Deployment for Region B

13 FEB 2018

VMware Validated Design 4.2

VMware Validated Design for Software-Defined Data Center 4.2

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 Region B

1

VMware Validated Design Deployment for Region B provides step-by-step instructions for installing, configuring, and operating a software-defined data center (SDDC) based on the VMware Validated Design for Software-Defined Data Center.

VMware Validated Design Deployment for Region B does not contain step-by-step instructions for performing all of the required post-configuration tasks because they often depend on customer requirements.

Intended Audience

The *VMware Validated Design Deployment for Region B* 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 Deployment for Region B is compliant and validated with certain product versions. See *VMware Validated Design Release Notes* for more information about supported product versions.

Region B Virtual Infrastructure Implementation 2

The virtual infrastructure is the foundation of an operational SDDC, and consists primarily of the physical host's hypervisor and the control of these hypervisors. The management workloads consist of elements in the virtual management layer itself, along with elements in the Cloud Management Layer, Service Management, Business Continuity, and Security areas.

The following procedures describe the validated flow of installation and configuration for the Virtual Infrastructure in Region B.

Procedure

1 Install and Configure ESXi Hosts in Region B

   Start the deployment of your virtual infrastructure in Region B by installing and configuring all the ESXi hosts.

2 Deploy and Configure the Platform Services Controller and vCenter Server Components in Region B

   Deploy and configure the cluster components for both the management cluster and the shared edge and compute cluster.

3 Deploy and Configure the Management Cluster NSX Instance in Region B

   This design uses two separate NSX instances per region. One instance is tied to the Management vCenter Server, and the other instance is tied to the Compute vCenter Server. Deploy and configure the NSX instance for the management cluster in Region B.

4 Deploy and Configure the Shared Edge and Compute Cluster Components Region B

   Deploy and configure the shared edge and compute cluster components.

5 Deploy and Configure the Shared Edge and Compute Cluster NSX Instance in Region B

   Deploy and configure the NSX instance for the shared edge and compute cluster in Region B.

Install and Configure ESXi Hosts in Region B

Start the deployment of your virtual infrastructure in Region B by installing and configuring all the ESXi hosts.

Procedure

1. Prerequisites for Installation of ESXi Hosts for Region B

   Install and configure the ESXi hosts for the management cluster and the shared edge and compute cluster by using the same process.

2. Install ESXi Interactively on All Hosts in Region B

   Install all ESXi hosts for all clusters interactively.

3. Configure the Network on All Hosts in Region B

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

4. Configure vSphere Standard Switch on a Host in the Management Cluster in Region B

   You must perform network configuration from the VMware Host Client for one host in each cluster. You perform all other host networking configuration after the deployment of the vCenter Server system that manages the hosts.

5. Configure SSH and NTP on the First Host in Region B

   Time synchronization issues can result in serious problems with your environment. Configure NTP and SSH on the first host. NTP and SSH configuration for the remaining hosts will take place after the installation of vCenter Server.

Prerequisites for Installation of ESXi Hosts for Region B

Install and configure the ESXi hosts for the management cluster and the shared edge and compute cluster by using the same process.

Before you start:

- Make sure that you have a Windows host that has access to your data center in Region B. You use this host to connect to your hosts and perform configuration steps.
- Ensure that routing is in place between the two regional management networks 172.16.11.0/24 and 172.17.11.0/24 as this is necessary to join the common SSO domain.

You must also prepare the installation files.

- 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 *vSphere Installation and Setup*.

IP Addresses, Hostnames, and Network Configuration

The following tables contain all the values needed to configure your ESXi hosts.

Table 2-1. Management Cluster Hosts in Region B

FQDN	IP	Management VLAN	Default Gateway	NTP Server
lax01m01esx01.lax01.rainpole.local	172.17.11.101	1711	172.17.11.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
lax01m01esx02.lax01.rainpole.local	172.17.11.102	1711	172.17.11.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
lax01m01esx03.lax01.rainpole.local	172.17.11.103	1711	172.17.11.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
lax01m01esx04.lax01.rainpole.local	172.17.11.104	1711	172.17.11.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local

Table 2-2. Shared Edge and Compute Cluster Hosts in Region B

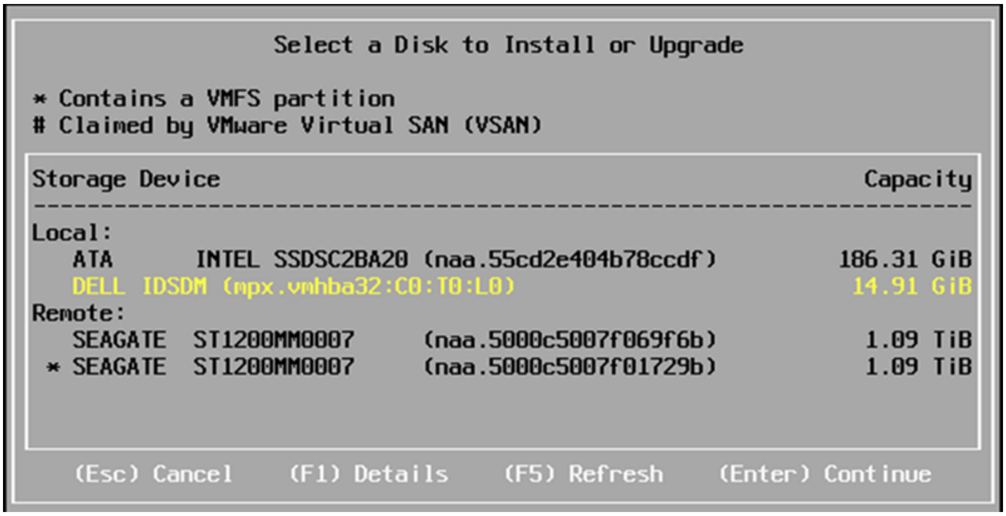
FQDN	IP	Management VLAN	Default Gateway	NTP Server
lax01w01esx01.lax01.rainpole.local	172.17.31.101	1731	172.17.31.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
lax01w01esx02.lax01.rainpole.local	172.17.31.102	1731	172.17.31.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
lax01w01esx03.lax01.rainpole.local	172.17.31.103	1731	172.17.31.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
lax01w01esx04.lax01.rainpole.local	172.17.31.104	1731	172.17.31.253	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local

Install ESXi Interactively on All Hosts in Region B

Install all ESXi hosts for all clusters interactively.

Procedure

1. Power on the `lax01m01esx01` host in Region B.
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.



```
                    Select a Disk to Install or Upgrade

* Contains a VMFS partition
# Claimed by VMware Virtual SAN (VSAN)

Storage Device                                                    Capacity
--------------------------------------------------------------------------
Local:
   ATA       INTEL SSDSC2BA20 (naa.55cd2e404b78ccdf)             186.31 GiB
   DELL IDSDM (mpx.vmhba32:C0:T0:L0)                              14.91 GiB
Remote:
   SEAGATE  ST1200MM0007     (naa.5000c5007f069f6b)                1.09 TiB
 * SEAGATE  ST1200MM0007     (naa.5000c5007f01729b)                1.09 TiB


    (Esc) Cancel     (F1) Details     (F5) Refresh     (Enter) Continue
```

6 Select the keyboard layout, and press Enter.

7 Enter the ***esxi_root_user_password***, enter the password a second time to confirm the spelling, and press Enter.

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

9 After the installation completes 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 the Network on All Hosts in Region B

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 host FQDN for the ESXi host.

Repeat this procedure for all hosts in the management and shared edge and compute pods. Enter the respective values from the prerequisites section for each host that you configure. See Prerequisites for Installation of ESXi Hosts for Region B.

Procedure

1. Open the DCUI on the physical ESXi host `lax01m01esx01`.

   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	***`esxi_root_user_password`***

2. Configure the network.

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

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

   c. Enter **1711** as the VLAN ID for the Management Network, and press Enter.

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

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

Setting	Value
Set static IPv4 address and network configuration	Selected
IPv4 Address	172.17.11.101
Subnet Mask	255.255.255.0
Default Gateway	172.17.11.253

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

   g. Configure the DNS using the following 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	lax01m01esx01.lax01.rainpole.local

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

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

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

4. Repeat this procedure for all hosts in the management and shared edge and compute pods.

Configure vSphere Standard Switch on a Host in the Management Cluster in Region B

You must perform network configuration from the VMware Host Client for one host in each cluster. You perform all other host networking configuration after the deployment of the vCenter Server system that manages the hosts.

You configure a vSphere Standard Switch with two port groups:

- The existing virtual machine port group.
- VMkernel port group.

This configuration provides connectivity and common network configuration for virtual machines that reside on each host.

Procedure

1 Log in to the vSphere host using the VMware Host Client.

  a Open a Web browser and go to `https://lax01m01esx01.lax01.rainpole.local`.

  b Log in using the following credentials.

Options	Description
User name	root
Password	*esxi_root_user_password*

2 Click **OK** to Join the Customer Experience Improvement Program.

3 Configure a VLAN for the VM Network Portgroup.

  a In the Navigator, click **Networking**, click the **Port Groups** tab, select the VM Network port group, and click **Edit Settings**.

  b On the Edit port group - VM Network window, enter **1711** for **VLAN ID**, and click **OK**.

Configure SSH and NTP on the First Host in Region B

Time synchronization issues can result in serious problems with your environment. Configure NTP and SSH on the first host. NTP and SSH configuration for the remaining hosts will take place after the installation of vCenter Server.

Procedure

1. Log in to the vSphere host using the VMware Host Client.

   a. Open a Web browser and go to **`https://lax01m01esx01.lax01.rainpole.local`**.

   b. Log in using the following credentials.

Options	Description
User name	root
Password	*esxi_root_user_password*

2. Configure SSH.

   a. In the Navigator, click **Manage**, click the **Services** tab, select the **TSM-SSH** service, and click the **Actions** menu. Select **Policy** and click **Start and stop with host**.

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

3. Configure the NTP Daemon (ntpd).

   a. In the Navigator, 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, change the NTP service startup policy to **Start and stop with host**, and enter **`ntp.lax01.rainpole.local,ntp.sfo01.rainpole.local`** as NTP servers.

   c. Click **Save** to save these changes.

   d. Start the service by clicking **Actions**, hover over **NTP service**, and select **Start**.

Deploy and Configure the Platform Services Controller and vCenter Server Components in Region B

Deploy and configure the cluster components for both the management cluster and the shared edge and compute cluster.

Procedure

1. Deploy the External Platform Services Controllers for the vCenter Server Instances in Region B

   Two external Platform Services Controller instances must be deployed in Region B. The first instance is associated with the management cluster and the second with the shared edge and compute cluster. Both instances belong to the same SSO domain for Identity Management. Work through this procedure twice, using the vCenter Server appliance ISO file and the customized data for each instance.

2. Join the Platform Services Controller Instances to Active Directory in Region B

   After you have successfully installed the Platform Services Controller instances, you must add the appliances to your Active Directory domain. The identity sources configured for the vSphere Domain automatically propagate to Region B. Users can then be assigned permissions to view or manage SDDC components for this region.

3 Replace the Platform Services Controller Certificates in Region B

To establish trusted connection with the other SDDC management components, you replace the machine SSL certificate on each Platform Services Controller instance in Region B with a custom certificate that is signed by the certificate authority (CA) available on the parent Active Directory (AD) server or on the intermediate Active Directory (AD) server.

4 Update the Platform Services Controller SSO Configuration and Endpoints in Region B

Before installing vCenter Server the Platform Services Controller endpoints must be updated to reflect the name of the load balancer's virtual IP.

5 Deploy the Management vCenter Server Instance in Region B

You can now install the vCenter Server appliance for the management applications and configure licensing and security.

6 Replace the Certificate of the Management vCenter Server in Region B

To establish trusted connection with the other SDDC management components, you replace the machine SSL certificate on each vCenter Server instance in Region B with a custom certificate that is signed by the certificate authority (CA) available on the parent Active Directory (AD) server or on the intermediate Active Directory (AD) server.

7 Set SDDC Deployment Details on the Management vCenter Server in Region B

Set an identity of your SDDC deployment on the Management vCenter Server in Region B. You can also use this identity as a label in tools for automated SDDC deployment.

8 Configure the Management Cluster in Region B

You must now create and configure the management cluster.

9 Create a vSphere Distributed Switch for the Management Cluster in Region B

After adding all ESXi hosts to the cluster, you create a vSphere Distributed Switch. You must also create port groups to prepare your environment to migrate the Platform Services Controller and vCenter Server instances to the distributed switch.

10 Create vSAN Disk Groups for the Management Cluster in Region B

vSAN disk groups must be created on each host that is contributing storage to the vSAN datastore.

11 Enable vSphere HA on the Management Cluster in Region B

Before creating the host profile for the management cluster enable vSphere HA.

12 Change Advanced Options on the ESXi Hosts in the Management Cluster in Region B

Change the default ESX Admins group to achieve greater levels of security and enable vSAN to provision the Virtual Machine Swap files as thin to conserve space in the vSAN datastore.

13 Mount NFS Storage for the Management Cluster in Region B

You must mount an NFS datastore where vSphere Data Protection is later deployed.

14 Create and Apply the Host Profile for the Management Cluster in Region B

Host Profiles ensure all hosts in the cluster have the same configuration.

15 Set Virtual SAN Policy on Management Virtual Machines in Region B

After you apply the host profile to all hosts, set the storage policy of the management virtual machines to the default Virtual SAN storage policy. Set the Platform Services Controller and vCenter Server appliances to the default vSAN storage policy.

16 Create the VM and Template Folders in Region B

Create folders to group objects of the same type for easier management.

17 Create Anti-Affinity Rules for the Platform Services Controllers in Region B

Anti-Affinity rules prevent virtual machines from running on the same host. This helps to maintain redundancy in the event of host failures.

18 Create VM Groups to Define Startup Order in the Management Cluster in Region B

VM Groups allow you to define the startup order of virtual machines. Startup orders are used during vSphere HA events such that vSphere HA powers on virtual machines in the correct order.

Deploy the External Platform Services Controllers for the vCenter Server Instances in Region B

Two external Platform Services Controller instances must be deployed in Region B. The first instance is associated with the management cluster and the second with the shared edge and compute cluster. Both instances belong to the same SSO domain for Identity Management. Work through this procedure twice, using the vCenter Server appliance ISO file and the customized data for each instance.

Repeat this procedure for each platform services controller, using the respective values for each indicated in the procedure steps.

Procedure

1 Log in to the Windows host that has access to your data center as an administrator.

2 Start the **vCenter Server Appliance Installer** wizard.

   a Browse the vCenter Server Appliance ISO file.

   b Open the `<dvd-drive>:\vcsa-ui-installer\win32\Installer.exe` application file.

3 Complete Stage 1 of the **vCenter Server Appliance Installer** wizard.

   a Click **Install** to start the installation.

   b Click **Next** on the **Introduction** page.

   c On the **End User License Agreement** page, select the **I accept the terms of the license agreement** check box, and click **Next**.

   d On the **Select deployment type** page, click **Platform Services Controller** and click **Next**.

e On the **Appliance deployment target** page, enter the following settings and click **Next**.

Setting	Value
FQDN or IP Address	lax01m01esx01.lax01.rainpole.local
HTTPS port	443
User name	root
Password	*esxi_root_user_password*

f In the **Certificate Warning** dialog box, click **Yes** to accept the host certificate.

g On the **Set up appliance VM** page, enter the following settings, and click **Next**.

Setting	Management Value	Edge/Compute Value
VM name	lax01m01psc01	lax01w01psc01
Root password	*mgmtpsc_root_password*	*comppsc_root_password*
Confirm root password	*mgmtpsc_root_password*	*comppsc_root_password*

h On the **Select datastore** page, select **Install on a new Virtual SAN datastore on the target host**, and click **Next**.

Note This step is performed only once for the first deployment. During the second PSC deployment, choose the existing vSAN datastore.

i Confirm at least one **Cache tier** and two **Capacity tier** disks have been claimed, select **Enable Thin Disk Mode**, and click **Next**.

j On the **Configure network settings** page, enter the following settings, and click **Next**.

Setting	Management Value	Edge/Compute Value
Network	VM Network	VM Network
IP version	IPv4	IPv4
IP assignment	static	static
System name	lax01m01psc01.lax01.rainpole.local	lax01w01psc01.lax01.rainpole.local
IP address	172.17.11.61	172.17.11.63
Subnet mask or prefix length	255.255.255.0	255.255.255.0
Default gateway	172.17.11.253	172.17.11.253
DNS servers	172.17.11.5,172.17.11.4	172.17.11.5,172.17.11.4

k On the **Ready to complete stage 1** page, review the configuration and click **Finish** to start the deployment.

l When the deployment completes, click **Continue** to proceed to second stage of the installation, setting up the Platform Services Controller Appliance.

4 Complete Stage 2 of the **Set Up Platform Services Controller Appliance** wizard.

   a Click **Next** on the **Introduction** page.

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

Setting	Value
Time synchronization mode	Synchronize time with NTP servers
NTP servers (comma-separated list)	ntp.lax01.rainpole.local
SSH access	Enabled

   c On the **SSO configuration** page, enter the following settings, and click **Next**.

Setting	Management Value	Edge/Compute Value
SSO configuration	Join an existing SSO domain	Join an existing SSO domain
Platform Services Controller	sfo01m01psc01.sfo01.rainpole.local	lax01m01psc01.lax01.rainpole.local
HTTPS port	443	443
SSO domain name	vsphere.local	vsphere.local
SSO password	*sso_password*	*sso_password*

   d On the **SSO Site Name** page, enter the following settings, and click **Next**.

Setting	lax01m01psc01	lax01w01psc01
SSO Site Creation	Create a new site	Join an existing site
Site name	LAX01	LAX01

   e On the **Configure CEIP** page, verify that the **Join the VMware's Customer Experience Improvement Program (CEIP)** check box is checked and click **Next**

   f On the **Ready to complete** page, review the configuration and click **Finish** to complete the setup.

   g Click **OK** on the **Warning**.

5 Repeat this procedure for each Platform Services Controller, using the respective values for each.

6 Create replication agreement between the Platform Services Controllers for the compute clusters in the regions.

   a Open an SSH connection to the virtual appliance by using the following settings.

Setting	Value
SSH Server	sfo01w01psc01.sfo01.rainpole.local
User name	root
Password	*mgmtpsc_root_password*

   b Execute the following commands to enable BASH access, and launch BASH.

   ```
   shell.set --enabled True
   shell
   ```

   c Create a new replication agreement between the Platform Services Controllers for the compute clusters.

   Note You execute this command in Region B only. The command uses the credentials of the administrator@vsphere.local account.

   ```
   /usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement -2 -h
   sfo01w01psc01.sfo01.rainpole.local -u Administrator -w vcenter_admin_password -H
   lax01w01psc01.lax01.rainpole.local
   ```

Join the Platform Services Controller Instances to Active Directory in Region B

After you have successfully installed the Platform Services Controller instances, you must add the appliances to your Active Directory domain. The identity sources configured for the vSphere Domain automatically propagate to Region B. Users can then be assigned permissions to view or manage SDDC components for this region.

Repeat this procedure twice, once for the management cluster and again for the shared edge and compute cluster.

Platform Services Controller	URL
Platform Services Controller for the management cluster	https://lax01m01psc01.lax01.rainpole.local
Platform Services Controller for the shared edge and compute cluster	https://lax01w01psc01.lax01.rainpole.local

Procedure

1 Log in to the administration interface of the Platform Services Controller.

   a Open a Web browser and go to `https://lax01m01psc01.lax01.rainpole.local`.

   b Click the link for **Platform Services Controller web interface**.

   c Log in using the following credentials.

Options	Description
User name	Administrator@vsphere.local
Password	*vsphere_admin_password*

2 Add the management Platform Services Controller instance to the Active Directory domain.

   a In the **Navigator**, click **Appliance Settings**, click the **Manage** tab, and click **Join**.

   b In the **Join Active Directory Domain** dialog box, enter the following settings and click **OK**.

Setting	Value
Domain	lax01.rainpole.local
User name	svc-domain-join@rainpole.local
Password	*svc-domain-join_password*

3 Reboot the Platform Services Controller instance to apply the changes.

   a Click the **Appliance settings** tab, and click the **VMware Platform Services Appliance** link.

   b Log in to the VMware vCenter Server Appliance administration interface with the following credentials.

Setting	Value
User name	root
Password	*psc_root_password*

   c On the **Summary** page, click **Reboot**.

   d In the **System Reboot** dialog box, click **Yes**.

   e Wait for the reboot process to complete.

4 Log in to `https://lax01m01psc01.lax01.rainpole.local/` again using the following credentials.

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

5 Verify that the Platform Services Controller has successfully joined the domain, click **Appliance Settings**, and click the **Manage** tab.

6 In the **Navigator**, click **Configuration**, and click the **Identity Sources** tab.

Verify that the `rainpole.local` domain is available as an Identity Source.

7 Repeat this procedure for the Platform Services Controller of the shared edge and compute cluster.

Replace the Platform Services Controller Certificates in Region B

To establish trusted connection with the other SDDC management components, you replace the machine SSL certificate on each Platform Services Controller instance in Region B with a custom certificate that is signed by the certificate authority (CA) available on the parent Active Directory (AD) server or on the intermediate Active Directory (AD) server.

The machine certificate on both Platform Services Controller instances in the region must be the same because they are load-balanced according to this validated design. The certificate must have a common name that is equal to the load-balanced Fully Qualified Domain Name (FQDN). Each Platform Services Controller FQDN and short name, and the load-balanced FQDN and short name must be in the Subject Alternate Name (SAN) of the generated certificate.

