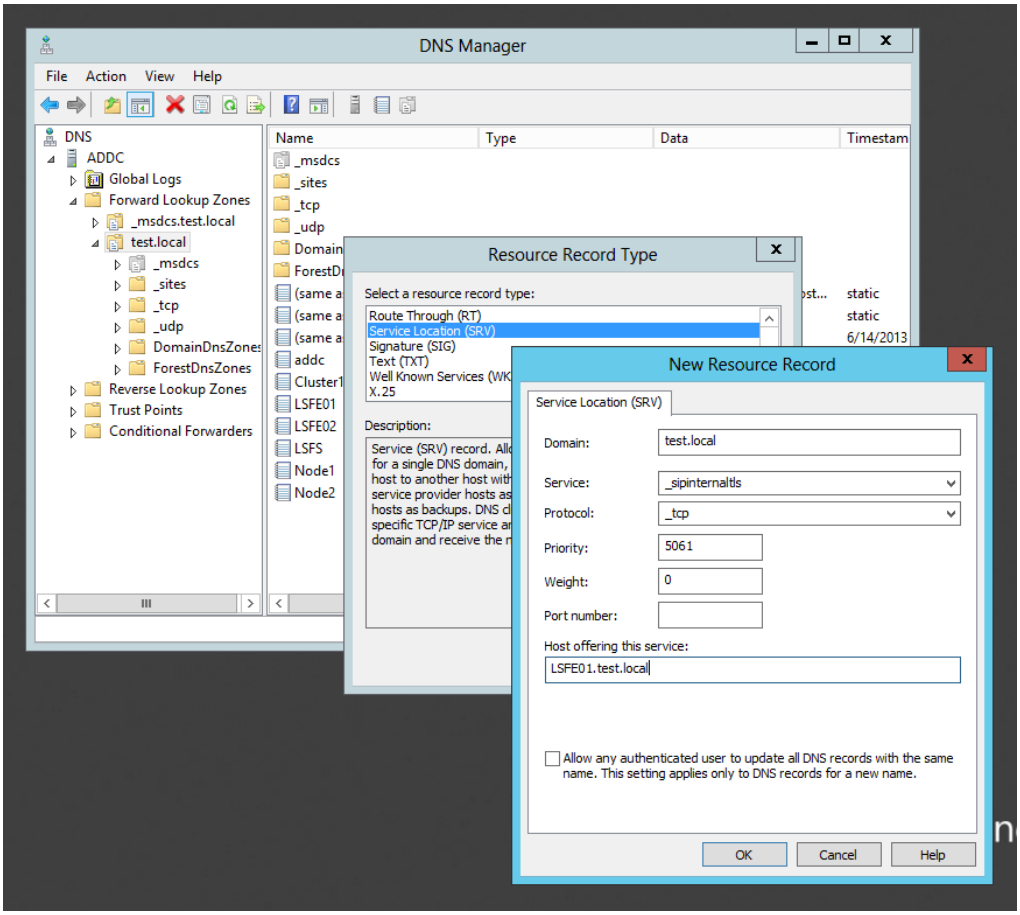

Figure 16: Creating a Service Location Record for the primary Front End VM.

4. Create DNS hosts on the Front End IP address for the following (Figure 17; Use your Front End IP address):
    - meet
    - dialin
    - admin

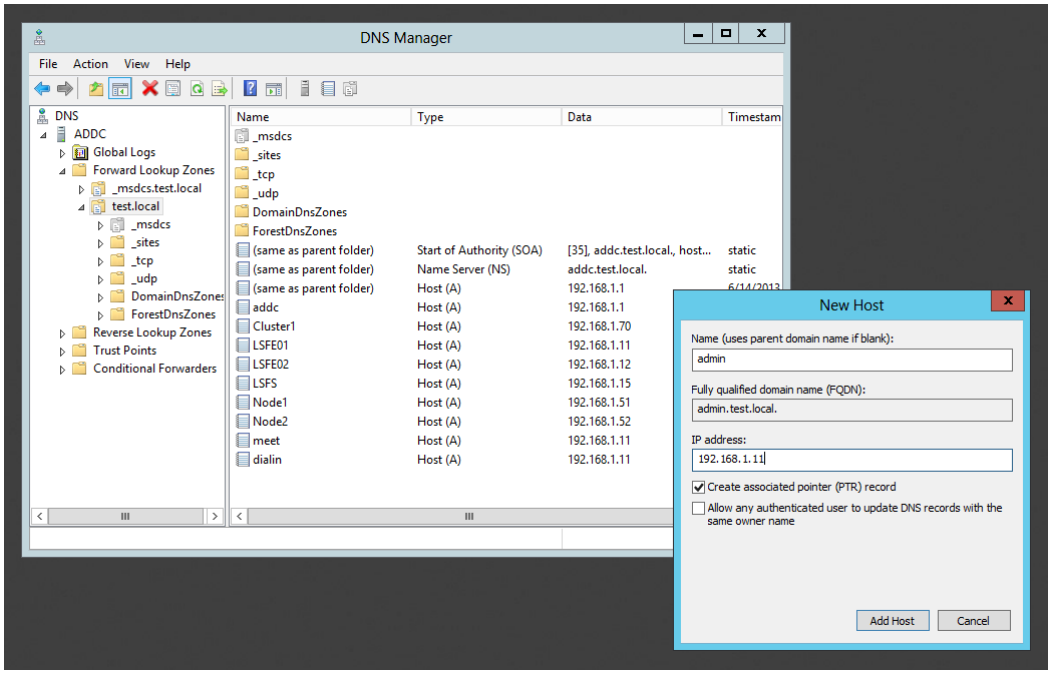

Figure 17: Creating the meet, dialin, and admin DNS entries.

Preparing the primary Front End VM

1. Attach the Windows Server 2012 installation media to the VM and run the following PowerShell command:

   ```
   Install-WindowsFeature RSAT-ADDS, Web-Server, Web-Static-Content, Web-Default-Doc, Web-Http-Errors, Web-Asp-Net, Web-Net-Ext, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Http-Logging, Web-Log-Libraries, Web-Request-Monitor, Web-Http-Tracing, Web-Basic-Auth, Web-Windows-Auth, Web-Client-Auth, Web-Filtering, Web-Stat-Compression, Web-Dyn-Compression, NET-WCF-HTTP-Activation45, Web-Asp-Net45, Web-Mgmt-Tools, Web-Scripting-Tools, Web-Mgmt-Compat, Windows-Identity-Foundation, Desktop-Experience, Telnet-Client, BITS -Source D:\sources\sxs -Restart
   ```

2. After the VM has restarted, attach the Lync Server 2013 installation media and use the setup GUI to run Prepare First Standard Edition Server (Figure 18).

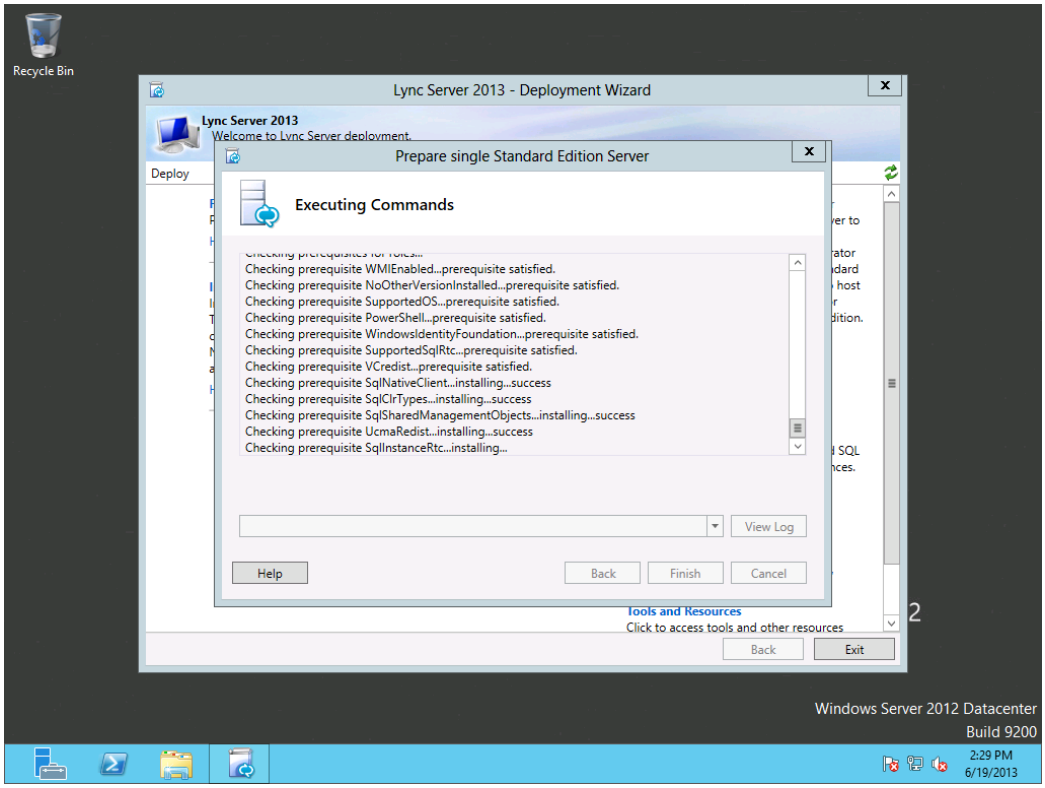

Figure 18: Preparing the primary Front End.

Building the topology

For more detailed steps, see Appendix F.

1. Use the Lync Server 2013 setup GUI to install the Lync administrative tools.
2. Use the Lync Server Topology Builder to create a new topology.
3. Add a new Standard Edition Front End Server to the topology with the desired features and one of the shared directories as the Lync file store (Figures 19 and 20).
   a. For our setup, we chose a basic deployment with the following features:
      - Conferencing with Dial-in
      - Call Admission Control
      - Collocate Mediation Server

      For more information on deploying other features such as Enterprise Voice, Archiving, Monitoring, and external user access, see http://technet.microsoft.com/en-us/library/gg398664.aspx.

