Deployment for Multiple Availability Zones

17 JUL 2018
VMware Validated Design 4.3
VMware Validated Design for Software-Defined Data Center 4.3

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About VMware Validated Design Deployment for Multiple Availability Zones

1

VMware Validated Design for Deployment for Multiple Availability Zones provides step-by-step instructions for installing and configuring multiple availability zones in the Software-Defined Data Center (SDDC).

VMware Validated Design for Deployment for Multiple Availability Zones does not contain instructions for performing all the required post-configuration tasks because they often depend on customer requirements.

Intended Audience

The *VMware Validated Design for Deployment for Multiple Availability Zones* document is intended for cloud architects, infrastructure administrators, and cloud administrators who are familiar with and want to use VMware software to deploy in a short time and manage an SDDC that meets the requirements for capacity, scalability, backup and restore, and extensibility for disaster recovery support.

Required VMware Software

VMware Validated Design for Deployment for Multiple Availability Zones is compliant and validated with certain product versions. See *VMware Validated Design Release Notes* for more information about supported product versions.

Prerequisites for Deployment of a Second Availability Zone

2

Deploy both Region A and Region B before you start deploying a second availability zone. You must set up another environment that has a specific compute, storage, and network configuration for the Availability Zone 2 in Region A.

This chapter includes the following topics:

VLANs and IP Subnets for a Second Availability Zone in Region A

Use the following VLANs and IP subnets in Availability Zone 2.

You must configure your physical network according to the following requirements.

- Stretch the ESXi management VLAN of Availability Zone 1 over Availability Zone 2.
- Configure and use the same VLAN ID for NSX VXLAN traffic. This VLAN ID does not have to be stretched across the two availability zones.
- Configure routing on the physical switch for vSAN VLANs of Availability Zone 1, Availability Zone 2 and Region B.

Table 2-1. VLAN and IP Subnet Configuration in Availability Zone 2

Cluster in Region A	VLAN Function	VLAN ID	Subnet	Gateway
Management Cluster	Availability Zone 1 Management	1611 (Stretched L2)	172.16.11.0/24	172.16.11.253
	Availability Zone 2 Management	1621	172.16.21.0/24	172.16.21.253
	vSphere vMotion	1622	172.16.22.0/24	172.16.22.253
	vSAN	1623	172.16.23.0/24	172.16.23.253
	VXLAN (NSX VTEP)	1614	172.16.14.0/24	172.16.14.253
	■ vSphere Replication ■ vSphere Replication NFC	1626	172.16.26.0/24	172.16.26.253

Table 2-1. VLAN and IP Subnet Configuration in Availability Zone 2 (Continued)

Cluster in Region A	VLAN Function	VLAN ID	Subnet	Gateway
	Uplink01	1650	172.16.50.0/24	172.16.50.253
	Uplink02	1651	172.16.51.0/24	172.16.51.253

Note Use these VLAN IDs and IP subnets as samples. Configure the actual VLAN IDs and IP subnets according to your environment.

Host Names and IP Addresses

Define the host names and IP addresses required for Availability Zone 2. You must also configure some of these host names in DNS with fully qualified domain names (FQDNs) that map the hostnames to the IP addresses.

Allocate host names and IP addresses to all components you deploy for the virtual infrastructure layer of the SDDC according to this VMware Validated Design.

Table 2-2. Host Names and IP Addresses for the Virtual Infrastructure Layer

Component Group	Host Name	DNS Zone	IP Address	Description
vSAN witness host	sfo03m01vsanw01	sfo01.rainpole.local	172.17.11.201	vSAN witness host in Region B
vSphere	sfo02m01esx01	sfo01.rainpole.local	172.16.21.101	ESXi hosts in Availability Zone 2.
	sfo02m01esx02	sfo01.rainpole.local	172.16.21.102	
	sfo02m01esx03	sfo01.rainpole.local	172.16.21.103	
	sfo02m01esx04	sfo01.rainpole.local	172.16.21.104	
NSX for vSphere	sfo02m01esg01	-	■ 172.16.50.2 ■ 172.16.51.3 ■ 192.168.10.20	ECMP-enabled NSX Edge devices for North-South management traffic
	sfo02m01esg02	-	■ 172.16.50.3 ■ 172.16.51.2 ■ 192.168.10.21	

Deploy and Configure the vSAN Witness Host in Region B

3

vSAN stretched cluster requires a witness host deployed in a third location, different from the location of both availability zones.

Instead of using a dedicated physical ESXi host as a witness host, you can deploy the vSAN witness appliance. Unlike a general purpose ESXi host, the witness appliance does not run virtual machines. It's only purpose is to serve as a vSAN witness.

Procedure

1 Deploy the vSAN Witness Host in Region B

Start the deployment of multiple availability zones by deploying the vSAN witness host in Region B.

2 Configure Management Network on the vSAN Witness Host in Region B

After the initial boot, use the ESXi Direct Console User Interface (DCUI) for vSAN witness host management network configuration.

3 Add the vSAN Witness Host as a Standalone Host in Region A

You must add the vSAN witness host as a standalone host in the Region A Management vCenter Server, to use it as the witness host of the vSAN stretched cluster.

4 Configure the vSAN Witness Host

Configure the witness network on the vSAN witness host to enable vSAN data network communication to both availability zones.

Deploy the vSAN Witness Host in Region B

Start the deployment of multiple availability zones by deploying the vSAN witness host in Region B.

Prerequisites

Download the vSAN witness host virtual appliance `.ova` file to the machine where you use the vSphere Web Client.

Procedure

1 Log in to vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://lax01m01vc01.lax01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Navigator** pane, expand the entire **lax01m01vc01.lax01.rainpole.local** tree.

3 Right-click the **lax01-m01-mgmt01** cluster and click **Deploy OVF Template**.

4 On the **Select template** page, click **Browse**, select the vSAN witness host `.ova` file on your local file system, and click **Next**.

5 On the **Select name and location** page, enter the following settings, and click **Next**.

Setting	Value
Name	sfo03m01vsanw01
Data center or folder	lax01-m01fd-mgmt

6 On the **Select a resource** page, select the following values, and click **Next**.

Setting	Value
Cluster	lax01-m01-mgmt01

7 On the **Review details** page click **Next**.

8 On the **Accept license agreements** page, click **Accept** and click **Next**.

9 On the **Select configuration** page, select **Medium (up to 500 VMs)**.

10 On the **Select storage** page, enter the following settings, and click **Next**.

Setting	Value
Select virtual disk format	Thin provision
VM storage policy	vSAN Default Storage Policy
Datastore	lax01-m01-vsan01

11 On the **Setup networks** page, enter the following settings, and click **Next**.

Source Network	Destination Network
Witness network	lax01-m01-vds01-vsan
Management network	lax01-m01-vds01-management

12 On the **Customize template** page, expand all options, enter the following settings, and click **Next**.

Setting	Value
Root password / Enter password	*vsan_witness_root_password*
Root password / Confirm password	*vsan_witness_root_password*

13 On the **Ready to Complete** page, click **Finish**.

14 In the **Navigator** pane, expand the entire **lax01m01vc01.lax01.rainpole.local** tree, select the virtual machine **sfo03m01vsanw01**, and click the **Power on** button.

Configure Management Network on the vSAN Witness Host in Region B

After the initial boot, use the ESXi Direct Console User Interface (DCUI) for vSAN witness host management network configuration.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to `https://lax01m01vc01.lax01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Navigator** pane, expand the entire **lax01m01vc01.lax01.rainpole.local** tree.

3 Right-click the virtual machine **sfo03m01vsanw01**, and click **Open Console**.

4 Open the DCUI on the vSAN witness host **sfo03m01vsanw01**.

   a In the remote console, wait until the witness host is fully started.

   b Press F2 to enter the DCUI.

   c Log in using the following credentials.

Setting	Value
User name	root
Password	*vsan_witness_root_password*

5 Configure the management network.

   a Select **Configure Management Network** and press Enter.

   b Select **IPv4 Configuration** and press Enter.

c Configure the IPv4 network using the following settings, and press Enter.

Setting	Value
Set static IPv4 address and network configuration	Selected
IPv4 Address	172.17.11.201
Subnet Mask	255.255.255.0
Default Gateway	172.17.11.253

d Select **DNS Configuration** and press Enter.

e Configure the following DNS settings, and press Enter.

Setting	Value
Use the following DNS Server address and hostname	Selected
Primary DNS Server	172.17.11.5
Alternate DNS Server	172.17.11.4
Hostname	sfo03m01vsanw01.sfo01.rainpole.local

f Select **Custom DNS Suffixes** and press Enter.

g Verify that the list contains no suffixes, and press Enter.

6 After completing all host network settings press Escape to exit, and press Y to confirm the changes.

Add the vSAN Witness Host as a Standalone Host in Region A

You must add the vSAN witness host as a standalone host in the Region A Management vCenter Server, to use it as the witness host of the vSAN stretched cluster.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Add the vSAN witness host as a standalone host in the Region A Management vCenter Server.

a In the **Navigator** pane, expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

b Right-click the **sfo01-m01dc** datacenter and click **Add Host**.

c On the **Name and location** page, enter the following settings, and click **Next**.

Setting	Value
Host name or IP address	sfo03m01vsanw01.sfo01.rainpole.local

d On the **Connection settings** page, enter the following credential, and click **Next**.

Setting	Value
User name	root
Password	*vsan_witness_root_password*

e In the **Security Alert** dialog box, click **Yes**.

f On the **Host summary** page, review the host information, and click **Next**.

g On the **Assign license** page, keep the default license, and click **Next**.

h On the **Lockdown mode** page click **Next**.

i On the **VM location** page click **Next**.

j On the **Ready to complete** page, review the entries, and click **Finish**.