Table 2-3. Certificate-Related Files on Platform Services Controllers

Platform Services Controller	Certificate File Name
lax01m01psc01.lax01.rainpole.local	■ lax01psc01.1.cer ■ lax01psc01.key ■ Root64.cer
lax01w01psc01.lax01.rainpole.local	■ lax01psc01.1.cer ■ lax01psc01.key ■ Root64.cer

Prerequisites

- CA-signed certificate files generated by using VMware Validated Design Certificate Generation Utility (`CertGenVVD`). See the *VMware Validated Design Planning and Preparation* documentation.
- A Windows host with an SSH terminal access software such as PuTTY and an `scp` software such as WinSCP installed.

Procedure

1 Open a Secure Shell (SSH) connection to the Platform Services Controller virtual machine.

a Open an SSH connection to lax01m01psc01.lax01.rainpole.local and log in with the following credentials.

Setting	Value
Username	root
Password	*mgmtpsc_root_password*

2 Change the Platform Services Controller command shell to the Bash shell to allow secure copy (`scp`) connections for the root user.

```
shell
chsh -s "/bin/bash" root
```

3 Copy the generated certificates to the Platform Services Controllers.

a Run the following command to create a new temporary folder

```
mkdir -p /root/certs
```

b Copy the certificate files `lax01psc01.1.cer`, `lax01psc01.key`, and `Root64.cer` to the `/root/certs` folder.

You can use an `scp` software such as WinSCP.

4 Replace the certificate on the Platform Services Controller instance.

a Start the vSphere Certificate Manager utility on Platform Services Controller.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

b Select **Option 1 (Replace Machine SSL certificate with Custom Certificate)**

c Enter default vCenter Single Sign-On user name **`administrator@vsphere.local`** and the ***`vsphere_admin`*** password.

d Select **Option 2 (Import custom certificate(s) and key(s) to replace existing Machine SSL certificate).**

e When prompted for the custom certificate, enter **`/root/certs/lax01psc01.1.cer`**

f When prompted for the custom key, enter **`/root/certs/lax01psc01.key`**

g When prompted for the signing certificate, enter **`/root/certs/Root64.cer`**

h When prompted to `Continue operation`, enter **`Y`**.

The Platform Services Controller services automatically restart.

5 After Certificate Manager replaces the certificate, restart the vami-lighttp service to update the certificate in the application virtual management interface (VAMI) of and to remove certificate files from Platform Services Controller.

```
service vami-lighttp restart
cd /root/certs
rm lax01psc01.1.cer lax01psc01.key Root64.cer
```

6 Repeat the procedure to replace the certificate on lax01w01psc01.lax01.rainpole.local.

Update the Platform Services Controller SSO Configuration and Endpoints in Region B

Before installing vCenter Server the Platform Services Controller endpoints must be updated to reflect the name of the load balancer's virtual IP.

Prerequisites

Before completing this procedure, a DNS A record must be created. This A record is the FQDN of the load balancer with the IP address of lax01m01psc01.lax01.rainpole.local. After the load balancer is set up, this DNS record is changed to the virtual IP of the load balancer.

Procedure

1 Create a DNS record for the load balancer FQDN.

   a Open a remote desktop connection to your DNS server.

   b Create a DNS A record with the following values:

FQDN	IP
lax01psc01.lax01.rainpole.local	172.17.11.61

   Note After the load balancer is configured the IP address is updated to reflect the load balancer's VIP instead of the IP address of lax01m01psc01.lax01.rainpole.local

2 Update the Platform Services Controller SSO configuration on lax01m01psc01.lax01.rainpole.local.

   a Open an SSH connection to **`lax01m01psc01.lax01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtpsc_root_password*

   c Enter **`cd /usr/lib/vmware-sso/bin/`** and press **`Enter`**.

   d Enter **`python updateSSOConfig.py --lb-fqdn=lax01psc01.lax01.rainpole.local`** and press **`Enter`**.

3 Update the Platform Services Controller SSO configuration on lax01w01psc01.lax01.rainpole.local.

   a Open an SSH connection to **`lax01w01psc01.lax01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*comppsc_root_password*

c Enter **`cd /usr/lib/vmware-sso/bin/`** and press **`Enter`**.

d Enter **`python updateSSOConfig.py --lb-fqdn=lax01psc01.lax01.rainpole.local`** and press **`Enter`**.

4 Update the Platform Services Controller endpoints.

Only perform this procedure on one of the Platform Services Controllers.

a Open an SSH connection to **`lax01m01psc01.lax01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtpsc_root_password*

c Enter **`cd /usr/lib/vmware-sso/bin/`** and press **`Enter`**.

d Enter
`python UpdateLsEndpoint.py --lb-fqdn=lax01psc01.lax01.rainpole.local --user=Administrator@vsphere.local` and press **`Enter`**.

e Enter the *vsphere_admin_password* when prompted.

Deploy the Management vCenter Server Instance in Region B

You can now install the vCenter Server appliance for the management applications and configure licensing and security.

Procedure

1 Start the **vCenter Server Appliance Deployment** wizard.

a Browse to the vCenter Server Appliance ISO file.

b Open the `<dvd-drive>:\vcsa-ui-installer\win32\Installer` application file.

2 Complete the **vCenter Server Appliance Deployment** wizard.

a Click **Install** to start the installation.

b Click **Next** on the **Introduction** page.

c On the **End User License Agreement** page, select the **I accept the terms of the license agreement** check box and click **Next**.

d On the **Select deployment Type** page, under **External Platform Services Controller**, select the **vCenter Server (Requires External Platform Services Controller)** radio button and click **Next**.

e On the **Appliance deployment target** page, enter the following settings and click **Next**.

Setting	Value
ESXi host or vCenter Server name	lax01m01esx01.lax01.rainpole.local
HTTPS port	443
User name	root
Password	*esxi_root_user_password*

f In the **Certificate Warning** dialog box, click **Yes** to accept the host certificate.

g On the **Set up appliance VM** page, enter the following settings and click **Next**.

Setting	Value
Appliance name	lax01m01vc01
OS password	*mgmtvc_root_password*
Confirm OS password	*mgmtvc_root_password*

h On the **Select deployment size** page, select **Small vCenter Server** and click **Next**.

i On the **Select datastore** page, select the **vsanDatastore** datastore, select the **Enable Thin Disk Mode** check box, enter **`lax01-m01dc`** for the Datacenter Name, **`lax01-m01-mgmt01`** for the Cluster Name and click **Next**.

j On the **Configure network settings** page, enter the following settings and click **Next**.

Setting	Value
Network	VM Network
IP version	IPv4
IP assignment	static
System name	lax01m01vc01.lax01.rainpole.local
IP address	172.17.11.62
Subnet mask or prefix length	255.255.255.0
Default gateway	172.17.11.253
DNS servers	172.17.11.5,172.17.11.4

k On the **Ready to complete stage 1** page, review the configuration and click **Finish** to start the deployment.

l When the deployment completes, click **Continue** to proceed to stage 2 of the installation.

3 Install - Stage 2: Complete the **Set Up vCenter Server Appliance** wizard.

a Click **Next** on the **Introduction** page.

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

Setting	Value
Time Synchronization mode	Synchronize time with NTP servers
NTP servers (comma-separated list)	ntp.lax01.rainpole.local
SSH access	Enabled

c On the **SSO configuration** page, enter the following settings and click **Next**.

Setting	Value
Platform Services Controller	lax01psc01.lax01.rainpole.local
HTTPS port	443
SSO domain name	vsphere.local
SSO password	*sso_password*

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

e Click **OK** on the **Warning** dialog box.

4 Assign license for this vCenter Server instance.

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*

c Click the **Home** icon above the **Navigator** and select the **Administration** menu item.

d On the **Administration** page, click **Licenses** and click the **Assets** tab.

e Select the vCenter Server instance, and click the **Assign License** icon.

f Select the vCenter Server license that you entered earlier, and click **OK**.

5 Assign the vCenterAdmins domain group to the vCenter Server Administrator role.

a In the **Navigator**, click **Administration**.

b In the **Administration** window, click **Global Permissions**.

c In the **Global Permissions** box, click the **Manage** tab, then click the **Add permission** button.

d In the **Global Permissions Root - Add Permissions** window, click the **Add** button.

e Select **lax01.rainpole.local** from the **Domain** drop-down list.

f Enter `vCenterAdmins` in the **Search** text box and press **`Enter`**.

g Select the **vCenterAdmins** group, click the **Add** button, and then click **OK**.

h Ensure **Administrator** is selected and the **Propagate to Children** check box is selected under **Assigned Role** and click **OK**.

Replace the Certificate of the Management vCenter Server in Region B

To establish trusted connection with the other SDDC management components, you replace the machine SSL certificate on each vCenter Server instance in Region B with a custom certificate that is signed by the certificate authority (CA) available on the parent Active Directory (AD) server or on the intermediate Active Directory (AD) server.

Table 2-4. Certificate-Related Files on the vCenter Server Instances

vCenter Server FQDN	Files for Certificate Replacement
lax01m01vc01.lax01.rainpole.local	■ lax01m01vc01.key ■ lax01m01vc01.1.cer ■ Root64.cer

Prerequisites

- CA-signed certificate files generated by using VMware Validated Design Certificate Generation Utility (`CertGenVVD`). See the *VMware Validated Design Planning and Preparation* documentation.
- A Windows host with an SSH terminal access software such as PuTTY and an `scp` software such as WinSCP installed.

Procedure

1 Log in to vCenter Server by using Secure Shell (SSH) client.

a Open an SSH connection to the virtual machine lax01m01vc01.lax01.rainpole.local.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

2 Change the vCenter Server appliance command shell to the Bash shell to allow secure copy (`scp`) connections for the root user.

```
shell
chsh -s "/bin/bash" root
```

3 Copy the generated certificates from the Windows host where you run the `CertGenVVD` utility to the vCenter Server Appliance.

   a Run the following command to create a new temporary folder.

   ```
   mkdir -p /root/certs
   ```

   b Copy the certificate files `lax01m01vc01.1.cer`, `lax01m01vc01.key`, `Root64.cer` from the Windows host where you run the `CertGenVVD` utility to the `/root/certs` folder on the vCenter Server Appliance.

   You can use an `scp` software such as WinSCP.

4 Replace the CA-signed certificate on the vCenter Server instance.

   a Start the vSphere Certificate Manager utility on the vCenter Server instance.

   ```
   /usr/lib/vmware-vmca/bin/certificate-manager
   ```

   b Select **Option 1 (Replace Machine SSL certificate with Custom Certificate)**, enter the default vCenter Single Sign-On user name **`administrator@vsphere.local`** and the ***`vsphere_admin-password`*** password.

   c When prompted for the **Infrastructure Server IP**, enter the IP address of the Platform Services Controller that manages this vCenter Server instance.

Platform Services Controller Load Balancer VIP	IP Address of Platform Services Controller Load Balancer VIP
lax01m01vc01.lax01.rainpole.local	172.17.11.61

   d Select **Option 2 (Import custom certificate(s) and key(s) to replace existing Machine SSL certificate)**.

   e When prompted, provide the full path to the custom certificate, the root certificate file, and the key file that you generated earlier, and confirm the import with **`Yes (Y)`**.

vCenter Server	Path to Certificate-Related Files
lax01m01vc01.lax01.rainpole.local	Please provide valid custom certificate for Machine SSL. File: **`/root/certs/lax01m01vc01.1.cer`** Please provide valid custom key for Machine SSL. File: **`/root/certs/lax01m01vc01.key`** Please provide the signing certificate of the Machine SSL certificate File: **`/root/certs/Root64.cer`**

5 After Status shows `100% Completed`, wait several minutes until all vCenter Server services are restarted.

6 Run the following command to restart vami-lighttp service and to remove certificate files .

```
service vami-lighttp restart
cd /root/certs
rm lax01m01vc01.1.cer lax01m01vc01.key chainRoot64.cer
```

Set SDDC Deployment Details on the Management vCenter Server in Region B

Set an identity of your SDDC deployment on the Management vCenter Server in Region B. You can also use this identity as a label in tools for automated SDDC deployment.

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 From the **Home** menu of the vSphere Web Client, select **Global Inventory Lists**.

3 In the **Navigator**, click **vCenter Servers** under **Resources**.

4 Click the **lax01m01vc01.lax01.rainpole.local** vCenter Server object and click the **Configure** tab in the central pane.

5 Under the **Settings** pane, click **Advanced Settings** and click the **Edit** button.

6 In the **Edit Advanced vCenter Server Settings** dialog box, set the following value pairs one by one, clicking **Add** after each entry.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.2.0
config.SDDC.Deployed.WorkloadDomain	Management

Name	Value
config.SDDC.Deployed.Method	DIY
config.SDDC.Deployed.InstanceId	unique_identifier*

Note * To generate a unique identifier, use the Online UUID Generator website https://www.uuidgenerator.net/ and copy/paste the UUID into the config.SDDC.Deployed.InstanceId value. The Online UUID Generator is a universally unique identifier that generates random numbers using a secure random number generator.

7 Click **OK** to close the window.

Configure the Management Cluster in Region B

You must now create and configure the management cluster.

This process consists of the following actions:

- Configure DRS.
- Add the hosts to the cluster.
- Add a host to the active directory domain.
- Create vSAN disk groups.
- Mount the NFS volume for vSphere Data Protection Backups.
- Change the default ESX Admin group.
- Enable and configure vSphere HA
- Create and apply a host profile.
- Set the Platform Services Controller and vCenter Server appliances to the default vSAN storage policy.

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 Enable vSphere DRS.

a Expand the **lax01-m01dc** Datacenter object.

b Click the **lax01-m01-mgmt01** cluster object then click the **Configure** tab.

c Select the **vSphere DRS** page, and click **Edit**.

d Select the **Turn On vSphere DRS** checkbox then click **OK**.

3 Enable VMware EVC.

a Select the **VMware EVC** page from **Configuration**, and click **Edit**.

b *Set EVC mode to the highest available setting supported for the hosts in the cluster*, and click **OK**.

4 Add a management host to the management cluster.

a Right-click the **lax01-m01-mgmt01** cluster, and click **Add Host**.

b On the **Name and location** page, enter `lax01m01esx02.lax01.rainpole.local` in the **Host name or IP address** text box and click **Next**.

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

Setting	Value
User name	root
Password	*esxi_root_user_password*

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

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

f On the **Assign license** page, select the ESXi license key that you entered during the vCenter Server deployment and click **Next**.

g On the **Lockdown Mode** page, click **Next**.

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

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

5 Repeat the previous step for the three remaining hosts to add them to the management cluster.

Setting	Value
Host 3	lax01m01esx03.lax01.rainpole.local
Host 4	lax01m01esx04.lax01.rainpole.local

6 Add an ESXi host to the Active Directory domain.

a In the **Navigator**, click **Hosts and Clusters** and expand the entire **lax01m01vc01.lax01.rainpole.local** tree.

b Select the **lax01m01esx01.lax01.rainpole.local** host.

c Click the **Configure** tab.

d Under **System**, select **Authentication Services**.

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

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

Setting	Value
Domain	lax01.rainpole.local
Using credentials	Selected
User name	svc-domain-join@rainpole.local
Password	*svc-domain-join_password*

7 Set the Active Directory Service to Start and stop with host.

a In the **Navigator**, click **Hosts and Clusters** and expand the entire **lax01m01vc01.lax01.rainpole.local** tree.

b Select the **lax01m01esx01.lax01.rainpole.local** host.

c Click the **Configure** tab.

d Under **System**, select **Security Profile**.

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

f Select the **Active Directory** service and change the **Startup Policy** to `Start and stop with host` and click **OK**.

8 Rename the vSAN datastore.

a In the Navigator, click **Storage** and expand the entire **lax01m01vc01.lax01.rainpole.local** tree.

b Select **vsanDatastore**, and select **Actions > Rename.**.

c In the **Datastore - Rename** dialog box, enter **`lax01-m01-vsan01`** as the datastore name, and click **OK**.

Create a vSphere Distributed Switch for the Management Cluster in Region B

After adding all ESXi hosts to the cluster, you create a vSphere Distributed Switch. You must also create port groups to prepare your environment to migrate the Platform Services Controller and vCenter Server instances 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://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 Create vSphere Distributed Virtual Switch.

   a In the **Navigator**, click **Networking** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

   b Right-click the **lax01-m01dc** datacenter, and select **Distributed Switch > New Distributed Switch** to start the **New Distributed Switch** wizard.

   c On the **Name and location** page, enter **`lax01-m01-vds01`** as the name and click **Next**.

   d On the **Select version** page, ensure the **Distributed switch: 6.5.0** radio button is selected and click **Next**.

   e On the **Edit settings** page, enter the following values and click **Next**.

Setting	Value
Number of uplinks	2
Network I/O Control	Enabled
Create a default port group	Deselected

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

3 Edit the settings of the `lax01-m01-vds01` distributed switch.

   a Right-click the **lax01-m01-vds01** distributed switch, and select **Settings > Edit Settings**.

   b Click the **Advanced** tab.

   c Enter **`9000`** as MTU (Bytes) value, and click **OK**.

4 Create port groups in the `lax01–m01–vds01` distributed switch for the management traffic types.

   a Right-click the **lax01-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
lax01-m01-vds01-management	Ephemeral - no binding	VLAN	1711
lax01-m01-vds01-vmotion	Static binding	VLAN	1712
lax01-m01-vds01-vsan	Static binding	VLAN	1713
lax01-m01-vds01-nfs	Static binding	VLAN	1715
lax01-m01-vds01-replication	Static binding	VLAN	1716
lax01-m01-vds01-ext-management	Static binding	VLAN	150
lax01-m01-vds01-uplink01	Static binding	VLAN	2714
lax01-m01-vds01-uplink02	Static binding	VLAN	2715

   Note The port group for VXLAN traffic is automatically created later during the configuration of the NSX Manager for the management cluster.

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

   d Repeat this step for each port group.

5 Change the port groups to use the Route Based on Physical NIC Load teaming algorithm.

   a Right-click the **lax01-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 lax01-m01-vds01-uplink01 and lax01-m01-vds01-uplink02 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**.

6 Configure the uplinks for the lax01-m01-vds01-uplink01 and lax01-m01-vds01-uplink02 port groups.

   a Right click the **lax01-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 **lax01-m01-vds01-uplink02** port group, and click **Edit Settings**.

   e Select **Teaming and Failover**.

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

7 Connect the ESXi host, **lax01m01esx01.lax01.rainpole.local**, to the `lax01-m01-vds01` distributed switch by migrating their VMkernel and virtual machine network adapters.

   a Right-click the **lax01-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 **lax01m01esx01.lax01.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 box, select **Uplink 1** and click **OK**.

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

8 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 **lax01-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 **lax01-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, select **Use static IPv4 settings**, enter the IP address `172.17.13.101`, enter the subnet `255.255.255.0`, and click **Next**.

   g Click **Finish**.

   h Repeat steps 8c. - 8f. to create the remaining VMkernel network adapters.

Port Group	Port Properties	IPv4 Address	Netmask
lax01-m01-vds01-replication	■ vSphere Replication traffic ■ vSphere Replication NFC traffic	172.17.16.101	255.255.255.0
lax01-m01-vds01-nfs	N/A	172.17.15.101	255.255.255.0

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

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

9 Create the vMotion VMkernel adapter.

   a In the **Navigator**, click **Host and Clusters** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

   b Click **lax01m01esx01.lax01.rainpole.local**.

c Click the **Configure** tab then select **VMkernel adapters**.

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

e On the **Add Networking** page, select **Select an existing network**, browse to select the **lax01-m01-vds01-vmotion** port group, click **OK**, and click **Next**.

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

g On the **IPv4 settings** page, select **Use static IPv4 settings**, enter the IP address `172.17.12.101`, enter the subnet `255.255.255.0`, and click **Next**.

h Click **Finish**.

10 Configure the MTU on the vMotion VMkernel adapter.

a Select the vMotion VMkernel adapter 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**.

11 Configure the vMotion TCP/IP stack.

a Click **TCP/IP configuration**.

b Select **vMotion** and click the **Edit** icon.

c Click **Routing** and enter `172.17.12.253` for the **default gateway** and click **OK**.

12 Migrate the Management Platform Services Controller and vCenter Server instances from the standard switch to the distributed switch.

a In the **Navigator**, click **Networking** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

b Right-click the **lax01-m01-vds01** distributed switch and click **Migrate VM to Another Network**.

c On the **Select source and destination networks** page, browse the following networks and click **Next**.

Setting	Value
Source network	VM Network
Destination network	lax01-m01-vds01-management

d On the **Select VMs to migrate** page, select **lax01m01psc01.lax01.rainpole.local**, **lax01w01psc01.lax01.rainpole.local** and **lax01m01vc01.lax01.rainpole.local**, and click **Next**.

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

13 Define Network I/O Control shares for the different traffic types on the **lax01-m01-vds01** distributed switch.

   a Click the **lax01-m01-vds01** distributed switch, click the **Configure** tab, and click **Resource Allocation > System traffic**.

   b Under **System Traffic**, configure each of the following traffic types with the following values.

