Deployment guide:

Configuring a highly available Microsoft® Exchange Server 2013 environment on a Dell™ PowerEdge™ VRTX

Principled Technologies®

DELL

Microsoft

A Principled Technologies deployment guide commissioned by Dell Inc.

TABLE OF CONTENTS

INTRODUCTION

When considering a high availability configuration for your business' e-mail server needs, selecting the correct hardware combination of servers, networking, and storage that are guaranteed to work together is easy with the Dell PowerEdge VRTX shared infrastructure solution, which unites all of the above in a manageable, compact enclosure. The VRTX offers a powerful yet quiet solution for small businesses or remote offices that is easy to configure, delivers the performance they require, streamlines management and maintenance, provides all necessary hardware resources in one spot, and maintains high availability. Setting up a highly available Microsoft Exchange Server 2013 environment on the Dell PowerEdge VRTX provides all the benefits of the latest Exchange Server release and keeps your important mail workloads running. But how do you configure Exchange Server 2013 on the Dell PowerEdge VRTX?

In this guide, we take you through the simple, straightforward process of setting up a highly available Microsoft Exchange Server 2013 environment on the Dell PowerEdge VRTX. We set up this environment on the VRTX in our labs, so we provide each step we took along with any best practices we recommend. First, read more about the components of the Dell PowerEdge VRTX. Then, continue on for overview of how to configure a Microsoft Exchange Server 2013 environment (for detailed steps, see the corresponding appendices).

ABOUT THE COMPONENTS

About the Dell PowerEdge VRTX

The Dell PowerEdge VRTX is a shared infrastructure solution in a 5U rack-able tower chassis. Designed to be quiet under normal operating conditions, the Dell PowerEdge VRTX can be stowed under a desk in a small office without disrupting conversations. Its four bays house M520 or M620 compute nodes, providing a space-saving alternative to having four separate tower or rack servers. In addition to space savings, the Dell PowerEdge VRTX provides administrators with a unified interface, the Chassis Management Controller (CMC), for performing routine systems management tasks. The Dell PowerEdge VRTX chassis supports up to 48 TB of shared internal storage that is presentable as virtual drives to single or multiple compute nodes, and provides optional pass-through and eight PCIe slots for additional device connectivity. The chassis integrated storage can be configured with 25 bays for 2.5-inch drives or with 12 bays for 3.5-inch drives. The Dell PowerEdge VRTX integrated switch contains multiple external network ports for easy expansion or integration into any computing environment.

For more information about the Dell PowerEdge VRTX, visit www.dell.com/poweredge.

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 compute 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 keep track of 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 new 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 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 Exchange Server 2013

Microsoft Exchange Server 2013 equips you with a robust communications platform that can also give your users anywhere access, increasing their mobility. According to Microsoft, Exchange Server 2013 uses features such as Data Loss Prevention (DLP) and site mailboxes to help you better manage your mail server and decrease management time. Exchange Server 2013 is also designed to ensure greater uptime, has features that can keep you compliant with regulations, and offers flexible deployment options. For more information about Microsoft Exchange Server 2013, visit www.office.microsoft.com/en-us/exchange/.

WE SHOW YOU HOW – INSTALLING EXCHANGE SERVER 2013 ON THE DELL POWEREDGE VRTX

Prerequisites for this guide

This guide assumes that you will be deploying a virtualized instance of Exchange Server 2013 onto a Windows Server 2012 with Hyper-V Failover Cluster with cluster shared volumes from the VRTX shared storage already configured. We recommend this configuration as it takes advantage of both guest-level and application-level high availability features. For instructions on how to create a failover cluster using Microsoft Windows Server 2012 with Hyper-V, see the companion failover cluster deployment guide at www.principledtechnologies.com/Dell/VRTX_failover_cluster_guide_0713.pdf.

Additionally, this guide assumes that all virtual machines and server nodes are running Windows Server 2012, which is particularly important for this deployment. Microsoft Exchange Server 2013 database availability groups (DAGs) require Windows Server 2012 Datacenter, Windows Server 2012 Standard, or Windows Server 2008 R2 Datacenter edition.

Networking overview

In this section, we present an overview of the virtual network configuration for this guide. For step-by-step instructions on creating a virtual switch, see Appendix A.

As outlined in the companion failover cluster deployment guide, you should have a virtual switch on each node connecting into your existing network and Active Directory domain controller. There should also be a Live Migration network configured, using up the first port on the mezzanine cards. We will use the remaining mezzanine ports to configure a dedicated network for database replication.

Use the VRTX Web GUI to create a new VLAN for replication traffic, and assign it to the second port on each mezzanine card. Create an external virtual switch on each node using this port. Ensure that the switches for replication have the same name across nodes.

Creating the virtual machines

In this section, we present an overview of how to create and setup the VMs we will use for the Exchange DAG. For step-by-step instructions, see Appendix A.

1. Use Failover Cluster Manager to create the appropriate number of VMs for your deployment (see Figure 2). In the Failover Cluster Manager, choose a node for each VM. For our testing purposes, we created five VMs, two for Mailbox server roles, two for Client Access server roles, and one as a File Witness. We recommend dividing the Mailbox and Client Access roles evenly across both server nodes.

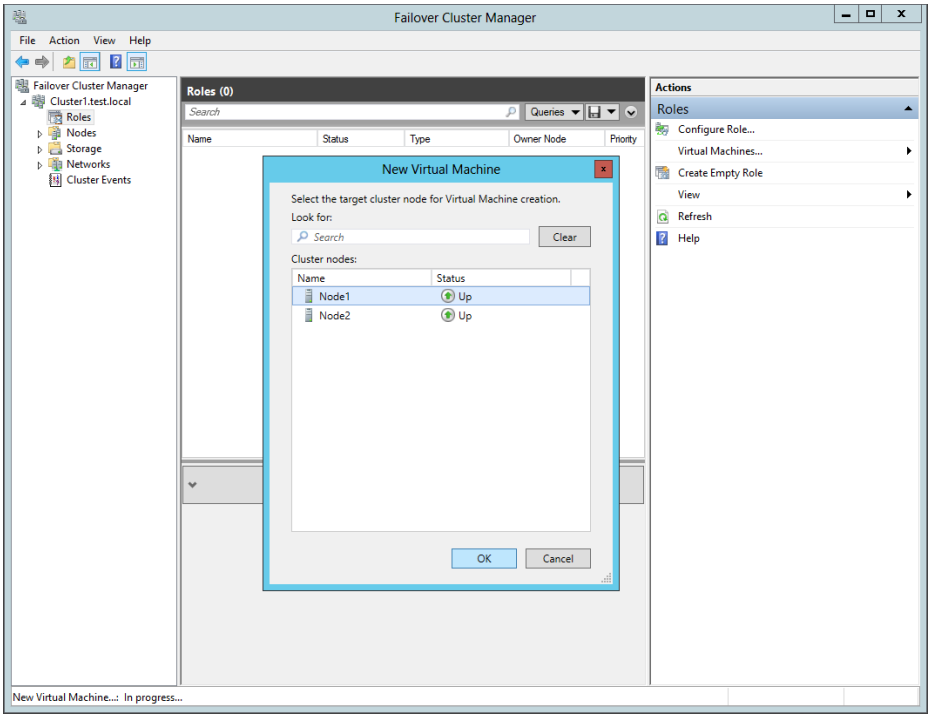

Figure 2: Creating a VM in FC Manager.

2. As you build the VMs, adjust virtual hardware specifications to reflect your available hardware and organizational needs. See Figure 3 for how we provisioned virtual hardware to each VM for our test purposes. For more information on Exchange Server 2013 hardware requirements, see technet.microsoft.com/en-us/library/aa996719(v=exchg.150).aspx.