3 Enable the SSH service on the vSAN witness host.

a In the **Navigator** pane, expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

b Select host **sfo03m01vsanw01.sfo01.rainpole.local**, and click the **Configure** tab,

c Under the **System** section, select **Security Profile** and under **Services**, click the **Edit** button. .

d In the **Edit Security Profile** dialog box, select **SSH**, change the **Startup policy** to **Start and stop with host**, and click the **Start** button.

e Click **OK** to save these changes.

Configure the vSAN Witness Host

Configure the witness network on the vSAN witness host to enable vSAN data network communication to both availability zones.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Navigator** pane, expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Select the **sfo03m01vsanw01.sfo01.rainpole.local** host, and click the **Configure** tab.

4 Under **Networking** click **VMkernel adapters**.

5 In the **VMkernel adapters** panel, select **vmk1** which has **witnessPg** as **Network Label**, and click the **Edit settings** icon.

6 In the **vmk1 - Edit Settings** dialog box, click **IPv4 settings**, select **Use static IPv4 settings**, enter the following settings and click **OK**.

Setting	Value
IPv4 address	172.17.13.201
Subnet mask	255.255.255.0
Default gateway	Deselected

7 Provision swap files on vSAN as thin for the vSAN witness host.

   a In the **Navigator** pane, click **Hosts and Clusters** and expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

   b Select the **sfo03m01vsanw01.sfo01.rainpole.local** host.

   c Click the **Configure** tab and under **System** click **Advanced System Settings**.

   d Click the **Edit** button.

   e In the **Filter** text box, enter `vsan.swap`.

   f Change the value of **VSAN.SwapThickProvisionDisabled** to `1` and click **OK**.

8 Create IP Sets and Security Groups on the NSX Manager for the vSAN witness host.

   a In the **Navigator** pane click **Networking & Security**.

   b Click **NSX Managers** and click the **172.16.11.65** instance.

   c Click **Manage**, click **Grouping Objects**, and click **IP Sets**.

   d Select **SDDC**, click the **Edit IP Set** icon.

   e In the **Edit IP Set** dialog box, add both witness host management IP address and witness network IP address, `172.17.11.201,172.17.13.201` as **IP Addresses** and click **OK**.

   f Click the **Add new IP Set** icon. In the **New IP Set** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	vSAN Witness
IP Address	172.17.11.201
Mark this object for Universal Synchronization	Selected

g Click **Security Group**, click the **Add new Security Group** icon, enter the following settings and click **Next**.

Setting	Value
Name	vSAN Witness
Mark this object for Universal Synchronization	Selected

h Choose the **vSAN Witness** IP Set, move it to the **Selected column** and click **Finish**.

9 Enable administrator SSH access to the vSAN witness host.

a In the **Navigator** pane, click **Networking & Security** and click **Firewall**.

b From the **NSX Manager** drop-down menu, select **172.16.11.65**.

c Select the **Allow SSH to admins** rule, and click the **Edit** icon in the **Destination column**.

d Change the **Object Type** to **Security Groups**, add **vSAN Witness** to the **Selected Objects** list, and click **OK**.

e Click **Publish Changes**.

Install and Configure ESXi Hosts for Availability Zone 2 in Region A

4

Begin the deployment of Availability Zone 2 in Region A by installing and configuring all the ESXi hosts.

This chapter includes the following topics:

Prerequisites for Installation of ESXi Hosts for Availability Zone 2

Install and configure the ESXi hosts for Availability Zone 2.

Before you begin with the installation:

- Make sure that you have a Windows host with access to your data center. You use this host to connect to the ESXi hosts and perform the configuration steps.
- Download the ESXi ISO installer.
- Create a bootable USB drive that contains the ESXi Installation. See *Format a USB Flash Drive to Boot the ESXi Installation or Upgrade* in the *vSphere Installation and Setup* document.

IP Addresses, Hostnames, and Network Configuration

The following table contains the values necessary for hosts configuration.

Table 4-1. Availability Zone 2 Hosts in Region A

FQDN	IP	Management VLAN	Default Gateway	NTP Server
sfo02m01esx01.sfo01.rainpole.local	172.16.21.101	1621	172.16.21.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
sfo02m01esx02.sfo01.rainpole.local	172.16.21.102	1621	172.16.21.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Table 4-1. Availability Zone 2 Hosts in Region A (Continued)

FQDN	IP	Management VLAN	Default Gateway	NTP Server
sfo02m01esx03.sfo01.rainpole.local	172.16.21.103	1621	172.16.21.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
sfo02m01esx04.sfo01.rainpole.local	172.16.21.104	1621	172.16.21.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Install ESXi Interactively on All Hosts in Availability Zone 2

Install all ESXi hosts for all clusters interactively.

Procedure

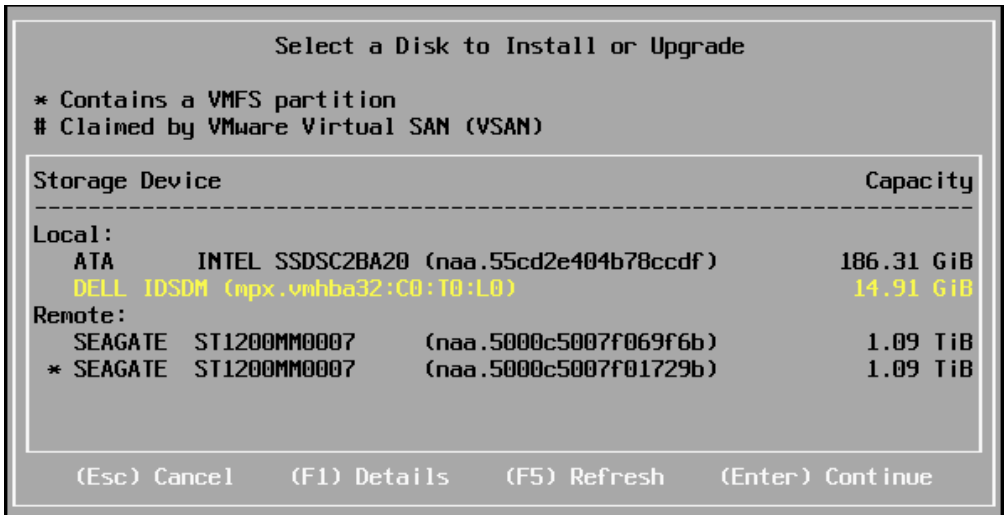
1 Power on the sfo02m01esx01 host in Region A.

2 Mount the USB drive containing the ESXi ISO file, and boot from that USB drive.

3 On the **Welcome to the VMware 6.5.0 Installation** screen, press Enter to start the installation.

4 On the **End User License Agreement (EULA)** screen, press F11 to accept the EULA.

5 On the **Select a Disk to Install or Upgrade** screen, select the USB drive or SD card under local storage to install ESXi, and press Enter to continue.



6 Select the keyboard layout, and press Enter.

7 Enter the ***esxi_root_user_password***, confirm, and press Enter.

8 On the **Confirm Install** screen, press F11 to start the installation.

9 After the installation has completed successfully, unmount the USB drive, and press Enter to reboot the host.

10 Repeat this procedure for all hosts in the data center, using the respective values for each host you configure.

Configure Management Network on All Hosts in Availability Zone 2

After the initial boot, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access.

Perform the following tasks to configure the host network settings:

- Set network adapter (vmk0) and VLAN ID for the Management Network.
- Set IP address, subnet mask, gateway, DNS server, and FQDN for the ESXi host.

Repeat this procedure for all ESXi hosts in the management cluster in Availability Zone 2. Enter the respective values from the prerequisites section for each host that you configure. See Prerequisites for Installation of ESXi Hosts for Availability Zone 2.

Procedure

1 Open the DCUI on the physical ESXi host **sfo02m01esx01**.

   a Open a console window to the host.

   b Press F2 to enter the DCUI.

   c Log in using the following credentials.

Setting	Value
User name	root
Password	*vsan_witness_root_password*

2 Configure the management network.

   a Select **Configure Management Network** and press Enter.

   b Select **VLAN (Optional)** and press Enter.

   c Enter **1621** as the VLAN ID for the Management Network and press Enter.

   d Select **IPv4 Configuration** and press Enter.

   e Configure IPv4 network using the following settings, and press Enter.

Setting	Value
Set static IPv4 address and network configuration	Selected
IPv4 Address	172.16.21.101
Subnet Mask	255.255.255.0
Default Gateway	172.16.21.253

   f Select **DNS Configuration** and press Enter.

g Configure the following DNS settings, and press Enter.

Setting	Value
Use the following DNS Server address and hostname	Selected
Primary DNS Server	172.16.11.5
Alternate DNS Server	172.16.11.4
Hostname	sfo02m01esx01.sfo01.rainpole.local

h Select **Custom DNS Suffixes** and press Enter.

i Ensure there are no suffixes listed, and press Enter.

3 After completing all host network settings, press Escape to exit, and press Y to confirm the changes.

4 Repeat this procedure for all hosts in Availability Zone 2.

Configure SSH and NTP on the First ESXi Host in Availability Zone 2

Time synchronization issues can result in serious problems with your environment. Configure NTP for each of the ESXi hosts in Availability Zone 2.

Procedure

1 Log in to the ESXi host sfo02m01esx01 using the VMware Host Client.

a Open a Web browser and go to **`https://sfo02m01esx01.sfo01.rainpole.local`**.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2 Configure SSH options.

a In the **Navigator** pane, click **Manage**, and click the **Services** tab.

b Select the **TSM-SSH** service, click the **Actions** menu, select **Policy**, and click **Start and stop with host**.

c Click **Start** to start the service.

3 Configure the NTP Daemon (ntpd) options.

a In the **Navigator** pane, click **Manage**, click the **System** tab, click **Time & date**, and click **Edit Settings**.

b In the **Edit time configuration** dialog box, select the **Use Network Time Protocol (enable NTP client)** radio button, enter the following settings, and click **Save**.

Setting	Value
NTP service startup policy	**Start and stop with host**
NTP servers	`ntp.sfo01.rainpole.local,ntp.lax01.rainpole.local`

c Start the service by clicking **Actions**, point to **NTP service**, and choose **Start**.