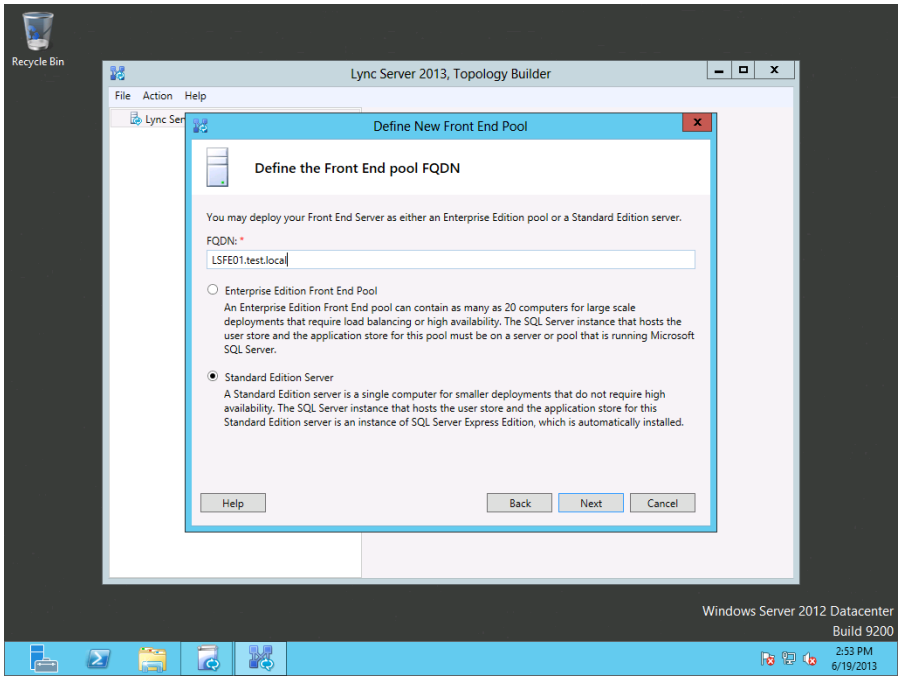

Figure 19: Defining the primary Front End pool FQDN.

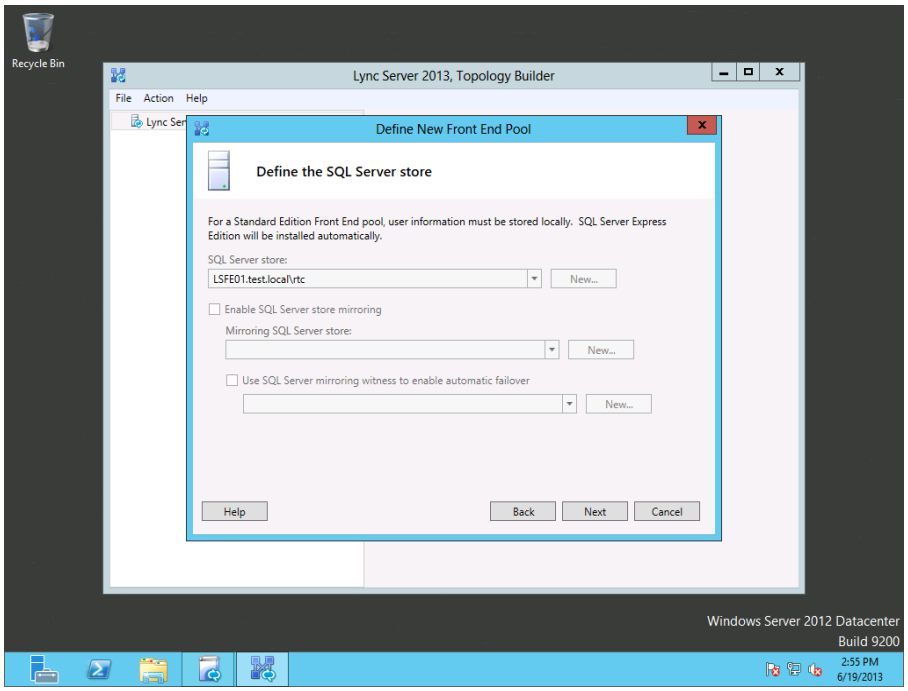

Figure 20: Defining the SQL Server store.

4. Edit the topology properties to set the Administrative access URL (We used `https://admin.test.local`) and the server to host the Central

Management Store. For our setup, we used the primary Front End VM (Figure 21).

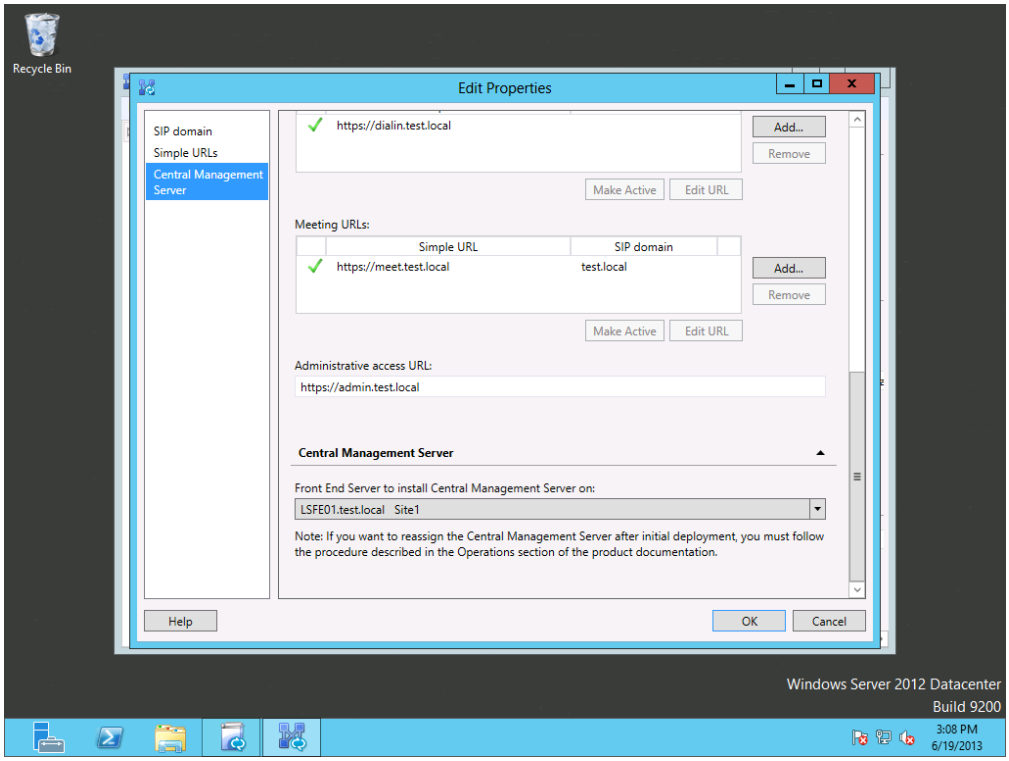

Figure 21: Setting the Administrative access URL and the Central Management Server.

5. Publish the topology (Figure 22).

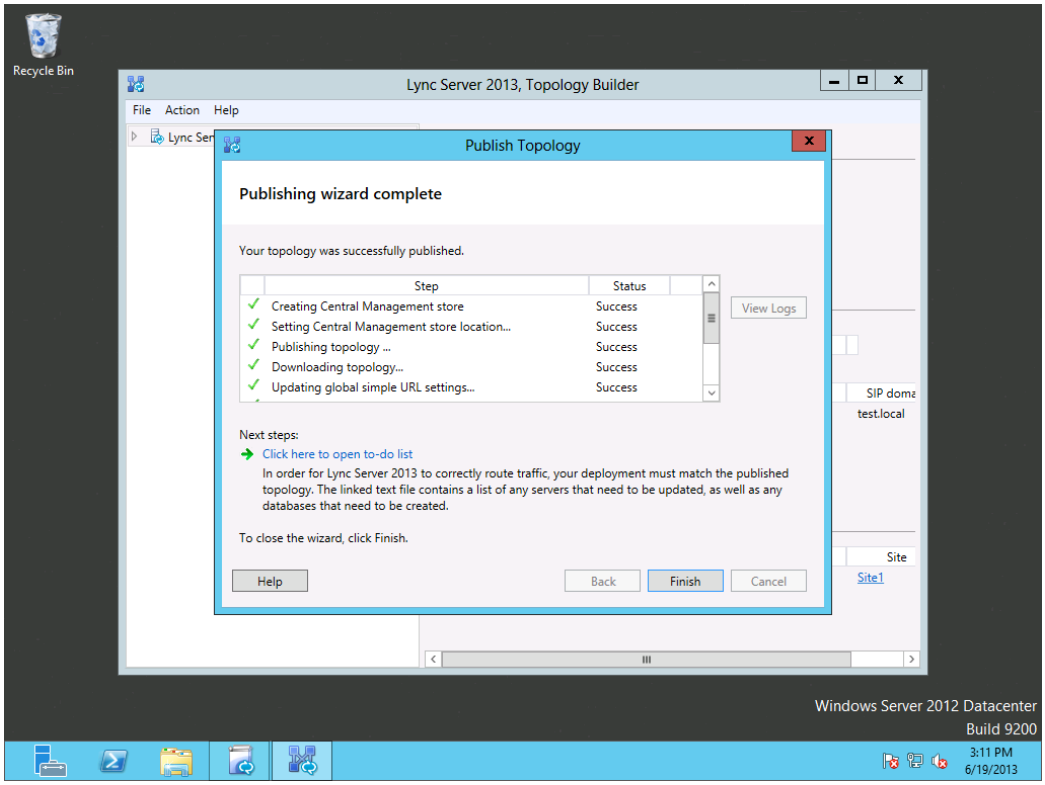

Figure 22: Publishing the topology.

Installing the configuration to the primary Front End VM

1. Log into the primary Front End VM with Domain Admin credentials.
2. In the Lync Server 2013 setup GUI, navigate to the section titled Install or Update Lync Server System, which takes you to the installation components page (Figure 23). As a general note, steps 2 (Setup or Remove Lync Server Components) and 4 (Start Services) will need to be run on each Front End after each time the topology is published.