	Number of vCPUs	GB of vRAM	VHD size (GB)
Node 1			
Mailbox role VM	2	4	50
Client Access role VM	2	4	50
File Witness VM	1	2	50
Node 2			
Mailbox role VM	2	4	50
Client Access role VM	2	4	50

Figure 3: VM specifications for our environment.

3. Install Windows Server 2012 Datacenter on each VM. (The next sections cover how to configure each type of VM.)

Preparing the VMs for Exchange Server 2013

This section presents an overview of how to prepare the VMs you created for Microsoft Exchange Server 2013. For step-by-step instructions, see Appendix A.

1. Attach the domain virtual switch to each VM. If using a dedicated replication network, attach the Replication switch to all VMs that will host the Mailbox role. For the domain-connected adapters, set up static IP addresses on each VM and join the VMs to the domain (see Figures 4 and 5). We discuss configuring the replication-connected adapters later in this guide.

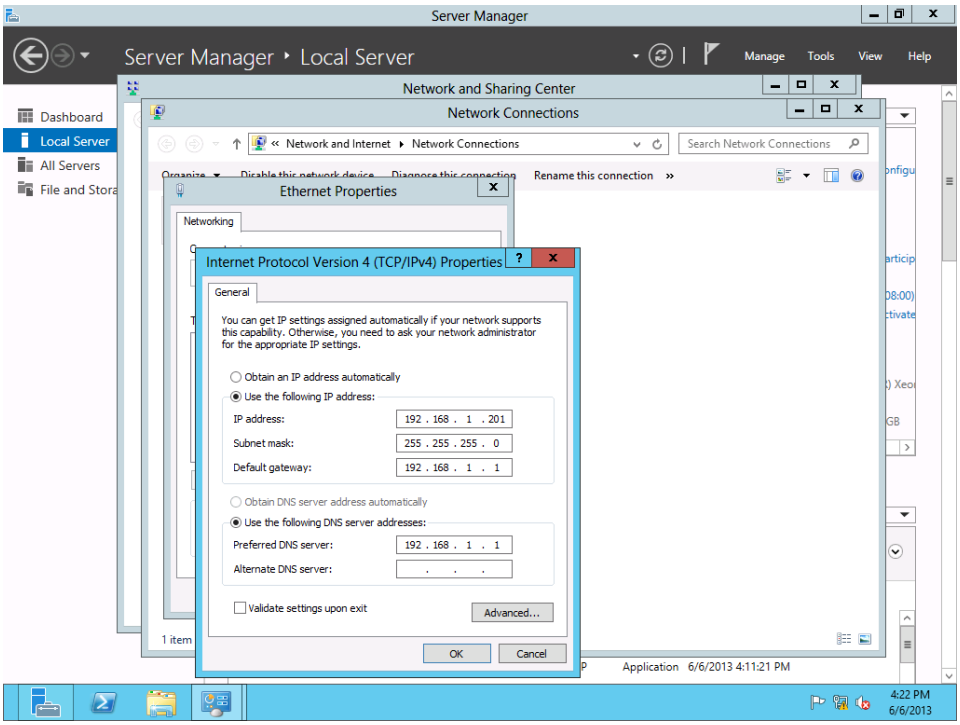

Figure 4: Setting an IP.

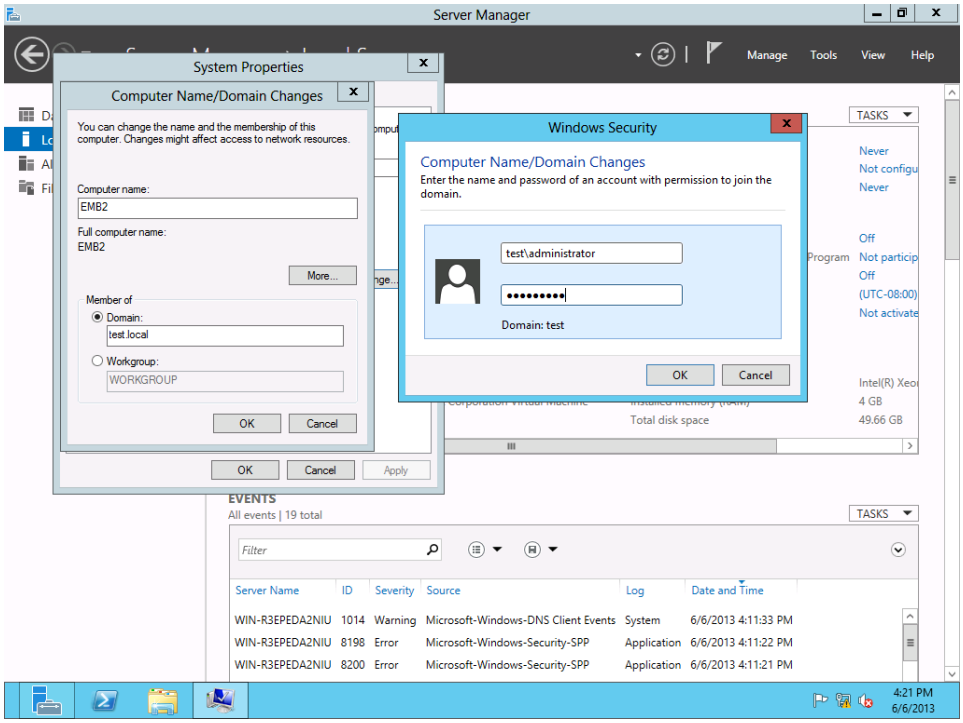

Figure 5: Joining the domain.

2. On each VM to be used for the Mailbox or Client Access role, use PowerShell to run the following command. This will install Windows Server 2012 features needed for the Exchange Server 2013 deployment. If you prefer, you can also install these features using Server Manager.

```
Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation
```

3. Restart the VMs, and download and install the following software on each Mailbox and Client Access VM:
   - Microsoft Office 2010 Filter Pack 64-bit (go.microsoft.com/fwlink/p/?linkID=191548)
   - Microsoft Office 2010 Filter Pack SP1 64-bit (go.microsoft.com/fwlink/p/?LinkId=254043)
4. Download and install the following software on the Mailbox VMs only:
   - Microsoft Unified Communications Manage API 4.0, Core Runtime 64-bit (go.microsoft.com/fwlink/p/?linkId=258269)

Installing the Mailbox and Client Access roles

The following steps are an overview of installing the Mailbox and Client Access roles for your VMs. For detailed steps, see Appendix B.

1. Connect the installation media, and complete the setup wizard on each VM. The installer prompts you to decide between the Mailbox role, Client Access role, and both. Install each Mailbox role first, and then install each Client Access role (see Figure 6). Run only one instance of the setup wizard at a time, to avoid conflicting updates to the Active Directory.