Configure the Management Cluster in Region A for Availability Zone 2

5

You must now configure the management cluster in Region A and add all the ESXi hosts in Availability Zone 2.

This chapter includes the following topics:

Detach Host Profile from the Management Cluster and Attach it to All Hosts in Availability Zone 1

The hosts in the two availability zones use different VLANs and subnets, and you cannot use the same host profile for both availability zones. Detach the original host profile from the management cluster in Region A and attach it only to the ESXi hosts in Availability Zone 1.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Detach the sfo01-m01-mgmt01 host profile from the management cluster in Region A.

   a From the **Home** menu select **Policies and Profiles**.

   b In the **Navigator** pane, click **Host Profiles**.

   c Right-click **sfo01-m01hp-mgmt01** and select **Attach/Detach Hosts and Clusters**.

   d On the **Select hosts/clusters** page, select the **sfo01-m01-mgmt01** cluster on the right and click **Detach**.

   e On the **Customize hosts** page, click **Finish**.

3 Attach the sfo01-m01-mgmt01 host profile to the ESXi hosts in Availability Zone 1.

   a From the **Home** menu select **Policies and Profiles**.

   b In the **Navigator** pane, click **Host Profiles**.

   c Right-click **sfo01-m01hp-mgmt01** and select **Attach/Detach Hosts and Clusters**.

   d On the **Select hosts/clusters** page, expand the **sfo01-m01-mgmt01** cluster on the left, select all the ESXi hosts in Availability Zone 1, and click **Attach**.

Setting	Value
Host 1	sfo01m01esx01.sfo01.rainpole.local
Host 2	sfo01m01esx02.sfo01.rainpole.local
Host 3	sfo01m01esx03.sfo01.rainpole.local
Host 4	sfo01m01esx04.sfo01.rainpole.local

   e Select **Skip Host Customization** and click **Finish**.

Create Host Groups and Rules for Availability Zone 1

Create rules to ensure that all virtual machines that are created in Availability Zone 1 run on ESXi hosts in the same zone.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Navigator** pane, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.

4 Create a host group containing all ESXi hosts of Availability Zone 1.

   a Under **Configuration**, click **VM/Host Groups**.

   b On the **VM/Host Groups** page, click the **Add** button.

   c In the **Create VM/Host Group** dialog, enter **`availability-zone-1-hosts`** in the **Name** field, select **Host Group** from the **Type** drop-down menu, and click the **Add** button.

   d In the **Add VM/Host Group Member** dialog box, select all the ESXi hosts in Availability Zone 1 and click **OK**.

Setting	Value
Host 1	sfo01m01esx01.sfo01.rainpole.local
Host 2	sfo01m01esx02.sfo01.rainpole.local
Host 3	sfo01m01esx03.sfo01.rainpole.local
Host 4	sfo01m01esx04.sfo01.rainpole.local

   e Click **OK** to create the host group.

5 Create a VM group containing all virtual machines of Availability Zone 1.

   a Under **Configuration**, click **VM/Host Groups**.

   b On the **VM/Host Groups** page, click the **Add** button.

   c In the **Create VM/Host Group** dialog, enter **`availability-zone-1-vms`** in the **Name** field, select **VM Group** from the **Type** drop-down menu, and click the **Add** button.

   d In the **Add VM/Host Group Member** dialog box, select all the VMs of Availability Zone 1, and click **OK**.

   e Click **OK** to create the VM group.

6 Create a rule to run virtual machines in Availability Zone 1 on hosts in the same zone.

a Under **Configuration**, click **VM/Host Rules**.

b On the **VM/Host Rules** page, click the **Add** button.

c In the **Create VM/Host Rule** dialog, enter the following settings, and click **OK**.

Setting	Value
Name	hostgroup-availability-zone-1
Enable rule	Selected
Type	Virtual Machines to Hosts
VM Group	availability-zone-1-vms
	Should run on hosts in group
Host Group	availability-zone-1-hosts

Add All the ESXi Hosts in Availability Zone 2 to the Management Cluster in Region A

You must now add all ESXi hosts in Availability Zone 2 into the Region A management cluster.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Add all the ESXi hosts in Availability Zone 2 to the management cluster in Region A.

a From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc** tree.

b Right-click the **sfo01-m01-mgmt01** cluster, and click **Add Host**.

c On the **Name and location** page, enter `sfo02m01esx01.sfo01.rainpole.local` in the **Host name or IP address** text box and click **Next**.

d On the **Connection settings** page, enter the following credentials and click **Next**.

Setting	Value
User name	root
Password	*esxi_root_user_password*

e In the **Security Alert** dialog, click **Yes**.

f On the **Host summary** page, review the host information and click **Next**.

g On the **Resource pool** page, click **Next**.

h On the **Ready to complete** page, review your entries and click **Finish**.

i Repeat this step for the remaining hosts of Availability Zone 2 and add them to the management cluster in Region A.

Setting	Value
Host 2	sfo02m01esx02.sfo01.rainpole.local
Host 3	sfo02m01esx03.sfo01.rainpole.local
Host 4	sfo02m01esx04.sfo01.rainpole.local

3 Add an ESXi host to the Active Directory domain.

a From the **Home** menu, select **Hosts and Clusters** and expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

b Select the **sfo02m01esx01.sfo01.rainpole.local** host and click the **Configure** tab.

c Under **System**, click **Authentication Services**.

d In the **Authentication Services** panel, click the **Join Domain** button.

e In the **Join Domain** dialog, enter the following settings and click **OK**.

Setting	Value
Domain	sfo01.rainpole.local
Using credentials	Selected
User name	svc-domain-join@rainpole.local
Password	*svc-domain-join_password*

4 Set the Active Directory Service to start and stop with host.

a From the **Home** menu, select **Hosts and Clusters** and expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

b Select the **sfo02m01esx01.sfo01.rainpole.local** host and click the **Configure** tab.

c Under **System**, click **Security Profile**.

d Click the **Edit** button next to **Services**.

e Select the **Active Directory Service**, and change the **Startup Policy** to **Start and stop with host**, and click **OK**.

Change Advanced Options on the First ESXi Host of Availability Zone 2

Change the default ESX Admins group to achieve greater levels of security and enable vSAN to provision virtual machine swap files as thin to save space in the vSAN datastore.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Change the default ESX Admins group.

   a In the **Navigator** pane, click **Hosts and Clusters** and expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

   b Select the **sfo02m01esx01.sfo01.rainpole.local** host and click the **Configure** tab.

   c Under **System**, click **Advanced System Settings**, and click the **Edit** button.

   d In the **Filter** text box, enter **`esxAdmins`**.

   e Change the value of **Config.HostAgent.plugins.hostsvc.esxAdminsGroup** to **`SDDC-Admins`**, and click **OK**.

3 Provision virtual machine swap files on vSAN as thin.

   a In the **Navigator** pane, click **Hosts and Clusters** and expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

   b Select the **sfo02m01esx01.sfo01.rainpole.local** host and click the **Configure** tab..

   c Under **System**, click **Advanced System Settings**, and click the **Edit** button.

   d In the **Filter** text box, enter **`vsan.swap`**.

   e Change the value of **VSAN.SwapThickProvisionDisabled** to **`1`**, and click **OK**.

4 Disable the SSH warning banner.

   a In the **Navigator** pane, click **Hosts and Clusters** and expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

   b Select the **sfo02m01esx01.sfo01.rainpole.local** host and click the **Configure** tab..

   c Under **System**, click **Advanced System Settings**, and click the **Edit** button.

d In the **Filter** text box, enter `ssh` .

e Change the value of **UserVars.SuppressShellWarning** to `1`, and click **OK**.

Configure vSphere Distributed Switch for Availability Zone 2

After you add all ESXi hosts in Availability Zone 2 to the management cluster in Region A, you must create port groups to handle the management traffic in Availability Zone 2. You must also migrate the ESXi host management VMkernel adapters to the vSphere Distributed Switch.

Create Port Groups for Management Traffic in Availability Zone 2

After you added all ESXi hosts to the cluster, create the distributed switch port groups required for Availability Zone 2.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Navigator** pane, click **Networking** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Create port groups in the **sfo01-m01-vds01** distributed switch for Availability Zone 2.

a Right-click the **sfo01-m01-vds01** distributed switch, and select **Distributed Port Group > New Distributed Port Group**.

b Create port groups with the following settings and click **Next**.

Port Group Name	Port Binding	VLAN Type	VLAN ID
sfo02-m01-vds01-management	Ephemeral binding	VLAN	1621
sfo02-m01-vds01-vmotion	Static binding	VLAN	1622
sfo02-m01-vds01-vsan	Static binding	VLAN	1623
sfo02-m01-vds01-replication	Static binding	VLAN	1626
sfo02-m01-vds01-uplink01	Static binding	VLAN	1650
sfo02-m01-vds01-uplink02	Static binding	VLAN	1651

c On the **Ready to complete** page, review your entries, and click **Finish**.

d Repeat this step for each port group.

4 Configure the port groups to use the **Route Based on Physical NIC Load** teaming algorithm.

   a Right-click the **sfo01-m01-vds01** distributed switch and select **Distributed Port Group > Manage Distributed Port Groups**.

   b On the **Select port group policies** page, select **Teaming and failover** and click **Next**.

   c Click the **Select distributed port groups** button, add all port groups except **sfo02-m01-vds01-uplink01** and **sfo02-m01-vds01-uplink02**, click **OK** and click **Next**.

   d On the **Teaming and failover** page, select **Route based on physical NIC load** from the **Load balancing** drop-down menu and click **Next**.

   e Click **Finish**.

5 Configure the uplinks for the **sfo02-m01-vds01-uplink01** and **sfo02-m01-vds01-uplink02** port groups.

   a Right click the **sfo02-m01-vds01-uplink01** port group, and click **Edit Settings**.

   b Select **Teaming and Failover**.

   c Move **dvUplink2** to **Unused uplinks** and click **OK**.

   d Right click the **sfo02-m01-vds01-uplink02** port group, and click **Edit Settings**.

   e Select **Teaming and Failover**.

   f Move **dvUplink1** to **Unused uplinks** and click **OK**.