Traffic Type	Physical Adapter Shares
vSAN Traffic	High
NFS Traffic	Low
vMotion Traffic	Low
vSphere Replication (VR) Traffic	Low
Management Traffic	Normal
vSphere Data Protection Backup Traffic	Low
Virtual Machine Traffic	High
Fault Tolerance Traffic	Low
iSCSI Traffic	Low

14 Migrate the last physical adapter from the standard switch to the **lax01-m01-vds01** distributed switch.

   a In the **Navigator**, click **Networking** and expand the **LAX01** datacenter.

   b Right-click the **lax01-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 box, select lax01m01esx01.lax01.rainpole.local, and click **OK**.

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

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

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

   i In the **Select an Uplink for vmnic1** dialog box, select **Uplink 2**, and click **OK**, and click **Next**.

   j On the **Analyze Impact** page, click **Next**.

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

15 Enable vSphere Distributed Switch Health Check.

   a In the **Navigator**, click **Networking** and expand the **lax01m01vc01.lax01.rainpole.local** datacenter.

   b Select the **lax01-m01-vds01** distributed switch and click the **Configure** tab.

   c In the **Navigator**, select **Health check** and click the **Edit** button.

   d Select **Enabled** for **VLAN and MTU** and **Teaming and failover** and click **OK**.

16 Delete the vSphere Standard Switch.

   a In the **Navigator**, click on **Hosts and Clusters** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

   b Click on **lax01m01esx01.lax01.rainpole.local** and then click the **Configure** tab.

   c On the **Configure** page, select **Virtual switches**, choose **vSwitch0**, and then click on the **Remove selected switch** icon.

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

Create vSAN Disk Groups for the Management Cluster in Region B

vSAN disk groups must be created on each host that is contributing storage to the vSAN datastore.

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**, select **Hosts and Clusters** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

3 Click on the **lax01-m01-mgmt01** cluster and click the **Configure** tab.

4 Under **Virtual SAN**, click **Disk Management**.

5 Click on **lax01m01esx02.lax01.rainpole.local** and click on 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 **lax01m01esx03.lax01.rainpole.local**and **lax01m01esx04.lax01.rainpole.local**.

8 Assign a license to vSAN.

   a Right click the **lax01-m01-mgmt01** cluster and select **Assign License**.

   b In the **lax01-m01-mgmt01 - Assign License** window select the previously added **VSAN License** and click **OK**.

Enable vSphere HA on the Management Cluster in Region B

Before creating the host profile for the management cluster enable vSphere HA.

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**, click **Hosts and Clusters** and Expand the **lax01m01vc01.lax01.rainpole.local** tree.

3 Select the **lax01-m01-mgmt01** cluster.

4 Click the **Configure** tab, click **vSphere Availability**, and click **Edit**.

5 In the **Edit Cluster Settings** dialog box, select the **Turn on vSphere HA** check box.

6 Select **Failures and Responses** and select the following values from the drop-down menus.

Setting	Value
Enable Host Monitoring	Selected
Host Failure Response	Restart VMs
Response for Host Isolation	Power off and restart VMs
Datastore with PDL	Disabled
Datastore with APD	Disabled
VM Monitoring	VM Monitoring Only

7 Click **Admission Control**.

8 In the **Admission Control** page, enter following settings.

Setting	Value
Host failures cluster tolerates	1
Define host failover capacity by	Cluster resource percentage
Override calculated failover capacity	Deselected
Performance degradation VMs tolerate	100%

9 Click **OK**.

Note When you enable vSphere HA, the operation fails on hosts 2,3, and 4. This is expected behavior, networking is configured during host profile steps setup.

Change Advanced Options on the ESXi Hosts in the Management Cluster in Region B

Change the default ESX Admins group to achieve greater levels of security and enable vSAN to provision the Virtual Machine Swap files as thin to conserve space in the vSAN datastore.

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 Change the default ESX Admins group.

   a In the **Navigator**, click **Hosts and Clusters**.

   b Expand the entire **lax01m01vc01.lax01.rainpole.local** vCenter inventory tree, and select the **lax01m01esx01.lax01.rainpole.local** host.

   c Click the **Configure** tab, click **System > Advanced System Settings**.

   d Click the **Edit** button.

   e In the **filter** box, enter `esxAdmins` and wait for the search results.

   f 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**, click **Hosts and Clusters**.

   b Expand the entire **lax01m01vc01.lax01.rainpole.local** vCenter inventory tree, and select the **lax01m01esx01.lax01.rainpole.local** host.

   c Click the **Configure** tab, click **System > Advanced System Settings**.

   d Click the **Edit** button.

   e In the **filter** box, enter `vsan.swap` and wait for the search results.

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

4 Disable the SSH warning banner.

   a In the **Navigator**, click **Hosts and Clusters**.

   b Expand the entire **lax01m01vc01.lax01.rainpole.local** vCenter inventory tree, and select the **lax01m01esx01.lax01.rainpole.local** host.

   c Click the **Configure** tab, click **System > Advanced System Settings**.

   d Click the **Edit** button.

   e In the **filter** box, enter **`ssh`** and wait for the search results.

   f Change the value of **UserVars.SuppressShellWarning** to **1** and click **OK**.

Mount NFS Storage for the Management Cluster in Region B

You must mount an NFS datastore where vSphere Data Protection is later deployed.

Create a new datastore for the lax01-m01-mgmt01 cluster.

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**, click **Host and Clusters** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

3 Click on **lax01m01esx01.lax01.rainpole.local**.

4 Click on **Datastores**.

5 Click the **Create a New Datastore** icon.

   The **New Datastore** wizard opens.

6 On the **Type** page, select **NFS** and click **Next**.

7 On the **Select NFS version** page, select **NFS 3** and click **Next**.

8 On the **Name and configuration** page, enter the following datastore information and click **Next**.

Setting	Value
Datastore Name	lax01-m01-vdp01
Folder	/V2D_vDP_MgmtB_6TB
Server	172.17.15.251

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

Create and Apply the Host Profile for the Management Cluster in Region B

Host Profiles ensure all hosts in the cluster have the same configuration.

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 Create a Host Profile from lax01m01esx01.lax01.rainpole.local

   a In the **Navigator**, select **Hosts and Clusters** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

   b Right-click the ESXi host **lax01m01esx01.lax01.rainpole.local** and select **Host Profiles > Extract Host Profile**.

   c In the **Extract Host Profile** window, enter **`lax01-m01hp-mgmt01`** for the **Name** and click **Next**.

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

3 Attach the Host Profile to the management cluster.

   a In the **Navigator**, select **Hosts and Clusters** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

   b Right-click on the **lax01-m01-mgmt01** cluster and select **Host Profiles > Attach Host Profile**.

   c In the **Attach Host Profile** window, click the **lax01-m01hp-mgmt01** Host Profile, select the **Skip Host Customization** checkbox, and click **Finish**.

4 Create a Host Customizations profile for the hosts in the management cluster.

   a In the **Navigator**, select **Policies and Profiles**.

   b Click **Host Profiles**, then right click **lax01-m01hp-mgmt01** and select **Export Host Customizations**.

   c Click **Save**.

   d Select a file location to save the *lax01-m01hp-mgmt01_host_customizations.csv* file.

   e Open the *lax01-m01hp-mgmt01_host_customizations.csv* in Excel.

f Edit the Excel file to include the following values.

ESXi Host	Active Directory Configuration Password	Active Directory Configuration Username	NetStack Instance defaultTcpipStack->DNS configuration Name for this host	NetStack Instance vmotion->DNS configuration
lax01m01esx01.lax01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	lax01m01esx01	lax01m01esx01
lax01m01esx02.lax01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	lax01m01esx02	lax01m01esx02
lax01m01esx03.lax01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	lax01m01esx03	lax01m01esx03
lax01m01esx04.lax01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	lax01m01esx04	lax01m01esx04

ESXi Host	Host virtual NIC lax01-m01-mgmt01:lax01-m01-mgmt01-management:management->IP address settings Host IPv4 address	Host virtual NIC lax01-m01-mgmt01:lax01-m01-mgmt01-management:management->IP address settings SubnetMask
lax01m01esx01.lax01.rainpole.local	172.17.11.101	255.255.255.0
lax01m01esx02.lax01.rainpole.local	172.17.11.102	255.255.255.0
lax01m01esx03.lax01.rainpole.local	172.17.11.103	255.255.255.0
lax01m01esx04.lax01.rainpole.local	172.17.11.104	255.255.255.0

ESXi Host	Host virtual NIC lax01-m01-mgmt01:lax01-m01-mgmt01-nfs:<UNRESOLVED>->IP address settings Host IPv4 address	Host virtual NIC lax01-m01-mgmt01:lax01-m01-mgmt01-nfs:<UNRESOLVED>->IP address settings SubnetMask
lax01m01esx01.lax01.rainpole.local	172.17.15.101	255.255.255.0
lax01m01esx02.lax01.rainpole.local	172.17.15.102	255.255.255.0
lax01m01esx03.lax01.rainpole.local	172.17.15.103	255.255.255.0
lax01m01esx04.lax01.rainpole.local	172.17.15.104	255.255.255.0

ESXi Host	Host virtual NIC lax01-m01-mgmt01:lax01-m01-mgmt01-replication:vSphereReplication,vSphereReplicationNFC->IP address settings Host IPv4 address	Host virtual NIC lax01-m01-mgmt01 replication:vSphereReplication,vSp >IP address settings SubnetMask
lax01m01esx01.lax01.rainpole.local	172.17.16.101	255.255.255.0
lax01m01esx02.lax01.rainpole.local	172.17.16.102	255.255.255.0
lax01m01esx03.lax01.rainpole.local	172.17.16.103	255.255.255.0
lax01m01esx04.lax01.rainpole.local	172.17.16.104	255.255.255.0

ESXi Host	Host virtual NIC lax01-m01-mgmt01:lax01-m01-mgmt01-vsan:vsan->IP address settings Host IPv4 address	Host virtual NIC lax01-m01-mgmt01:lax01-m01-mgmt01-vsan:vsan->IP address settings SubnetMask
lax01m01esx01.lax01.rainpole.local	172.17.13.101	255.255.255.0
lax01m01esx02.lax01.rainpole.local	172.17.13.102	255.255.255.0
lax01m01esx03.lax01.rainpole.local	172.17.13.103	255.255.255.0
lax01m01esx04.lax01.rainpole.local	172.17.13.104	255.255.255.0

ESXi Host	Host virtual NIC lax01-m01-mgmt01:lax01-m01-mgmt01-vmotion:vmotion->IP address settings Host IPv4 address	Host virtual NIC lax01-m01-mgmt01:lax01-m01-mgmt01-vmotion:vmotion->IP address settings SubnetMask
lax01m01esx01.lax01.rainpole.local	172.17.12.101	255.255.255.0
lax01m01esx02.lax01.rainpole.local	172.17.12.102	255.255.255.0
lax01m01esx03.lax01.rainpole.local	172.17.12.103	255.255.255.0
lax01m01esx04.lax01.rainpole.local	172.17.12.104	255.255.255.0

g When you have updated the Excel file, save it in the CSV file format and close Excel.

h Click the **Configure** tab.

i Click the **Edit Host Customizations** button.

j In the **Edit Host Customizations** window, select all hosts and click **Next**.

k On the **Customize hosts** page, click the **Browse** button, select the customization CSV file you created previously, and click **Finish.**

5 Remediate the hosts in the management cluster .

a Click the **Monitor** tab and click **Compliance**.

b Select **lax01-m01-mgmt01** and click the **Check Host Profile Compliance** button.

c Select **lax01m01esx02.lax01.rainpole.local**, click the **Remediate host based on its host profile** button, and click **Finish** in the **Ready to complete** window.

d Select **lax01m01esx03.lax01.rainpole.local**, click the **Remediate host based on its host profile** button, and click **Finish** in the **Ready to complete** window.

e Select **lax01m01esx04.lax01.rainpole.local**, click the **Remediate host based on its host profile** button, and click **Finish** in the **Ready to complete** window.

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

6 Schedule nightly compliance checks.

   a On the **Policies and Profiles** page, click **lax01-m01hp-mgmt01**, click the **Monitor** tab, and click the **Scheduled Tasks** subtab.

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

   c In the **Check Host Profile Compliance (scheduled)** window, click **Scheduling Options**.

   d Enter `lax01-m01hp-mgmt01 Compliance Check` in the **Task Name** field.

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

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

   g Click **OK** in the **Check Host Profile Compliance (scheduled)** window.

Set Virtual SAN Policy on Management Virtual Machines in Region B

After you apply the host profile to all hosts, set the storage policy of the management virtual machines to the default Virtual SAN storage policy. Set the Platform Services Controller and vCenter Server appliances to the default vSAN storage policy.

Set the Platform Services Controller and vCenter Server appliances to the default Virtual SAN storage policy.

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**, click **Hosts and Clusters**.

3 Expand the **lax01m01vc01.lax01.rainpole.local** tree.

4 Select the **lax01m01psc01** virtual machine.

5 Click the **Configure** tab, click **Policies**, and click **Edit VM Storage Policies**.

6 In the **lax01m01psc01:Manage VM Storage Policies** dialog box, from the **VM storage policy** drop-down menu, select **vSAN Default Storage Policy**, and click **Apply to all**.

7 Click **OK** to apply the changes.

8 Verify that the **Compliance Status** column shows `Compliant` status for all items in the table.

9 Repeat this step to apply the vSAN Default Storage Policy on **lax01w01psc01** and **lax01m01vc01** virtual machines.

Create the VM and Template Folders in Region B

Create folders to group objects of the same type for easier management.

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 Create a folder for each of the management applications.

   a In the **Navigator**, click **VMs and Templates** and Expand the **lax01m01vc01.lax01.rainpole.local** tree.

   b Right-click the **lax01-m01dc** data center and select **New Folder** > **New VM and Template Folder**.

   c In the **New Folder** dialog box, enter `lax01-m01fd-mgmt` as the name to label the folder, and click **OK**.

   d Repeat this step to create the remaining folders.

Table 2‑5. Folders for the Management Applications in Region B

Management Applications	Folder
vCenter Server, Platform Services Controllers, and Update Manager Download Service	lax01-m01fd-mgmt
vRealize Automation, vRealize Orchestrator, and vRealize Business	lax01-m01fd-vra
vRealize Automation (Proxy Agent) and vRealize Business (Data Collector)	lax01-m01fd-vraias
vRealize Operations Manager	lax01-m01fd-vrops
vRealize Operations Manager (Remote Collectors)	lax01-m01fd-vropsrc
vRealize Log Insight	lax01-m01fd-vrli
NSX Manager, Controllers, and Edges	lax01-m01fd-nsx
VMware Site Recovery Manager and vSphere Data Protection	lax01-m01fd-bcdr

3 Move the vCenter Server and Platform Services Controller virtual machines to the lax01-m01fd-mgmt folder.

   a In the **Navigator**, click **VMs and Templates**.

   b Expand the **lax01m01vc01.lax01.rainpole.local** tree.

   c Expand the **Discovered Virtual Machines** folder.

   d Drag **lax01m01vc01**, **lax01m01psc01**, and **lax01w01psc01** to the **lax01-m01fd-mgmt** folder.

4 Delete the **Discovered Virtual Machines** folder.

   a In the **Navigator**, click **VMs and Templates**.

   b Expand the **lax01m01vc01.lax01.rainpole.local** tree.

   c Right click the **Discovered Virtual Machines** folder and select **Remove from Inventory**.

Create Anti-Affinity Rules for the Platform Services Controllers in Region B

Anti-Affinity rules prevent virtual machines from running on the same host. This helps to maintain redundancy in the event of host failures.

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**, select **Hosts and Clusters** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

3 Select the **lax01-m01-mgmt01** cluster and click the **Configure** tab.

4 On the **Configure** page, click **VM/Host Rules**.

5 On the **VM/Host Rules** page, click the **Add** button to create a new VM/Hosts Rule.

6 In the **Create VM/Host Rule** dialog, enter `anti-affinity-rule-psc` in the **Name** field, ensure that the **Enable rule** checkbox is selected, select **Separate Virtual Machines** from the **Type** drop down menu, and click the **Add** button.

7 In the **Add Rule Member** dialog, select **lax01m01psc01** and **lax01w01psc01** and click **OK**.

8 Click **OK** to create the rule.

Create VM Groups to Define Startup Order in the Management Cluster in Region B

VM Groups allow you to define the startup order of virtual machines. Startup orders are used during vSphere HA events such that vSphere HA powers on virtual machines in the correct order.

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** select **Hosts and Clusters** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

3 Create a VM Group for the Platform Services Controllers.

   a Select the **lax01-m01-mgmt01** cluster and click on **Configure**.

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

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

   d In the **Create VM/Host Group** dialog, enter `Platform Services Controllers` in the **Name** text box, select **VM Group** from the **Type** drop down menu, and click the **Add** button.

   e In the **Add VM/Host Group Member** dialog box, select **lax01m01psc01** and **lax01w01psc01** and click **OK.**

4 Create a VM Group for the vCenter Server virtual machine.

   a Select the **lax01-m01-mgmt01** cluster and click on **Configure**.

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

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

   d In the **Create VM/Host Group** dialog, enter **`vCenter Servers`** in the **Name** text box, select **VM Group** from the **Type** drop down, and click the **Add** button.

   e In the **Add VM/Host Group Member** dialog, select **lax01m01vc01** and click **OK**.

5 Create a Rule to power on the Platform Services Controllers followed by vCenter Servers.

   a Select the **lax01-m01-mgmt01** cluster and click on **Configure**.

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

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

d In the **Create VM/Host Rule** dialog, enter `SDDC Management Virtual Machines` in the **Name** text box, ensure that the **Enable rule** check box is selected, and select **Virtual Machines to Virtual Machines** from the **Type** drop down.

e Select **Platform Services Controllers** from the **First restart VMs in VM group** drop-down.

f Select **vCenter Servers** from the **Then restart VMs in VM group** and click **OK**.

Deploy and Configure the Management Cluster NSX Instance in Region B

This design uses two separate NSX instances per region. One instance is tied to the Management vCenter Server, and the other instance is tied to the Compute vCenter Server. Deploy and configure the NSX instance for the management cluster in Region B.

Procedure

1 Deploy the NSX Manager for the Management Cluster NSX Instance in Region B

For this implementation NSX Manager and vCenter Server have a one-to-one relationship. For every instance of NSX Manager, there is one connected vCenter Server.

2 Join the Management NSX Manager to the Primary NSX Instance in Region B

You join the secondary NSX instance in Region B to the respective primary instance in Region A.

3 Prepare the ESXi Hosts in the Management Cluster for NSX in Region B

NSX kernel modules packaged in VIB files run within the hypervisor kernel and provide services such as distributed routing, distributed firewall, and VXLAN bridging capabilities. To use NSX, you must install the NSX kernel modules on the ESXi hosts.

4 Configure the NSX Logical Network for the Management Cluster in Region B

After all the deployment tasks are ready, you must configure the NSX logical network.

5 Update the Host Profile for the Management Cluster in Region B

After you configure NSX logical networking on the management hosts in Region B, update the host profile of the management cluster, and remediate the hosts to align their configuration.

6 Deploy the Platform Services Controllers Load Balancer in Region B

You configure load balancing for all services and components related to Platform Services Controllers (PSC) using an NSX Edge load balancer.

7 Configure NSX Dynamic Routing in the Management Cluster in Region B

NSX for vSphere creates a network virtualization layer on top of which all virtual networks are created. This layer is an abstraction between the physical and virtual networks. You configure NSX dynamic routing within the management cluster, deploying two NSX Edge devices and configure a Universal Distributed Logical Router (UDLR).

8 Update Distributed Firewall for Region B

After deploying the vCenter Server you must add it to the distributed firewall exclusion list. The default rule in Region B must be changed to deny.

9 Test the Management Cluster NSX Configuration in Region B

Test the configuration of the NSX logical network using a ping test. A ping test checks if two hosts in a network can reach each other.

10 Test the Management Clusters Routing Failover

After the clusters are fully configured in Region A and Region B, verify that the network connectivity between them works as expected.

11 Deploy Application Virtual Networks in Region B

Deploy the application virtual networks for the region.

12 Deploy the NSX Load Balancer in Region B

Deploy a load balancer for use by management applications connected to the application virtual network Mgmt-xRegion01-VXLAN.

Deploy the NSX Manager for the Management Cluster NSX Instance in Region B

For this implementation NSX Manager and vCenter Server have a one-to-one relationship. For every instance of NSX Manager, there is one connected vCenter Server.

Deploy the NSX Manager virtual appliance for the management cluster. After the NSX Manager is deployed, connect it to the Management vCenter Server instance.

Deploy the NSX Manager Appliance in Region B

You deploy the NSX Manager appliance from the OVA file to the lax01-m01-mgmt01 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://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**, expand the entire **lax01m01vc01.lax01.rainpole.local** tree.

3 Right-click the **lax01-m01-mgmt0101** cluster and click **Deploy OVF Template**.

4 On the **Select template** page, click the **Browse** button, select the VMware NSX Manager `.ova` file, and click **Next.**

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

Setting	Value
Name	lax01m01nsx01
Select a datacenter or folder	lax01-m01fd-nsx

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 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

10 On the **Setup networks** page, under **Destination Network**, select **lax01-m01-vds01-management** and click **Next.**

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

Setting	Value
DNS Server List	172.17.11.5,172.17.11.4
Domain Search List	lax01.rainpole.local
Default IPv4 Gateway	172.17.11.253
Hostname	lax01m01nsx01.lax01.rainpole.local
Network 1 IPv4 Address	172.17.11.65
Network 1 Netmask	255.255.255.0
Enable SSH	Selected
NTP Server List	ntp.lax01.rainpole.local,ntp.sfo01.rainpole.local
CLI "admin" User Password / enter	*mgmtnsx_admin_password*
CLI "admin" User Password / confirm	*mgmtnsx_admin_password*
CLI Privilege Mode Password / enter	*mgmtnsx_priviledge_password*
CLI Privilege Mode Password / confirm	*mgmtnsx_priviledge_password*

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

13 In the **Navigator**, expand the entire **lax01m01vc01.lax01.rainpole.local** tree, select the virtual machine **lax01m01nsx01**, and click the **Power on** button.