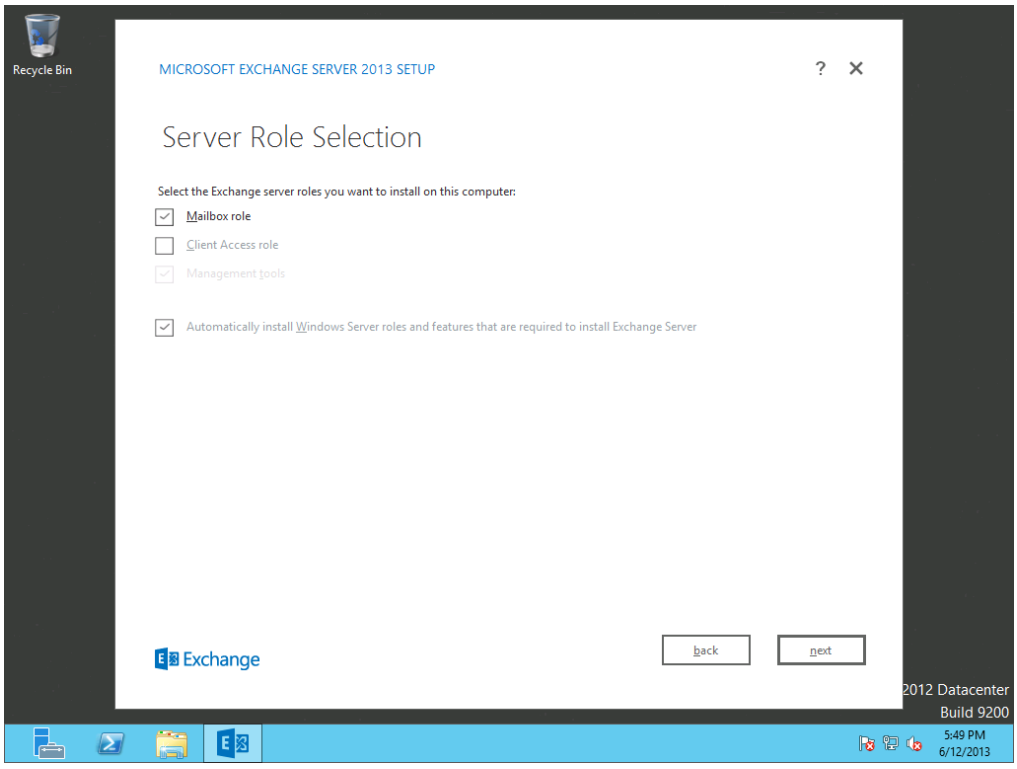

Figure 6: Selecting the Mailbox role in Exchange Server 2013.

2. Choose an installation location, and choose to enable or disable malware scanning.

Configuring load balancing for the Client Access VMs

In this section, we show you how to configure Windows-based network load balancing between the two Client Access server VMs. Although this solution will achieve basic load balancing, we recommend using a hardware load balancing solution for best performance. For more detailed steps, see Appendix C.

1. On both Client Access VMs, use PowerShell or Server Manager to add the Network Load Balancing feature.
2. From one of the Client Access VMs, use the Network Load Balancing Manager to create a new cluster.
3. Add the remaining VMs to the cluster (see Figure 7). You can configure port rules for your setup, but the default settings will distribute traffic to the NIC with the least network load, giving all VMs equal priority weight.

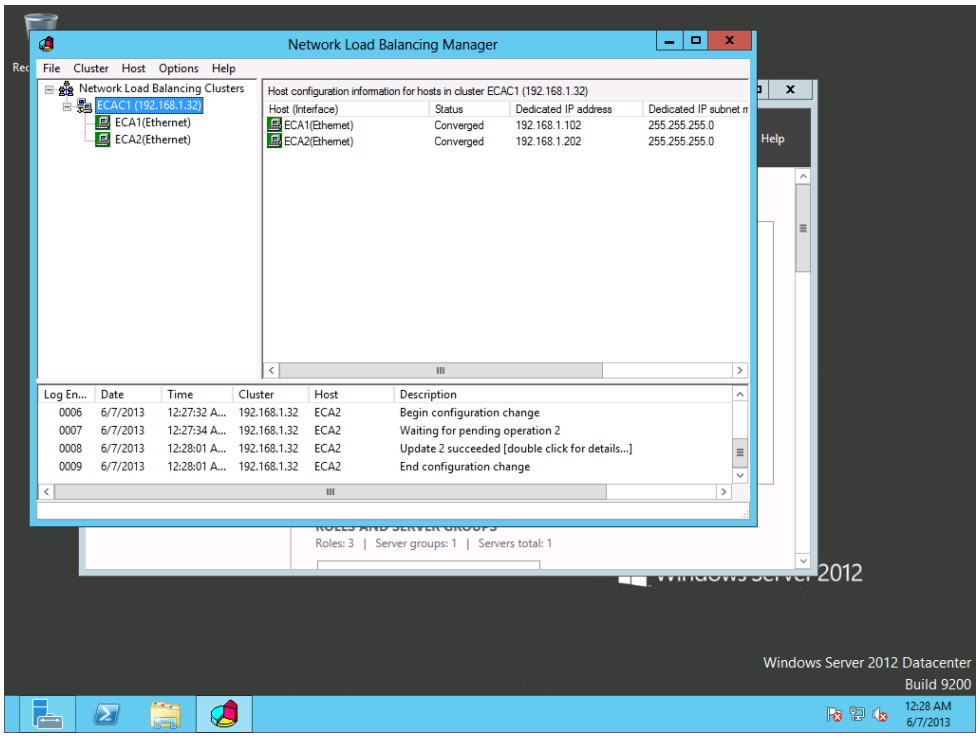

Figure 7: Completed NLB cluster configuration.

Configuring the File Witness server

Creating a database availability group requires a File Witness server. We used a VM on the cluster shared storage for this purpose. For more detailed steps, see Appendix C.

1. Join the File Witness VM to the domain and log in with domain administrator credentials.
2. Using the Computer Management snap-in, add the Exchange Trusted Subsystem to the local Administrators group (see Figures 8, 9, 10, and 11).

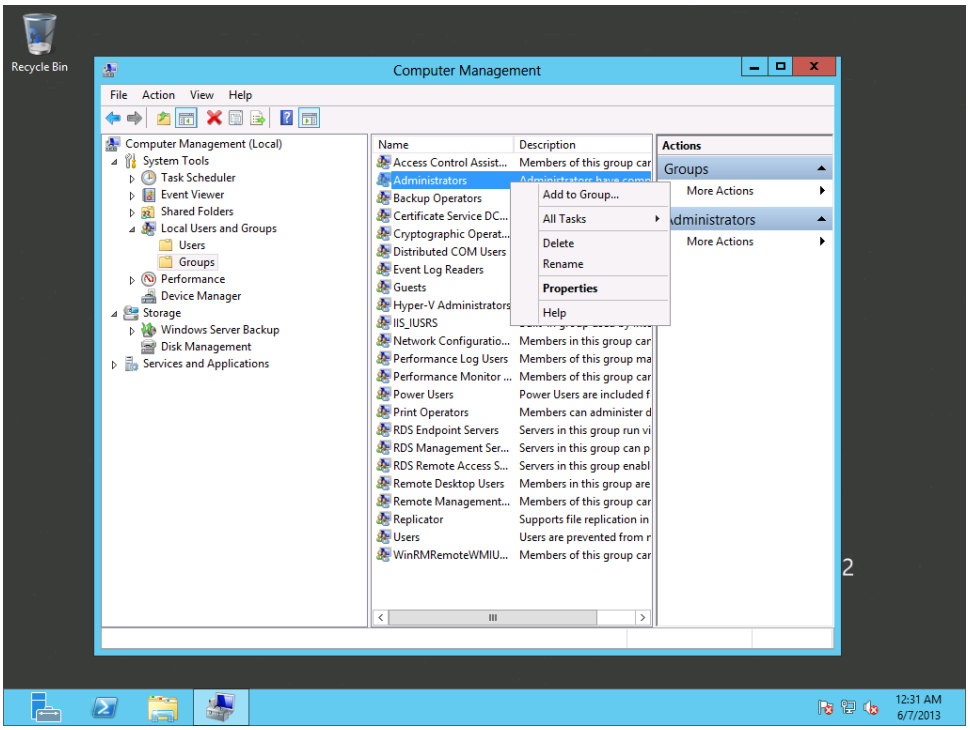

Figure 8: Locating the local Administrators group properties.