Connect the First ESXi Host in Availability Zone 2 to vSphere Distributed Switch

After you created the port groups for Availability Zone 2, attach the first ESXi host in Availability Zone 2 to the distributed switch.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Navigator** pane, click **Networking** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Connect the sfo02m01esx01.sfo01.rainpole.local ESXi host to the sfo01-m01-vds01 distributed switch by migrating its VMkernel network adapters.

   a Right-click the **sfo01-m01-vds01** distributed switch, and click **Add and Manage Hosts**.

   b On the **Select task** page, select **Add hosts** and click **Next**.

   c On the **Select hosts** page, click **New hosts**.

   d In the **Select new hosts** dialog box, select **sfo02m01esx01.sfo01.rainpole.local** and click **OK**.

   e On the **Select hosts** page, click **Next**.

   f On the **Select network adapter tasks** page, ensure that **Manage physical adapters** and **Manage VMkernel adapters** check boxes are selected, and click **Next**.

   g On the **Manage physical network adapters** page, click **vmnic1** and click **Assign uplink**.

   h In the **Select an Uplink for vmnic1** dialog, select **dvUplink2** and click **OK**.

   i On the **Manage physical network adapters** page, click **Next**.

4 Configure the VMkernel network adapters, edit the existing, and add new adapters as needed.

   a On the **Manage VMkernel network adapters** page, click **vmk0** and click **Assign port group**.

   b Select **sfo02-m01-vds01-management** and click **OK**.

   c On the **Manage VMkernel network adapters** page, click **On this switch** and click **New adapter**.

   d On the **Add Networking** page, select **Select an existing network**, browse to select the **sfo02-m01-vds01-vsan** port group, click **OK**, and click **Next**.

   e On the **Port properties** page, select the **vSAN** check box and click **Next**.

   f On the **IPv4 settings** page, enter the following settings, click **Next** and click **Finish**.

Setting	Value
IP address	172.16.23.101
Subnet mask	255.255.255.0
Use static IPv4 settings	Selected

   g Repeat steps 4c. - 4f. to create the remaining VMkernel network adapters, and click **Next**.

Port Group	Port Properties	IPv4 Address	Subnet mask
sfo02-m01-vds01-replication	■ vSphere Replication ■ vSphere Replication NFC	172.16.26.101	255.255.255.0

   h On the **Analyze impact** page, click **Next**.

   i On the **Ready to complete** page, review your entries and click **Finish**.

5 Create the vSphere vMotion VMkernel adapter.

a In the **Navigator** pane, click **Host and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

b Select **sfo02m01esx01.sfo01.rainpole.local**, click the **Configure** tab and under **Networking** click **VMkernel adapters**.

c Click the **Add host networking** icon, select **VMkernel Network Adapter** and click **Next**.

d On the **Add Networking** page, click **Select an existing network**, browse to select the **sfo02-m01-vds01-vmotion** port group, click **OK**, and click **Next**.

e On the **Port properties** page, select **vMotion** from the **TCP/IP Stack** drop-down and click **Next**.

f On the **IPv4 settings** page, enter the following settings, click **Next** and click **Finish**..

Setting	Value
IP address	172.16.22.101
Subnet	255.255.255.0
Use static IPv4 settings	Selected

6 Configure the MTU on the vMotion VMkernel adapter.

a Select the vMotion VMkernel adapter you created in the previous step, and click **Edit Settings**.

b Click the **NIC Settings** page.

c Enter `9000` for the **MTU** value and click **OK**.

7 Configure the vMotion TCP/IP stack.

a Click **TCP/IP configuration**.

b Select **vMotion** and click the **Edit TCP/IP stack configuration** icon.

c Click **Routing** and enter `172.16.22.253` for the **VMkernel gateway** and click **OK**.

8 Migrate the last physical adapter from the standard switch to the sfo01-m01-vds01 distributed switch.

a In the **Navigator** pane, click **Networking** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

b Right-click the **sfo01-m01-vds01** distributed switch and select **Add and Manage Hosts**.

c On the **Select task** page, select **Manage host networking**, and click **Next**.

d On the **Select hosts** page, click **Attached hosts**.

e In the **Select member hosts** dialog, select **sfo02m01esx01.sfo01.rainpole.local**, click **OK** and click **Next**.

f On the **Select network adapter tasks** page, select only **Manage physical adapters**, and click **Next**.

g On the **Manage physical network adapters** page, select **vmnic0**, and click **Assign uplink**.

h In the **Select an Uplink for vmnic1** dialog box, select **dvUplink1**, click **OK**, and click **Next**.

i On the **Analyze Impact** page, click **Next** and click **Finish**.

9 Remove the default vSwitch0 standard switch.

a In the **Navigator** pane, click **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

b Select **sfo02m01esx01.sfo01.rainpole.local** and click the **Configure** tab.

c Under **Virtual switches**, select **vSwitch0**, and click the **Remove selected standard switch** icon.

d In the **Remove Standard Switch** dialog box, click **Yes** to confirm the removal.

Create vSAN Disk Groups for All Hosts in Availability Zone 2

Create vSAN disk groups on each ESXi host in Availability Zone 2 that is contributing storage to the vSAN datastore.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.

4 Under **vSAN**, click **Disk Management**.

5 Click **sfo02m01esx01.sfo01.rainpole.local** and click the **Create a New Disk Group** button.

6 In the **Create Disk Group** window, select a flash disk for the **cache tier**, two hard disk drives for the **capacity tier**, and click **OK**.

7 Repeat steps 5 and 6 for all remaining ESXi hosts in Availability Zone 2.

Setting	Value
Host 2	sfo02m01esx02.sfo01.rainpole.local
Host 3	sfo02m01esx03.sfo01.rainpole.local
Host 4	sfo02m01esx04.sfo01.rainpole.local

Add Static Routes for Both Availability Zones and the vSAN Witness Host

Configure static routes on the first ESXi hosts in Availability Zone 1 and Availability Zone 2, and the vSAN witness host to enable network communication for the vSAN kernel traffic.

Procedure

1 Configure static routes on the first ESXi host of Availability Zone 1 by using Secure Shell (SSH) client.

a Open an SSH connection to **`sfo01m01esx01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

c Add static route to Availability Zone 2 vSAN network by running the following command.

```
esxcli network ip route ipv4 add –n 172.16.23.0/24 –g 172.16.13.253
```

d Add static route to vSAN witness host witness network by running the following command.

```
esxcli network ip route ipv4 add –n 172.17.13.0/24 –g 172.16.13.253
```

2 Configure static routes on the first ESXi host of Availability Zone 2 by using Secure Shell (SSH) client.

a Open an SSH connection to **`sfo02m01esx01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

c Add static route to Availability Zone 1 vSAN network by running the following command.

```
esxcli network ip route ipv4 add –n 172.16.13.0/24 –g 172.16.23.253
```

d Add static route to vSAN witness host witness network by running the following command.

```
esxcli network ip route ipv4 add –n 172.17.13.0/24 –g 172.16.23.253
```

3 Configure static routes on the vSAN witness host by using Secure Shell (SSH) client.

a Open an SSH connection to **sfo03m01vsanw01.sfo01.rainpole.local**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vsan_witness_root_password*

c Add static route to Availability Zone 1 vSAN network by running the following command.

```
esxcli network ip route ipv4 add –n 172.16.13.0/24 –g 172.17.13.253
```

d Add static route to Availability Zone 2 vSAN network by running the following command.

```
esxcli network ip route ipv4 add –n 172.16.23.0/24 –g 172.17.13.253
```

Update the Host Profile in Availability Zone 1

The host profile of Availability Zone 1 must be updated to capture the static route configuration and then remediate the remaining ESXi hosts in Availability Zone 1.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Update the host profile from the sfo01m01esx01.sfo01.rainpole.local ESXi host.

a From the **Home** menu, select **Policies and Profiles**.

b In the **Navigator** pane, click **Host Profiles**.

c Right-click the **sfo01-m01hp-mgmt01** host profile and choose **Copy Settings from Host**.

d In the **Copy Settings from Host** dialog box, select the **sfo01m01esx01.sfo01.rainpole.local** host and click **OK**.

3 Remediate all the ESXi hosts in Availability Zone 1.

a From the **Home** menu, select **Policies and Profiles**.

b In the **Navigator** pane, click **Host Profiles**.

c Double-click the **sfo01-m01hp-mgmt01** host profile, click the **Monitor** tab, and click **Compliance**.

d Select the **sfo01m01esx01.sfo01.rainpole.local** host and click the **Check Host Profile Compliance** icon.

e Repeat this for all remaining ESXi hosts in Availability Zone 1.

Setting	Value
Host 2	sfo01m01esx02.sfo01.rainpole.local
Host 3	sfo01m01esx03.sfo01.rainpole.local
Host 4	sfo01m01esx04.sfo01.rainpole.local

This compliance test will show that sfo01m01esx01.sfo01.rainpole.local is `Compliant`, but the remaining hosts are `Not Compliant`

f Select each of the non-compliant hosts and click the **Remediate host based on its host profile** icon.

g In the **Remediate Hosts Based on its Host Profile** wizard, click **Next**, and click **Finish** on the **Ready to complete** page.

All hosts have `Compliant` status in the **Host Compliance** column.

Create and Apply the Host Profile for All Hosts in Availability Zone 2

Create a separate host profile to ensure all the ESXi hosts in Availability Zone 2 have the same configuration.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Create a host profile from the sfo02m01esx01.sfo01.rainpole.local ESXi host.

a From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

b Right-click **sfo02m01esx01.sfo01.rainpole.local** and select **Host Profiles > Extract Host Profile**.

c In the **Extract Host Profile** window, enter **sfo02-m01hp-mgmt01** as the **Name** of the host profile and click **Next**.

d On the **Ready to complete** page, click **Finish**.