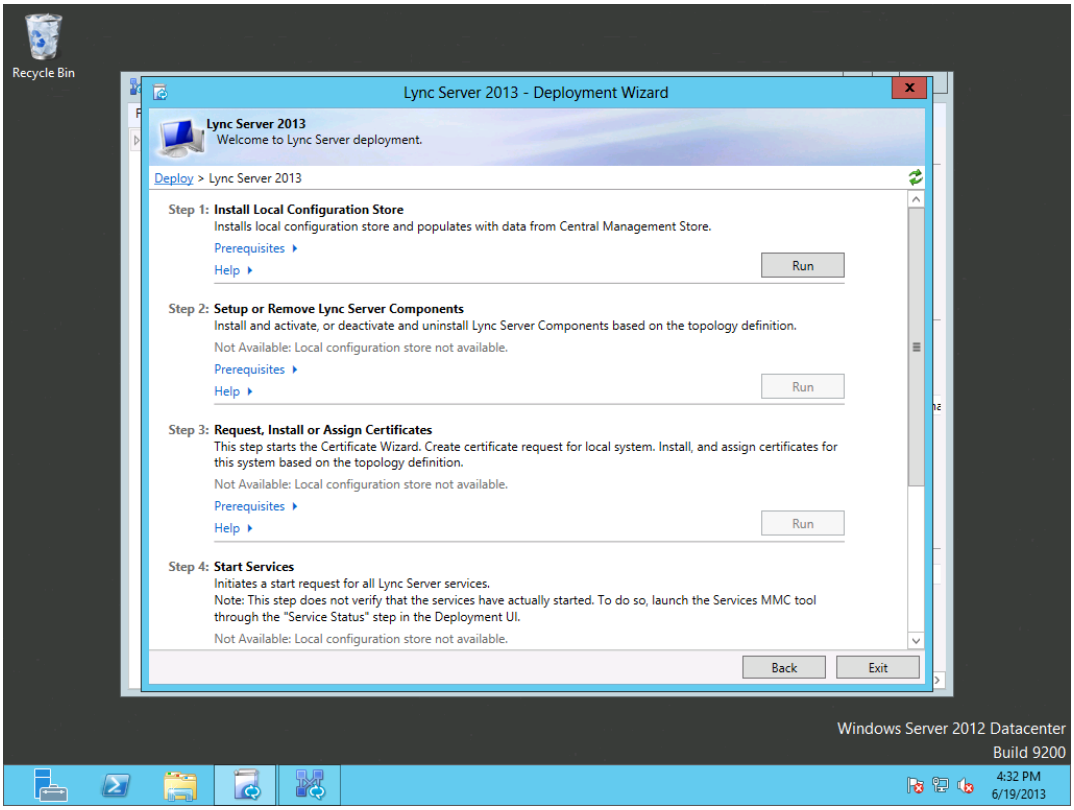

Figure 23: Installing the configuration to the primary Front End VM.

3. Run Step 1: Install Local Configuration Store. Retrieve the configuration directly from the Central Management store.
4. Run Step 2: Setup or Remove Lync Server Components.
5. Run Step 3: Request, Install or Assign Certificates. Request and assign the Default and OAuthTokenIssuer certificates (Figures 24 and 25).

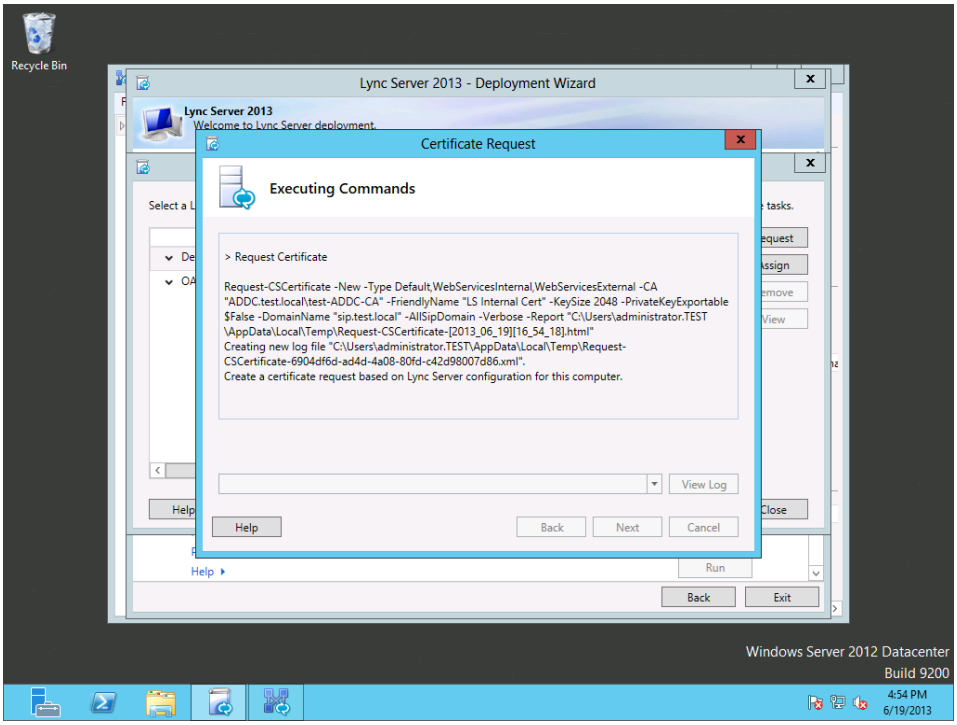

Figure 24: Requesting the default certificate.

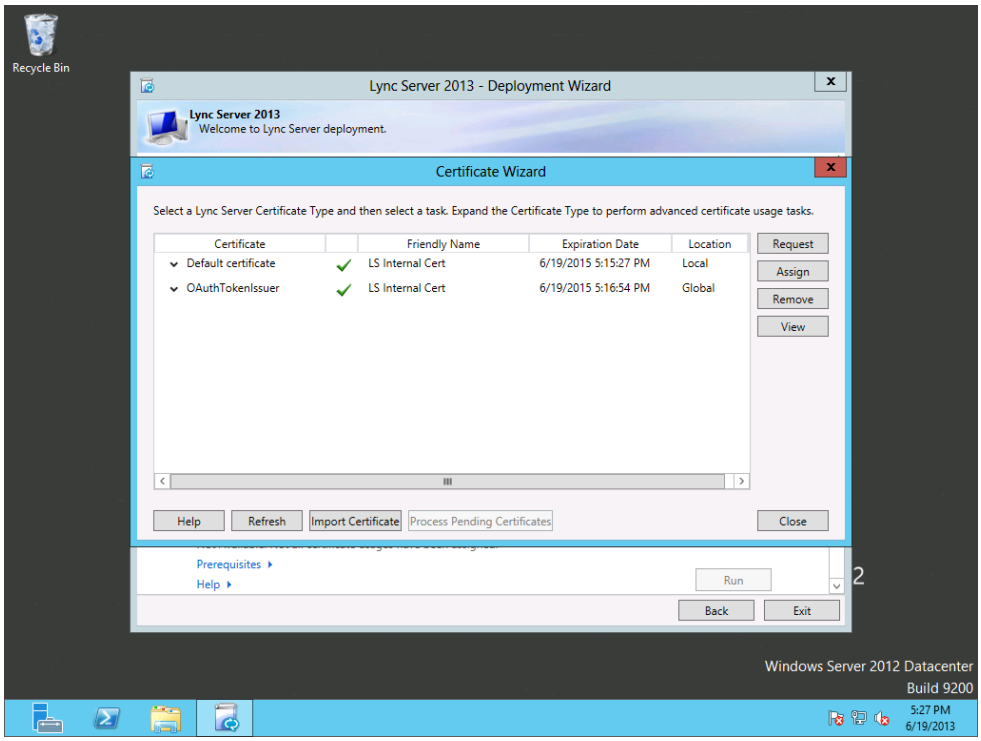

Figure 25: Certificates successfully assigned.

6. Run Step 4: Start Services. Ensure that all Lync services are running.

Adding the secondary Front End VM to the topology

1. In Lync Server Topology Builder, right-click Standard Edition Front End Servers, and click New Front End Pool (Figure 26).

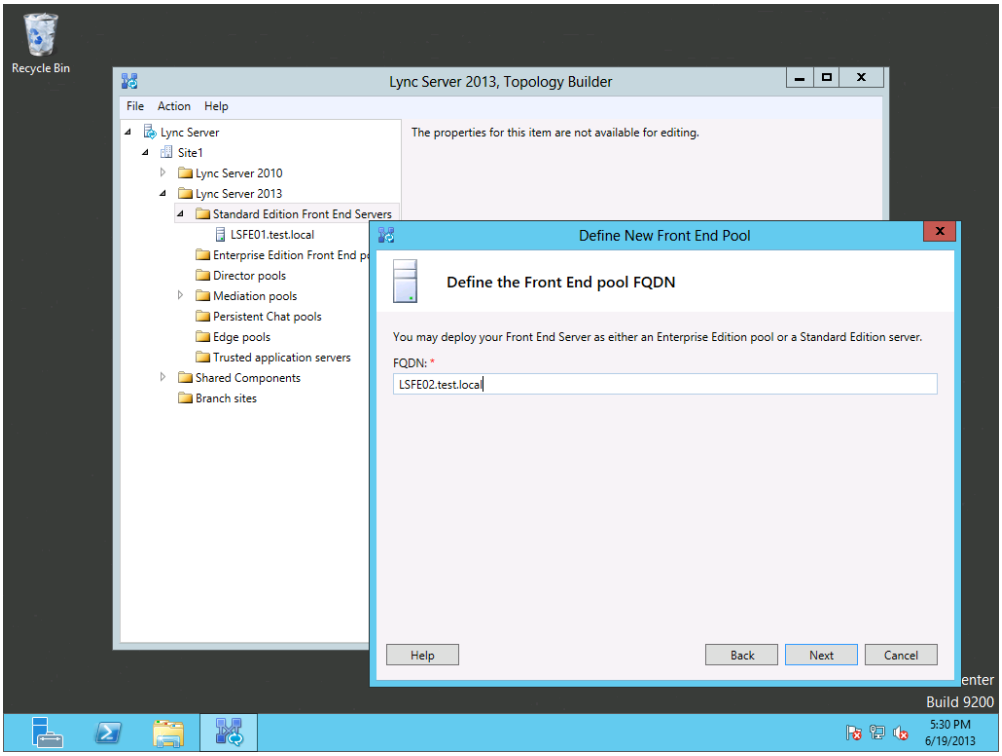

Figure 26: Adding the secondary Front End VM to the topology.

2. Follow the wizard to select features for the secondary Front End VM. In general, these should match the features selected for the primary Front End (Figure 27). Use the second shared directory for the file store.