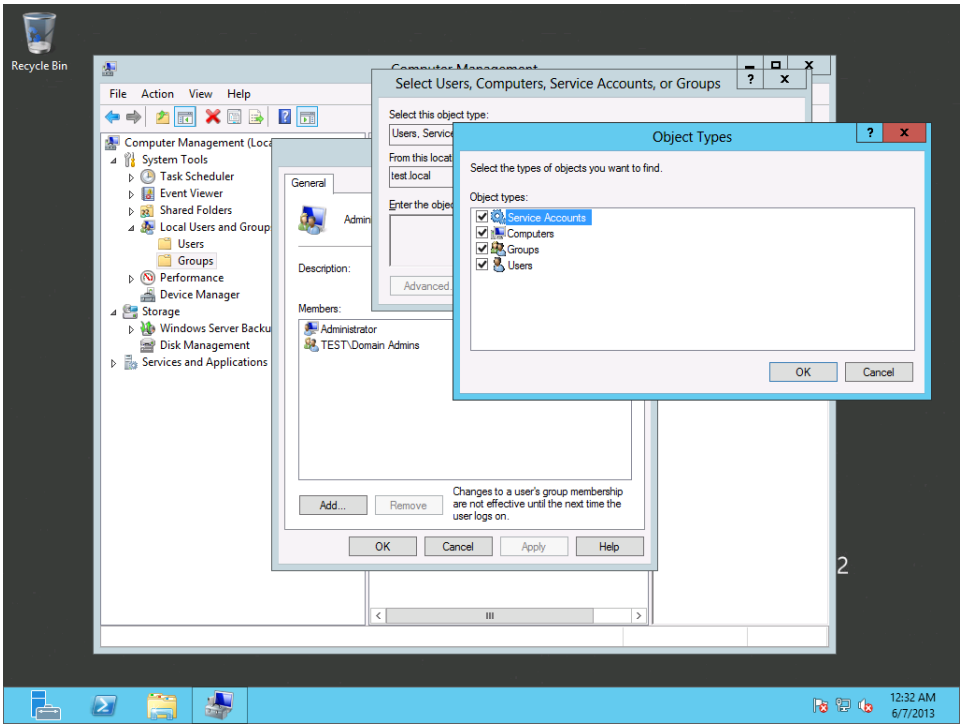

Figure 9: Checking the Computer object type.

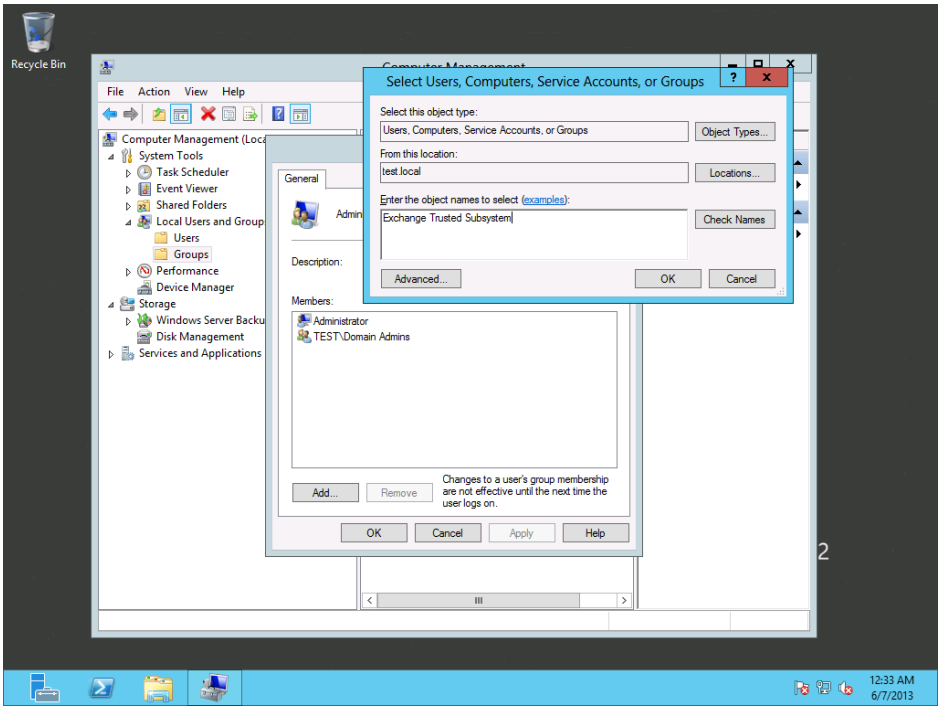

Figure 10: Finding the Exchange Trusted Subsystem object.

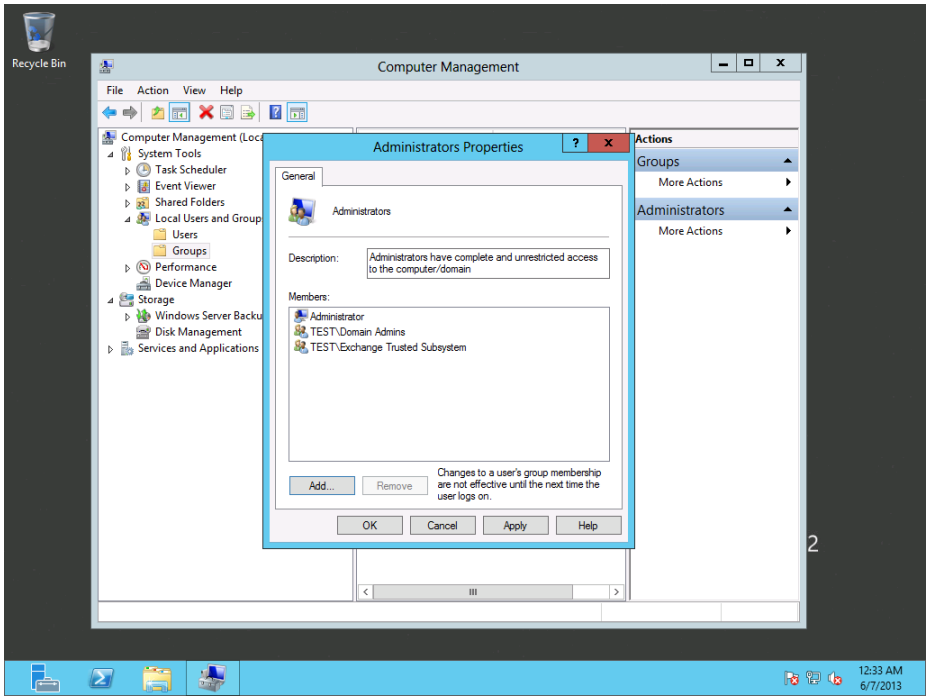

Figure 11: Exchange Trusted Subsystem successfully added to local Administrators group.

3. Use PowerShell or Server Manager to add the File Server feature. To find this feature, navigate to File and Storage Services→File and iSCSI Services→File Server.
4. Configure the Windows firewall to allow file and printer sharing on the domain.
5. Create a folder on the C:\ drive to be used as the file witness directory.
6. Share the folder and give the Exchange Trusted Subsystem read and write permissions (see Figure 12).