3 Attach the host profile to all the ESXi hosts in Availability Zone 2.

a From the **Home** menu, select **Policies and Profiles**.

b In the **Navigator** pane, click **Host Profiles**.

c Right-click the **sfo02-m01hp-mgmt01** host profile and select **Attach/Detach Hosts and Clusters**.

d On the **Attach/Detach Hosts and Clusters** page, expand the **sfo01-m01-mgmt01** cluster, select all the ESXi hosts in Availability Zone 2 and click **Attach**.

Setting	Value
Host 1	sfo02m01esx01.sfo01.rainpole.local
Host 2	sfo02m01esx02.sfo01.rainpole.local
Host 3	sfo02m01esx03.sfo01.rainpole.local
Host 4	sfo02m01esx04.sfo01.rainpole.local

e Select **Skip Host Customization** and click **Finish**.

4 Create a host customization profile for the hosts in Availability Zone 2.

a From the **Home** menu, select **Policies and Profiles**.

b In the **Navigator** pane, click **Host Profiles**.

c Right-click the **sfo02-m01hp-mgmt01** host profile, select **Export Host Customizations** and click **Save**.

d Select a file location to save the `sfo02-m01hp-mgmt01_host_customizations.csv` file.

e Open the `sfo02-m01hp-mgmt01_host_customizations.csv` file in Excel.

f Edit the `csv` file to include the following values.

ESXi Host	Active Directory Configuration Password	Active Directory Configuration user name	NetStack Instance defaultTcpipStack->DNS configuration Name for this host	NetStack Instance vMotion->DNS configuration
sfo02m01esx01.sfo01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	sfo02m01esx01	sfo02m01esx01
sfo02m01esx02.sfo01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	sfo02m01esx02	sfo02m01esx02
sfo02m01esx03.sfo01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	sfo02m01esx03	sfo02m01esx03
sfo02m01esx04.sfo01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	sfo02m01esx04	sfo02m01esx04

ESXi Host	Host virtual NIC sfo01-m01-vds01:sfo02-m01-vds01-management:management->IP address settings Host IPv4 address	Host virtual NIC sfo01-m01-vds01:sfo02-m01-vds01-management:management->IP address settings SubnetMask
sfo02m01esx01.sfo01.rainpole.local	172.16.21.101	255.255.255.0
sfo02m01esx02.sfo01.rainpole.local	172.16.21.102	255.255.255.0
sfo02m01esx03.sfo01.rainpole.local	172.16.21.103	255.255.255.0
sfo02m01esx04.sfo01.rainpole.local	172.16.21.104	255.255.255.0

ESXi Host	Host virtual NIC sfo01-m01-vds01:sfo02-m01-vds01-replication:vSphereReplication,vSphereReplicationNFC->IP address settings Host IPv4 address	Host virtual NIC sfo01-m01-vds01: replication:vSphereReplication,vS ->IP address settings SubnetMask
sfo02m01esx01.sfo01.rainpole.local	172.16.26.101	255.255.255.0
sfo02m01esx01.sfo01.rainpole.local	172.16.26.102	255.255.255.0
sfo02m01esx01.sfo01.rainpole.local	172.16.26.103	255.255.255.0
sfo02m01esx04.sfo01.rainpole.local	172.16.26.104	255.255.255.0

ESXi Host	Host virtual NIC sfo01-m01-vds01:sfo02-m01-vds01-vsan:vsan->IP address settings Host IPv4 address	Host virtual NIC sfo01-m01-vds01:sfo02-m01-vds01-vsan:vsan->IP address settings SubnetMask
sfo02m01esx01.sfo01.rainpole.local	172.16.23.101	255.255.255.0
sfo02m01esx02.sfo01.rainpole.local	172.16.23.102	255.255.255.0
sfo02m01esx03.sfo01.rainpole.local	172.16.23.103	255.255.255.0
sfo02m01esx04.sfo01.rainpole.local	172.16.23.104	255.255.255.0

ESXi Host	Host virtual NIC sfo01-m01-vds01:sfo02-m01-vds01-vmotion:vmotion->IP address settings Host IPv4 address	Host virtual NIC sfo01-m01-vds01:sfo02-m01-vds01-vmotion:vmotion->IP address settings SubnetMask
sfo02m01esx01.sfo01.rainpole.local	172.16.22.101	255.255.255.0
sfo02m01esx02.sfo01.rainpole.local	172.16.22.102	255.255.255.0
sfo02m01esx03.sfo01.rainpole.local	172.16.22.103	255.255.255.0
sfo02m01esx04.sfo01.rainpole.local	172.16.22.104	255.255.255.0

g Save the file in the `csv` format and close Excel.

h Right-click **sfo02-m01hp-mgmt01** and select **Edit Host Customizations**.

i On the **Select hosts** page, select all hosts and click **Next**.

j On the **Customize hosts** page, click **Browse** to select the *sfo02-m01hp-mgmt01_host_customizations.csv* file, and click **Finish**.

5 Remediate all the ESXi hosts in Availability Zone 2.

a From the **Home** menu, select **Policies and Profiles**.

b In the **Navigator** pane, click **Host Profiles**.

c Double-click the **sfo02-m01hp-mgmt01** host profile, click the **Monitor** tab, and click **Compliance**.

d Select **sfo02m01esx01.sfo01.rainpole.local** in the **Host/Cluster** column and click **Check Host Profile Compliance**.

e Repeat this for all remaining ESXi hosts in Availability Zone 2.

Setting	Value
Host 2	sfo02m01esx02.sfo01.rainpole.local
Host 3	sfo02m01esx03.sfo01.rainpole.local
Host 4	sfo02m01esx04.sfo01.rainpole.local

This compliance test shows that sfo02m01esx01.sfo01.rainpole.local is `Compliant`, but the other hosts are `Not Compliant`.

f Select each of the non-compliant hosts, click **Remediate Hosts Based on its Host Profile**, and click **Finish** in the **Ready to complete** window.

All hosts now show a `Compliant` status in the **Host Compliance** column.

6 Schedule nightly compliance checks.

a From the **Home** menu, select **Policies and Profiles**.

b In the **Navigator** pane, click **Host Profiles**.

c Double-click **sfo02-m01hp-mgmt01**, click the **Monitor** tab, and click **Scheduled Tasks**.

d Click **Schedule a New Task** and click **Check Host Profile Compliance**.

e In the **Check Host Profile Compliance (scheduled)** dialog box, click **Scheduling Options**.

f Enter **`sfo02-m01hp-mgmt01 Compliance Check`** in the **Task Name** text box.

g Click the **Change** button on the **Configured Scheduler** line.

h In the **Configure Scheduler** dialog box, select **Setup a recurring schedule for this action**, select **Daily**, change the **Start time** to **`10:00 PM`**, and click **OK**.

i Click **OK** to save the task.

Configure vSAN Stretched Cluster for the Management Cluster in Region A

6

After you have prepared all the ESXi hosts and the network for multiple availability zones, configure the vSAN stretched cluster on the management cluster in Region A.

This chapter includes the following topics:

Enable and Configure vSAN Stretched Cluster in Region A

You must now enable vSAN stretched cluster on the management cluster in Region A.

Procedure

1. Log in to the Management vCenter Server by using the vSphere Web Client.
   a. Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.
   b. Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2. From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.
3. Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.
4. Under **vSAN**, click **Fault Domains & Stretched Cluster**, and click the **Configure** button.

5 On the **Configure fault domains** page, enter `Preferred` as the **Name** of **Preferred fault domain** and enter `Secondary` as the **Name** of **Secondary fault domain**.

6 Select all the ESXi hosts of Availability Zone 2, click the **Move** button to move them to **Secondary fault domain** and click **Next**.

Setting	Value
Host 1	sfo02m01esx01.sfo01.rainpole.local
Host 2	sfo02m01esx02.sfo01.rainpole.local
Host 3	sfo02m01esx03.sfo01.rainpole.local
Host 4	sfo02m01esx04.sfo01.rainpole.local

7 On the **Select witness host** page, expand **sfo01-m01dc**, select **sfo03m01vsanw01.sfo01.rainpole.local** and click **Next**.

8 On the **Claim disks for witness host** page, select the following disks for each tier, click **Next** and click **Finish**.

Setting	Value
Local VMware Disk (mpx.vmhba1:C0:T2:L0)	cache tier
Local VMware Disk (mpx.vmhba1:C0:T1:L0)	capacity tier

Update the vSphere High Availability Settings of the Management Cluster in Region A

Change the vSphere availability settings of the Region A management cluster to support high availability (HA) failover in case of an availability zone failure.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Select the **sfo01-m01-mgmt01** cluster, and click the **Configure** tab.

4 Under **Services**, click **vSphere Availability**, and click **Edit**.

5 On the **Admission Control** page of the **Edit Cluster Settings** dialog box, set **Host failures cluster tolerates** to **4** and click **OK**.

6 On the **Advanced Options** page, click the **Add** button, add the following options, and click **OK**.

Option	Value
das.isolationaddress0	172.16.13.253
das.isolationaddress1	172.16.23.253
das.usedefaultisolationaddress	false

Update the vSAN Default Storage Policy of the Management Cluster in Region A

To tolerate an availability zone failure, update the vSAN default storage policy for a secondary level of failures.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Select the **sfo01-m01-mgmt01** cluster, and click the **Configure** tab.

4 Under **vSAN**, click **Health and Performance**.

5 Under **Performance Service is Turned ON**, click **vSAN Default Storage Policy**.

6 Click the **Manage** tab, and click **Edit**.

7 In the **Edit VM Storage Policy** dialog box, click the **Rule-set 1** page, select **Secondary level of failures to tolerate** from the **<Add Rule>** drop-down menu, enter **1** for **Secondary level of failures to tolerate**, and click **OK**.

8 In the **VM Default Storage Policy: vSAN Storage Policy in Use** dialog box, select **Now** for the **Reapply to VMs** drop-down menu, click **Yes**, and wait for the reconfiguration of all the existing VMs to finish.