Replace the Certificate of NSX Manager for the Management Cluster in Region B

After you deploy the appliance of NSX Manager for the management cluster, replace the default certificate for NSX Manager. NSX Manager can communicate with the other management solutions over a trusted connection.

Table 2-6. Certificate-Related Files on the NSX Manager Instance for the Management Cluster in Region B

NSX Manager FQDN	Certificate File Name
lax01m01nsx01.lax01.rainpole.local	lax01m01nsx01.4.p12

Prerequisites

- CA-signed certificate files generated by using VMware Validated Design Certificate Generation Utility (`CertGenVVD`). See the *VMware Validated Design Planning and Preparation* documentation.

Procedure

1 Log in to the appliance interface of NSX Manager for the management cluster.

   a Open a Web browser and go to **`https://lax01m01nsx01.lax01.rainpole.local`** .

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 On the **Home** page, select **Manage Appliance Settings**.

3 On the **Manage** tab, click **SSL Certificates and click Upload PKSCS#12 Keystore**.

4 Browse to the certificate chain file `lax01m01nsx01.4.p12`, provide the keystore password or passphrase, and click **Import**.

5 Restart NSX Manager to propagate the CA-signed certificate.

   a In the right corner of the NSX Manager page, click the **Settings** icon.

   b From the drop-down menu, select **Reboot Appliance**.

Connect NSX Manager to the Management vCenter Server in Region B

Procedure

1 Log in to the appliance interface of NSX Manager for the management cluster.

   a Open a Web browser and go to **`https://lax01m01nsx01.lax01.rainpole.local`** .

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 Click **Manage vCenter Registration**.

3 Under **Lookup Service**, click the **Edit** button.

4 In the **Lookup Service** dialog box, enter the following settings, and click **OK**.

Setting	Value
Lookup Service Host	lax01psc01.lax01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	*vsphere_admin_password*

5 In the **Trust Certificate?** dialog box, click **Yes**.

6 Under **vCenter Server**, click the **Edit** button.

7 In the **vCenter Server** dialog box, enter the following settings, and click **OK**.

Setting	Value for NSX Manager for the Management Cluster
vCenter Server	lax01m01vc01.lax01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

8 In the Trust Certificate? dialog box, click **Yes**.

9 Wait for the **Status** indicators for the Lookup Service and vCenter Server to change to a `Connected` status.

Assign Administrative Access to NSX Manager for the Management Cluster in Region B

Assign the administrator@vsphere.local account to the NSX Enterprise Administrator Role.

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**, click **Networking & Security** and click **Users and Domains.**

3 Under **NSX Managers**, click the **172.17.11.65** instance.

4 Click the **Add** icon.

5 On the **Identify User** page, enter **`administrator@vsphere.local`** in the **User** text filed and click **Next**.

6 On the **Select Roles** page, select the **Enterprise Administrator** radio button and click **Finish**.

Join the Management NSX Manager to the Primary NSX Instance in Region B

You join the secondary NSX instance in Region B to the respective primary instance in Region A.

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 Assign the secondary role to the management NSX Manager in Region B.

   a Under **Inventories**, click **Networking & Security**.

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

   c On the **Management** tab, select the primary **172.16.11.65** instance.

   d Select **Actions > Add Secondary NSX Manager**.

e In the **Add secondary NSX Manager** dialog box, enter the following settings and click **OK**.

Setting	Value
NSX Manager	172.17.11.65
User name	admin
Password	*mgmtnsx_admin_password*
Confirm Password	*mgmtnsx_admin_password*

f In the **Trust Certificate** confirmation dialog box, click **Yes**.

Prepare the ESXi Hosts in the Management Cluster for NSX in Region B

NSX kernel modules packaged in VIB files run within the hypervisor kernel and provide services such as distributed routing, distributed firewall, and VXLAN bridging capabilities. To use NSX, you must install the NSX kernel modules on the ESXi hosts.

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**, click **Networking & Security**.

3 Click **Installation and Upgrade**, and click the **Host Preparation** tab.

4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.

5 Under **NSX Component Installation on Hosts**, click **Actions** then **Install** for the **lax01-m01-mgmt01** cluster and click **Yes** in the confirmation dialog box.

6 Verify that the **Installation Status** column displays the NSX version for all hosts in the cluster, confirming that the NSX kernel modules are successfully installed.

Configure the NSX Logical Network for the Management Cluster in Region B

After all the deployment tasks are ready, you must configure the NSX logical network.

To configure the NSX logical network, you perform the following tasks:

- Configure the Segment ID allocation.

- Configure the VXLAN networking.
- Configure the transport zone.

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. Configure the Segment ID allocation.
   a. In the **Navigator**, click **Networking & Security**.
   b. Click **Installation and Upgrade**, click **Logical Network Preparation**, and click **Segment ID**.
   c. Select **172.17.11.65** from the **NSX Manager** drop-down menu.
   d. Click **Edit**, enter the following values, and click **OK**.
3. Configure the VXLAN networking.
   a. Click the **Host Preparation** tab.
   b. Under **VXLAN**, click **Not Configured** on the lax01-m01-mgmt01 row, enter the following values, and click **OK**.

Setting	Value
Switch	lax01-m01-vds01
VLAN	3019
MTU	9000
VMKNic IP Addressing	Use DHCP
VMKNic Teaming Policy	Load Balance - SRCID
VTEP	2

4. Configure the transport zone.
   a. On the **Installation and Upgrade** page, click the **Logical Network Preparation** tab and click **Transport Zones**.
   b. Select **172.17.11.65** from the **NSX Manager** drop-down menu.
   c. Select the **Mgmt Universal Transport Zone** and click the **Connect Clusters** icon.
   d. In the **Connect Clusters** dialog box, select **lax01-m01-mgmt01** and click **OK**.

Update the Host Profile for the Management Cluster in Region B

After you configure NSX logical networking on the management hosts in Region B, update the host profile of the management cluster, and remediate the hosts to align their 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. Update the host profile for the management cluster.
   - a In the **Navigator**, select **Policies and Profiles**.
   - b Click **Host Profiles**, right-click **lax01-m01hp-mgmt01**, and select **Copy settings from Host**.
   - c Select **lax01m01esx01.lax01.rainpole.local** and click **OK**.
3. Verify compliance and remediate the management hosts in Region B.
   - a On the **Policies and Profiles** page, select the **lax01-m01-mgmt01** host profile.
   - b On the **Monitor** tab, click the **Compliance** tab.
   - c Select **lax01-m01-mgmt01** in the **Host/Cluster** column and click **Check Host Profile Compliance**.

     This compliance test shows that the first host is `Compliant`, but the other hosts are `Not Compliant`.
   - d Click each of the non-compliant hosts, click **Remediate Hosts Based on its Host Profile**.
   - e In the **Remediate Hosts Based on its Host Profile** wizard, enter **`Host Name`** if prompted for **NetStack Instance vxlan->DNS configuration**, and click **Next**.
   - f On the **Ready to complete** page, click **Finish**.

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

Deploy the Platform Services Controllers Load Balancer in Region B

You configure load balancing for all services and components related to Platform Services Controllers (PSC) using an NSX Edge load balancer.

Procedure

1. Deploy the Platform Services Controller NSX Load Balancer in Region B

   The first step in deploying load balancing for the Platform Services Controller is to deploy the edge services gateway.

2. Create Platform Services Controller Application Profiles in Region B

   Create an application profile to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

3. Create Platform Services Controller Server Pools in Region B

   A server pool consists of backend server members. After you create a server pool, you associate a service monitor with the pool to manage and share the backend servers flexibly and efficiently.

4. Create Platform Services Controller Virtual Servers in Region B

   After load balancing is set up, the NSX load balancer distributes network traffic across multiple servers. When a virtual server receives a request, it chooses the appropriate pool to send traffic to. Each pool consists of one or more members. You create virtual servers for all the configured server pools.

5. Update DNS Records for the Platform Services Controller Load Balancer in Region B

   You must modify the DNS Address in Region B after setting up load balancing.

Deploy the Platform Services Controller NSX Load Balancer in Region B

The first step in deploying load balancing for the Platform Services Controller is to deploy the edge services gateway.

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. Click **Networking & Security**.

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

4. Select **172.17.11.65** from the NSX Manager drop-down menu.

5. Click the **Add** icon tab to create an NSX Edge.

   The **New NSX Edge** wizard appears.

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

Setting	Value
Install Type	Edge Services Gateway
Name	lax01psc01
Hostname	lax01psc01.lax01.rainpole.local
Deploy NSX EDGE	Selected
Enable High Availability	Selected

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

Setting	Value
User Name	admin
Password	*edge_admin_password*
Enable SSH access	Selected
Enable auto rule generation	Selected
Edge Control Level logging	INFO

8 On the **Configure deployment** page, perform the following configuration steps and click **Next**.

a Select **lax01-m01dc**, from the **Datacenter** drop-down menu.

b Click **Large** to specify the **Appliance Size**.

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

Setting	Value
Resource pool	lax01-m01-mgmt01
Datastore	lax01-m01-vsan01
Folder	lax01-m01fd-nsx
Resource Reservation	System Managed

d To create a second appliance, click the **Add** icon again, make the same selections in the **New NSX Appliance** dialog box, and click **OK**.

9 On the **Configure Interfaces** page, click the **Add** icon to configure the lax01psc01 interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	lax01psc01
Type	Internal
Connected To	lax01-m01-vds01-management
Connectivity Status	Connected
Primary IP Address	172.17.11.71

Setting	Value
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

10 On the **Default gateway** settings page, click **Next**.

11 On the **Firewall and HA** page, select the following settings and click **Next**.

Setting	Value
Configure Firewall default policy	Selected
Default Traffic Policy	Accept
Logging	Disable
vNIC	any
Declare Dead Time	15

12 On the **Ready to complete** page, review the configuration settings you entered and click **Finish**.

13 Enable HA logging.

a In the **Navigator**, click **NSX Edges**.

b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

c Double-click the device labeled **lax01psc01**.

d Click the **Manage** tab and click the **Settings** tab.

e Click **Change** in the **HA Configuration** window.

f Select the `Enable Logging` checkbox and click **OK**.

14 Configure the Default Gateway.

a In the **Navigator**, click **NSX Edges**.

b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

c Double-click the device labeled lax01psc01.

d Click the **Manage** tab and click the **Routing** tab.

e Click **Edit** to configure the **Default Gateway**.

f In the **Edit Default Gateway** dialog, enter **`172.17.11.1`** for the **Gateway IP** and click **OK**.

g Click **Publish Changes**.

15 Enable the Load Balancer service.

a In the **Navigator**, click **NSX Edges**.

b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

c Double-click the device labeled **lax01psc01**.

d Click the **Manage** tab and click the **Load Balancer** tab.

e Click **Global Configuration** and click **Edit**.

f In the **Edit load balancer global configuration** dialog box, select **Enable Load Balancer** and click **OK**.

Create Platform Services Controller Application Profiles in Region B

Create an application profile to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

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 Click **Networking & Security**.

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

4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **lax01psc01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Application Profiles**.

6 Click the **Add** icon and in the **New Profile** dialog box, enter the following values.

Setting	Value	Value
Name	psc-tcp	psc-https
Type	TCP	HTTPS
Enable SSL Passthrough	Deselected	Selected
Persistence	Source IP	Source IP
Expires in (Seconds)	60	60

7 Click **OK** to save the configuration.

Create Platform Services Controller Server Pools in Region B

A server pool consists of backend server members. After you create a server pool, you associate a service monitor with the pool to manage and share the backend servers flexibly and efficiently.

Repeat this procedure to create two server pools. Use the values indicated in the procedure to create the first and second server pools.

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 Click **Networking & Security**.

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

4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **lax01psc01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.

6 Click the **Add** icon and in the **New Pool** dialog box, enter the following values.

Setting	Value	Value
Name	psc-https-443	psc-tcp-389
Algorithm	ROUND-ROBIN	ROUND-ROBIN
Monitors	default-tcp-monitor	default-tcp-monitor

7 **New Members** dialog box, click the **Add** icon to add the first pool member.

8 In the **New Member** dialog box, enter the following values, and click **OK**.

Setting	Values for First Server Pool	Values for Second Server Pool
Name	lax01m01psc01	lax01m01psc01
IP Address/VC Container	lax01m01psc01	lax01m01psc01
Monitor Port	443	389
Weight	1	1

9 **Under Members**, click the **Add** icon to add the second pool member.

10 In the **New Member** dialog box, enter the following values, click **OK**, and click **OK** to save the PSC server pools.

Setting	Values for First Server Pool	Values for Second Server Pool
Enable Member	Selected	Selected
Name	lax01w01psc01	lax01w01psc01
IP Address/VC Container	lax01w01psc01	lax01w01psc01
Port		
Monitor Port	443	389
Weight	1	1

11 Repeat the procedure to create the remaining server pool.

Create Platform Services Controller Virtual Servers in Region B

After load balancing is set up, the NSX load balancer distributes network traffic across multiple servers. When a virtual server receives a request, it chooses the appropriate pool to send traffic to. Each pool consists of one or more members. You create virtual servers for all the configured server pools.

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 Click **Networking & Security**.

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

4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **lax01psc01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Virtual Servers**.

6 Click the **Add** icon, and in the **New Virtual Server** dialog box configure the values for the virtual server you are adding, and click **OK**.

Setting	Value	Value
Enable Virtual server	Selected	Selected
Application Profile	psc-tcp	psc-https
Name	psc-tcp -389	psc-https-443

Setting	Value	Value
Description	389-LDAP,2012-Control Interface,2014-RPC Port,2020-Authentication,636-SSL LDAP	Data from the vSphere Web Client
IP Address	172.17.11.71	172.17.11.71
Protocol	TCP	HTTPS
Port	389,636,2012,2014,2020	443
Default Pool	psc-tcp	psc-https

7 Repeat Step 6 to create a virtual server for each component. Upon completion, verify that you have successfully entered the virtual server names and their respective configuration values.

Update DNS Records for the Platform Services Controller Load Balancer in Region B

You must modify the DNS Address in Region B after setting up load balancing.

For the Platform Services Controller Load Balancer, you edit the DNS entry of lax01psc01.lax01.rainpole.local to point to the virtual IP address (VIP) of the Load Balancer (172.17.11.71) instead of pointing to the IP address of lax01m01psc01.

Procedure

1 Log in to DNS server **dc01lax.lax01.rainpole.local** that resides in the lax01.rainpole.local domain.

2 Open the Windows **Start** menu, enter **dns** in the **Search** text box, and press Enter.

The **DNS Manager** dialog box appears.

3 In the **DNS Manager** dialog box, under **Forward Lookup Zones**, select the **lax01.rainpole.local** domain and locate the **lax01psc01** record on the right.

4 Double-click the **lax01psc01** record, change the IP address of the record from 172.17.11.61 to **`172.17.11.71`**, and click **OK**.

Setting	Value
Fully Qualified domain name (FQDN)	lax01psc01.lax01.rainpole.local
IP Address	172.17.11.71
Update Associated Pointer (PTR) record	Selected

Configure NSX Dynamic Routing in the Management Cluster in Region B

NSX for vSphere creates a network virtualization layer on top of which all virtual networks are created. This layer is an abstraction between the physical and virtual networks. You configure NSX dynamic routing within the management cluster, deploying two NSX Edge devices and configure a Universal Distributed Logical Router (UDLR).

Procedure

1 Deploy NSX Edge Devices for North-South Routing in Region B

Deploy two NSX Edge devices for North-South Routing.

2 Disable the Firewall Service in Region B

Disable the firewall of the NSX Edge devices. This is required for equal-cost multi-path (ECMP) to operate correctly. Perform this procedure for each NSX Edge device.

3 Enable and Configure Routing in Region B

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

4 Verify Peering of Upstream Switches and Establishment of BGP in Region B

The NSX Edge devices must establish a connection to each of its upstream BGP switches before BGP updates can be exchanged. Verify that the NSX Edges devices are successfully peering, and that BGP routing has been established.

5 Configure Universal Distributed Logical Router for Dynamic Routing in Region B

Configure the universal distributed logical router (UDLR) to use dynamic routing in Region B.

6 Verify Establishment of BGP for the Universal Distributed Logical Router in Region B

Verify that the UDLR is successfully peering, and that BGP routing has been established.

7 Configure Static Routes on the Universal Distributed Logical Router in Region B

Configure the universal distributed logical router (UDLR) to use static routes for routing to the management servers in Region B.

Deploy NSX Edge Devices for North-South Routing in Region B

Deploy two NSX Edge devices for North-South Routing.

Perform this procedure twice to deploy two NSX Edge devices. Enter name and IP addresses for the respective device by using the values in the tables.

Table 2-7. NSX Edge Settings

NSX Edge Device	Device Name
NSX Edge Device 1	lax01m01esg01
NSX Edge Device 2	lax01m01esg02

Table 2-8. NSX Edge Interfaces Settings

Interface	Primary IP Address lax01m01esg01	Primary IP Address lax01m01esg02
Uplink01	172.27.14.2	172.27.14.3
Uplink02	172.27.15.3	172.27.15.2
sfo01m01udlr01	192.168.10.50	192.168.10.51

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 Under **Inventories**, click **Networking & Security**.

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

4 Select **172.17.11.65** 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	lax01m01esg01	lax01m01esg02
Install Type	Edge Service Gateway	Edge Service Gateway
Name	lax01m01esg01	lax01m01esg02
Deploy NSX Edge	Selected	Selected
Enable High Availability	Deselected	Deselected

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

Settings	Value
User Name	admin
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 the **Large** radio button to specify the Appliance Size and click the **Add** icon.

   The **Add NSX Edge Appliance** dialog box appears.

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

Setting	Value
Cluster/Resource Pool	lax01-m01-mgmt01
Datastore	lax01-m01-vsan01
Folder	lax01-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	lax01m01esg01	lax01m01esg02
Name	Uplink01	Uplink01
Type	Uplink	Uplink
Connected To	lax01-m01-vds01-uplink01	lax01-m01-vds01-uplink01
Connectivity Status	Connected	Connected
Primary IP Address	172.27.14.2	172.27.14.3
Subnet Prefix Length	24	24
MTU	9000	9000
Send ICMP Redirect	Selected	Selected

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

Setting	lax01m01esg01	lax01m01esg02
Name	Uplink02	Uplink02
Type	Uplink	Uplink
Connected To	lax01-m01-vds01-uplink02	lax01-m01-vds01-uplink02
Connectivity Status	Connected	Connected
Primary IP Address	172.27.15.3	172.27.15.2
Subnet Prefix Length	24	24
MTU	9000	9000
Send ICMP Redirect	Selected	Selected

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

Setting	lax01m01esg01	lax01m01esg02
Name	sfo01m01udlr01	sfo01m01udlr01
Type	Internal	Internal
Connected To	Universal Transit Network	Universal Transit Network
Connectivity Status	Connected	Connected
Primary IP Address	192.168.10.50	192.168.10.51
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 you entered and click **Finish**.

6 Repeat this procedure to configure another NSX edge using the settings for the second NSX Edge device.

7 Configure DRS affinity rules for the Edge Services Gateways.

a Go back to the **Home** page.

b In the **Navigator**, click **Hosts and Clusters**, and expand the **lax01m01vc01.lax01.rainpole.local** tree control.

c Select the **lax01-m01-mgmt01** cluster, and click the **Configure** tab.

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

e Click **Add**.

f In the **lax01-m01-mgmt01 - Create VM/Host Rule** dialog box, enter the following settings and click **Add**.

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

g In the **Add Rule Member** dialog box, select the check box next to each of the two, newly deployed NSX ESGs, and click **OK**.

h In the **lax01-m01-mgmt01 - Create VM/Host Rule** dialog box, click **OK**.

Disable the Firewall Service in Region B

Disable the firewall of the NSX Edge devices. This is required for equal-cost multi-path (ECMP) to operate correctly. Perform this procedure for each NSX Edge device.

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 Under **Inventories**, click **Networking & Security**.

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

4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.

5 Double-click the **lax01m01esg01** NSX Edge device.

6 Click the **Manage** tab and click **Firewall**.

7 On the Firewall page, click the **Stop** button.

8 Click the **Publish Changes** button.

9 Repeat this procedure for the NSX Edge device **lax01m01esg02**.

Enable and Configure Routing in Region B

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

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 Under **Inventories**, click **Networking & Security**.

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

4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.

5 Double-click the **lax01m01esg01** NSX Edge device.

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

7 On the **Global Configuration** page, enter the following settings.

   a Click the **Start** button for **ECMP**.

   b To configure dynamic routing, click the **Edit** button next to Dynamic Routing Configuration.

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

   d Click **Publish Changes**.

8 On the **Routing** tab, select **Static Routes** to configure it.

   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
MTU	9000
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
MTU	9000
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
MTU	9000
Admin Distance	210

   d Click **Publish Changes**.

9 On the **Routing** tab, select **BGP** to configure it.

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

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
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. You add two neighbors: the first Top of Rack Switch and the second Top of Rack Switch.

c In the **New Neighbor** dialog box, enter the following values for the first Top of Rack Switch, and click **OK**.