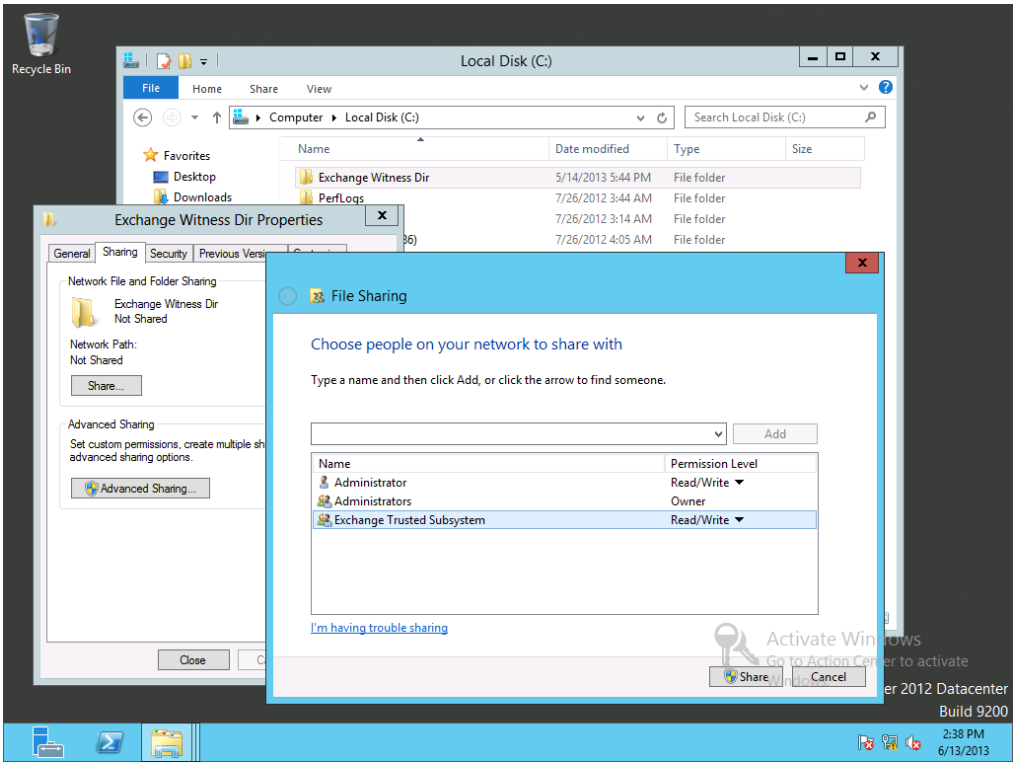

Figure 12: Sharing the File Witness directory.

Configuring the replication network

It is a Microsoft best practice to have a dedicated network between all Mailbox servers for database replication. Complete the following steps on each replication-connected adapter. For more detailed steps, see Appendix C.

1. Set a static IP address using a subnet that is not on the domain. Ensure that the default gateway and DNS server entries are enabled but left blank.
2. Under Advanced→DNS, uncheck the box for Register this connection's addresses in DNS.

Microsoft Exchange 2013 will attempt to automatically configure the networking when you create the Database Availability Group. After the DAG is created, you can check the networking configuration by running the following cmdlet in PowerShell or Exchange Management Shell:

```
Get-DatabaseAvailabilityGroupNetwork
```

For more information, see technet.microsoft.com/en-us/library/dd297938(v=exchg.150).aspx.

Creating the database availability group

In this section, we show you how to create the database availability group (DAG), add servers to it, and configure database copies. For detailed steps, see Appendix D.

1. Using Active Directory Users and Computers, create a new computer object on the domain with the name that you will use for the DAG.
2. Disable the account.
3. Give full control of the account to the Mailbox server VM that will be the first member of the DAG (see Figure 13). Note: Enable Advanced Features in the View menu of Active Directory Users and Computers to access the security properties.

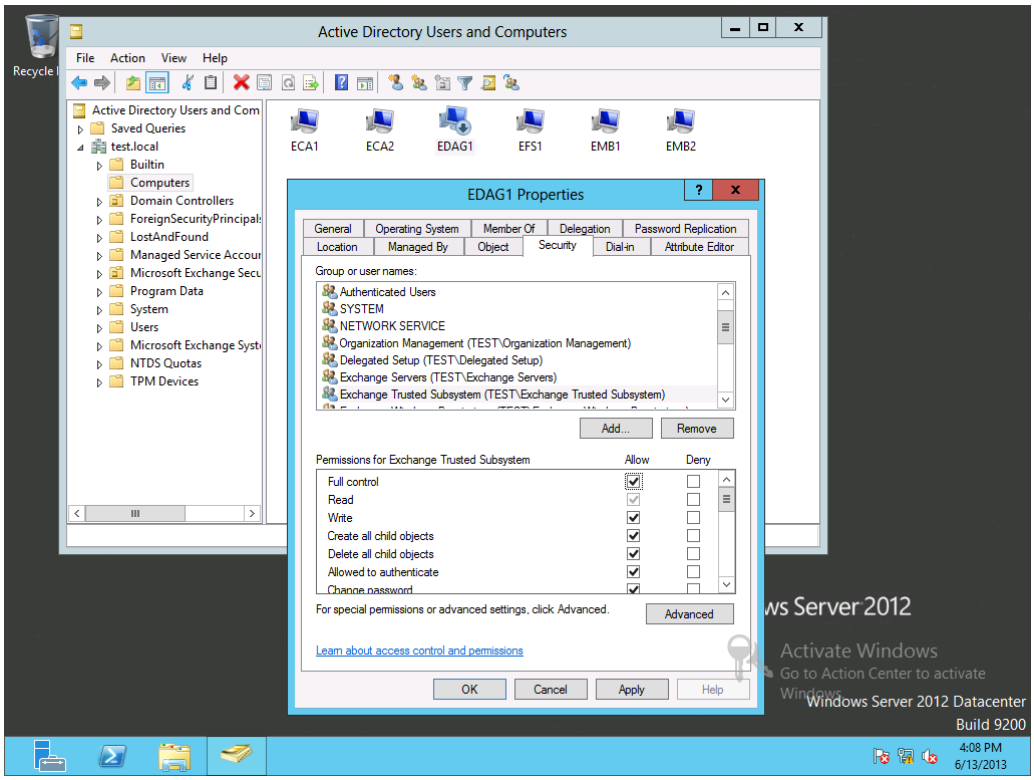

Figure 13: Pre-staging the cluster name object.

4. Using a domain-connected computer and the latest version of Internet Explorer, access the Exchange Control Panel at `https://<Client Access VM FQDN>/ecp` and log in with appropriate credentials. This must be a user with domain administrator privileges.

5. Navigate to Servers→Database Availability Groups to create a new DAG (see Figure 14). Make sure that the DAG name is identical to the object created in the step 1 of this section. Note: When saving the DAG, disregard if you see a warning about the Exchange Trusted Subsystem not being a member of the File Witness server's local Administrators group. For more information, see support.microsoft.com/kb/2644540.