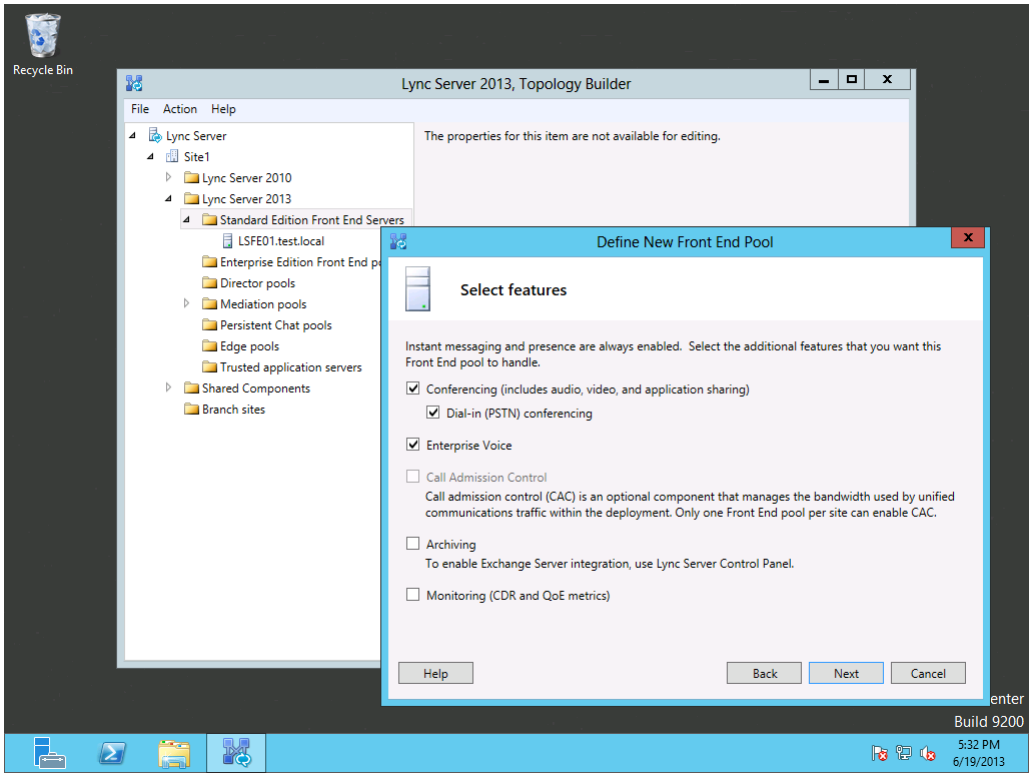

Figure 27: Selecting features for the secondary Front End VM.

3. Publish the topology.

Updating the primary Front End VM

1. On the primary Front End VM, re-run steps 2 and 4 under Install or Update Lync Server System (Figure 28).

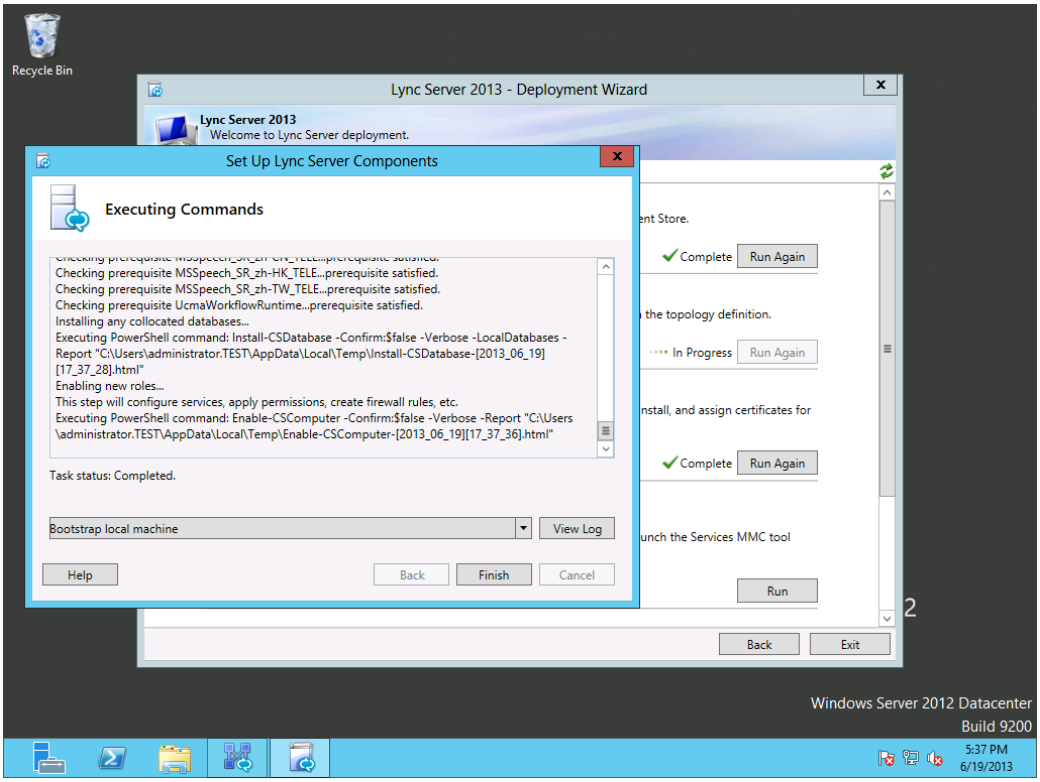

Figure 28: Updating the primary Front End VM.

Installing the configuration to the secondary Front End VM

1. On the secondary Front End VM, run the following Windows PowerShell command:

   ```
   Install-WindowsFeature RSAT-ADDS, Web-Server, Web-Static-Content, Web-Default-Doc, Web-Http-Errors, Web-Asp-Net, Web-Net-Ext, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Http-Logging, Web-Log-Libraries, Web-Request-Monitor, Web-Http-Tracing, Web-Basic-Auth, Web-Windows-Auth, Web-Client-Auth, Web-Filtering, Web-Stat-Compression, Web-Dyn-Compression, NET-WCF-HTTP-Activation45, Web-Asp-Net45, Web-Mgmt-Tools, Web-Scripting-Tools, Web-Mgmt-Compat, Windows-Identity-Foundation, Desktop-Experience, Telnet-Client, BITS -Source D:\sources\sxs –Restart
   ```

2. After the VM restarts, run all four steps under Install or Update Lync Server System (Figure 29). The OAuthTokenIssuer certificate should already be assigned.

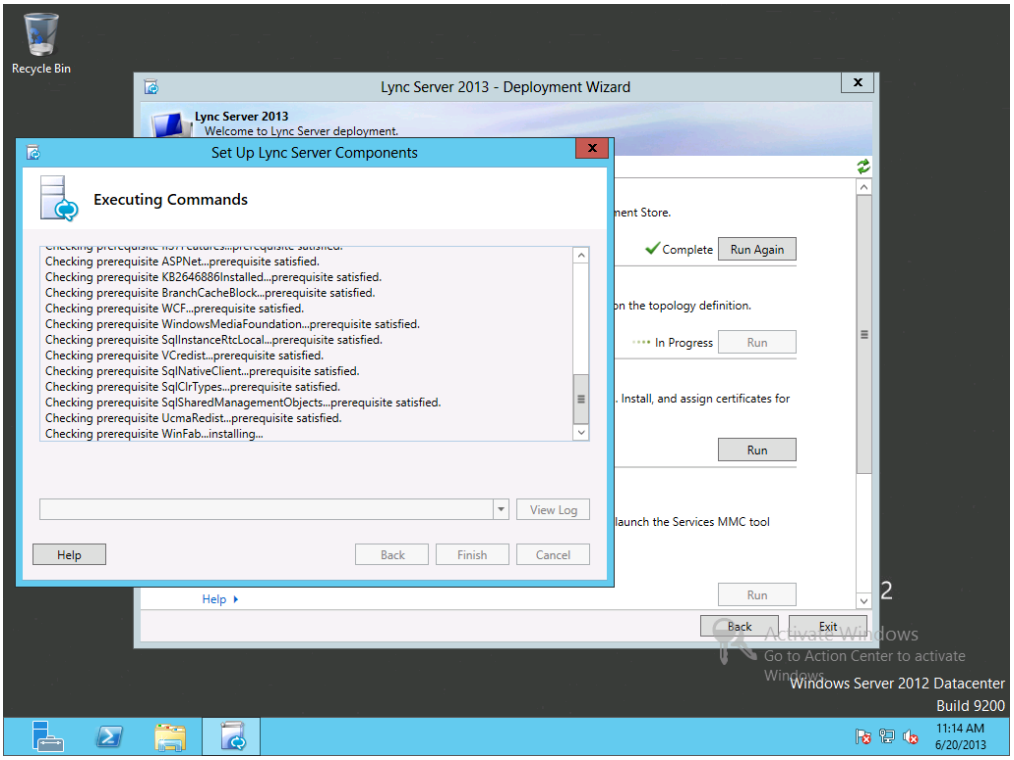

Figure 29: Installing the configuration to the secondary Front End VM.

Designating the secondary Front End pool as a backup

1. In Lync Server Topology Builder, open the primary Front End VM properties.
2. Under Resiliency, add the secondary Front End VM as a backup. Check the box for Automatic failover and failback for Voice and adjust the intervals to values appropriate for your organization (Figure 30).

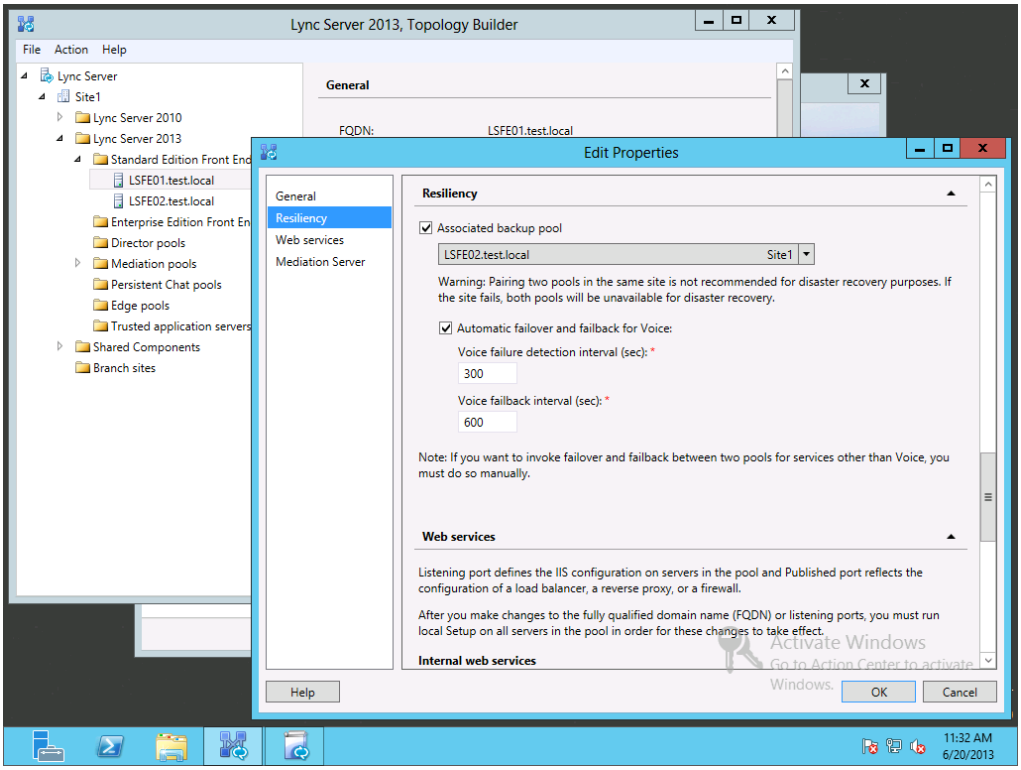

Figure 30: Designating the secondary Front End VM as the backup.