Setting	Value
IP Address	172.27.14.1
Remote AS	65002
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, whose IP address is 172.27.15.1.

e In the **New Neighbor** dialog box, enter the following values for the second Top of Rack Switch, and click **OK**.

Setting	Value
IP Address	172.27.15.1
Remote AS	65002
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 (lax01m01udlr01) 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
Weight	10
Keep Alive Time	1
Hold Down Time	3
Password	*BGP_password*

h Click **Publish Changes**.

The three neighbors you added are now visible in the **Neighbors** table.

10 On the **Routing** tab, select **Route Redistribution** to configure it.

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 is now visible in the **Route Redistribution** table.

11 Repeat this procedure for the lax01m01esg02 NSX Edge.

Verify Peering of Upstream Switches and Establishment of BGP in Region B

The NSX Edge devices must establish a connection to each of its upstream BGP switches before BGP updates can be exchanged. Verify that the NSX Edges devices are successfully peering, and that BGP routing has been established.

You repeat this procedure two times for each of the NSX Edge devices: lax01m01esg01 and lax01m01esg02.

Procedure

1 Log in to the NSX Edge device using a Secure Shell (SSH) client.

   a Open an SSH connection to the **lax01m01esg01** NSX Edge device.

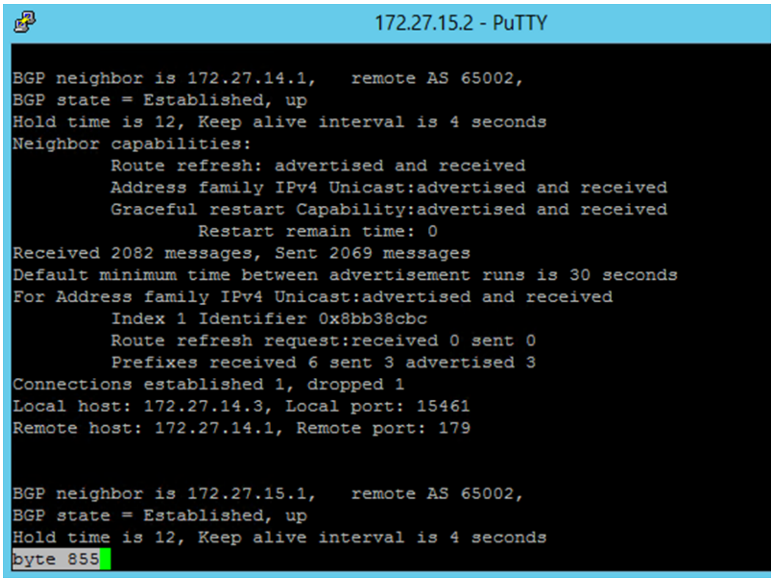
   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*edge_admin_password*

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

The BGP State displays `Established, UP` if you have peered with the upstream switches.

Note You have not yet configured the universal distributed logical router (UDLR), the BGP State does not display the `Established, UP` status message.

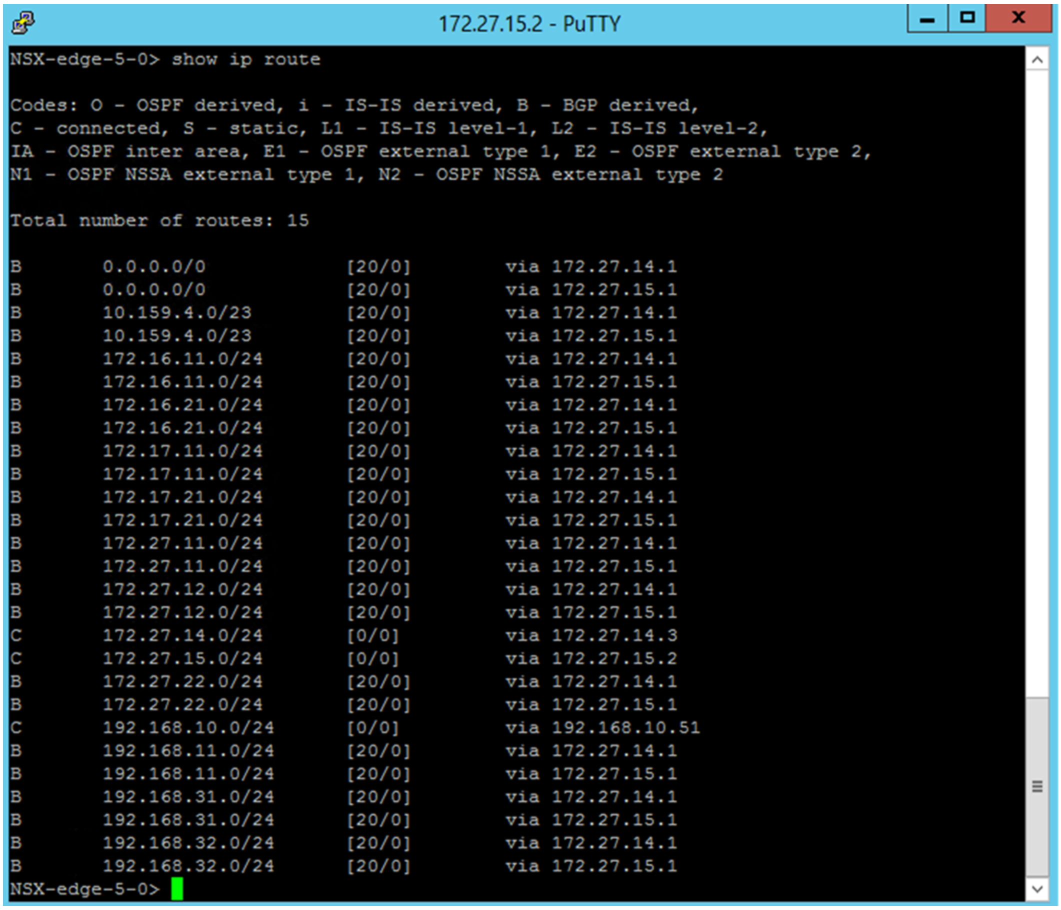


```
BGP neighbor is 172.27.14.1,   remote AS 65002,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
Neighbor capabilities:
         Route refresh: advertised and received
         Address family IPv4 Unicast:advertised and received
         Graceful restart Capability:advertised and received
                 Restart remain time: 0
Received 2082 messages, Sent 2069 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
         Index 1 Identifier 0x8bb38cbc
         Route refresh request:received 0 sent 0
         Prefixes received 6 sent 3 advertised 3
Connections established 1, dropped 1
Local host: 172.27.14.3, Local port: 15461
Remote host: 172.27.14.1, Remote port: 179


BGP neighbor is 172.27.15.1,   remote AS 65002,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
byte 855
```

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

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 following image there are two different routes to the following BGP networks: `0.0.0.0/0` and `172.27.22.0/24`. 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: 15

B       0.0.0.0/0            [20/0]        via 172.27.14.1
B       0.0.0.0/0            [20/0]        via 172.27.15.1
B       10.159.4.0/23        [20/0]        via 172.27.14.1
B       10.159.4.0/23        [20/0]        via 172.27.15.1
B       172.16.11.0/24       [20/0]        via 172.27.14.1
B       172.16.11.0/24       [20/0]        via 172.27.15.1
B       172.16.21.0/24       [20/0]        via 172.27.14.1
B       172.16.21.0/24       [20/0]        via 172.27.15.1
B       172.17.11.0/24       [20/0]        via 172.27.14.1
B       172.17.11.0/24       [20/0]        via 172.27.15.1
B       172.17.21.0/24       [20/0]        via 172.27.14.1
B       172.17.21.0/24       [20/0]        via 172.27.15.1
B       172.27.11.0/24       [20/0]        via 172.27.14.1
B       172.27.11.0/24       [20/0]        via 172.27.15.1
B       172.27.12.0/24       [20/0]        via 172.27.14.1
B       172.27.12.0/24       [20/0]        via 172.27.15.1
C       172.27.14.0/24       [0/0]         via 172.27.14.3
C       172.27.15.0/24       [0/0]         via 172.27.15.2
B       172.27.22.0/24       [20/0]        via 172.27.14.1
B       172.27.22.0/24       [20/0]        via 172.27.15.1
C       192.168.10.0/24      [0/0]         via 192.168.10.51
B       192.168.11.0/24      [20/0]        via 172.27.14.1
B       192.168.11.0/24      [20/0]        via 172.27.15.1
B       192.168.31.0/24      [20/0]        via 172.27.14.1
B       192.168.31.0/24      [20/0]        via 172.27.15.1
B       192.168.32.0/24      [20/0]        via 172.27.14.1
B       192.168.32.0/24      [20/0]        via 172.27.15.1
NSX-edge-5-0>
```

4 Repeat this procedure for the NSX Edge device lax01m01esg02.

Configure Universal Distributed Logical Router for Dynamic Routing in Region B

Configure the universal distributed logical router (UDLR) to use dynamic routing in Region B.

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 Under Inventories, click **Networking & Security**.

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

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

5 Configure the Universal Distributed Logical Router.

   a Double-click **sfo01m01udlr01**.

   b Click the **Manage** tab, click **Routing**, and select **BGP**.

   c On the **BGP** page, click the **Add Neighbor** icon.

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

   Repeat two times to configure the UDLR for both NSX Edge devices: lax01m01esg01 and lax01m01esg02.

Setting	lax01m01esg01 Value	lax01m01esg02 Value
IP Address	192.168.10.50	192.168.10.51
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	10	10
Keep Alive Time	1	1
Hold Down Time	3	3
Password	*BGP_password*	*BGP_password*

   e Click **Publish Changes**.

Verify Establishment of BGP for the Universal Distributed Logical Router in Region B

Verify that the UDLR is successfully peering, and that BGP routing has been established.

Procedure

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

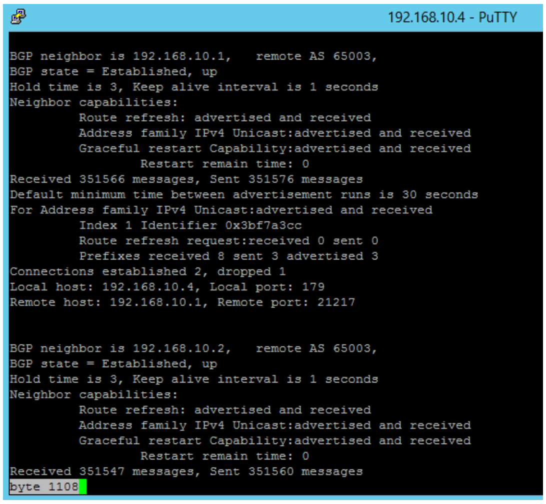
   a Open an SSH connection to `sfo01m01udlr01`, the UDLR whose peering and BGP configuration you want to verify.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*udlr_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 Edge Service Gateway.

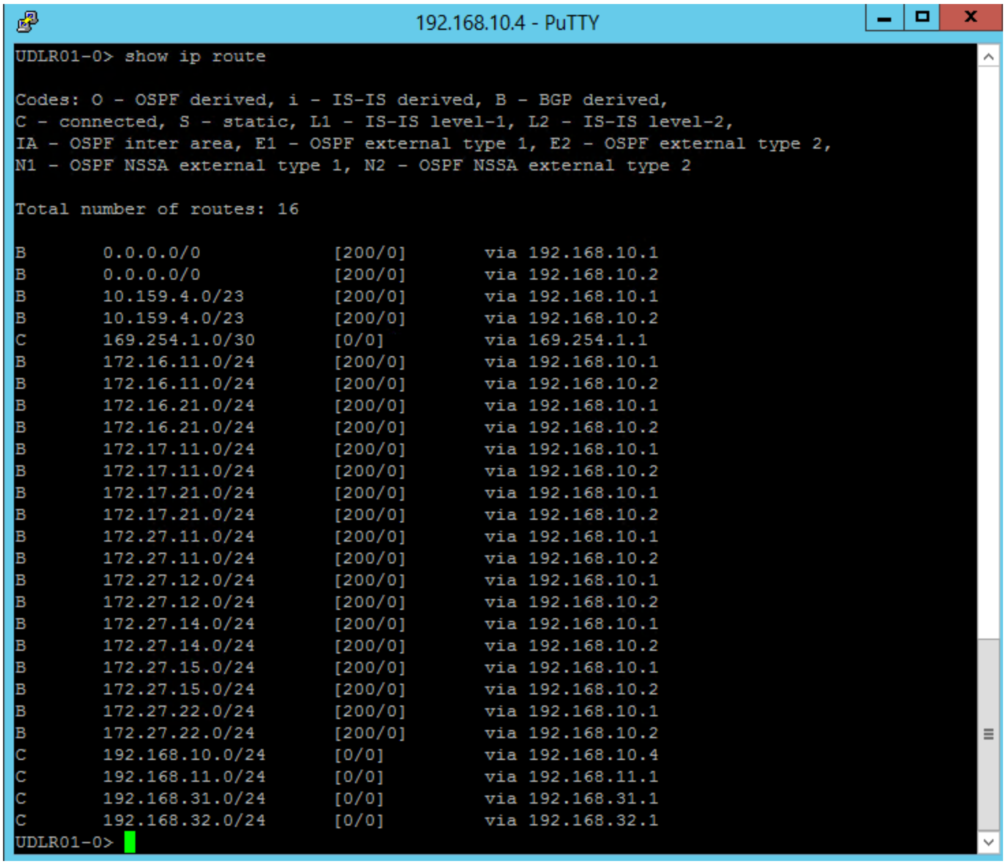


```
BGP neighbor is 192.168.10.1,   remote AS 65003,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
         Route refresh: advertised and received
         Address family IPv4 Unicast:advertised and received
         Graceful restart Capability:advertised and received
                 Restart remain time: 0
Received 351566 messages, Sent 351576 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
         Index 1 Identifier 0x3bf7a3cc
         Route refresh request:received 0 sent 0
         Prefixes received 8 sent 3 advertised 3
Connections established 2, dropped 1
Local host: 192.168.10.4, Local port: 179
Remote host: 192.168.10.1, Remote port: 21217


BGP neighbor is 192.168.10.2,   remote AS 65003,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 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 351547 messages, Sent 351560 messages
byte 1108
```

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

The letter B before the route indicates that BGP is used.



```
UDLR01-0> 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: 16

B       0.0.0.0/0            [200/0]       via 192.168.10.1
B       0.0.0.0/0            [200/0]       via 192.168.10.2
B       10.159.4.0/23        [200/0]       via 192.168.10.1
B       10.159.4.0/23        [200/0]       via 192.168.10.2
C       169.254.1.0/30       [0/0]         via 169.254.1.1
B       172.16.11.0/24       [200/0]       via 192.168.10.1
B       172.16.11.0/24       [200/0]       via 192.168.10.2
B       172.16.21.0/24       [200/0]       via 192.168.10.1
B       172.16.21.0/24       [200/0]       via 192.168.10.2
B       172.17.11.0/24       [200/0]       via 192.168.10.1
B       172.17.11.0/24       [200/0]       via 192.168.10.2
B       172.17.21.0/24       [200/0]       via 192.168.10.1
B       172.17.21.0/24       [200/0]       via 192.168.10.2
B       172.27.11.0/24       [200/0]       via 192.168.10.1
B       172.27.11.0/24       [200/0]       via 192.168.10.2
B       172.27.12.0/24       [200/0]       via 192.168.10.1
B       172.27.12.0/24       [200/0]       via 192.168.10.2
B       172.27.14.0/24       [200/0]       via 192.168.10.1
B       172.27.14.0/24       [200/0]       via 192.168.10.2
B       172.27.15.0/24       [200/0]       via 192.168.10.1
B       172.27.15.0/24       [200/0]       via 192.168.10.2
B       172.27.22.0/24       [200/0]       via 192.168.10.1
B       172.27.22.0/24       [200/0]       via 192.168.10.2
C       192.168.10.0/24      [0/0]         via 192.168.10.4
C       192.168.11.0/24      [0/0]         via 192.168.11.1
C       192.168.31.0/24      [0/0]         via 192.168.31.1
C       192.168.32.0/24      [0/0]         via 192.168.32.1
UDLR01-0>
```

Configure Static Routes on the Universal Distributed Logical Router in Region B

Configure the universal distributed logical router (UDLR) to use static routes for routing to the management servers in Region B.

Procedure

1. Log in to vCenter Server by using the vSphere Web Client.
   1. Open a Web browser and go to **`https://lax01m01vc01.lax01.rainpole.local/vsphere-client`**.
   2. Log in using the following credentials.

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

2. Configure the Universal Distributed Logical Router static routes.
   1. Under **Inventories**, click **Networking and Security**.
   2. In the **Navigator**, click **NSX Edges**.
   3. Select **172.16.11.65** from the **NSX Manager** drop-down menu.
   4. Double-click **sfo01m01udlr01**.
   5. Click the **Manage** tab, click **Routing**, and select **Static Routes**.
   6. On the **Static Routes** page, click the **Add** button.
   7. In the **Add Static Route** dialog box, enter the following values and click **OK**.

Setting	Value
Network	172.17.11.0/24
Next Hop	192.168.10.50,192.168.10.51
MTU	9000
Admin Distance	1

   8. Click **Publish Changes**.

Update Distributed Firewall for Region B

After deploying the vCenter Server you must add it to the distributed firewall exclusion list. The default rule in Region B must be changed to deny.

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 Exclude vCenter Server in Region B from firewall protection.

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

  b Click **Firewall** and select the **Exclustion List** tab.

  c Select 17.17.11.65 from the NSX Manager drop-down menu.

  d Click the **Add** button.

  e Add **lax01m01vc01** to the **Selected Objects list** and click **OK**.

3 Change the default rule action from **Allow** to **Block** for Region B.

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

  b From the **NSX Manager** drop-down menu, select **172.17.11.65**.

  c Under **Default Section Layer3**, in the **Action** column for the Default Rule, change the action to **Block**.

  d Click **Publish Changes**.

Test the Management Cluster NSX Configuration in Region B

Test the configuration of the NSX logical network using a ping test. A ping test checks if two hosts in a network can reach each other.

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 Use the Ping Monitor to test connectivity.

   a Under **Logical Switches**, double-click **Universal Transit Network**.

   b Click the **Monitor** tab.

   c From the **Source host** drop-down menu, select **lax01m01esx01.lax01.rainpole.local**.

   d From the **Destination host** drop-down menu, select **lax01m01esx03.lax01.rainpole.local**.

   e Click **Start Test**.

   The host-to-host ping test results are displayed in the **Results** text box. Verify that there are no error messages.

Test the Management Clusters Routing Failover

After the clusters are fully configured in Region A and Region B, verify that the network connectivity between them works as expected.

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 Shut down the NSX Edge service gateways in Region A.

   a In the **Navigator**, click **Hosts and Clusters**.

   b Expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree**.**

   c Right-click **sfo01m01esg01-0** and select **Power > Shut Down Guest OS**.

   d Right-click **sfo01m01esg02-0** and select **Power > Shut Down Guest OS**.

3 Log in to the universal distributed logical router by using a Secure Shell (SSH) client and verify the BGP routing state.

   a Open an SSH connection to `sfo01m01udlr01`.

   b Log in using the following credentials.

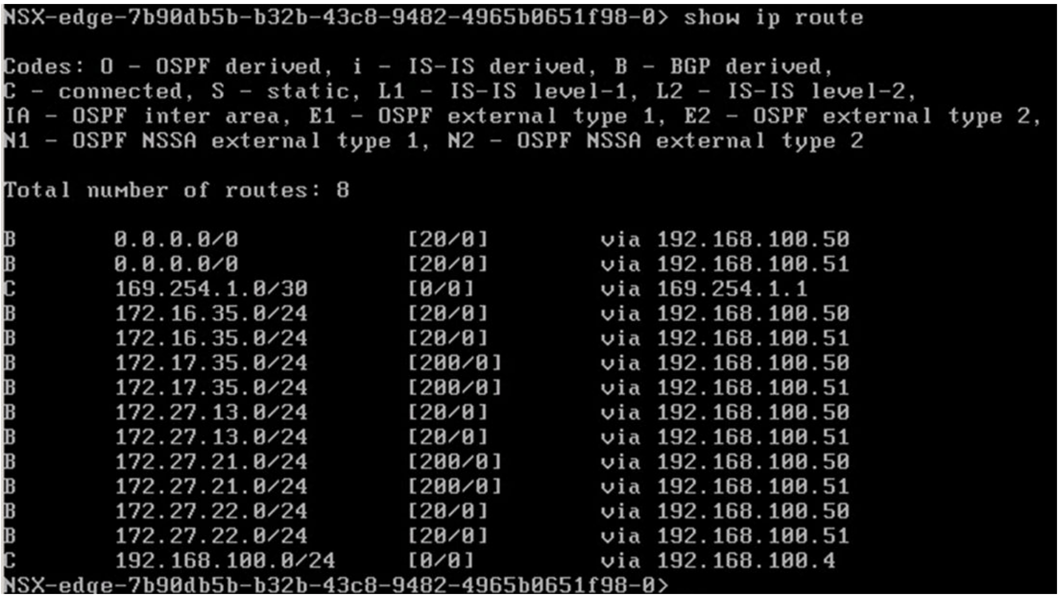
Setting	Value
User name	admin
Password	*udlr_admin_password*

c Run the `show ip route` command to verify that you are receiving routes via BGP.

  The letter `B` before the route indicates that BGP is used.

d Verify that multiple routes to BGP learned networks exist.

e Verify that routes come from Region B's ESGs.