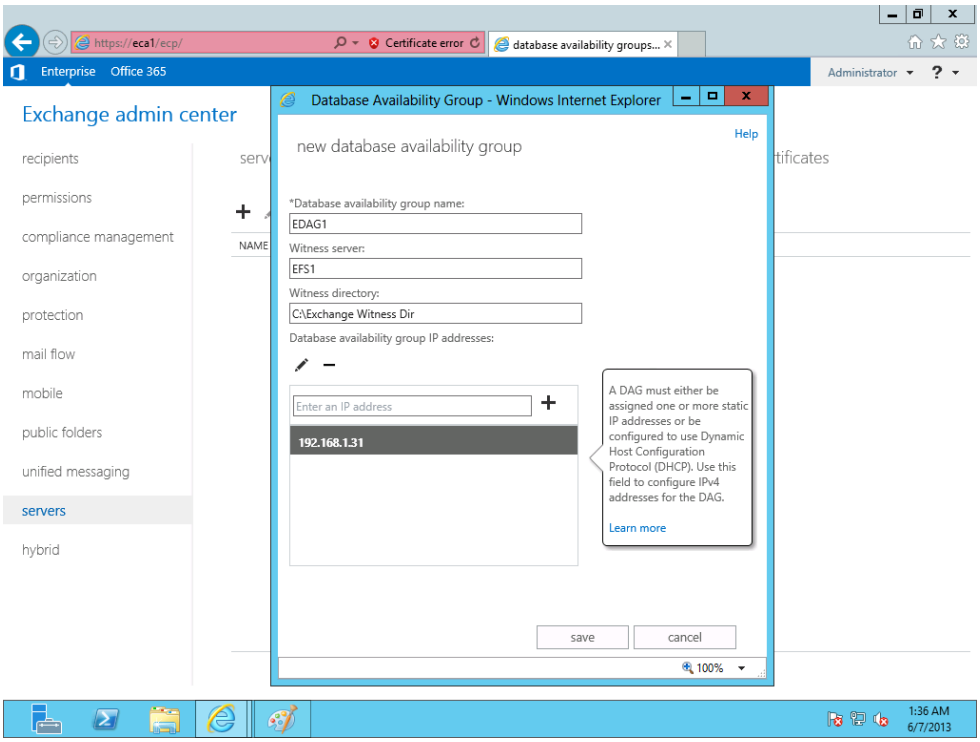

Figure 14: Creating the DAG.

6. Restart the Client Access, Mailbox, and File Witness VMs. In Exchange Admin Center, navigate to Servers→Database Availability Groups, and select the newly created DAG. Use the + symbol to add servers to the DAG (see Figure 15).

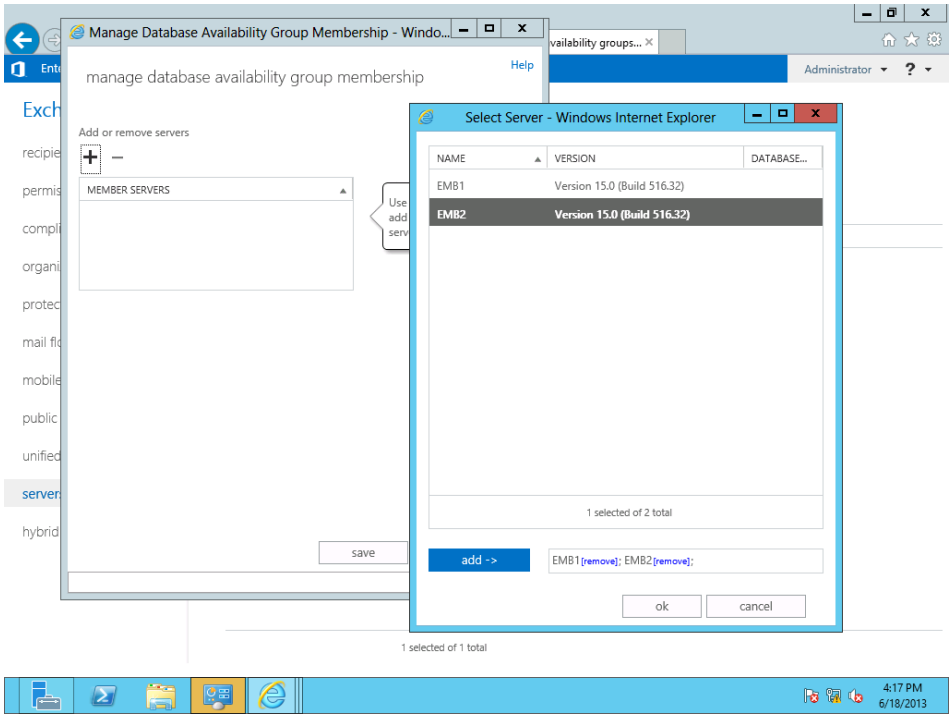

Figure 15: Adding servers to the DAG.

7. Navigate to the databases. For each database, add a database copy on every available Mailbox server (see Figures 16 and 17). If your organization is using more than two Mailbox servers, configure the priorities in a round robin fashion. For more information, see technet.microsoft.com/en-us/library/dd638129(v=exchg.150).aspx.

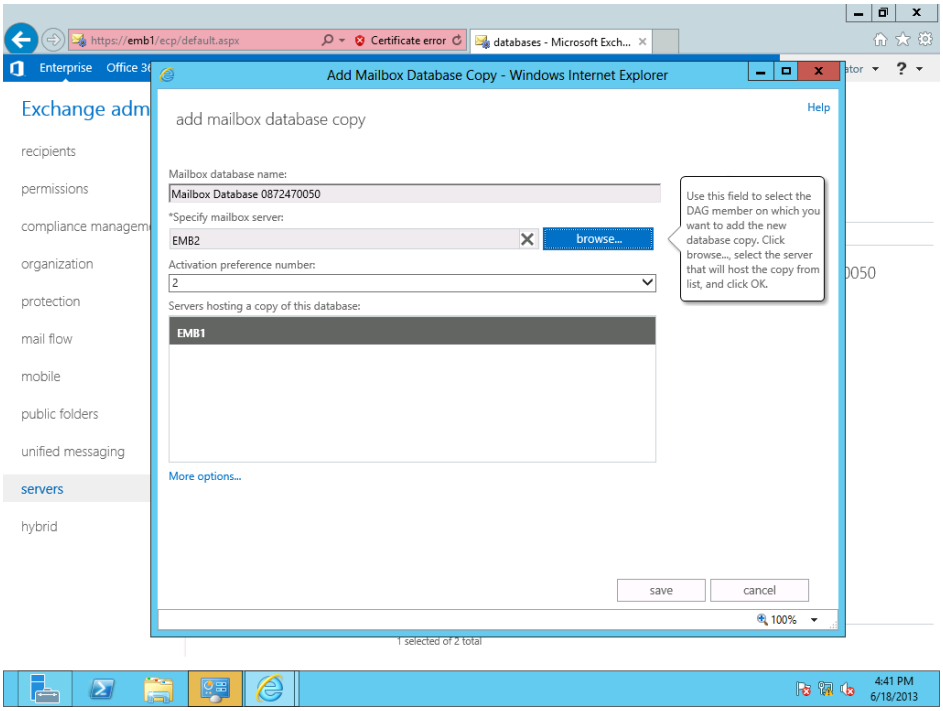

Figure 16: Configuring the database copies.