3. Publish the topology.
4. On each Front End VM, re-run steps 2 and 4 under Install or Update Lync Server System in the Lync Server setup GUI.
5. From the primary Front End VM, run the following Windows PowerShell commands (Figure 31; Use your Front End FQDNs):

```
Invoke-CSBackupServiceSync –PoolFqdn LSFE01.test.local
Invoke-CSBackupServiceSync –PoolFqdn LSFE02.test.local
```

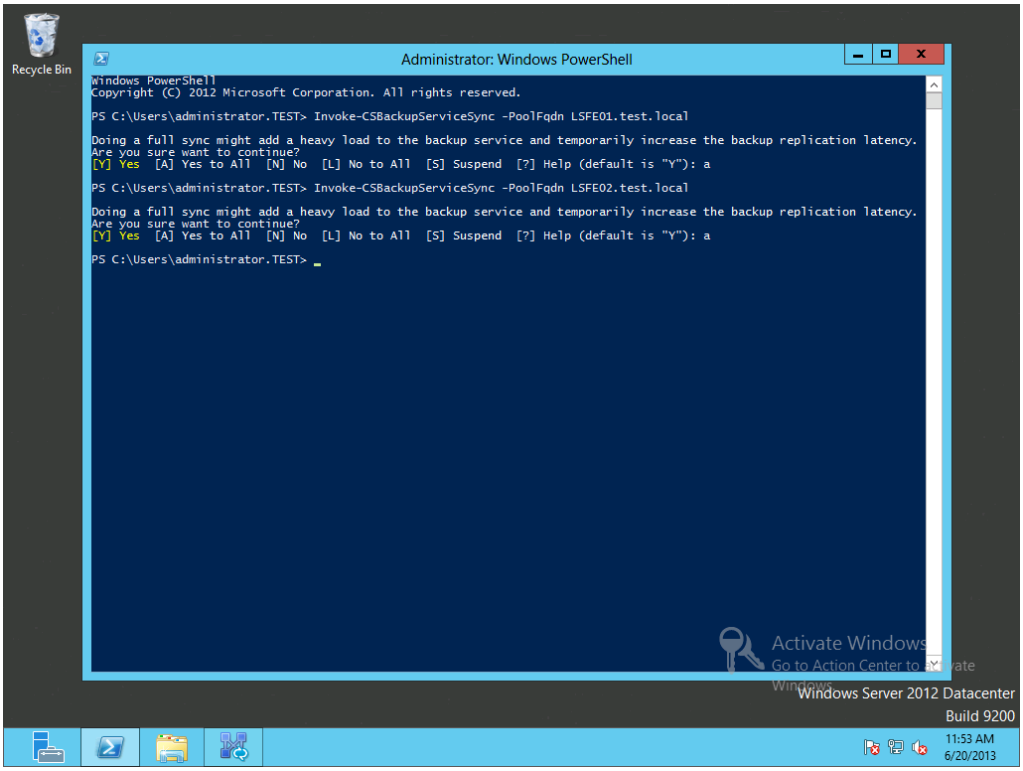

Figure 31: Syncing the backup service.

Adding the backup SRV

1. Using DNS Manager, create a new Service Location record with the following properties (Figure 32; Use your own backup Front End FQDN and take note that the priority and weight are different from the SRV created earlier):
    - Service: `_sipinternaltls`
    - Protocol: `_tcp`
    - Priority: `10`
    - Weight: `10`
    - Port Number: `5061`
    - Host offering this service: `LSFE02.test.local`

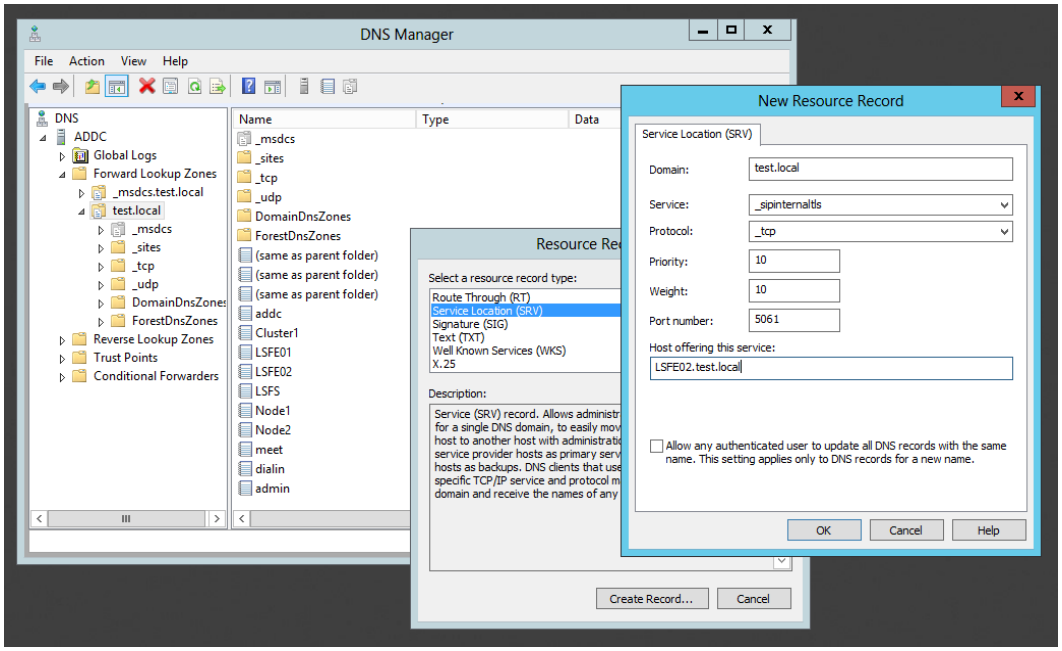

Figure 32: Adding the backup SRV.

Commands for manual failover

Lync Server Standard Edition will fail over Voice features automatically, but other features can be failed over manually. Use these commands to perform this operation. Please note that you must replace the FQDN in the sample commands below with the appropriate FQDN of your Front End VMs. In this example, LSFE01.test.local is the FDQN of the primary Front End VM, and LSFE02.test.local is the FDQN of the secondary Front End VM.

- To obtain the location of the Active Central Management Database:
  `Get-CsService –CentralManagement`
- To find the backup server (use your primary Front End FQDN):
- `Get-CsPoolBackupRelationship –PoolFqdn LSFE01.test.local` To check on the availability of the Central Management Store:
  `Get-CsManagementStoreReplicationStatus –CentralManagementStoreStatus`
- To manually fail over the Central Management Store to the backup server (replace the FQDN):
- `Invoke-CsManagementServerFailover –BackupSqlerverFqdn LSFE02.test.local –`

```
BackupSqlInstanceName RTC –Force
```
To manually fail over the Front End pool to the backup server:

```
Invoke-CsPoolFailOver –PoolFqdn LSFE01.test.local
–Disastermode –Verbose
```

- To fail back to the primary server:

```
Invoke-CsPoolFailback –PoolFqdn LSFE01.test.local
–Verbose
```

```
Invoke-CsManagementServerFailover –
BackupSqlServerFqdn LSFE01.test.local –
BackupSqlInstanceName RTC -Force
```

SUMMING IT ALL UP

As this guide has shown, setting up a highly available Microsoft Lync Server 2013 environment on Dell architecture is a straightforward process. In little time, you can deploy two Dell PowerEdge M620 M-series servers, switches, and Dell EqualLogic storage using Microsoft Windows Server 2012, and set up your Lync Server 2013 infrastructure. By setting up a highly available Lync Server 2013 environment on your Dell architecture solution, you can ensure your office communications stay running with little to no downtime to keep your business moving.

APPENDIX A – INSTALLING THE HARDWARE AND CONFIGURING THE NETWORKING

Installing the hardware

1. Provide a DHCP-enabled network connection to both Chassis Management Controller (CMC) modules on the back of the M1000e blade enclosure. This will provide the CMCs and the blade server iDRACs with IP addresses. If you are not using DHCP, you will need to specify a static IP address and subnet mask for the CMC using the front control panel. Specifying IP addresses for the iDRACs is optional for this guide.
2. Inside each blade server, there are two mezzanine slots: fabric B and fabric C (fabric A corresponds to the embedded NICs). Choose a slot in which to place the mezzanine NIC card. The chosen slot must match the fabric that will be used for the Dell PowerConnect M8028-k 10Gb Ethernet switches. In our setup, we used fabric B.
3. Insert the Dell PowerEdge M620 blade servers into slots 1 and 2 on the front of the enclosure and ensure that they are locked into place.
4. Insert the Dell EqualLogic PS-M4110 blade storage into slots 3 and 4 on the front of the enclosure and ensure that it is locked into place.
5. Insert the first pair of Dell PowerConnect M8024-k 10Gb Ethernet switches into slots A1 and A2 on the back of the enclosure and ensure that they are locked into place.
6. Insert the remaining Dell PowerConnect M8024-k 10Gb Ethernet switches into slot B1 and B2 on the back of the enclosure and ensure that they are locked into place.
7. Provide domain-connected network connection to one port on each of the M8024-k modules in slots A1 and A2. Any port can be used except 17 and 18, because these will be used for stacking.
8. Provide two 10Gb connections between the M8024-k modules in fabric A: Connect slot A1, port 17 to slot A2, port 18. Connect slot A1, port 18 to slot A2, port 17.
9. Provide two 10Gb connections between the M8024-k modules in fabric B: Connect slot B1, port 17 to slot B2, port 18. Connect slot B1, port 18 to slot B2, port 17.
10. Power on the enclosure.

Configuring the PowerConnect M8024-k 10GbE modules

1. Use the enclosure front control panel to find the CMC IP address.
2. From a computer on the network, use Internet Explorer to navigate to the CMC.
3. Log in with the default credentials. The default Username is `root` and the Password is `calvin`
4. Click Slot A1 under Chassis Overview→I/O Module Overview→10 GbE KR.
5. Click Launch I/O Module GUI.
6. Log in with the same `root` credentials.
7. Click System→Stack Management→Stack Port Summary.
8. Check the Edit checkboxes next to ports 0/17 and 0/18.
9. Under Configured Stack-mode, change the mode from Ethernet to Stack on both ports.
10. Click Apply.
11. Click the Save icon in the top right. Your changes will not persist after a reboot unless saved in this manner.
12. Repeat steps 4 through 11 for the remaining three M8024-k modules. The switches are now stacked and each fabric will function as one unit.
13. Return to the I/O Module GUI for the M8024-k in slot A1, and navigate to Switching→VLAN→Port Settings.
14. For Unit 1, Port Te1/0/1, use the Port VLAN Mode drop-down menu to select Trunk.
15. Click Apply.
16. Click Save.
17. For Unit 1, Port Te1/0/2, use the Port VLAN Mode drop-down menu to select Trunk.
18. Click Apply.
19. Click Save.