```
NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0> 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: 8

B       0.0.0.0/0            [20/0]        via 192.168.100.50
B       0.0.0.0/0            [20/0]        via 192.168.100.51
C       169.254.1.0/30       [0/0]         via 169.254.1.1
B       172.16.35.0/24       [20/0]        via 192.168.100.50
B       172.16.35.0/24       [20/0]        via 192.168.100.51
B       172.17.35.0/24       [200/0]       via 192.168.100.50
B       172.17.35.0/24       [200/0]       via 192.168.100.51
B       172.27.13.0/24       [20/0]        via 192.168.100.50
B       172.27.13.0/24       [20/0]        via 192.168.100.51
B       172.27.21.0/24       [200/0]       via 192.168.100.50
B       172.27.21.0/24       [200/0]       via 192.168.100.51
B       172.27.22.0/24       [20/0]        via 192.168.100.50
B       172.27.22.0/24       [20/0]        via 192.168.100.51
C       192.168.100.0/24     [0/0]         via 192.168.100.4
NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0>
```

4 Power on the NSX Edge services gateways in Region A.

a In the **Navigator**, click **Hosts and Clusters**.

b Expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree**.**

c Right-click **sfo01m01esg01-0** and select **Power > Power On**.

d Right-click **sfo01m01esg02-0** and select **Power > Power On**.

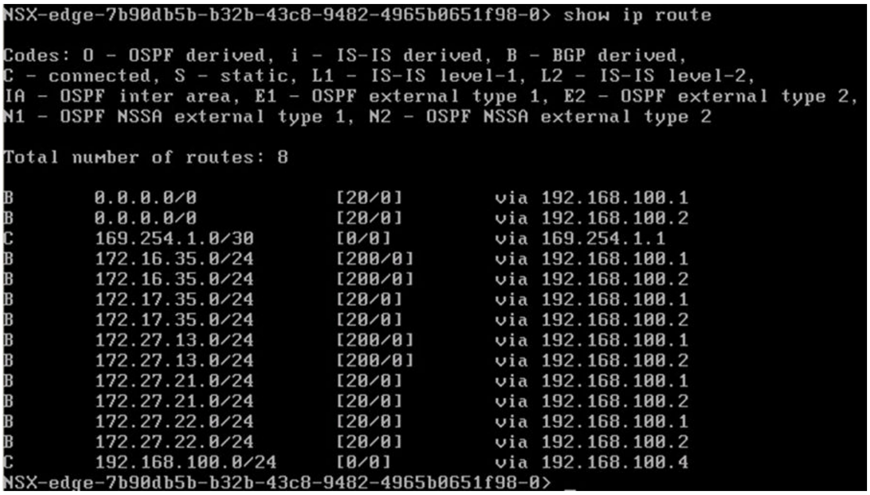
5 Verify the new state of the BGP routing.

   a Go back to the SSH connection to **sfo01m01udlr01** and run the `show ip route` command.

   b Verify that you receive routes via BGP.

      The letter B before the route indicates that BGP is used.

   c Verify that you have multiple routes to BGP learned networks and that routes also come from the NSX Edge services gateways in Region A.



```
NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0> 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: 8

B       0.0.0.0/0           [20/0]        via 192.168.100.1
B       0.0.0.0/0           [20/0]        via 192.168.100.2
C       169.254.1.0/30      [0/0]         via 169.254.1.1
B       172.16.35.0/24      [200/0]       via 192.168.100.1
B       172.16.35.0/24      [200/0]       via 192.168.100.2
B       172.17.35.0/24      [20/0]        via 192.168.100.1
B       172.17.35.0/24      [20/0]        via 192.168.100.2
B       172.27.13.0/24      [200/0]       via 192.168.100.1
B       172.27.13.0/24      [200/0]       via 192.168.100.2
B       172.27.21.0/24      [20/0]        via 192.168.100.1
B       172.27.21.0/24      [20/0]        via 192.168.100.2
B       172.27.22.0/24      [20/0]        via 192.168.100.1
B       172.27.22.0/24      [20/0]        via 192.168.100.2
C       192.168.100.0/24    [0/0]         via 192.168.100.4
NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0> _
```

Deploy Application Virtual Networks in Region B

Deploy the application virtual networks for the region.

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 Create a Universal Logical Switch for workloads specific to Region B.

   a Under **Inventories**, click **Networking & Security**.

   b In the **Navigator**, click **Logical Switches**.

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

d Click the **Add** icon to create a new Logical Switch.

e In the **New Logical Switch** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	Mgmt-RegionB01-VXLAN
Transport Zone	Mgmt Universal Transport Zone
Replication Mode	Hybrid

3 Connect the Mgmt-RegionB01-VXLAN to the **sfo01m01udlr01** Universal Distributed Logical Router.

a On the **Logical Switches** page, select the **Mgmt-RegionB01-VXLAN** logical switch.

b Click the **Connect Edge** icon.

c On the **Connect an Edge** page, select **sfo01m01udlr01** and click **Next**.

d On the **Edit NSX Edge Interface** page, enter the following settings and click **Next**.

Setting	Value
Name	Mgmt-RegionB01-VXLAN
Type	Internal
Connectivity Status	Connected
Primary IP Address	192.168.32.1
Subnet Prefix Length	24

e On the Ready to Complete page click **Finish**.

4 Configure the MTU for the Logical Switches.

a In the **Navigator**, select **NSX Edges**.

b Double-click sfo01m01udlr01.

c Click the **Manage** tab and click **Settings**.

d On the **Settings** page, click on **Interfaces**.

e Under **Interfaces**, select **Mgmt-RegionB01-VXLAN**, and click **Edit**.

f On the **Edit Logical Router Interface**, enter 9000 for the **MTU**, and click **OK**.

Deploy the NSX Load Balancer in Region B

Deploy a load balancer for use by management applications connected to the application virtual network Mgmt-xRegion01-VXLAN.

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 Under **Inventories**, click **Networking Security**.

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

4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.

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

6 On the **Name and Description** page, enter the following settings, and click **Next**.

Setting	Value
Install Type	Edge Services Gateway
Name	lax01m01lb01
Hostname	lax01m01lb01.lax01.rainpole.local
Deploy NSX Edge	Selected
Enable High Availability	Selected

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

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

8 On the **Configure Deployment** page, perform the following configuration steps, and click **Next**.

   a Select **lax01-w01dc** from the **Datacenter** drop-down menu.

   b Select the **Large** radio button to specify the **Appliance Size**.

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

   Perform twice to add two NSX Edge appliances with the same settings.

Setting	Value
Resource pool	lax01-m01-mgmt01
Datastore	lax01-m01-vsan01
Folder	lax01-m01fd-nsx
Resource Reservation	System Managed

9 On the **Configure Interfaces** page, click the **Add** icon to configure the OneArmLB interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	OneArmLB
Type	Internal
Connected To	Mgmt-xRegion01-VXLAN
Connectivity Status	Connected
Primary IP Address	192.168.11.2
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

10 On the **Default Gateway Settings** page, click **Next**.

11 On the **Firewall and HA** page, select the following settings and click **Next**.

Setting	Value
Configure Firewall default policy	Selected
Default Traffic Policy	Accept
Logging	Disable
vNIC	any
Declare Dead Time	15

12 On the **Ready to Complete** page, review the configuration settings you entered and click**Finish**.

13 Enable HA logging.

   a In the **Navigator**, click **NSX Edges**.

   b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

   c Double-click the device labeled **lax01m01lb01**.

   d Click the **Manage** tab and click the **Settings** tab.

   e Click **Change** in the **HA Configuration** page.

   f Select the `Enable Logging` checkbox and click **OK**.

14 Configure the Default Gateway.

   a In the Navigator, click **NSX Edges**.

   b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

   c Double-click the device labeled **lax01m01lb01**.

   d Click the **Manage** tab and click the **Routing** tab.

   e Click the **Edit** button to configure the **Default Gateway** and enter **192.168.11.1**.

   f Click **Publish Changes**.

15 Disconnect the Load Balancer after the deployment.

   a In the **Navigator**, click **NSX Edges**.

   b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

   c Double-click the **lax01m01lb01** device.

   d Click the **Manage** tab and click the **Settings** tab.

   e Click **Interfaces**, select the **OneArmLB** virtualized Network Interface Card (vNIC), and click **Edit**.

   f In the **Edit NSX Edge Interface** dialog box, select **Disconnected** as **Connectivity Status**.

16 Enable the Load Balancer service.

   a In the **Navigator**, click **NSX Edges**.

   b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

   c Double-click the **lax01m01lb01** device.

   d Click the **Manage** tab and click the **Load Balancer** tab.

   e Select **Global Configuration** and click **Edit**.

   f In the **Edit Load Balancer Global Configuration** dialog box, select **Enable Load Balancer** and click **OK**.

Deploy and Configure the Shared Edge and Compute Cluster Components Region B

Deploy and configure the shared edge and compute cluster components.

Procedure

1 Deploy the Compute vCenter Server Instance in Region B

   You can now install the vCenter Server appliance and add the license.

2 Replace the Certificate of the Compute vCenter Server in Region B

To establish trusted connection with the other SDDC management components, you replace the machine SSL certificate on each vCenter Server instance in Region B with a custom certificate that is signed by the certificate authority (CA) available on the parent Active Directory (AD) server or on the intermediate Active Directory (AD) server.

3 Set SDDC Deployment Details on the Compute vCenter Server in Region B

Set an identity of your SDDC deployment on the Compute vCenter Server in Region B. You can also use this identity as a label in tools for automated SDDC deployment.

4 Add New vCenter Server Licenses in Region B

(Optional) If a license was not assigned during deployment of the Management vCenter Server and ESXi hosts, you can add new licenses for this vCenter Server instance if needed.

5 Add the Shared Edge and Compute vCenter to the vCenter Servers VM Group in Region B

After the vCenter Server for the Shared Edge and Computer cluster is deployed, you add it to the vCenter Server VM Group.

6 Exclude the Compute vCenter Server from the Distributed Firewall in Region B

Exclude vCenter Server from all of your distributed firewall rules. This ensures that network access between vCenter Server and NSX is not blocked.

7 Configure the Shared Edge and Compute Cluster in Region B

After you deploy the Compute vCenter Server, you must create and configure the shared edge and compute cluster.

8 Create a vSphere Distributed Switch for the Shared Edge and Compute Cluster in Region B

After all ESXi hosts have been added to the cluster, create a vSphere Distributed Switch.

9 Enable vSphere HA on the Shared Edge and Compute Cluster in Region B

Before creating the host profile for the shared edge and compute cluster, enable vSphere HA.

10 Configure SSH, NTP, and Advanced Options on the First ESXi Host in the Shared Edge and Compute Cluster in Region B

Time synchronization issues can result in serious problems with your environment. Configure NTP for each of your hosts in the management and the shared edge and compute clusters. Change the default ESX Admins group to achieve greater levels of security by removing a known administrative access point.

11 Mount NFS Storage for the Shared Edge and Compute Cluster in Region B

You must mount an NFS datastore for the content library consumed by vRealize Automation for virtual machine provisioning.

12 Create and Apply the Host Profile for the Shared Edge and Compute Cluster in Region B

Host Profiles ensure that all hosts in the cluster have the same configuration.

13 Configure Lockdown Mode on All ESXi Hosts in Region B

To increase security of your ESXi hosts, you put them in Lockdown mode, so that administrative operations can be performed only from vCenter Server.

14 Create the VM and Template Folders in Region B

Create folders to group objects of the same type for easier management.

Deploy the Compute vCenter Server Instance in Region B

You can now install the vCenter Server appliance and add the license.

Procedure

1 Start the **vCenter Server Appliance Deployment** wizard.

a Browse to the vCenter Server Appliance ISO file.

b Open the `<dvd-drive>:\vcsa-ui-installer\win32\Installer` application file.

2 Install - Stage 1: Complete the **vCenter Server Appliance Deployment** wizard.

a Click **Install** to start the installation.

b Click **Next** on the **Introduction** page.

c On the **End User License Agreement** page, select the **I accept the terms of the license agreement** check box and click **Next**.

d On the **Select deployment Type** page, select the **vCenter Server (Requires External Platform Services Controller)** radio button and click **Next**.

e On the **Appliance deployment target** page, enter the following settings and click **Next**.

Setting	Value
ESXi host or vCenter Server name	lax01m01vc01.lax01.rainpole.local
HTTPS port	443
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

f In the **Certificate Warning** dialog box, click **Yes** to accept the host certificate.

g On the **Select folder** page, select **lax01-m01fd-mgmt**.

h On the **Select compute resource** page, select the **lax01-m01-mgmt01** cluster.

i On the **Set up appliance VM** page, enter the following settings and click **Next**.

Setting	Value
Appliance name	lax01w01vc01
OS password	*compvc_root_password*
Confirm OS password	*compvc_root_password*

j On the **Select deployment size** page, select **Large vCenter Server** and click **Next**.

k On the **Select datastore** page, select the **lax01-m01-vsan01** datastore, select the **Enable Thin Disk Mode** check box, and click **Next**.

l On the **Configure network settings** page, enter the following settings and click **Next**.

Setting	Value
Network	lax01-m01-vds01-management
IP version	IPv4
IP assignment	Static
System name	lax01w01vc01.lax01.rainpole.local
IP address	172.17.11.64
Subnet mask or prefix length	255.255.255.0
Default gateway	172.17.11.253
DNS servers	172.17.11.5,172.17.11.4

m On the **Ready to complete stage 1** page, review the configuration and click **Finish** to start the deployment.

n When the deployment completes, click **Continue** to proceed to stage 2 of the installation.

3 Install - Stage 2: Complete the **Set Up vCenter Server Appliance** wizard.

a Click **Next** on the **Introduction** page.

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

Setting	Value
Time Synchronization mode	Synchronize time with NTP servers
NTP servers (comma-separated list)	ntp.lax01.rainpole.local
SSH access	Enabled

c On the **SSO configuration** page, enter the following settings and click **Next**.

Setting	Value
Platform Services Controller	lax01psc01.lax01.rainpole.local
HTTPS port	443
SSO domain name	vsphere.local
SSO password	*sso_password*

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

e Click **OK** on the Warning.

Replace the Certificate of the Compute vCenter Server in Region B

To establish trusted connection with the other SDDC management components, you replace the machine SSL certificate on each vCenter Server instance in Region B with a custom certificate that is signed by the certificate authority (CA) available on the parent Active Directory (AD) server or on the intermediate Active Directory (AD) server.

Table 2-9. Certificate-Related Files on the vCenter Server Instance

vCenter Server FQDN	Files for Certificate Replacement
lax01w01vc01.sfo01.rainpole.local	■ lax01w01vc01.key ■ lax01w01vc01.1.cer ■ Root64.cer

Prerequisites

- CA-signed certificate files generated by using VMware Validated Design Certificate Generation Utility (`CertGenVVD`). See the *VMware Validated Design Planning and Preparation* documentation.
- A Windows host with an SSH terminal access software such as PuTTY and an `scp` software such as WinSCP installed.

Procedure

1 Log in to Compute vCenter Server by using Secure Shell (SSH) client.

a Open an SSH connection to the virtual machine lax01w01vc01.lax01.rainpole.local.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

2 Change the vCenter Server appliance command shell to the Bash shell to allow secure copy (`scp`) connections for the root user.

```
shell
chsh -s "/bin/bash" root
```

3 Copy the generated certificates to the vCenter Server Appliance.

a Run the following command to create a new temporary folder.

```
mkdir -p /root/certs
```

b Copy the certificate files `lax01w01vc01.1.cer`, `lax01w01vc01.key`, and `Root64.cer` to the `/root/certs` folder.

You can use an `scp` software such as WinSCP.

4 Replace the CA-signed certificate on the vCenter Server instance.

a Start the vSphere Certificate Manager utility on the vCenter Server instance.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

b Select **Option 1 (Replace Machine SSL certificate with Custom Certificate)**, enter the default vCenter Single Sign-On user name **`administrator@vsphere.local`** and the ***`vsphere_admin_password`*** password.

c When prompted for the Infrastructure Server IP, enter the IP address of the Platform Services Controller that manages this vCenter Server instance.

Option	IP Address of Connected Platform Services Controller
lax01w01vc01.sfo01.rainpole.local	172.17.11.71

d Select **Option 2 (Import custom certificate(s) and key(s) to replace existing Machine SSL certificate)**.

e When prompted, provide the full path to the custom certificate, the root certificate file, and the key file that you copied over earlier, and confirm the import with **Yes (Y)**.

vCenter Server	Input to the vSphere Certificate Manager Utility
lax01w01vc01.sfo01.rainpole.local	Please provide valid custom certificate for Machine SSL. File : **`/root/certs/lax01w01vc01.1.cer`** Please provide valid custom key for Machine SSL. File : **`/root/certs/lax01w01vc01.key`** Please provide the signing certificate of the Machine SSL certificate. File : **`/root/certs/Root64.cer`**

5 After Status shows `100% Completed`, wait several minutes until all vCenter Server services are restarted.

6 Restart the vami-lighttp service to update the certificate on the virtual appliance management interface (VAMI) and to remove certificate files.