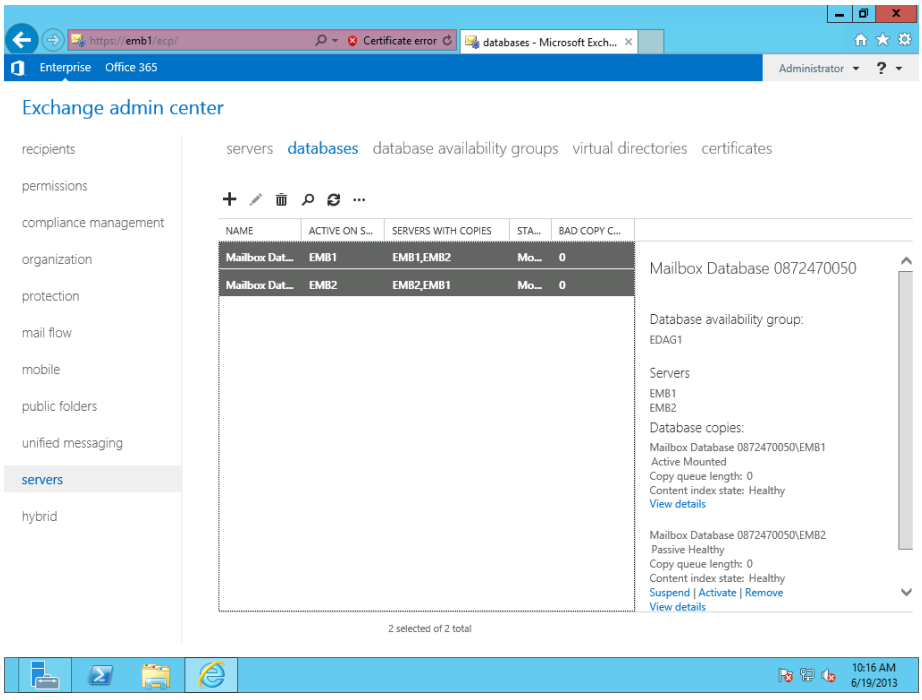

Figure 17: Database copies configured.

Installing Cumulative Update 1

In this section, we show you how to install the latest available update package as of when this guide was written. For step-by-step instructions, see Appendix E.

1. Download Microsoft Exchange 2013 Cumulative Update 1 from www.microsoft.com/en-us/download/details.aspx?id=38176 and run Exchange-x64.exe on the first Mailbox server VM. The wizard will automatically detect the installation and allow you to upgrade the role.
2. Run the wizard on the second Mailbox server VM, and then run the wizard on each Client Access server VM.
3. After Cumulative Update 1 is applied to each role, restart all four VMs.

SUMMING IT ALL UP

As this guide has shown, setting up a highly available Microsoft Exchange Server 2013 environment on the Dell PowerEdge VRTX is a straightforward process. In very little time, you can deploy Dell PowerEdge VRTX with up to four M-series nodes, switches, and storage in a redundant configuration using Microsoft Windows Server 2012 Hyper-V, and setup your Exchange Server infrastructure. By setting up a highly available Exchange Server 2013 environment on your compact PowerEdge VRTX, you can ensure your Exchange workloads stay running to keep your business moving.

APPENDIX A – CREATING AND CONFIGURING THE VMS

Adding a VLAN for replication traffic

1. Open a Web browser, and enter the address listed for the CMC IP on the front LCD display.
2. Log in with the appropriate credentials.
3. Expand I/O Module Overview.
4. Click Gigabit Ethernet.
5. Click the Properties tab.
6. Click the Launch I/O Module GUI button**.**
7. Log in with the appropriate credentials.
8. Click Submit.
9. Expand Switching→VLAN, and click VLAN Membership.
    a. Under the VLAN Membership tab, click Add.
    b. Enter a VLAN ID number (`100`).
    c. Enter a VLAN Name (`Replication`).
    d. Click Apply.
10. Click Switching→VLAN→Port Settings.
    a. Under the Port Settings tab, click Edit.
    b. Select the Internal Port radio button.
    c. After the screen populates, use the drop-down menu to select gi1/4.
    d. In the VLAN list, click 1, and click Remove.
    e. Enter `100` in the VLAN list box, and click Add.
    f. Click Apply.
    g. Use the drop-down menu to select gi2/4.
    h. In the VLAN list, click 1, and click Remove.
    i. In the VLAN list, enter `100`, and click Add.
    j. Click Apply.
11. In the upper-right corner of the configuration pane, click the floppy drive icon to save all new settings to start-up configuration.
12. Click Logout.
13. Click OK.

Creating a virtual switch for replication

Repeat these steps for each 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 the appropriate NIC port.
4. At the connectivity warning, click Yes.

Creating the VMs

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:
   - EMB1
   - ECA1
   - EFS1
   - EMB2
   - ECA2
6. At the Assign Memory screen, enter an amount appropriate for the server role, and click Next. You can find Exchange 2013 hardware requirements at technet.microsoft.com/en-us/library/aa996719(v=exchg.150).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. Click Add Hardware, and select Network Adapter. Click Add.
12. Use the drop-down menu to select the virtual switch for replication.

13. 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. You can map the VRTX DVD drive to different server nodes using the chassis LCD.
4. Click OK.
5. Right-click the VM, and click Start.
6. Right-click the VM, and click Connect.
7. 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 domain-connected 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.

Preparing VMs for Mailbox and/or Client Access server roles

Complete these steps on all VMs to be used for Exchange Mailbox and/or Client Access server roles. If you install the Mailbox and Client Access roles on different VMs, you must install the Mailbox role first.

1. Log into the VM using domain administrator credentials.
2. Open Windows Powershell, and run the following command:

   ```
   Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation
   ```

3. Restart the VM.
4. Download the Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit. (go.microsoft.com/fwlink/p/?linkId=258269)
5. Run UcmaRuntimeSetup.exe.
6. When the installation completes, click Finish.
7. If the server has the Client Access role only, this step is unnecessary. Otherwise, download the Microsoft Office 2010 Filter Pack 64bit. (go.microsoft.com/fwlink/p/?linkID=191548)
8. Run FilterPack64bit.exe.
9. When the installation completes, click OK.
10. If the server has the Client Access role only, this step is unnecessary. Otherwise, download the Microsoft Office 2010 Filter Pack SP1 64bit (go.microsoft.com/fwlink/p/?LinkId=254043)
11. Run filterpack2010sp1-kb2460041-x64-fullfile-en-us.exe.
12. When the installation completes, click OK.

APPENDIX B - INSTALLING THE EXCHANGE 2013 MAILBOX AND CLIENT ACCESS SERVER ROLES

Prior to these steps, ensure that the account used for this installation is in the Schema Admins and Enterprise Admins groups. Domain Admins will have these permissions by default. Complete the following steps on all VMs to be used for Mailbox or Client Access roles.

1. Log onto the server using the appropriate credentials.
2. Navigate to the location of the installation media, and double-click Setup.exe.
3. At the Check for Updates? screen, check the Connect to the Internet and check for updates checkbox, and click Next.
4. When the updates complete, click Next.
5. At the Introduction screen, click Next.
6. At the License Agreement screen, check the box to accept the terms, and click Next.
7. At the Recommended Settings screen, check the Don't use recommended settings checkbox, and click Next.
8. At the Server Role Selection, select Mailbox or Client Access role, and click Next. Install each Mailbox role first, and then install each Client Access role. For our testing, we chose the Mailbox role on two VMs, and the Client Access role on two additional VMs.
9. At the Installation Space and Location screen, select a location for the installation, and click Next. For our testing, we left the default location.
10. At the Exchange Organization screen, enter a name for your organization. If necessary, check the Apply Active Directory split permissions security model to the Exchange organization checkbox. Click Next.
11. At the Malware Protection Settings, choose to enable or disable malware scanning, and click Next. For our testing, we enabled malware scanning.
12. At the Readiness Checks screen, allow the verification to complete. If there are no failures, click Install.
13. When the installation completes, click Finish, and restart the VM.

APPENDIX C – PREPARING FOR HIGH AVAILABILITY

Configuring NLB on the Client Access VMs

In this section, we show you how to configure Windows-based network load balancing between the two Client Access server VMs. Although this solution will achieve basic load balancing, we recommend using a hardware load balancing solution for best performance.