Configuring the PS-M4110 networking

1. From the CMC, select SLOT-03 under Chassis Overview→Server Overview→SLOT-03.
2. Under Array Properties, click Configure Array.
3. Enter the following information in the appropriate fields:
    - Member Name. We used `PSM4110-1`.

- Member IP. This needs to be on the subnet to be used for iSCSI. We used `192.168.10.61`.
- Member Netmask. We used `255.255.255.0`.
- Member Gateway. We left this blank.
- Use Existing Group. Check this if you are adding the PS-M4110 to an existing PS-series group. In our setup, we created a new group instead.
- Group Name. We used `PSGRP-1`.
- Group IP Address. This needs to be on the subnet used for iSCSI. We used `192.168.10.60`.
- Group Membership Management Password. This is the password that new members will use to gain membership.
- Group Administration (grpadmin) Password. This is the password for the top-level management account (grpadmin).
- Selected Fabric. The PS-M4110 defaults to Fabric B, but can use Fabric A if the enclosure has midplane version 1.1 or higher. The fabric must have 10GbE modules installed to be used for the PS-M4110. In our setup, we used Fabric B.

4. Click Apply.
5. Click SLOT-03 again to confirm that the settings are in place.

APPENDIX B – CONFIGURING THE M620 BLADES

Complete the steps in this section on both Dell PowerEdge M620 blades.

Installing Windows Server 2012 Datacenter Edition on the M620s

1. Attach a monitor and keyboard to the VGA and USB outputs on the front or back of the M1000e blade enclosure.
2. Press the Ctrl key twice quickly to bring up the KVM menu and select Slot 1.
3. Attach an external DVD drive with the installation media inside to the front of the first M620 and power the blade on.
4. Follow the on-screen instructions to install Windows Server 2012 Datacenter with a GUI.

Creating a network for Live Migration

1. Click Start, and type `ncpa.cpl`. Press Enter.
2. Right-click the adapter to be used for Live Migration, and click Properties.
3. Click Configure.
4. Click Advanced.
5. Select VLAN ID, and enter a value (for our testing purposes, we used 20).
6. Click OK.
7. Right-click the Live Migration adapter, and click Properties.
8. Select IPv4, and click Properties.
9. Select the Use the following IP address and Use the following DNS server addresses radio buttons.
10. Enter an IP address, subnet mask, default gateway, and preferred DNS server. Click OK.

Joining the M620s to the domain

1. Click Start, and type `ncpa.cpl`. Press Enter.
2. Right-click the adapter, and click Properties.
3. Select IPv4, and click Properties.
4. Select the Use the following IP address and Use the following DNS server addresses radio buttons.
5. Enter an IP address, subnet mask, default gateway, and preferred DNS server. Click OK.
6. In Server Manager, in the left pane, select Local Server.

7. Click the computer name.
8. Click Change.
9. Enter an appropriate hostname for the node, and select the Domain radio button.
10. Enter the name of your domain, and click OK.
11. Enter the administrative credentials to connect to the domain, and click OK.
12. At the welcome screen, click OK.
13. Restart the blade, and use the domain credentials to log in again.

Adding the MPIO feature

1. In Server Manager, click Manage→Add Roles and Features.
2. At the Before you begin screen, click Next.
3. At the Select installation type screen, leave the default selection of Role-based or feature-based installation, and click Next.
4. At the Select destination server screen, leave the default selection, and click Next.
5. At the Select server roles screen, click Next.
6. When the Add Roles and Features Wizard window pops up, click Add Features.
7. Click Next.
8. At the Select features screen, check the box for Multipath I/O, and click Next.
9. At the Confirm installation selections screen, click Install.
10. When the installation completes, click Close.

APPENDIX C – CONFIGURING THE STORAGE

Configuring the PS-M4110 RAID policy

1. From one of the M620s, use Internet Explorer to navigate to the PS group IP address (alternatively, use the PS-M4110 member IP address). Click OK at the warning.
2. If necessary, install the Java SE Runtime Environment.
3. Log in with the grpadmin credentials you specified during networking configuration.
4. Expand Members, and right-click PSM4110-1 (unconfigured). Click Configure member.
5. At the General Settings screen, click Next.
6. At the RAID Configuration screen, select a RAID policy and initial RAID capacity appropriate for your needs. In our setup, we chose RAID 10 and Immediately expand group capacity.
7. At the Summary screen, click Finish.

Finding the initiator IQN

These are generic steps for finding the iSCSI Qualified Name (IQN) for an initiator (a server that will access an iSCSI target). Refer to this section whenever an initiator IQN is needed.

1. Press the Windows key, and type `iscsi initiator`. Press Enter.
2. If prompted, start the Microsoft iSCSI Initiator service.
3. Click the Configuration tab.
4. Copy the Initiator Name.

Creating volumes on the PS-M4110

The volumes created in this section will appear as physical disks to Windows Server 2012 Datacenter. Use these steps to create volumes as needed for your organization. In our setup, we created two full provisioned volumes:

- Quorum (10 GB)
- VHDs (2 TB)

1. In the EqualLogic PS Series Group Manager, click Storage Pools→Default.
2. Click Create volume.
3. At the Volume Settings screen, enter a name for the volume, and click Next.

4. At the Space screen, enter a size for the volume. Choose full or thin provisioning. Choose a snapshot reserve percentage. Click Next.
5. At the iSCSI Access screen, select the Restricted access radio button and check the Limit access to iSCSI initiator name checkbox. Enter the IQN of the first M620. Ensure that the Set read-write radio button is selected and check the Allow simultaneous connections from initiators with different IQNs checkbox. Click Next.
6. At the Summary screen, click Finish.

Providing multiple IQNs access to a volume

Complete these steps to provide volume access to the second M620 server using the IQN.

1. In the Group Manager left pane, expand Volumes, and select the volume to be modified.
2. Select the Access tab.
3. Click Add.
4. Check the Limit access to iSCSI initiator name checkbox.
5. Enter the IQN of the desired initiator.
6. Click OK.

Connecting the M620s to the volumes

Complete these steps on both M620s.

1. Open iSCSI Initiator.
2. Click the Discovery tab.
3. Click Discover Portal.
4. Enter the PS Group IP address, and click OK.
5. Click the Targets tab.
6. Select the first volume IQN, and click Connect.
7. Check the Enable multi-path checkbox, and click OK.
8. Repeat steps 6 and 7 for the remaining volumes.

Preparing the volumes for cluster shared storage

Repeat these steps for all volumes to be added to the cluster.

1. On the first M620, open Disk Management by clicking Tools→Disk Management in Server Manager.
2. Right-click the name of the first offline volume, and click Online.

3. Right-click the name of the same volume, and click Initialize Disk.
4. Leave MBR selected, and click OK.
5. Right-click the white space of the volume, and click New Simple Volume.
6. Click Next.
7. Specify a size, and click Next. We used the maximum disk space.
8. Select the Do not assign a drive letter or drive path radio button, and click Next.
9. Enter a label for the volume, and click Next.
10. Click Finish.
11. On the second node, open Disk Management and bring the volume online. The volume properties will transfer over. The management console may need to be refreshed to complete this operation.

APPENDIX D – CREATING THE FAILOVER CLUSTER AND BUILDING THE VMS

Creating the failover cluster

On both M620s, use Server Manager to install the Failover Clustering feature and prerequisites.

1. Restart both nodes.
2. From the first M620, open the Failover Cluster Manager by clicking Tools→Failover Cluster Manager.
3. Click Validate Configuration.
4. Click Next.
5. Enter the hostname of the first node, and click Add.
6. Enter the hostname of the second node, and click Add.
7. Click Next.
8. Select Run all tests, and click Next.
9. Confirm the settings, and click Next.
10. When the validation completes, click View Report and verify that there are no errors. Check that the iSCSI volumes are shown under both nodes in List Potential Cluster Disks.
11. In the validation wizard, leave the Create the cluster now using the validated nodes checkbox checked, and click Finish.
12. At the Before You Begin screen, click Next.
13. Enter a name and IP address for the cluster, and click Next. We used `Cluster1` and `192.168.1.70`.
14. Check the Add all eligible storage to the cluster checkbox, and click Next.
15. Click Finish.
16. Download and install Update for Windows Server 2012 (KB2803748) from http://www.microsoft.com/en-us/download/details.aspx?id=36468, a hotfix to prevent Microsoft Management Console crashes in Failover Cluster Manager, and restart.

Configuring the failover cluster

1. In Failover Cluster Manager, select the cluster, and click Networks.
2. For any networks unrelated to the cluster, right-click the network, and click Properties.

3. Select the radio button for Do not allow cluster network communication on this network. Note: The iSCSI network will be disabled by default and is a correct setting.
4. Click Live Migration Settings.
5. Select the network to be used for live migration, and click Up until it is at the top of the list.
6. Click OK.
7. In the left pane, click Storage→Disks.
8. The disk to be used for quorum may be automatically assigned. If not, select the cluster, and click More Actions→Configure Cluster Quorum Settings.
    a. Click Next.
    b. Select Advanced quorum configuration and witness selection, and click Next.
    c. Select All nodes, and click Next.
    d. Leave the Allow cluster to dynamically manage the assignment of node votes checkbox checked, and click Next.
    e. Select Configure a disk witness, and click Next.
    f. Select the disk to be used for quorum, and click Next.
    g. Click Next.
    h. Click Finish.
9. Right-click the Cluster Disk to be used for VHDs, and click Add to Cluster Shared Volumes.

Installing Dell EqualLogic Host Integration Tools 4.5.0

Complete these steps on each failover cluster node:

1. Insert the installation media, and click Setup64.exe.
2. At the Welcome screen, click Next.
3. At the License Agreement screen, review and accept the terms of the license agreement, and click Next.
4. At the Destination Folder screen, click Next.
5. At the Select Type screen, select Complete, and click Next.
6. At the Ready to Install the Program screen, click Install.
7. At the Installation Complete screen, click Finish.
8. In the pop-up window that follows to restart the system, click Yes.

Configuring MPIO settings

Complete these steps on each failover cluster node:

1. Press the Windows key, and open Auto-Snapshot Manager.
2. In the left pane, click Settings→MPIO Settings.
3. In the Included section, click Exclude next to any subnets not to be used for iSCSI traffic.
4. Click Save.