   Note Reconfiguration of the NSX Controller VMs and NSX Edge VMs fails. You must manually redeploy them.

Redeploy NSX Edges and NSX Controllers in the Management Cluster

To use the updated vSAN default storage policy that allows for tolerance of an availability zone failure you must re-deploy NSX Controller and NSX Edge virtual machines.

Redeploy All NSX Edge Devices

Re-deploy all the NSX Edge virtual machines to use the updated vSAN storage policy. That allows them to tolerate an availability zone failure.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Redeploy all the NSX Edge virtual machines in Region A management cluster.

   a From the **Home** menu, select **Networking & Security**.

   b In the **Navigator** pane, click **NSX Edges**.

   c Select **172.16.11.65** from the **NSX Manager** drop-down menu.

   d Select **sfo01m01esg01**, click **Redeploy NSX Edge** icon and click **Yes** in the **Redeploy Edge** warning box.

   Wait for the deployment of sfo01m01esg01 to complete.

   e Repeat this procedure to redeploy the following NSX Edge virtual machines.

NSX Edge
sfo01m01esg02
sfo01m01udlr01
sfo01m01lb01
sfo01psc01

3 Configure DRS ant-affinity rules for the NSX Edge services gateways.

a From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

b Select the **sfo01-m01-mgmt01** cluster, and click the **Configure** tab.

c Under **Configuration**, click **VM/Host Rules**, and click **Add**.

d In the **sfo01-m01-mgmt01 - Create VM/Host Rule** dialog box, enter the following settings and click **Add**.

Setting	Value
Name	anti-affinity-rule-ecmpedges-01
Enable rule	Selected
Type	Separate Virtual Machine

e In the **Add Rule Member** dialog box, select the check box next to **sfo01m01esg01-0** and **sfo01m01esg02-0**, and click **OK**.

f In the **sfo01-m01-mgmt01 - Create VM/Host Rule** dialog box, click **OK**.

Redeploy All NSX Controller Nodes

Redeploy all the NSX Controller virtual machines to use the updated vSAN storage policy. That allows them to tolerate an availability zone failure.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Redeploy all the NSX Controller nodes of Region A management cluster.

a From the **Home** menu, select **Networking & Security**.

b In the **Navigator** pane, click **Installation and Upgrade**.

c On the **Management** tab, under **NSX Managers**, select **172.16.11.65**.

d Under **NSX Controller nodes** tab, select **sfo01m01nsxc01**, **sfo01m01nsxc02**, and **sfo01m01nsxc03** and click the **Delete** icon.

e Under **NSX Controller nodes**, click the **Add** icon to redeploy three NSX Controller nodes with the same configuration.

f On the **Add Controller** page, under **Password Settings**, enter the following, and click **Next**.

Note You configure a password only during the deployment of the first controller. The other controllers use the same password.

Setting	Value
NSX Manager	172.16.11.65
Password	*nsx_controllers_password*
Confirm Password	*nsx_controllers_password*

g In the **Add Controller** page, under **Deployment & Connectivity**, enter the following values and click **`Finish`**.

Setting	Value
Name	sfo01m01nsxc01
Datacenter	sfo01-m01dc
Cluster/Resource Pool	sfo01-m01-mgmt01
Datastore	sfo01-m01-vsan01
Folder	sfo01-m01fd-nsx
Connected To	sfo01-m01-vds01-management
Select IP Pool	sfo01-mgmt01-nsxc01

h After the **Status** of the controller node changes to `Connected`, repeat the step to redeploy the remaining NSX Controller nodes using the same configuration.

Controller Name
sfo01m01nsxc02
sfo01m01nsxc03

Note To maintain the NSX availability during the redeployment of NSX Controller nodes, redeploy only one NSX Controller at a time.

3 Configure DRS anti-affinity rules for the NSX Controller nodes.

a From the **Home** menu, select **Hosts and Clusters**.

b In the **Navigator** pane, expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

c Select the **sfo01-m01-mgmt01** cluster, and click the **Configure** tab.

d Under **Configuration**, click **VM/Host Rules**, and click **Add**.

e In the **sfo01-m01-mgmt01 - Create VM/Host Rule** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	anti-affinity-rule-nsxc
Enable rule	Selected
Type	Separate Virtual Machine

f In the **Add Rule Member** dialog box, select the check box next to each of the three NSX Controller virtual machines and click **OK**.

g In the **sfo01-m01-mgmt01 - Create VM/Host Rule** dialog box, click **OK**.

Update Host Profiles to Capture the vSAN Stretched Cluster Configuration

Update the host profiles in both availability zones to capture the vSAN stretched cluster configuration changes.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Update the host profile in Availability Zone 1.

a From the **Home** menu, select **Policies and Profiles**.

b In the **Navigator** pane, click **Host Profiles**.

c Right-click the **sfo01-m01hp-mgmt01** host profile and select **Copy Settings from Host**.

d In the **Copy Settings from Host** dialog box, select the **sfo01m01esx01.sfo01.rainpole.local** host and click **OK**.

3 Check compliance for the ESXi hosts in Availability Zone 1.

a From the **Home** menu, select **Policies and Profiles**.

b In the **Navigator** pane, click **Host Profiles**.

c Double-click the **sfo01-m01hp-mgmt01** host profile, click the **Monitor** tab, and click **Compliance**.

d Select the **sfo01m01esx01.sfo01.rainpole.local** host and click the **Check Host Profile Compliance** icon.

e Repeat this for all remaining ESXi hosts in Availability Zone 1.

Setting	Value
Host 2	sfo01m01esx02.sfo01.rainpole.local
Host 3	sfo01m01esx03.sfo01.rainpole.local
Host 4	sfo01m01esx04.sfo01.rainpole.local

All hosts have `Compliant` status in the **Host Compliance** column.

4 Update the host profile in Availability Zone 2.

a From the **Home** menu, select **Policies and Profiles**.

b In the **Navigator** pane, click **Host Profiles**.

c Right-click the **sfo02-m01hp-mgmt01** host profile and select **Copy Settings from Host**.

d In the **Copy Settings from Host** dialog box, select the **sfo02m01esx01.sfo01.rainpole.local** host and click **OK**.

5 Check compliance for the ESXi hosts in Availability Zone 2.

a From the **Home** menu, select **Policies and Profiles**.

b In the **Navigator** pane, click **Host Profiles**.

c Double-click the **sfo02-m01hp-mgmt01** host profile, click the **Monitor** tab, and click the **Compliance** tab.

d Select the **sfo02m01esx01.sfo01.rainpole.local** host and click the **Check Host Profile Compliance** icon.

e Repeat this for all remaining ESXi hosts in Availability Zone 2.

Setting	Value
Host 2	sfo02m01esx02.sfo01.rainpole.local
Host 3	sfo02m01esx03.sfo01.rainpole.local
Host 4	sfo02m01esx04.sfo01.rainpole.local

All hosts have `Compliant` status in the **Host Compliance** column.

Add All NSX Edges and Controllers to the VM Group of Availability Zone 1

VM/Host groups and VM/Host rules are used to ensure all the virtual machines that are created in Availability Zone 1 run on ESXi hosts in the same zone.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.

4 Under **Configuration**, click **VM/Host Groups**.

5 Under **VM/Host Groups**, select **availability-zone-1-vms**.

6 Under **VM/Host Group Members**, click the **Add** button.

7 In the **Add Group Member** dialog box, select all the VMs that are running in Availability Zone 1, and click **OK**.

Configure NSX Dynamic Routing for Availability Zone 2 in Region A

7

Deploy two ECMP-enabled NSX Edge devices and enable North-South routing in Availability Zone 2.

This chapter includes the following topics:

Deploy NSX Edge Devices for North-South Routing in Availability Zone 2

Deploy two NSX Edge devices for North-South routing.

Perform this procedure two times to deploy two NSX Edge devices.

Table 7-1. NSX Edge Devices

NSX Edge Device	Device Name
NSX Edge device 1	sfo02m01esg01
NSX Edge device 2	sfo02m01esg02

Table 7-2. NSX Edge Interfaces Settings

Interface	Primary IP Address sfo02m01esg01	Primary IP Address sfo02m01esg02
Uplink01	172.16.50.2	172.16.50.3
Uplink02	172.16.51.3	172.16.51.2
sfo01m01udlr01	192.168.10.20	192.168.10.21

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Networking & Security**.

3 In the **Navigator** pane, click **NSX Edges**.

4 Select **172.16.11.65** from the **NSX Manager** drop-down menu.

5 Click the **Add** icon to deploy a new NSX Edge.

   The **New NSX Edge** wizard appears.

   a On the **Name and description** page, enter the following settings and click **Next**.

Settings	sfo02m01esg01	sfo02m01esg02
Install Type	Edge Service Gateway	Edge Service Gateway
Name	sfo02m01esg01	sfo02m01esg02
Hostname	sfo02m01esg01.sfo01.rainpole.local	sfo02m01esg02.sfo01.rainpole.local
Deploy NSX Edge	Selected	Selected
Enable High Availability	Deselected	Deselected
Logging	Deselected	Deselected

   b On the **Settings** page, enter the following settings and click **Next**.

Settings	Value
User Name	admin
Password	*edge_admin_password*
Confirm password	*edge_admin_password*
Enable SSH access	Selected
Enable FIPS mode	Deselected
Enable auto rule generation	Selected
Edge Control Level logging	INFO

   c On the **Configure deployment** page, select **Large** to specify the **Appliance Size** and click the **Add** icon.

d In the **Add NSX Edge Appliance** dialog box, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Cluster/Resource Pool	sfo01-m01-mgmt01
Datastore	sfo01-m01-vsan01
Folder	sfo01-m01fd-nsx
Resource Reservation	System Managed

e On the **Configure interfaces** page, click the **Add** icon to configure the Uplink01 interface, enter the following settings, and click **OK**.