```
service vami-lighttp restart
cd /root/certs/
rm lax01w01vc01.1.cer lax01w01vc01.key Root64.cer
```

Set SDDC Deployment Details on the Compute vCenter Server in Region B

Set an identity of your SDDC deployment on the Compute vCenter Server in Region B. You can also use this identity as a label in tools for automated SDDC deployment.

Procedure

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

   a Open a Web browser and go to **`https://lax01w01vc01.lax01.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 of the vSphere Web Client, select **Global Inventory Lists**.

3 In the **Navigator**, click **vCenter Servers** under **Resources**.

4 Click the **lax01w01vc01.lax01.rainpole.local** vCenter Server object and click the **Configure** tab in the central pane.

5 Under the **Settings** pane, click **Advanced Settings** and click the **Edit** button.

6 In the **Edit Advanced vCenter Server Settings** dialog box, set the following value pairs one by one, clicking **Add** after each entry.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.2.0
config.SDDC.Deployed.WorkloadDomain	Management
config.SDDC.Deployed.Method	DIY
config.SDDC.Deployed.InstanceId	unique_identifier*

Note * To generate a unique identifier, use the Online UUID Generator website https://www.uuidgenerator.net/ and copy/paste the UUID into the config.SDDC.Deployed.InstanceId value. The Online UUID Generator is a universally unique identifier that generates random numbers using a secure random number generator.

7 Click **OK** to close the window.

Add New vCenter Server Licenses in Region B

(Optional) If a license was not assigned during deployment of the Management vCenter Server and ESXi hosts, you can add new licenses for this vCenter Server instance if needed.

Procedure

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

   a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 Click the **Home** icon above the **Navigator** and select the **Administration** menu item.

3 On the **Administration** page, click **Licenses** and click the **Licenses** tab.

4 Click the **Create New Licenses** icon to add license keys.

5 On the **Enter license keys** page, enter license keys for vCenter Server and ESXi, one per line, and click **Next**.

6 On the **Edit license name** page, enter a descriptive name for each license key, and click **Next**.

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

8 Assign the newly added licenses to the respective assets.

   a Click the **Assets** tab.

   b Select the vCenter Server instance, and click the **Assign License** icon.

   c Select the vCenter Server license that you entered in the previous step and click **OK**.

Add the Shared Edge and Compute vCenter to the vCenter Servers VM Group in Region B

After the vCenter Server for the Shared Edge and Computer cluster is deployed, you add it to the vCenter Server VM Group.

Add **lax01w01vc01** to the vCenter Servers VM Group.

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**, select **Hosts and Clusters** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

3 Select the **lax01-m01-mgmt01** cluster and click **Configure**.

4 On the **Configure** page, click **VM/Host Groups**.

5 On the **VM/Host Groups** page, select the **vCenter Servers** VM Group.

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

7 In the **Add Group Member** dialog, select **lax01w01vc01** and click **OK**.

8 In the **Navigator**, select **Hosts and Clusters** and expand the **lax01w01vc01.lax01.rainpole.local** tree.

Exclude the Compute vCenter Server from the Distributed Firewall in Region B

Exclude vCenter Server from all of your distributed firewall rules. This ensures that network access between vCenter Server and NSX is not blocked.

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, click **Networking & Security**.

3 Click **Firewall** and select the **Exclustion List** tab.

4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.

5 Click the **Add** button.

6 Add **lax01w01vc01** to the **Selected Objects** list, and click **OK**.

Configure the Shared Edge and Compute Cluster in Region B

After you deploy the Compute vCenter Server, you must create and configure the shared edge and compute cluster.

To create and configure the shared edge and compute cluster, you perform the following procedures:

- Create the cluster.
- Configure DRS.
- Add the hosts to the cluster.
- Add the hosts to the active directory domain.
- Create Resource Pools.

Procedure

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

   a Open a Web browser and go to **`https://lax01w01vc01.lax01.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 Datacenter object.

   a In the **Navigator**, click **Hosts and Clusters**.

   b Right-click the **lax01w01vc01.lax01.rainpole.local** instance and select **New Datacenter**.

   c In the **New Datacenter** dialog box, enter **`lax01-w01dc`** as name and click **OK**.

3 Create the shared edge and compute cluster.

   a Right-click the **lax01-w01dc** datacenter and click **New Cluster**.

   b In the **New Cluster** wizard, enter the following values and click **OK**.

Setting		Value
Name		lax01-w01-comp01
DRS	**Turn ON**	Selected
	Other DRS options	Default values
vSphere HA	**Turn ON**	Deselected
EVC		Set EVC mode to the lowest available setting supported for the hosts in the cluster
vSAN	**Turn ON**	Deselected

4 Add a host to the shared edge and compute cluster.

   a Right-click the **lax01-w01-comp01** cluster and click **Add Host**.

   b On the **Name and location** page, enter `lax01w01esx01.lax01.rainpole.local` in the **Host name or IP address** text box and click **Next**.

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

Setting	Value
User name	root
Password	*esxi_root_user_password*

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

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

   f On the **Assign license** page, select the ESXi license key, that you entered during the vCenter Server deployment, and click **Next**.

   g On the **Lockdown mode** page, click **Next**.

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

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

5 Repeat the previous step to add the remaining hosts to the cluster.

Setting	Value
Host 2	lax01w01esx02.lax01.rainpole.local
Host 3	lax01w01esx03.lax01.rainpole.local
Host 4	lax01w01esx04.lax01.rainpole.local

6 Add an ESXi host to the active directory domain.

   a In the **Navigator**, click **Hosts and Clusters** and expand the entire **lax01w01vc01.lax01.rainpole.local** tree.

   b Select the **lax01w01esx01.lax01.rainpole.local** host.

   c Click the **Configure** tab.

   d Under **System**, select **Authentication Services**.

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

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

Setting	Value
Domain	lax01.rainpole.local
User name	svc-domain-join@rainpole.local
Password	*svc-domain-join_password*

7 Set the Active Directory Service to **Start and stop with host**.

   a In the **Navigator**, click **Hosts and Clusters** and expand the entire **lax01w01vc01.lax01.rainpole.local** tree.

   b Select the **lax01w01esx01.lax01.rainpole.local** host.

   c Click the **Configure** tab.

   d Under **System**, select **Security Profile**.

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

   f Select the **Active Directory** service and change the **Startup Policy** to **Start and stop with host** and click **OK.**

8 Configure a resource pool for the shared edge and compute cluster.

   a Right-click the **lax01-w01-comp01** cluster and select **New Resource Pool**.

   b In the **New Resource Pool** dialog box, enter the following values and click **OK**.

Setting	Value
Name	lax01-w01rp-sddc-edge
CPU-Shares	High
CPU-Reservation	0
CPU-Reservation Type	Expandable selected
CPU-Limit	Unlimited
Memory-Shares	Normal
Memory-Reservation	16 GB
Memory-Reservation type	Expandable selected
Memory-Limit	Unlimited

9 Repeat step Step 8 to add two more additional resource pools.

Setting	Resource Pool 2	Resource Pool 3
Name	lax01-w01rp-user-edge	lax01-w01rp-user-vm
CPU-Shares	Normal	Normal
CPU-Reservation	0	0
CPU-Reservation Type	Expandable selected	Expandable selected
CPU-Limit	Unlimited	Unlimited
Memory-Shares	Normal	Normal
Memory-Reservation	0	0
Memory-Reservation type	Expandable selected	Expandable selected
Memory-Limit	Unlimited	Unlimited

Create a vSphere Distributed Switch for the Shared Edge and Compute Cluster in Region B

After all ESXi hosts have been added to the cluster, create a vSphere Distributed Switch.

Procedure

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

   a. Open a Web browser and go to **`https://lax01w01vc01.lax01.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 vSphere Distributed Switch for the shared edge and compute cluster.

   a. In the **Navigator**, click **Networking** and expand the **lax01w01vc01.lax01.rainpole.local** control tree.

   b. Right-click the **lax01-w01dc** datacenter and select **Distributed Switch > New Distributed Switch** to start the **New Distributed Switch** wizard.

   c. On the **Name and location** page, enter **`lax01-w01-vds01`** as the name, and click **Next**.

   d. On the **Select version** page, ensure the **Distributed switch version - 6.5.0** radio button is selected, and click **Next**.

   e. On the **Edit settings** page, enter the following values and click **Next**.

Setting	Value
Number of uplinks	2
Network I/O Control	Enabled
Create a default port group	Deselected

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

3. Edit the settings of the lax01-w01-vds01 distributed switch.

   a. Right-click the **lax01-w01-vds01** distributed switch and select **Settings > Edit Settings**.

   b. Click the **Advanced** tab.

   c. Enter **`9000`** as MTU (Bytes) value and click **OK**.

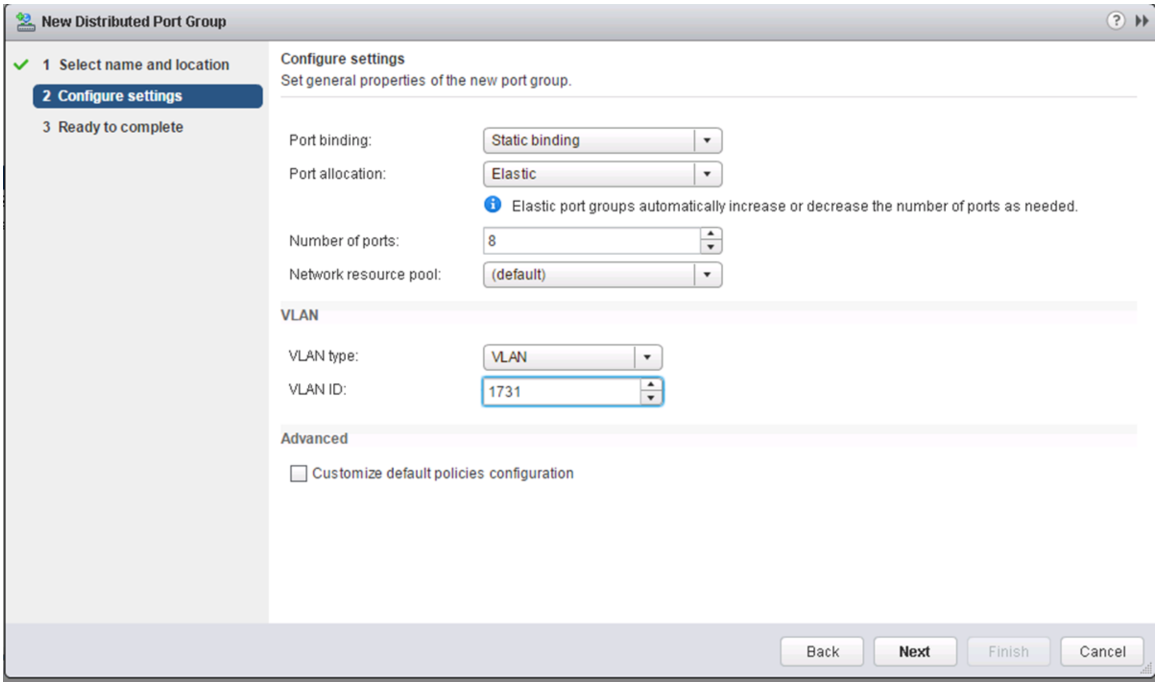
4 Create new port groups in the lax01-w01-vds01 distributed switch.

a Right-click the **lax01-w01-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
lax01-w01-vds01-management	Static binding	VLAN	1731
lax01-w01-vds01-vmotion	Static binding	VLAN	1732
lax01-w01-vds01-vsan	Static binding	VLAN	1733
lax01-w01-vds01-nfs	Static binding	VLAN	1725
lax01-w01-vds01-uplink01	Static binding	VLAN	1735
lax01-w01-vds01-uplink02	Static binding	VLAN	2721

Note You create the VXLAN port group during the configuration of NSX Manager.



Configure settings

Set general properties of the new port group.

Port binding: Static binding

Port allocation: Elastic

Elastic port groups automatically increase or decrease the number of ports as needed.

Number of ports: 8

Network resource pool: (default)

VLAN

VLAN type: VLAN

VLAN ID: 1731

Advanced

□ Customize default policies configuration

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

d Repeat this step for each port group.

5 Change Port Groups to use the Route Based on Physical NIC load teaming algorithm.

a Right-click the **lax01-w01-vds01** distributed switch and select **Distributed Port Groups > Manage Distributed Port Groups**.

b Select **Teaming and failover** and click **Next**.

c Click the **Select Distributed Port Groups** button, add all port groups, except lax01-w01-vds01-uplink01 and lax01-w01-vds01-uplink02, and click **Next**.

d Select **Route based on physical NIC load** under **Load Balancing** and click **Next**.

e Click **Finish**.

6 Configure the uplinks for the lax01-w01-vds01-uplink01 and lax01-w01-vds01-uplink02 port groups.

a Right click the **lax01-w01-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 **lax01-w01-vds01-uplink02** port group, and click **Edit Settings**.

e Select **Teaming and Failover**.

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

7 Connect the ESXi host, lax01w01esx01.lax01.rainpole.local, to the **lax01-w01-vds01** distributed switch by migrating its VMkernel and virtual machine network adapters.

a Right-click the **lax01-w01-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 **lax01w01esx01.lax01.rainpole.local** and click **OK**.

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

f On the **Select network adapter tasks** page, ensure both **Manage physical adapters** and **Manage VMkernel adapters** check boxes are checked 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 box, select **Uplink 1** and click **OK**.

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

8 Configure the VMkernel network adapters by editing the existing adapter and adding new adapters as needed.

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

b Select **lax01-w01-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 **lax01-w01-vds01-nfs** port group, click **OK**, and click **Next**.

e On the **Port properties** page, click **Next**.

f Under **IPv4 settings**, select **Use static IPv4 settings**, enter the IP address `172.17.25.101`, enter the subnet `255.255.255.0`, and click **Next**.

   g Click **Finish**.

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

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

9 Create the vMotion VMkernel adapter.

   a In the **Navigator**, click **Host and Clusters** and expand the **lax01w01vc01.lax01.rainpole.local** tree.

   b Click on **lax01w01esx01.lax01.rainpole.local**.

   c Click the **Configure** tab, then select **VMkernel adapters**.

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

   e On the **Add Networking** page, select **Select an existing network**, browse to select the **lax01-w01-vds01-vmotion** port group, click **OK**, and click **Next**.

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

   g Under **IPv4 settings**, select **Use static IPv4 settings**, enter the IP address `172.17.32.101`, enter the subnet `255.255.255.0`, and click **Next**.

   h Click **Finish**.

10 Configure the MTU on the vMotion VMkernel adapter.

   a Select the vMotion VMkernel adapter 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**.

11 Configure the vMotion TCP/IP stack.

   a Click **TCP/IP configuration**.

   b Select **vMotion** and click the **edit** icon.

   c Click **Routing**, enter `172.17.32.253` for the **default gateway** address, and click **OK**.

12 Define Network I/O Control shares for the different traffic types on the **lax01-w01-vds01** distributed switch.

   a In the **Navigator**, click **Networking** and click the **lax01-w01dc** datacenter.

   b Click the **lax01-w01-vds01** distributed switch.

c Click the **Configure** tab and click **Resource Allocation > System traffic**.

d Under **System Traffic**, edit each of the following traffic types with the values from the table.

Traffic Types	Shares
vSAN Traffic	Low
NFS Traffic	Low
vMotion Traffic	Low
vSphere Replication Traffic	Low
Management Traffic	Normal
vSphere Data Protection Backup Traffic	Low
Virtual Machine Traffic	High
Fault Tolerance Traffic	Low
iSCSI Traffic	Low

13 Migrate the last physical adapter from the standard switch to the lax01-w01-vds01 distributed switch.

a In the **Navigator**, click **Networking** and expand the **lax01-w01dc** datacenter.

b Right-click the **lax01-w01-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 box, select **lax01w01esx01.lax01.rainpole.local** and click **OK**.

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

g On the **Select network adapter tasks** page, select **Manage Physical adapters** and click **Next**.

h On the **Manage physical network adapters** page, under **lax01w01esx01.lax01.rainpole.local**, select **vmnic0** and click **Assign uplink**.

i In the **Select an Uplink** dialog box, select **Uplink 2** and click **OK**.

j On the **Analyze Impact** page, click **Next**.

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

14 Enable vSphere Distributed Switch Health Check.

a In the **Navigator**, click **Networking** and expand the **lax01-w01dc** datacenter.

b Select the **lax01-w01-vds01** distributed switch and click the **Configure** tab.

c In the **Navigator**, select **Health check** and click the **Edit** button.

d For **VLAN and MTU** and **Teaming and failover**, select **Enabled** and click **OK**.

15 Delete the vSphere Standard Switch.

   a In the **Navigator**, click on **Hosts and Clusters** and expand the **lax01w01vc01.lax01.rainpole.local** tree.

   b Select **lax01w01esx01.lax01.rainpole.local** and click **Configure**.

   c On the **Configure** page, select **Virtual Switches**.

   d On the **Virtual Switches** page, select **vSwitch0** and click the **Remove selected switch** button.

   e In the **Remove Standard Switch** dialog box, click **Yes**.

Enable vSphere HA on the Shared Edge and Compute Cluster in Region B

Before creating the host profile for the shared edge and compute cluster, enable vSphere HA.

Procedure

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

   a Open a Web browser and go to `https://lax01w01vc01.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, click Hosts and Clusters.

   a Expand the **lax01w01vc01.lax01.rainpole.local** inventory.

   b Select the **lax01-w01-comp01** cluster.

3 Click the **Configure** tab and click **vSphere Availability.**

4 Click **Edit**.

5 In the **Edit Cluster Settings** dialog box, select the **Turn on vSphere HA** check box.

6 In the **Edit Cluster Settings** dialog box, under **Failures and Responses**, select the following values.

Setting	Value
Enable Host Monitoring	Selected
Host Failure Response	Restart VMs
Response for Host Isolation	Power off and restart VMs
Datastore with PDL	Disabled
Datastore with APD	Disabled
VM Monitoring	VM Monitoring Only

7 Click **Admission Control**.

8 Under the **Admission Control** settings, enter the following settings.

Setting	Value
Host failures cluster tolerates	1
Define host failover capacity by	Cluster resource percentage
Override calculated failover capacity	Deselected
Performance degradation VMs tolerate	100%

9 Click **OK**.

Configure SSH, NTP, and Advanced Options on the First ESXi Host in the Shared Edge and Compute Cluster in Region B

Time synchronization issues can result in serious problems with your environment. Configure NTP for each of your hosts in the management and the shared edge and compute clusters. Change the default ESX Admins group to achieve greater levels of security by removing a known administrative access point.

Procedure

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

a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

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

2 Enable SSH and NTP.

a In the **Navigator**, click **Hosts and Clusters** and expand the **lax01w01vc01.lax01.rainpole.local** tree.

b Select the **lax01w01esx01.lax01.rainpole.local** host.

c Click the **Configure** tab and under **System**, click **Security Profile**.

d Under the **Services** section, click the **Edit** button.

e In the **Edit Security Profile** dialog box, select **SSH**, select **Start and stop with host** from the **Startup Policy** drop-down list, and click the **Start** button.

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

g Click **OK** to save the changes.

3 Configure the NTP Daemon (ntpd) options.

  a In the **Navigator**, click **Hosts and Clusters** and expand the **lax01w01vc01.lax01.rainpole.local** tree.

  b Select the **lax01w01esx01.sfo01.rainpole.local** host.

  c Click the **Configure** tab and under **System**, click **Time Configuration**.

  d In the **Edit Time Configuration** dialog box, select the **Use Network Time Protocol (Enable NTP client)** radio button, change the **NTP service startup policy** to **Start and stop with host**, enter **`ntp.lax01.rainpole.local,ntp.sfo01.rainpole.local`** as **NTP servers**, and click the **Start** button.

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

4 Change the default ESX Admins group.

  a In the **Navigator**, click **Hosts and Clusters**.

  b Expand the **lax01w01vc01.lax01.rainpole.local** vCenter inventory tree, and select the **lax01w01esx01.lax01.rainpole.local** host.

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

  d Click the **Edit** button.

  e In the filter box, enter **`esxAdmins`** and wait for the search results.

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

5 Disable the SSH warning banner.

  a In the **Navigator**, click **Hosts and Clusters**.

  b Expand the **lax01w01vc01.lax01.rainpole.local** vCenter inventory tree, and select the **lax01w01esx01.lax01.rainpole.local** host.

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

  d Click the **Edit** button.

  e In the filter box, enter **`ssh`** and wait for the search results.

  f Change the value of **UserVars.SuppressShellWarning** to **1** and click **OK**.

Mount NFS Storage for the Shared Edge and Compute Cluster in Region B

You must mount an NFS datastore for the content library consumed by vRealize Automation for virtual machine provisioning.

Procedure

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

   a Open a Web browser and go to `https://lax01w01vc01.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**, click **Hosts and Clusters** and expand the **lax01w01vc01.lax01.rainpole.local**.

3 Click on **lax01w01esx01.lax01.rainpole.local**.

4 Click on the **Datastores** tab.

5 Click the **Create a New Datastore** icon.

The **New Datastore** wizard opens.

6 On the **Type** page, select **NFS** and click **Next**.

7 On the **NFS version** page, select **NFS 3** and click **Next.**

8 On the **Name and configuration** page, enter the following datastore information and click **Next**.

Setting	Value
Datastore Name	lax01-w01-lib01
Folder	/V2D_vRA_ComputeB_1TB
server	172.17.25.251

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

Create and Apply the Host Profile for the Shared Edge and Compute Cluster in Region B

Host Profiles ensure that all hosts in the cluster have the same configuration.

Procedure

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

   a Open a Web browser and go to `https://lax01w01vc01.lax01.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 lax01w01esx01.lax01.rainpole.local.

   a In the **Navigator**, select **Hosts and Clusters** and expand the **lax01w01vc01.lax01.rainpole.local** tree.

   b Right-click **lax01w01esx01.lax01.rainpole.local** and select **Host Profiles > Extract Host Profile**.

   c In the **Extract Host Profile** page, enter `lax01-w01hp-comp01` for the **Name** and click **Next**.

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

3 Attach the Host Profile to the shared edge and compute cluster.

   a In the **Navigator**, select **Hosts and Clusters** and expand the **lax01w01vc01.lax01.rainpole.local** tree.

   b Right Click on the **lax01-w01-comp01** cluster and select**Host Profiles > Attach Host Profile**.

   c In the **Attach Host Profile** window, select the **lax01-w01hp-comp01** Host Profile, select the **Skip Host Customization** checkbox, and click **Finish**.

4 Create Host Customizations for the hosts in the shared edge and compute cluster.

   a In the **Navigator**, select **Policies and Profiles**.

   b Click on **Host Profiles**, then right-click on **lax01-w01hp-comp01**, and select **Export Host Customizations**.

   c In the dialog box, click **Save**.

   d Select file location to save the *lax01-w01hp-comp01_host_customizations.csv* file.

   e Open the *lax01-w01hp-comp01_host_customizations.csv* in Excel.

f Edit the file using the following configuration values.

ESXi Host	Active Directory Configuration Password	Active Directory Configuration Username	NetStack Instance defaultTcpipStack->DNS configuration Name for this host
lax01w01esx01.lax01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	lax01w01esx01
lax01w01esx02.lax01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	lax01w01esx02
lax01w01esx03.lax01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	lax01w01esx03
lax01w01esx04.lax01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	lax01w01esx04

ESXi Host	Host virtual NIC lax01-w01-vds01:lax01-w01-vds01-management:management->IP address settings IPv4 address	Host virtual NIC lax01-w01-vds01:lax01-w01-vds01-management:management->IP address settings SubnetMask
lax01w01esx01.lax01.rainpole.local	172.17.31.101	255.255.255.0
lax01w01esx02.lax01.rainpole.local	172.17.31.102	255.255.255.0
lax01w01esx03.lax01.rainpole.local	172.17.31.103	255.255.255.0
lax01w01esx04.lax01.rainpole.local	172.17.31.104	255.255.255.0

ESXi Host	Host virtual NIC lax01-w01-vds01:lax01-w01-vds01-nfs:<UNRESOLVED>->IP address settings IPv4 address	Host virtual NIC lax01-w01-vds01:lax01-w01-vds01-nfs:<UNRESOLVED>->IP address settings SubnetMask
lax01w01esx01.lax01.rainpole.local	172.17.25.101	255.255.255.0
lax01w01esx02.lax01.rainpole.local	172.17.25.102	255.255.255.0
lax01w01esx03.lax01.rainpole.local	172.17.25.103	255.255.255.0
lax01w01esx04.lax01.rainpole.local	172.17.25.104	255.255.255.0

ESXi Host	Host virtual NIC lax01-w01-vds01:lax01-w01-vds01-vmotion:vmotion->IP address settings IPv4 address	Host virtual NIC lax01-w01-vds01:lax01-w01-vds01-vmotion:vmotion->IP address settings SubnetMask
lax01w01esx01.lax01.rainpole.local	172.17.32.101	255.255.255.0