1. Using Server Manager, add the Network Load Balancing feature. Accept all required features. Repeat this step on all Client Access VMs.
2. Log onto the first Client Access VM using Domain Administrator credentials.
3. In Server Manager, click Tools→Network Load Balancing Manager.
4. Click Cluster→New.
5. In the Host field, enter the local IP address, and click Connect.
6. Select an interface that is on the client-facing network, and click Next.
7. At the Host Parameters screen, click Next.
8. At the Cluster IP Addresses screen, click Add.
9. Enter an IP address and subnet mask on the client-facing network, and click OK.
10. At the Cluster Parameters screen, enter a hostname for the cluster in the Full Internet name field. Select the Multicast radio button, and click Next.
11. At the Port Rules screen, click Finish.
12. Click Cluster→Add host to cluster.
13. Enter the IP address of a remaining Client Access VM, and click Connect.
14. Select the IP address that is on the client-facing network, and click Next.
15. At the Host Parameters screen, click Next.
16. At the Port Rules screen, click Finish.
17. Repeat steps 12 through 16 for any remaining Client Access VMs.

Configuring the File Witness VM

Two-node Exchange 2013 Database Availability Groups require a server to act as a quorum witness. To fulfill this requirement, we configured a File Witness virtual machine running Windows Server 2012. Once you have installed the OS, complete the following steps:

1. Add the File Witness VM to the domain, and restart the VM.
2. Log in with Domain Admin credentials.
3. In Server Manager, click Tools→Computer Management.

4. In the left pane, click Local Users and Groups→Groups.
5. Right-click Administrators, and click Properties.
6. Click Add.
7. Type `Exchange Trusted Subsystem` and press Enter.
8. Confirm that the domain account Exchange Trusted Subsystem was added to the local Administrators group, and click OK.
9. Use Server Manager to add the File Server feature and all requisites. You can find the feature under File And Storage Services→File and iSCSI Services→File Server.
10. Open the Start menu, and click Control Panel.
11. Click System and Security→Windows Firewall→Allow an app or feature through Windows Firewall.
12. Check the File and Printer Sharing checkbox for the Domain firewall, and click OK.
13. Create a new folder on the C:\ drive to use as a file witness directory. We called ours `Exchange Witness Dir`.
14. Right-click the witness directory, and click Properties.
15. Click the Sharing tab.
16. Click Share.
17. Open the drop-down menu, and click Find People.
18. Type `Exchange Trusted Subsystem` and click OK.
19. Click the drop-down menu next to Exchange Trusted Subsystem, and select Read/Write.
20. Click Share.
21. Click Done.
22. Click Close.

Configuring the replication network

Microsoft recommends that all Mailbox role servers reside on a dedicated, high-bandwidth network for data replication traffic. Complete the following steps:

1. Log into the first Mailbox VM using Domain Admin credentials.
2. From the Run prompt, type `ncpa.cpl` and press Enter.
3. Right-click the adapter for the replication network, and click Properties.
4. Select Internet Protocol Version 4 (TCP/IPv4), and click Properties.

5. Enter an IP address and subnet mask, while leaving the Default Gateway and DNS Server entries blank. Click Advanced.
6. Select the DNS tab, uncheck the Register this connection's address in DNS checkbox, and click OK.
7. Repeat steps 1 through 6 for all remaining Mailbox servers.

APPENDIX D - CREATING THE DATABASE AVAILABILITY GROUP

Pre-staging the Cluster Name Object

This step is required if the Database Availability Group (DAG) servers are running Windows Server 2012 and is otherwise a Microsoft recommended best practice.

1. Log into the Active Directory server with Domain Administrator credentials.
2. In Server Manager, click Tools→Active Directory Users and Computers.
3. In the left pane, click Computers.
4. Click Action→New→Computer.
5. In the Computer Name field, type the name that you will use for the DAG. In our setup, we used `EDAG1`. Click OK.
6. Right-click the newly created computer and click Disable Account. Click Yes at the warning. Click OK at the verification screen.
7. Click View→Advanced Features.
8. Right-click the DAG computer again, and click Properties.
9. Click the Security tab.
10. Click Add.
11. Click Object Types, and check the Computers checkbox. Click OK.
12. Type the name of the first DAG member (in our case, it was `EMB1)`. Press Enter.
13. Select the newly added DAG member, and check the Full control checkbox.
14. Click OK.

Creating the database availability group

1. Using a Web browser from a computer on the domain, navigate to the Exchange Admin Center (EAC), which you can access through the Client Access servers. In our setup, the address was `https://ECA1/ecp`. For the EAC to work properly, it may be necessary to use the latest version of Internet Explorer and install the Microsoft Visual C++ Redistributable Package, which you can download from www.microsoft.com/en-us/download/confirmation.aspx?id=14632.
2. At the certificate warning page, click Continue to this website (not recommended).
3. Log in with the credentials specified during the Exchange 2013 Mailbox role installation. For our setup, the user was `TEST\Administrator` and the password was `Password1`.

4. If this is the first time accessing the EAC, you will see a prompt for a language and time zone. Make the appropriate selections, and click Save.
5. Click Servers→Database Availability Groups, and click the + symbol.
6. Enter the following information:
    a. Database availability group name – This must be the same as the Cluster Named Object created in the previous section.
    b. Witness server – Enter the hostname of the File Witness server created in an earlier section. Alternatively, you can leave this blank and allow the EAC to find an appropriate server automatically.
    c. Witness directory – Enter a location on the File Witness server to store witness information. Alternatively, you can leave this blank and allow the EAC to find an appropriate directory automatically. For our setup, we used a folder on the C:\ drive.
    d. IP address – Enter an IP address to be used as the virtual address for the DAG and click the + symbol to add it. We used `192.168.1.31`.
7. Click Save. You may see a warning about the Exchange Trusted Subsystem not being a member of the File Witness server's local Administrators group. This is a known bug that you can ignore. For further information, see support.microsoft.com/kb/2644540.

Adding servers to the DAG

1. Restart the Client Access, Mailbox, and File Witness VMs.
2. Log into the EAC, and click Servers→Database Availability Groups.
3. Select the DAG, and click the Manage DAG Membership icon (just left of the Refresh icon).
4. Click the + symbol.
5. Select a VM you wish to add to the DAG, and click Add. Repeat for all VMs you wish to add.
6. Click OK.
7. Click Save.

Configuring the database copies

Configure the Mailbox Databases in such a way so that each Mailbox server hosts an active copy of its own database and passive copies of databases from other servers. If you have more than two Mailbox servers, configure the database copies in a round robin fashion for decreased downtime in the case of a failover. Further

information can be found here: technet.microsoft.com/en-us/library/dd638129(v=exchg.150).aspx

1. Log into the EAC, and click Servers→Databases.
2. Select the first mailbox, and click the … symbol. Click Add Database Copy.
3. Click Browse to specify a Mailbox VM.
4. Select the other Mailbox VM, and click OK.
5. Click Save.
6. When the operation completes, click Close.
7. Repeat steps 2 through 6 for the second mailbox.

APPENDIX E – INSTALLING UPDATES

Installing Cumulative Update 1

Repeat these steps on each VM that has a Mailbox or Client Access role installed. Update the Mailbox role VMs first, then the Client Access role VMs.

1. Download Cumulative update 1 from here www.microsoft.com/en-us/download/details.aspx?id=38176.
2. Run Exchange-x64.exe. Choose a directory to extract the installation files to, and click OK.
3. Navigate to the extraction location, and run Setup.exe.
4. At the Check for Updates? screen, select the Connect to the Internet and check for updates radio button, and click Next.
5. Install any updates that are found, and click Next.
6. At the Upgrade screen, click Next.
7. Accept the license terms, and click Next.
8. At the Readiness Checks screen, wait for the prerequisite check to complete, and click Install.
9. When the installation completes, reboot the VM.

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.