Setting	sfo02m01esg01	sfo02m01esg02
Name	Uplink01	Uplink01
Type	Uplink	Uplink
Connected To	sfo02-m01-vds01-uplink01	sfo02-m01-vds01-uplink01
Connectivity Status	Connected	Connected
Primary IP Address	172.16.50.2	172.16.50.3
Subnet Prefix Length	24	24
MTU	9000	9000
Send ICMP Redirect	Selected	Selected

f Click the **Add** icon to configure the Uplink02 interface, enter the following settings, and click **OK**.

Setting	sfo02m01esg01	sfo02m01esg02
Name	Uplink02	Uplink02
Type	Uplink	Uplink
Connected To	sfo02-m01-vds01-uplink02	sfo02-m01-vds01-uplink02
Connectivity Status	Connected	Connected
Primary IP Address	172.16.51.3	172.16.51.2
Subnet Prefix Length	24	24
MTU	9000	9000
Send ICMP Redirect	Selected	Selected

g Click the **Add** icon to configure the UDLR interface, enter the following settings click **OK**, and click **Next**.

Setting	sfo02m01esg01	sfo02m01esg02
Name	sfo01m01udlr01	sfo01m01udlr01
Type	Internal	Internal
Connected To	Universal Transit Network	Universal Transit Network
Connectivity Status	Connected	Connected
Primary IP Address	192.168.10.20	192.168.10.21
Subnet Prefix Length	24	24
MTU	9000	9000
Send ICMP Redirect	Selected	Selected

h On the **Default gateway settings** page, deselect the **Configure Default Gateway** check box and click **Next**.

i On the **Firewall and HA** page, click **Next**.

j On the **Ready to complete** page, review the configuration settings and click **Finish**.

k Repeat the steps to configure the second NSX Edge using the settings for sfo02m01esg02.

6 Disable the firewall on both NSX Edge devices.

a Double-click the **sfo02m01esg01** NSX Edge device.

b Click the **Manage** tab, and click **Firewall**.

c Click the **Stop** button, and click **Publish Changes**.

d Repeat the steps for the **sfo02m01esg02** NSX Edge device.

7 Configure DRS affinity rules for the Edge services gateways.

a From the **Home** menu, select **Hosts and Clusters**.

b In the **Navigator** pane, expand the **sfo01m01vc01.sfo01.rainpole.local** tree and select the **sfo01-m01-mgmt01** cluster.

c Click the **Configure** tab and under **Configuration**, click **VM/Host Rules**.

d Click the **Add** button.

e In the **sfo01-m01-mgmt01 - Create VM/Host Rule** dialog box, enter the following settings and click the **Add** button.

Setting	Value
Name	anti-affinity-rule-ecmpedges-02
Enable rule	Selected
Type	Separate Virtual Machine

f In the **Add Rule Member** dialog box, select sfo02m01esg01 and sfo02m01esg02 and click **OK**.

g In the **sfo01-m01-mgmt01 - Create VM/Host Rule** dialog box, click **OK**.

Configure Routing for Availability Zone 2

You must enable and configure dynamic routing on both North-South NSX Edge services gateways and NSX Universal Logical Router to enable routing to Availability Zone 2.

Enable and Configure Routing on NSX Edge Services Gateways

Enable Border Gateway Protocol (BGP) to exchange routing information between the NSX Edge services gateways.

Repeat this procedure two times to enable BGP for both NSX Edge devices: sfo02m01esg01 and sfo02m01esg02.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Networking & Security**.

3 In the **Navigator** pane, click **NSX Edges**.

4 Select **172.16.11.65** from the **NSX Manager** drop-down menu.

5 Double-click the **sfo02m01esg01** NSX Edge device.

6 Click the **Manage** tab, and click **Routing**.

7 On the **Global Configuration** page, perform the following actions.

a Click **Start** for ECMP.

b Click **Edit** for **Dynamic Routing Configuration**.

c Select **Uplink01** as the **Router ID** and click **OK**.

d Click **Publish Changes**.

8 On the **Routing** tab, click **Static Routes**.

a Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Network	192.168.11.0/24
Next Hop	192.168.10.3
Interface	sfo01m01udlr01
Admin Distance	210

b Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Network	192.168.31.0/24
Next Hop	192.168.10.3
Interface	sfo01m01udlr01
Admin Distance	210

c Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Network	192.168.32.0/24
Next Hop	192.168.10.3
Interface	sfo01m01udlr01
Admin Distance	210

d Click **Publish Changes**.

9 On the **Routing** tab, click **BGP**.

a Click **Edit**, enter the following settings, and click **OK**.

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Deselected
Enable Default Originate	Deselected
Local AS	65003

b On the **BGP** page, click the **Add** icon to add a neighbor.

The **New Neighbor** dialog box appears. Add the first top-of-rack switch.

c In the **New Neighbor** dialog box, enter the following values and click **OK**.

Setting	Value
IP Address	172.16.50.1
Remote AS	65001
Remote Private AS	Selected
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	*BGP_password*

d Click the **Add** icon to add another neighbor.

The **New Neighbor** dialog box appears. Add the second Top of Rack switch.

e In the **New Neighbor** dialog box, enter the following values and click **OK**.

Setting	Value
IP Address	172.16.51.1
Remote AS	65001
Remote Private AS	Selected
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	*BGP_password*

f Click the **Add** icon to add another neighbor.

The **New Neighbor** dialog box appears. Configure the universal distributed logical router (UDLR) as a neighbor.

g In the **New Neighbor** dialog box, enter the following values, and click **OK**.

Setting	Value
IP Address	192.168.10.4
Remote AS	65003
Remote Private AS	Selected
Weight	40
Keep Alive Time	1
Hold Down Time	3
Password	*BGP_password*

h Click **Publish Changes**.

The three neighbors you added appear in the **Neighbors** table.

10 On the **Routing** tab, click **Route Redistribution**.

a On the **Route Redistribution** page, click the **Edit** button.

b In the **Change redistribution settings** dialog box, select the **BGP** check box and click **OK**.

c Click the **Add** icon for **Route Redistribution table**.

d In the **New Redistribution criteria** dialog box, enter the following settings and click **OK**.

Setting	Value
Prefix	Any
Learner Protocol	BGP
OSPF	Deselected
Static routes	Selected
Connected	Selected
Action	Permit

e Click **Publish Changes**.

The route redistribution configuration appears in the **Route Redistribution** table.

11 Repeat this procedure for the second NSX Edge device sfo02m01esg02.

Configure Dynamic Routing on Universal Distributed Logical Router

Configure the universal distributed logical router (UDLR) to establish BGP peering with both North-South NSX Edge services gateways.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Add the two NSX Edge gateways as BGP neighbors.

a From the **Home** menu, select **Networking & Security**.

b In the **Navigator** pane, click **NSX Edges**.

c Select **172.16.11.65** from the **NSX Manager** drop-down menu.

d Double-click the **sfo01m01udlr01** NSX Edge device.

e Click the **Manage** tab, click **Routing**, and click **BGP**.

f Click the **Add** icon to add a neighbor.

g In the **New Neighbor** dialog box, enter the following values for both NSX Edge devices and click **OK**.

Setting	sfo02m01esg01 Value	sfo02m01esg02 Value
IP Address	192.168.10.20	192.168.10.21
Forwarding Address	192.168.10.3	192.168.10.3
Protocol Address	192.168.10.4	192.168.10.4
Remote AS	65003	65003
Weight	40	40
Keep Alive Time	1	1
Hold Down Time	3	3
Password	*BGP_password*	*BGP_password*

h Click **Publish Changes**.

Verify Peering and Establishment of BGP for Availability Zone 2

The Universal Distributed Logical Router (UDLR) needs to establish a connection to NSX Edge services gateway before BGP updates can be exchanged. Verify that the North-South NSX Edges services gateway is successfully peering, and that BGP routing has been established.

Procedure

1 Log in to the UDLR by using a Secure Shell (SSH) client.

a Open an SSH connection to **`sfo02m01esg01`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*edge_admin_password*

2 Run the `show ip bgp neighbors` command to display information about the BGP and TCP connections to neighbors.

The BGP State displays `Established, UP` if you have successfully peered with the following routers.

Setting	Value
First Top of Rack Switch	172.16.50.1
Second Top of Rack Switch	172.16.51.1
sfo01m01udlr01	192.168.10.4

```
BGP neighbor is 172.16.50.1,   remote AS 65001,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
Neighbor capabilities:
         Route refresh: advertised and received
         Address family IPv4 Unicast:advertised and received
         Graceful restart Capability:advertised and received
                 Restart remain time: 0
Received 702489 messages, Sent 702413 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
         Index 1 Identifier 0x2951511c
         Route refresh request:received 0 sent 0
         Prefixes received 13 sent 6 advertised 6
Connections established 2, dropped 3
Local host: 172.16.50.2, Local port: 13273
Remote host: 172.16.50.1, Remote port: 179


BGP neighbor is 172.16.51.1,   remote AS 65001,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
Neighbor capabilities:
         Route refresh: advertised and received
         Address family IPv4 Unicast:advertised and received
         Graceful restart Capability:advertised and received
                 Restart remain time: 0
Received 702353 messages, Sent 702367 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
         Index 2 Identifier 0x2951511c
         Route refresh request:received 0 sent 0
         Prefixes received 13 sent 6 advertised 6
Connections established 4, dropped 8
Local host: 172.16.51.3, Local port: 179
Remote host: 172.16.51.1, Remote port: 61483
```

3 Run the `show ip route` command to verify that you are receiving routes using BGP, and that multiple routes to BGP learned networks exist.