Installing the Hyper-V roles

Complete these steps on each failover cluster node using the same shared storage for the Default Stores:

1. Open Server Manager, and click Manage→Add Roles and Features.
2. At the Before You Begin screen, click Next.
3. At the Installation Type screen, click Next.
4. At the Server Selection screen, select one of the servers in the failover cluster.
5. At the Server Roles screen, check the Hyper-V checkbox. At the prerequisite pop-up, click Add Features. Click Next.
6. At the Features screen, click Next.
7. At the Hyper-V screen, click Next.
8. At the Virtual Switches screen, click Next.
9. At the Migration screen, click Next.
10. At the Default Stores screen, enter locations on the shared cluster storage. The default path is `C:\ClusterStorage`. For our setup, we used `C:\ClusterStorage\VHDs` for both paths. Click Next.
11. At the Confirmation screen, check the box to automatically restart the server after installation, and click Install.

Creating a virtual switch

Complete these steps on each failover cluster node:

1. In Hyper-V Manager, click Virtual Switch Manager.
2. In the left pane, select New virtual network switch. Leave External highlighted, and click Create Virtual Switch.
3. Enter a name for the virtual switch. This name must be identical between both nodes. Use the drop-down menu to select an adapter that can communicate with the external Active Directory. Click OK.

4. At the connectivity warning, click Yes.
5. If you didn't use a NIC team for the first switch, add a second virtual switch using a different domain-connected adapter.

Creating the VMs

Lync 2013 Standard Edition requires at least three VMs: two Front End VMs and one File Server VM to act as a quorum witness. Repeat these steps for each VM to be created.

1. In Failover Cluster Manager, click Roles.
2. In the right pane, click Virtual Machines→New Virtual Machine.
3. Select a node to install the VM on, and click OK.
4. At the Before You Begin screen, click Next.
5. At the Specify Name and Location screen, verify that the location is on cluster shared storage. Give the VM a name, and click Next. We used the following names for our VMs:
    - LSFE01
    - LSFE02
    - LSFS
6. At the Assign Memory screen, enter an amount appropriate for the server role, and click Next. You can find further information about Lync hardware requirements at technet.microsoft.com/en-us/library/gg398438.aspx.
7. At the Configure Networking screen, use the drop-down menu to select the domain-connected virtual switch, and click Next.
8. At the Connect Virtual Hard Disk screen, create a new disk, enter a size appropriate for the server role, and click Finish. We sized every VHD at `50 GB`.
9. At the Summary screen, click Finish.
10. Right-click the VM, and click Settings.
11. Select Add New Hardware→Network Adapter, and click Add.
12. Select the redundant domain-connected switch from the drop-down menu, and click OK.

Installing Windows Server 2012 Datacenter Edition on the VMs

Repeat these steps for each VM.

1. In Failover Manager, right-click the VM, and click Settings.
2. In the left pane, click DVD Drive.

3. Select the image file or the DVD drive containing the Windows Server installation media radio button. Click OK.
4. Right-click the VM, and click Start.
5. Right-click the VM, and click Connect.
6. Follow the on-screen instructions to install Windows Server 2012.

Joining the VMs to the domain

Repeat these steps for each VM.

1. Click Start, and type `ncpa.cpl`. Press Enter.
2. Right-click the adapter, and click Properties.
3. Select IPv4, and click Properties.
4. Select the Use the following IP address and Use the following DNS server addresses radio buttons.
5. Enter an IP address, subnet mask, default gateway, and preferred DNS server. Click OK.
6. In Server Manager, in the left pane, select Local Server.
7. Click the computer name.
8. Click Change.
9. Enter an appropriate hostname for the VM, and select the Domain radio button.
10. Enter the name of your domain, and click OK.
11. Enter the administrative credentials to connect to the domain, and click OK.
12. At the welcome screen, click OK.
13. Restart the VM, and use the domain credentials to log in again.

APPENDIX E – PREPARING THE ACTIVE DIRECTORY AND VMS FOR LYNC SERVER 2013

Preparing the Active Directory

This step must be completed from the Active Directory Domain Controller, or a server with Active Directory Remote Server Administrative tools installed.

1. Insert the Lync Server 2013 installation DVD into the optical drive.
2. Run setup.exe. If the Microsoft C++ Runtime warning appears, click Yes.
3. At the Lync Server 2013 splash screen, choose an appropriate installation location, and click Install. For our setup, we chose the default location.
4. At the License Agreement screen, accept the license terms, and click OK.
5. After unpacking, the Lync Server Deployment Wizard should open. If not, use the Start menu to locate and open the wizard.
6. At the welcome screen, click Prepare Active Directory.
7. Next to Prepare Schema, click Run.
   a. Click Next.
   b. Once the command completes, click Finish.
   c. Optionally, verify the replication by using the instructions found at technet.microsoft.com/en-us/library(OCS.15)/ms.lync.dep.DeployMainVerifySchemaPrep.aspx.
8. Next to Prepare Current Forest, click Run.
   a. Select the radio button for Domain FQDN and enter the name of your FQDN. For our setup, this was `test.local`.
   b. Once the command completes, click Finish.
   c. Optionally, verify the replication by using the instructions found at technet.microsoft.com/en-us/library(OCS.15)/ms.lync.dep.DeployMainVerifyForestPrep.aspx.
9. Next to Prepare Current Domain, click Run.
   a. Click Next.
   b. Once the command completes, click Finish.
   c. Optionally, verify the replication by using the instructions found at technet.microsoft.com/en-us/library(OCS.15)/ms.lync.dep.DeployMainVerifyDomainPrep.aspx

Providing Lync permissions to the Domain Admin

1. Log into the Active Directory machine with Domain Admin credentials.
2. In Server Manager, click Tools→Active Directory Users and Computers.
3. Expand the domain, and click Users.
4. Right-click CSAdministrator, and click Properties.
5. In the Members tab, click Add.
6. Type the name of the user you wish to give Lync Server access and press Enter. For our test purposes we used `test\Administrator`. For more information on Lync Server permissions, see technet.microsoft.com/en-us/library(OCS.15)/ms.lync.dep.DeployMainCreateCSCPAdmin.aspx
7. Click OK.
8. Right-click RTCUniversalServerAdmins, and click Properties.
9. In the Members tab, click Add.
10. Type the name of the user given in step 6 and press Enter.
11. Click OK.

Configuring the DNS

1. Log into the Active Directory with Domain Admin credentials.
2. Open the DNS Manager.
3. Under Forward Lookup Zones, right-click the domain, and click Other New Records.
4. Select Service Location, and click Create Record.
5. Enter the following information, replacing the last line with the Front End VM FQDN for your environment:
    - Service: `_sipinternaltls`
    - Protocol: `_tcp`
    - Port Number: `5061`
    - Host offering this service: `LSFE01.test.local`
6. Click OK.
7. Click Done.
8. Right-click the domain again, and click New Host (A or AAAA).
9. Enter the following information, replacing the IP address with the IP address of your Front End VM:
    - Name: meet

- IP address: 192.168.1.11

10. Check the Create associated pointer (PTR) record checkbox, and click Add Host.
11. Click OK at the PTR warning.
12. Repeat steps 8 through 11 for the DNS entries `dialin` and `admin`. Use the Front End IP address for both.

Creating the Lync Server file shares

1. Log into the file server VM with Domain Admin credentials.
2. Create a new folder with an appropriate name for the share. We used `LyncShare1`.
3. Right-click the folder, and click Properties.
4. In the Sharing tab, click Share.
5. Using the drop-down menu, click Find People.
6. Type RTC in the box, and click Check Names.
7. Hold down the Ctrl key and select the following users: RTCComponentUniversalServices, RTCHSUniversalServices, RTCUniversalConfigReplicator, and RTCUniversalServerAdmins. Click OK.
8. Click OK.
9. From the drop-down menu next to a newly added user, select Read/Write. Repeat for all newly added users.
10. Click Share.
11. Click Done.
12. Repeat steps 2 through 11 for a second folder title `LyncShare2`.

Preparing the primary Front End VM

1. Log in with Domain Admin credentials to the VM to be used as the primary Lync Standard Edition Front End VM.
2. Attach the Windows Server 2012 Datacenter Edition installation media to the VM.
3. Open Windows PowerShell.
4. Type the following command and press Enter:

```
Install-WindowsFeature RSAT-ADDS, Web-Server, Web-Static-Content, Web-Default-Doc, Web-Http-Errors, Web-Asp-Net, Web-Net-Ext, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Http-Logging, Web-Log-Libraries, Web-Request-Monitor, Web-Http-Tracing, Web-Basic-Auth, Web-
```

```
Windows-Auth, Web-Client-Auth, Web-Filtering, Web-
Stat-Compression, Web-Dyn-Compression, NET-WCF-HTTP-
Activation45, Web-Asp-Net45, Web-Mgmt-Tools, Web-
Scripting-Tools, Web-Mgmt-Compat, Windows-Identity-
Foundation, Desktop-Experience, Telnet-Client, BITS -
Source D:\sources\sxs –Restart
```

5. After the VM has restarted, attach the Lync Server 2013 installation media to the VM and run Setup.exe.
6. If this is the first time that setup.exe has been run, install the C++ Runtime and core components as prompted and accept the license agreement.
7. At the welcome screen, click Prepare First Standard Edition Server.
8. Click Next.
9. Once all commands are completed without errors, click Finish.

APPENDIX F – INSTALLING LYNC SERVER 2013 STANDARD EDITION

Building the topology

1. At the Lync Server 2013 installation welcome screen, click Install Administrative Tools.
2. Once the installation finishes, click Start→Lync Server Topology Builder.
3. Select the radio button for New Topology, and click OK.
4. Enter a name for the topology, and click Save. For our setup, we used `testtopo1.tbxml`.
5. Enter your Primary SIP domain, and click Next. For our setup, we used `test.local`.
6. Enter any additional SIP domains, and click Next. For our setup, we did not add any.
7. Enter a name for the first site, and click Next. For our setup, we used `Site1`.
8. Enter location details if desired, and click Next.
9. Leave the Open the New Front End Wizard when this wizard closes checkbox checked, and click Finish.
10. At the Define New Front End Pool wizard welcome screen, click Next.
11. In the Pool FQDN field, enter the FQDN of the current server. These must match exactly. For our setup, we used `LSFE01.test.local`. Select the radio button for Standard Edition Server, and click Next.
12. Select all features required for your organization. The Archiving and Monitoring features each require a dedicated SQL instance. We selected Conferencing with Dial-in, Call Admission Control, and Collocate Mediation Server. Click Next.
13. Leave the Collocate Mediation Server checkbox checked, and click Next.
14. Leave the Enable an Edge pool to be used by the media component of this Front End pool checkbox unchecked, and click Next.
15. At the Define the SQL Server store screen, click Next.
16. Select the radio button for Define a new file store and enter the appropriate information. For our setup, this was `LSFS.test.local` and `LyncShare1`. Click Next.
17. At the Specify the Web Services URL screen, click Next.
18. If your organization employs an Office Web Apps server, then check the Associate pool with an Office Web Apps Server checkbox, and click New. Enter the FQDN and Discover URL, and click OK. We did not use an Office Web Apps

server and did not check the checkbox. You can find further information on deploying an Office Web Apps server at www.technet.microsoft.com/en-us/library/jj219458.aspx.