   You verify multiple routes to BGP learned networks by locating the same route using a different IP address. The IP addresses are listed after the word `via` in the right-side column of the routing table output. In the image below there are two different routes to the following BGP networks: 0.0.0.0/0, 172.16.11.0/24, 172.16.21.0/24, and 172.16.31.0/24. You can identify BGP networks by the letter `B` in the left-side column. Lines beginning with `C` (connected) have only a single route.

```
NSX-edge-5-0> show ip route

Codes: O - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 18

B       0.0.0.0/0           [20/0]        via 172.16.50.1
B       0.0.0.0/0           [20/0]        via 172.16.51.1
B       172.16.11.0/24      [20/0]        via 172.16.50.1
B       172.16.11.0/24      [20/0]        via 172.16.51.1
B       172.16.21.0/24      [20/0]        via 172.16.50.1
B       172.16.21.0/24      [20/0]        via 172.16.51.1
B       172.16.31.0/24      [20/0]        via 172.16.50.1
B       172.16.31.0/24      [20/0]        via 172.16.51.1
```

4 Repeat this procedure to verify routing on the sfo02m01esg02 NSX Edge services gateway.

Create Host Groups and Rules for Availability Zone 2

Ensure that all the virtual machines that are created in Availability Zone 2 run on ESXi hosts in the same zone by creating a rule.

Procedure

1 Log in to the Management vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.

4 Create a host group containing all ESXi hosts of Availability Zone 2.

   a Under **Configuration**, click **VM/Host Groups**.

   b On the **VM/Host Groups** page, click the **Add** button.

   c In the **Create VM/Host Group** dialog box, enter **`availability-zone-2-hosts`** in the **Name** field, select **Host Group** from the **Type** drop-down menu, and click the **Add** button.

d In the **Add VM/Host Group Member** dialog box, select all the ESXi hosts of Availability Zone 2 and click **OK**.

Setting	Value
Host 1	sfo02m01esx01.sfo01.rainpole.local
Host 2	sfo02m01esx02.sfo01.rainpole.local
Host 3	sfo02m01esx03.sfo01.rainpole.local
Host 4	sfo02m01esx04.sfo01.rainpole.local

e Click **OK** to create the host group.

5 Create a VM Group containing all virtual machines of Availability Zone 2.

a Under **Configuration**, click **VM/Host Groups**.

b On the **VM/Host Groups** page, click the **Add** button.

c In the **Create VM/Host Group** dialog box, enter **`availability-zone-2-vms`** in the **Name** field, select **VM Group** from the **Type** drop-down menu, and click the **Add** button.

d In the **Add VM/Host Group Member** dialog box, select all VMs in Availability Zone 2 **sfo02m01esg01-01** and **sfo02m01esg02-01**, click **OK**.

e Click **OK** to create the VM group.

6 Create a rule to run virtual machines of Availability Zone 2 on hosts in the same zone.

a Under **Configuration**, click **VM/Host Rules**.

b On the **VM/Host Rules** page, click the **Add** button.

c In the **Create VM/Host Rule** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	hostgroup-availability-zone-2
Enable rule	Selected
Type	Virtual Machines to Hosts
VM Group	availability-zone-2-vms
	Should run on hosts in group
Host Group	availability-zone-2-hosts

Configure vSphere Replication Network Traffic for Availability Zone 2 in Region A

8

To avoid replication problems when the protected VMs fail over to hosts in Availability Zone 2 if there is Availability Zone 1 failure, add a third adapter to the vSphere Replication appliance in Region A.

You configure replication traffic for Availability Zone 2 by adding static routes on both vSphere Replication appliances and ESXi hosts in Availability Zone 2 and Region B.

Setting	Values for the Management Cluster in Region A	Values for the Management Cluster in Region B
vCenter Server URL	https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client/	https://lax01m01vc01.lax01.rainpole.local/vsphere-client/
Host profile	sfo02-m01hp-mgmt01	lax01-m01hp-mgmt01
Template ESXi host	sfo02m01esx01.sfo01.rainpole.local	lax01m01esx01.lax01.rainpole.local
Filter value	172.16.26.253	172.17.16.253
IP Next Hop	172.16.26.253	172.17.16.253
Destination network address	172.17.16.0	172.16.26.0
Device name	vmk2	vmk2
Host/Cluster	sfo02-m01-mgmt01	lax01-m01-mgmt01

Procedure

1 Log in to vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Shut down the vSphere Replication virtual appliance to allow for changes in the hardware configuration.

   a From the **Home** menu, select **Hosts and Clusters**.

   b In the **Navigator** pane, expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

   c Right-click the **sfo01m01vrms01** virtual appliance and select **Power > Shut Down Guest OS**.

   d In the **Confirm Guest Shut Down** dialog box, click **Yes**.

3 Add a VM network adapter to the vSphere Replication virtual appliance for replication traffic.

   a Right-click the **sfo01m01vrms01** virtual appliance and select **Edit Settings**.

   b In the **sfo01m01vrms01 - Edit Settings** dialog box, from the **New device** drop-down menu, select **Network**, and click**Add**.

   c From the **New Network** drop-down menu, select **sfo02-m01-vds01-replication** and click **OK**.

   d Right-click the **sfo01m01vrms01** virtual appliance and select **Power > Power On**.

   e In the **Confirm Power On** dialog box, click **Yes** and wait until the appliance is up and running.

4 Log in to the Virtual Appliance Management Interface of the vSphere Replication appliance.

   a Open a Web browser and go to `https://sfo01m01vrms01.sfo01.rainpole.local:5480`.

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vr_sfo_root_password*

5 Configure the network settings of the new network adapter `eth2`.

   a Click the **Network** tab and click **Address**.

   b Under the **eth2 info** section, enter the following settings and click **Save Settings**.

Setting	Value
IPv4 Address Type	Static
IPv4 Address	172.16.26.71
Netmask	255.255.255.0
IPv6 Address Type	Auto

6 Log in to vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

7 On the vSphere Replication appliances, add static network routes to the hosts in the other region.

VM Name	Appliance Host Name	Source Gateway	Target Network
sfo01m01vrms01	sfo01m01vrms01.sfo01.rainpole.local	172.16.26.253	172.17.16.0/24
lax01m01vrms01	lax01m01vrms01.lax01.rainpole.local	172.17.16.253	172.16.26.0/24

a From the **Home** menu, select **Hosts and Clusters**.

b In the **Navigator**, expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

c Right-click the **sfo01m01vrms01** virtual appliance and select **Open Console** to open the console to the appliance.

d To switch to the command prompt press ALT+F2.

e Log in using the following credentials.

Setting	Value
User name	root
Password	*vr_root_password*

f Open the`/etc/sysconfig/network/routes` file using `vi` editor.

```
vi /etc/sysconfig/network/routes
```

g To create a route to the recovery region for the hosts in Region A or to the protected region for the hosts in Region B, add the following line after the default gateway, and save the file.

Region of the vSphere Replication Appliance	Value
Region A	172.17.16.0/24 172.16.26.253 dev eth2
Region B	172.16.26.0/24 172.17.16.253 dev eth1

h Run the `service network restart` command.

i To verify the routing table, run the `route –n` command.

j Repeat the step on the **lax01m01vrms01** vSphere Replication appliance in the lax01-m01-mgmt01 cluster in Region B.

8 Add static network routes on the ESXi hosts in the management clusters in all regions.

Region	Host Name	Source Gateway	Target Network
Region A	sfo02m01esx01.sfo01.rainpole.local	172.16.26.253	172.17.16.0/24
Region B	lax01m01esx01.lax01.rainpole.local	172.17.16.253	172.16.26.0/24

a For each management host, open an SSH connection to the ESXi Shell and log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

b To create a route to the recovery region for the hosts in Region A or to the protected region for the hosts in Region B, run the following commands.

Region of the ESXi Host	Command
Region A	esxcli network ip route ipv4 add --gateway 172.16.26.253 --network 172.17.16.0/24
Region B	esxcli network ip route ipv4 add --gateway 172.17.16.253 --network 172.16.26.0/24

c Verify the routing table by running the following command.

```
esxcli network ip route ipv4 list
```

d Repeat the step on the lax01m01esx01.lax01.rainpole.local host in the lax01-m01-mgmt01 cluster in Region B.

9 Log in to vCenter Server by using the vSphere Web Client.

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

10 Update the host profile of the management cluster.

a From the **Home** menu, select **Policies and Profiles**.

b In the **Navigator** pane, click **Host Profiles**.

c Right-click **sfo02-m01hp-mgmt01** and select **Copy Settings from Host**.

d Select **sfo02m01esx01.sfo01.rainpole.local** and click **OK**.

11 Verify that the static route settings have been updated in the host profile.

a On the **Host Profiles** page, double-click **sfo02-m01hp-mgmt01** and click the **Configure** tab.

b In the **Filter** search box, enter **`172.16.26.253`**.

Under **Networking configuration > NetStack Instance > defaultTcpipStack > IP route configuration > IP route config**, locate the profile property.

c Select the **IP route config** entry from the list and verify the following values.

Settings	Value
IP Next Hop	172.16.26.253
Destination Network address	172.17.16.0
Device name	vmk2

12 Check compliance and remediate the remaining management hosts in Region A.

a From the **Home** menu, select **Policies and Profiles**.

b In the Navigator pane, click **Host Profiles**

c Double-click the **sfo02-m01hp-mgmt01** host profile, click the **Monitor** tab, and click **Compliance**.

d Select the **sfo02m01esx01.sfo01.rainpole.local** host and click the **Check Host Profile Compliance** icon.

e Repeat this step for all remaining ESXi hosts in Availability Zone 2.

Setting	Value
Host 2	sfo02m01esx02.sfo01.rainpole.local
Host 3	sfo02m01esx03.sfo01.rainpole.local
Host 4	sfo02m01esx04.sfo01.rainpole.local

This compliance test shows that sfo02m01esx01.sfo01.rainpole.local is `Compliant`, but the remaining hosts are `Not Compliant.`

f Select each of the non-compliant hosts and click the **Remediate host based on its host profile** icon.

g In the **Remediate Hosts Based on its Host Profile** wizard, click **Next**, and click **Finish** on the **Ready to complete** page.

All hosts have `Compliant` status in the **Host Compliance** column.

13 Repeat steps 9-12 for the management cluster in Region B.