19. If installing the Archiving and/or Monitoring roles, click Next to continue the wizard. On the following screens, enter the appropriate SQL instances to be used for these roles. If the Archiving and Monitoring roles are not to be configured at this time, click Finish to close the wizard.
20. In the Topology Builder, right-click Lync Server, and click Edit Properties.
21. Click Central Management Server.
22. In the Administrative access URL field, enter the admin URL. For our setup, this was `https://admin.test.local`.
23. Under Central Management Server, use the drop-down menu to select the Front End server.
24. Click OK.
25. Right-click Lync Server, and click Publish Topology.
26. Confirm that the listed tasks have been completed, and click Next.
27. Ensure that the Front End server is selected in the drop-down menu, and click Next.
28. After the process completes, click Finish.

Installing the configuration to the primary Front End VM

1. Log into the primary Front End VM with Domain Admin credentials. Navigate to the Lync Server 2013 installation media and run setup.exe.
2. At the Lync Server 2013 installation welcome screen, click Install or Update Lync Server System.
3. Next to Install Local Configuration Store, click Run.
   a. Select the radio button for Retrieve directly from the Central Management store (requires read access to the Central Management store), and click Next.
   b. Click Finish.
4. Next to Setup or Remove Lync Server Components, click Run.
   a. Click Next.
   b. Click Finish.
5. Next to Request, Install or Assign Certificates, click Run.
   a. Select Default certificate, and click Request.

b. When the wizard pops up, click Next.

c. Leave the Send the request immediately to an online certification authority radio button, and click Next.

d. Select your CA from the drop-down menu, and click Next.

e. Specify alternate credentials for the CA if needed, and click Next.

f. Leave the Use alternate certificate template for the selected certification authority checkbox unchecked, and click Next.

g. Enter a name for the certificate in the Friendly name field, select a Bit length of `2048`, and check the Mark the certificate's private key as exportable checkbox. Click Next. We named our certificate `LS Internal Cert`.

h. Enter your organization name and unit if desired, and click Next.

i. Enter your geographical information if desired, and click Next.

j. Review the Subject and Subject Alternative Names, and click Next.

k. Under Configured SIP domains, check the checkbox next to your domain, and click Next.

l. Add any additional subject alternative names if desired. For our setup, we did not require any more. Click Next.

m. Review the settings, and click Next.

n. After the operation completes, click Next.

o. Click Finish.

p. When the Certificate Assignment window pops up, click Next.

q. Click Next.

r. Click Finish.

s. Click Close.

t. Repeat step 5 for the `OAuthTokenIssuer` certificate.

6. Next to Start Services, click Run.

   a. Click Next.

   b. Click Finish.

Adding the secondary Front End pool

1. Open the current topology in Topology Builder. This can be done by importing the active configuration or simply opening the .tbxml file that was previously saved.

2. Click Lync Server→Site1→Lync Server 2013 and right-click Standard Edition Front End Servers. Click New Front End Pool.
3. Click Next.
4. Enter the FQDN of the secondary Front End VM, and click Next. For our setup, we used `LSFE02.test.local`.
5. Select the appropriate options for your environment. Call Admission Control will not be available if already installed on the primary Front End server. This feature can only have one instance per site. For our setup, we chose everything except for Archiving and Monitoring. Call Admission Control was already installed.
6. Leave the Collocate Mediation Server checkbox checked, and click Next.
7. Leave the Enable an Edge pool to be used by the media component of this Front End pool checkbox unchecked, and click Next.
8. At the Define the SQL Server store screen, click Next.
9. Select the radio button for Define a new file store and enter the appropriate information. For our setup, this was `LSFS.test.local` and `LyncShare2`. Click Next.
10. At the Specify the Web Services URL screen, click Next.
11. If your organization employs an Office Web Apps server, then check the Associate pool with an OWA Server checkbox, and click New. Enter the FQDN and Discover URL, and click OK. If not using an OWA server, click Finish. We did not use an OWA Server and did not check the checkbox.
12. If installing the Archiving and/or Monitoring roles, click Next to continue the wizard. On the following screens, enter the appropriate SQL instances to be used for these roles. If the Archiving and Monitoring roles are not to be configured at this time, click Finish to close the wizard.
13. In the Topology Builder, click Action→Publish Topology.
14. Click Next.
15. Once the commands complete, click Finish.

Updating the primary Front End VM

1. Log into the primary Front End VM with administrative credentials. Navigate to the Lync Server 2013 installation media and run setup.exe.
2. Click Install or Update Lync Server System.
3. Next to Setup or Remove Lync Server Components, click Run Again.
    a. Click Next.

b. Click Finish.

Installing the configuration to the secondary Front End VM

1. Log into the secondary Front End VM with Domain Admin credentials.
2. Attach the Windows Server 2012 installation media to the VM.
3. Open Windows PowerShell and run the following command:

```
Install-WindowsFeature RSAT-ADDS, Web-Server, Web-Static-Content, Web-Default-Doc, Web-Http-Errors, Web-Asp-Net, Web-Net-Ext, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Http-Logging, Web-Log-Libraries, Web-Request-Monitor, Web-Http-Tracing, Web-Basic-Auth, Web-Windows-Auth, Web-Client-Auth, Web-Filtering, Web-Stat-Compression, Web-Dyn-Compression, NET-WCF-HTTP-Activation45, Web-Asp-Net45, Web-Mgmt-Tools, Web-Scripting-Tools, Web-Mgmt-Compat, Windows-Identity-Foundation, Desktop-Experience, Telnet-Client, BITS -Source D:\sources\sxs –Restart
```

4. Attach the Lync Server 2013 installation media to the VM and run Setup.exe.
5. If this is the first time that setup.exe has been run, install the C++ Runtime and core components as prompted and accept the license agreement.
6. At the welcome screen, click Install or Update Lync Server System.
7. Next to Install Local Configuration Store, click Run.
   a. Select the radio button for Retrieve directly from the Central Management store (requires read access to the Central Management store), and click Next.
   b. Click Finish.
8. Next to Setup or Remove Lync Server Components, click Run.
   a. Click Next.
   b. Click Finish.
9. Next to Request, Install or Assign Certificates, click Run.
   a. Select Default certificate, and click Request.
   b. When the wizard pops up, click Next.
   c. Leave the Send the request immediately to an online certification authority radio button, and click Next.
   d. Select your CA from the drop-down menu, and click Next.
   e. Specify alternate credentials for the CA if needed, and click Next.

f. Leave the Use alternate certificate template for the selected certification authority checkbox unchecked, and click Next.

g. Enter a name for the certificate in the Friendly name field, select a Bit length of `2048`, and check the Mark the certificate's private key as exportable checkbox. Click Next. We named our certificate `LS Internal Cert`.

h. Enter your organization name and unit if desired, and click Next.

i. Enter your geographical information if desired, and click Next.

j. Review the Subject and Subject Alternative Names, and click Next.

k. Under Configured SIP domains, check the checkbox next to your domain, and click Next.

l. Add any additional subject alternative names if desired. For our setup, we did not require any more. Click Next.

m. Review the settings, and click Next.

n. After the operation completes, click Next.

o. Click Finish.

p. When the Certificate Assignment window pops up, click Next.

q. Click Next.

r. Click Finish.

s. Click Close.

10. Next to Start Services, click Run.

    a. Click Next.

    b. Click Finish.

Designating the secondary Front End pool as a backup

1. Open the current topology in Topology Builder. This can be done by importing the active configuration or simply opening the .tbxml file that was previously saved.
2. Click Lync Server→Site1→Lync Server 2013→Standard Edition Front End Servers and right-click the primary Front End server. Click Edit Properties.
3. Under Resiliency, check the Associated backup pool checkbox. Use the drop-down menu to select the secondary Front End server. Check the box for Automatic failover and failback for Voice and adjust the intervals to values appropriate for your organization. Click OK.
4. Click OK.
5. In the Topology Builder, click Action→Publish Topology.

6. Click Next.
7. Once the commands complete, click Finish.

Updating the Front End VMs

1. On both Front End servers, run steps 2 (Setup or Remove Lync Server Components) and 4 (Start Services) from the Install or Update Lync Server System category in the setup GUI.
2. From the primary Front End server, run the following PowerShell commands. Replace the FQDNs with your own:

```
Invoke-CSBackupServiceSync –PoolFqdn LSFE01.test.local
Invoke-CSBackupServiceSync –PoolFqdn LSFE02.test.local
```

Adding the backup SRV

1. Log into the Active Directory with Domain Admin credentials.
2. Open the DNS Manager.
3. Under Forward Lookup Zones, right-click the domain, and click Other New Records.
4. Select Service Location, and click Create Record.
5. Enter the following information, replacing the last line with the secondary Front End FQDN for your environment:
    - Service: `_sipinternaltls`
    - Protocol: `_tcp`
    - Priority: `10`
    - Weight: `10`
    - Port Number: `5061`
    - Host offering this service: `LSFE02.test.local`
6. Click OK.
7. Click Done.

ABOUT PRINCIPLED TECHNOLOGIES

Principled Technologies, Inc.
1007 Slater Road, Suite 300
Durham, NC, 27703
www.principledtechnologies.com

We provide industry-leading technology assessment and fact-based marketing services. We bring to every assignment extensive experience with and expertise in all aspects of technology testing and analysis, from researching new technologies, to developing new methodologies, to testing with existing and new tools.

When the assessment is complete, we know how to present the results to a broad range of target audiences. We provide our clients with the materials they need, from market-focused data to use in their own collateral to custom sales aids, such as test reports, performance assessments, and white papers. Every document reflects the results of our trusted independent analysis.

We provide customized services that focus on our clients' individual requirements. Whether the technology involves hardware, software, Web sites, or services, we offer the experience, expertise, and tools to help our clients assess how it will fare against its competition, its performance, its market readiness, and its quality and reliability.

Our founders, Mark L. Van Name and Bill Catchings, have worked together in technology assessment for over 20 years. As journalists, they published over a thousand articles on a wide array of technology subjects. They created and led the Ziff-Davis Benchmark Operation, which developed such industry-standard benchmarks as Ziff Davis Media's Winstone and WebBench. They founded and led eTesting Labs, and after the acquisition of that company by Lionbridge Technologies were the head and CTO of VeriTest.