lax01w01esx02.lax01.rainpole.local	172.17.32.102	255.255.255.0
lax01w01esx03.lax01.rainpole.local	172.17.32.103	255.255.255.0
lax01w01esx04.lax01.rainpole.local	172.17.32.104	255.255.255.0

   g When the file is updated, save it and close Excel.

   h Click the **Configure** tab.

   i Click the **Edit Host Customizations** button.

   j In the **Edit Host Customizations** window, select all hosts and click **Next**.

   k To use the customization file, click the **Browse** button, locate the *lax01-w01hp-comp01_host_customizations.csv* file, select it, click **Open**, and click **Finish**.

5 Remediate the hosts in the shared edge and compute cluster

   a Click the **Monitor** tab and click **Compliance**.

   b Select **lax01-w01-comp01** and click the **Check Host Profile Compliance** button.

   c Select **lax01w01esx02.lax01.rainpole.local** and click the **Remediate host based on its host profile** button.

   d Select **lax01w01esx03.lax01.rainpole.local** and click the **Remediate host based on its host profile** button.

   e Select **lax01w01esx04.lax01.rainpole.local** and click the **Remediate host based on its host profile** button.

   Note All hosts must show a status of `Compliant`.

6 Schedule nightly compliance checks.

   a On the **Policies and Profiles** page, click **lax01-w01hp-comp01**, click the **Monitor** tab, and click the **Scheduled Tasks** tab.

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

   c In the **Check Host Profile Compliance (scheduled)** window, click **Scheduling Options**.

   d Enter **`lax01-w01hp-comp01 Compliance Check`** in the **Task Name** field.

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

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

   g In the **Check Host Profile Compliance (scheduled)** page, click **Ok**.

Configure Lockdown Mode on All ESXi Hosts in Region B

To increase security of your ESXi hosts, you put them in Lockdown mode, so that administrative operations can be performed only from vCenter Server.

vSphere supports an Exception User list, which is for service accounts that have to log in to the host directly. Accounts with administrator privileges that are on the Exception Users list can log in to the ESXi Shell. In addition, these users can log in to a host's DCUI in normal lockdown mode and can exit lockdown mode.

You repeat this procedure to enable normal lockdown mode for all hosts in the data center. The following table lists all hosts.

Table 2-10. Hosts in the data center

Host	FQDN
Management host 1	lax01m01esx01.lax01.rainpole.local
Management host 2	lax01m01esx02.lax01.rainpole.local
Management host 3	lax01m01esx03.lax01.rainpole.local
Management host 4	lax01m01esx04.lax01.rainpole.local
Shared Edge and Compute host 1	lax01w01esx01.lax01.rainpole.local
Shared Edge and Compute host 2	lax01w01esx02.lax01.rainpole.local
Shared Edge and Compute host 3	lax01w01esx03.lax01.rainpole.local
Shared Edge and Compute host 4	lax01w01esx04.lax01.rainpole.local

Procedure

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

   a Open a Web browser and go to **`https://lax01w01vc01.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**, click **Hosts and Clusters** and expand the entire **lax01w01vc01.lax01.rainpole.local** tree control.

3 Select the **lax01w01esx01.lax01.rainpole.local** host.

4 Click **Configure**.

5 Under **System**, select **Security Profile**.

6 In the **Lockdown Mode** panel, click **Edit**.

7 In the **Lockdown Mode** dialog box, select the **Normal** radio button, and click **OK**.

8 Repeat the procedure to enable normal lockdown mode for all remaining hosts in the data center.

   Note   Lockdown Mode settings are not part of Host Profiles and must be manually enabled on all hosts.

Create the VM and Template Folders in Region B

Create folders to group objects of the same type for easier management.

You repeat this procedure eight times to create all management application folders listed in the following table.

Table 2-11. Folders for the Management Applications in Region B

Management Applications	Folder
NSX Manager + Controllers + Edges	lax01-w01fd-nsx

Procedure

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

   a Open a Web browser and go to `https://lax01w01vc01.lax01.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 folder for the vRealize Log Insight management application.

   a In the **Navigator**, click **VMs and Templates**.

   b Expand the **lax01w01vc01.lax01.rainpole.local** tree.

   c Right-click the **lax01-w01dc** data center and select **New Folder > New VM and Template Folder**.

   d In the **New Folder** dialog box, enter `lax01-w01fd-nsx` as the name to label the folder, and click **OK**.

   e Repeat this step to create the remaining folders.

3 Delete the **Discovered Virtual Machines** folder.

   a In the **Navigator**, click **VMs and Templates**.

   b Expand the **lax01w01vc01.lax01.rainpole.local** tree.

   c Right-click the **Discovered Virtual Machines** folder and select **Remove from Inventory**.

Deploy and Configure the Shared Edge and Compute Cluster NSX Instance in Region B

Deploy and configure the NSX instance for the shared edge and compute cluster in Region B.

Procedure

1 Deploy the NSX Manager for the Shared Edge and Compute Cluster NSX Instance in Region B

   For this implementation NSX Manager and vCenter Server have a one-to-one relationship. For every instance of NSX Manager, there is one connected vCenter Server.

2 Join the Shared Edge and Compute Cluster NSX Manager to the Primary NSX Instance in Region B

   You join the secondary NSX instance in Region B to the respective primary instance in Region A.

3 Prepare the ESXi Hosts in the Shared Edge and Compute Cluster for NSX in Region B

   NSX kernel modules packaged in VIB files run within the hypervisor kernel and provide services such as distributed routing, distributed firewall, and VXLAN bridging capabilities. To use NSX, you must install the NSX kernel modules on the ESXi hosts.

4 Configure the NSX Logical Network for the Shared Edge and Compute Cluster in Region B

   After all deployment tasks are ready, configure the NSX logical network.

5 Update the Host Profile for the Compute Cluster in Region B

   After an authorized change is made to a host the Host Profile must be updated to reflect the changes.

6 Configure NSX Dynamic Routing in the Shared Edge and Compute Cluster in Region B

   NSX for vSphere creates a network virtualization layer on top of which all virtual networks are created. This layer is an abstraction between the physical and virtual networks.

7 Test the Shared Edge and Compute Cluster NSX Configuration in Region B

   Test the configuration of the NSX logical network.

8 Test the Shared Edge and Compute Clusters Routing Failover

   After the clusters are fully configured in Region A and Region B, verify that the network connectivity between them works as expected.

Deploy the NSX Manager for the Shared Edge and Compute Cluster NSX Instance in Region B

For this implementation NSX Manager and vCenter Server have a one-to-one relationship. For every instance of NSX Manager, there is one connected vCenter Server.

Deploy the NSX Manager virtual appliance for the management cluster. After the NSX Manager is deployed, connect it to the Management vCenter Server instance.

Deploy the NSX Manager for the Shared Edge and Compute Cluster NSX Instance in Region B

You start implementing network virtualization for tenant workloads in Region B by deploying the NSX Manager virtual appliance.

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 Open the **Deploy OVF Template** wizard.

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

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

   The **Deploy OVF Template** appears.

3 On the **Select template** page, click the **Browse** button, select the VMware NSX Manager `.ova` file, and click **Next.**

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

Setting	Value
Name	lax01m01nsx01
Folder or Datacenter	lax01-m01fd-nsx

5 On the **Select Resource** page, select the following values, and click **Next**.

Setting	Value
Cluster	lax01-m01-mgmt01

6 On the **Review Details** page, select the **Accept extra configuration option** check box and click **Next**.

7 On the **Accept License Agreements** page, click **Accept** and click **Next**.

8 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

9 On the **Setup Networks** page, under **Destination**, select **lax01-m01-vds01-management** and click **Next.**

10 On the **Customize Template** page, expand the different options, enter the following settings, and click **Next**.

Setting	Value
DNS Server List	172.17.11.5,172.17.11.4
Domain Search List	lax01.rainpole.local
Default IPv4 Gateway	172.17.11.253
Hostname	lax01w01nsx01.lax01.rainpole.local
Network 1 IPv4 Address	172.17.11.66
Network 1 Netmask	255.255.255.0
Enable SSH	Selected
NTP Server List	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
CLI "admin" User Password / enter	*compnsx_admin_password*
CLI "admin" User Password / confirm	*compnsx_admin_password*
CLI Privilege Mode Password / enter	*compnsx_privilege_password*
CLI Privilege Mode Password / confirm	*compnsx_privilege_password*

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

12 In the **Navigator**, expand the **lax01w01vc01.lax01.rainpole.local** control tree, select the **lax01w01nsx01** virtual machine, and click the **Power on** button.

13 Log out from the vCenter Server session in the vSphere Web Client.

Replace the NSX Manager Certificate for Shared Edge and Compute Cluster in Region B

After you deploy the appliance of NSX Manager for the shared edge and compute cluster, replace the default certificate for NSX Manager. In this way, NSX Manager can communicate with the other management solutions over a trusted connection.

Table 2‑12. Certificate-Related Files on the NSX Manager Instance for the Management Cluster in Region B

NSX Manager FQDN	Certificate File Name
lax01w01nsx01.lax01.rainpole.local	lax01w01nsx01.4.p12

Prerequisites

- CA-signed certificate files generated by using VMware Validated Design Certificate Generation Utility (`CertGenVVD`). See the *VMware Validated Design Planning and Preparation* documentation.

Procedure

1. Log in to the appliance interface of NSX Manager for the shared edge and compute cluster.
   a. Open a Web browser and go to **`https://lax01w01nsx01.lax01.rainpole.local`** .
   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2. On the **Home** page, select **Manage Appliance Settings**.
3. On the **Manage** tab, click **SSL Certificates and click Upload PKSCS#12 Keystore**.
4. Browse to the certificate chain file `lax01w01nsx01.4.p12`, provide the keystore password or passphrase, and click **Import**.
5. Restart the NSX Manager to propagate the CA-signed certificate.
   a. In the right corner of the NSX Manager page, click the **Settings** icon.
   b. From the drop-down menu, select **Reboot Appliance**.

Connect NSX Manager to the Compute vCenter Server in Region B

After you deploy the NSX Manager virtual appliance for the shared edge and compute cluster, you connect the NSX Manager to the Compute vCenter Server.

Procedure

1. Log in to the appliance interface of NSX Manager for the shared edge and compute cluster.
   a. Open a Web browser and go to **`https://lax01w01nsx01.lax01.rainpole.local`** .
   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2. Click **Manage vCenter Registration**.
3. Under **Lookup Service**, click the **Edit** button.
4. In the **Lookup Service** dialog box, enter the following settings, and click **OK**.

Setting	Value
Lookup Service IP	lax01psc01.lax01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	*vsphere_admin_password*

5 In the **Trust Certificate?** dialog box, click **Yes**.

6 Under **vCenter Server**, click the **Edit** button.

7 In the **vCenter Server** dialog box, enter the following settings, and click **OK**.

Setting	Value
vCenter Server	lax01w01vc01.lax01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

8 In the **Trust Certificate?** dialog box, click **Yes**.

9 Wait for the **Status** indicators for the Lookup Service and vCenter Server to change to a `Connected` status.

Assign Administrative Access to NSX Manager for the Shared Edge and Compute Cluster in Region B

Assign the administrator@vsphere.local account to the NSX Enterprise Administrator Role.

Procedure

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

a Open a Web browser and go to **`https://lax01w01vc01.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**, click **Networking & Security** and click **Users and Domains.**

3 Under **NSX Managers**, click the **172.17.11.66** instance and click the **Add** icon.

4 On the **Identify User** page, enter **`administrator@vsphere.local`** in the **User** text filed and click **Next**.

5 On the **Select Roles** page, select the **Enterprise Administrator** radio button and click **Finish**.

Join the Shared Edge and Compute Cluster NSX Manager to the Primary NSX Instance in Region B

You join the secondary NSX instance in Region B to the respective primary instance in Region A.

Procedure

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

a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

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

2 Assign the secondary role to the shared edge and compute NSX Manager in Region B.

a Under **Inventories**, click **Networking & Security**.

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

c On the **Management** tab, select the **172.16.11.66** instance.

d Select **Actions > Add Secondary NSX Manager**.

e In the **Add Secondary NSX Manager** dialog box, enter the following settings and click **OK**.

Setting	Value
NSX Manager	172.17.11.66
User name	admin
Password	*mgmtnsx_admin_password*
Confirm Password	*mgmtnsx_admin_password*

f In the **Trust Certificate** confirmation dialog box, click **Yes**.

Prepare the ESXi Hosts in the Shared Edge and Compute Cluster for NSX in Region B

NSX kernel modules packaged in VIB files run within the hypervisor kernel and provide services such as distributed routing, distributed firewall, and VXLAN bridging capabilities. To use NSX, you must install the NSX kernel modules on the ESXi hosts.

Procedure

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

   a Open a Web browser and go to **`https://lax01w01vc01.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**, click **Networking & Security**.

3 Click **Installation and Upgrage** and click the **Host Preparation** tab.

4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.

5 Under **NSX Component Installation on Hosts**, click **Actions** , click **Install** for the **lax01-w01-comp01** cluster, and in the confirmation dialog box, click **Yes**.

6 Verify that the **Installation Status** column shows the NSX version for all hosts in the cluster to confirm that NSX kernel modules are successfully installed.

Configure the NSX Logical Network for the Shared Edge and Compute Cluster in Region B

After all deployment tasks are ready, configure the NSX logical network.

Complete this process in three main steps:

- Configure the Segment ID allocation.
- Configure the VXLAN networking.
- Add cluster to the universal transport zone.

Procedure

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

   a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 Configure the Segment ID allocation.

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

   b Click **Installation**, click **Logical Network Preparation**, and click **Segment ID**.

   c Select **172.17.11.66** from the **NSX Manager** drop-down menu.

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

Setting	Value
Segment ID pool	10000-14000
Enable Multicast addressing	Selected
Multicast addresses	239.6.0.0-239.6.255.255

3 Configure the VXLAN networking.

   a Click the **Host Preparation** tab.

   b Under **VXLAN**, click **Not Configured** on the **lax01-w01-comp01** row, enter the following settings, and click **OK.**

Setting	Value
Switch	lax01-w01-vds01
VLAN	1734
MTU	9000
VMKNic IP Addressing	Use DHCP
VMKNic Teaming Policy	Load Balance - SRCID
VTEP	2

4 Configure the Universal transport zone.

   a In the **Navigator**, click the **Logical Network Preparation** tab and click **Transport Zones**.

   b From the **Actions** menu, select the **Comp Universal Transport Zone** and select **Connect Clusters**.

   c In the **Connect Clusters** dialog box, select the **lax01-w01-comp01** cluster and click **OK**.

5 Configure the Global transport zone.

   a On the **Installation and Upgrade** page, click the **Logical Network Preparation** tab and click **Transport Zones**.

   b Select **172.17.11.66** from the **NSX Manager** drop-down menu.

c Click the **New Transport zone** icon.

d In the **New Transport Zone** dialog, enter the following settings and click **OK**.

Setting	Value
Name	Comp Global Transport Zone
Replication mode	Hybrid
Select clusters part of the Transport Zone	lax01-w01-comp01

Update the Host Profile for the Compute Cluster in Region B

After an authorized change is made to a host the Host Profile must be updated to reflect the changes.

Procedure

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

a Open a Web browser and go to **`https://lax01w01vc01.lax01.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 for the compute cluster.

a In the **Navigator** select **Policies and Profiles**.

b Click on **Host Profiles**, right-click on **lax01-w01-comp01**, and select **Copy settings from Host**.

c Select **lax01w01esx01.lax01.rainpole.local** and click **OK**.

3 Verify compliance for the hosts in the management cluster.

a On the **Policies and Profiles** page, click the **lax01-w01hp-comp01** host profile.

b Click the **Monitor** tab and click **Compliance**.

c Select **lax01-w01-comp01** and click the **Check Host Profile Compliance** button.

This compliance test shows that the first host is `Compliant`, but the other hosts are `Not Compliant`.

d Click each of the non-compliant hosts and click **Remediate Hosts Based on its Host Profile**.

e In the **Remediate Hosts Based on its Host Profile** wizard, enter **`Host Name`** if prompted for **NetStack Instance vxlan->DNS configuration**, and click **Next**.

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

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

Configure NSX Dynamic Routing in the Shared Edge and Compute Cluster in Region B

NSX for vSphere creates a network virtualization layer on top of which all virtual networks are created. This layer is an abstraction between the physical and virtual networks.

You configure NSX dynamic routing within the management cluster, deploying two NSX Edge devices and configure a Universal Distributed Logical Router (UDLR).

Procedure

1 Create Logical Switches in the Shared Edge and Compute Cluster in Region B

  Create a global transit logical switch for use as the transit network in the cluster.

2 Deploy NSX Edge Devices for North-South Routing in the Shared Edge and Compute Cluster in Region B

  Deploy NSX Edge Devices for North-South routing in the shared edge and compute cluster.

3 Disable the Firewall Service in the Shared Edge and Compute Cluster in Region B

  Disable the firewall of the two NSX Edge services gateways.

4 Enable and Configure Routing in the Shared Edge and Compute Cluster in Region B

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

5 Verify Peering of Upstream Switches and Establishment of BGP in Shared Edge and Compute Cluster in Region B

  The NSX Edge devices must establish a connection to each of their upstream BGP switches before BGP updates can be exchanged. Verify that the NSX Edges devices are successfully peering and that BGP routing has been established.

6 Configure Universal Distributed Logical Router for Dynamic Routing in the Shared Edge and Compute Cluster in Region B

  Configure the universal distributed logical router (UDLR) in the shared edge and compute cluster to use dynamic routing.

7 Verify Establishment of BGP for the Universal Distributed Logical Router in the Shared Edge and Compute Cluster in Region B

  The universal distributed logical router (UDLR) must establish a connection to Edge Services Gateway before BGP updates can be exchanged. Verify that the UDLR is successfully peering, and that BGP routing has been established.

8 Deploy the Distributed Logical Router in the Shared Edge and Compute Cluster in Region B

  Deploy the distributed logical routers (DLR).

9 Configure Distributed Logical Router for Dynamic Routing in Shared Edge and Compute Cluster in Region B

Configure the distributed logical router (DLR) in the shared edge and compute cluster to use dynamic routing.

10 Verify Establishment of BGP for the Distributed Logical Router in the Shared Edge and Compute Cluster in Region B

The distributed logical router (DLR) must establish a connection to Edge Services Gateway before BGP updates can be exchanged. Verify that the DLR is successfully peering, and that BGP routing has been established.

Create Logical Switches in the Shared Edge and Compute Cluster in Region B

Create a global transit logical switch for use as the transit network in the 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://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 Under Inventories, click **Networking & Security**.

3 In the **Navigator**, click **Logical Switches**.

4 Select **172.17.11.66** from the **NSX Manager** drop-down menu and click the **Add** icon.

5 In the **New Logical Switch** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	Global Transit Network
Transport Zone	Comp Global Transport Zone
Replication Mode	Hybrid
Enable IP Discovery	Selected
Enable MAC Learning	Deselected

Deploy NSX Edge Devices for North-South Routing in the Shared Edge and Compute Cluster in Region B

Deploy NSX Edge Devices for North-South routing in the shared edge and compute cluster.

Perform this procedure two times to deploy two NSX Edge devices: lax01w0esg01 and lax01w0esg02.

Table 2-13. NSX Edge Devices

NSX Edge Device	Device Name
NSX Edge Device 1	lax01w01esg01
NSX Edge Device 2	lax01w01esg02

Table 2-14. NSX Edge Interface Settings

Interface	Primary IP Address lax01w01esg01	Primary IP Address lax01w01esg02
Uplink01	172.17.35.2	172.17.35.3
Uplink02	172.27.21.3	172.27.21.2
sfo01w01udlr01	192.168.100.50	192.168.100.51
lax01w01dlr01	192.168.102.1	192.168.102.2

To complete this procedure, use the datastore that you configured for the shared edge and compute cluster.

Prerequisites

To complete this procedure, you must configure datastore for the shared edge and compute cluster in Region B.

Procedure

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

   a Open a Web browser and go to `https://lax01w01vc01.lax01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

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

2 Under **Inventories**, click **Networking & Security**.

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

4 Select **172.17.11.66** 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**.

Setting	lax01w01esg01	lax01w02esg02
Install Type	Edge Service Gateway	Edge Service Gateway
Name	lax01w01esg01	lax01w01esg02
Deploy NSX Edge	Selected	Selected
Enable High Availability	Deselected	Deselected

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

Setting	Value
User Name	admin
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 the **Large** radio button 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	lax01-w01rp-sddc-edge
Datastore	*lax01_shared_edge_and_compute_datastore*
Folder	lax01-w01fd-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	lax01w01esg01	lax01w01esg02
Name	Uplink01	Uplink01
Type	Uplink	Uplink
Connected To	lax01-w01-vds01-uplink01	lax01-w01-vds01-uplink01
Connectivity Status	Connected	Connected
Primary IP Address	172.17.35.2	172.17.35.3
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	lax01w01esg01	lax01w01esg02
Name	Uplink02	Uplink02
Type	Uplink	Uplink
Distributed Portgroup	lax01-w01-vds01-uplink02	lax01-w01-vds01-uplink02
Connectivity Status	Connected	Connected
Primary IP Address	172.27.21.3	172.27.21.2
Subnet Prefix Length	24	24
MTU	9000	9000
Send ICMP Redirect	Selected	Selected

g Click the **Add** icon to configure the sfo01w01udlr01 interface, enter the following settings, click **OK**, and click **Next**.

Setting	lax01w01esg01	lax01w01esg02
Name	sfo01w01udlr01	sfo01w01udlr01
Type	Internal	Internal
Connected To	Universal Transit Network	Universal Transit Network
Connectivity Status	Connected	Connected
Primary IP Address	192.168.100.50	192.168.100.51
Subnet Prefix Length	24	24
MTU	9000	9000
Send ICMP Redirect	Selected	Selected

h Click the **Add** icon to configure the lax01w01dlr01 interface, enter the following settings, click **OK**, and click **Next**.

Setting	lax01w01esg01	lax01w01esg02
Name	lax01w01dlr01	lax01w01dlr01
Type	Internal	Internal
Connected To	Global Transit Network	Global Transit Network
Connectivity Status	Connected	Connected
Primary IP Address	192.168.102.1	192.168.102.2
Subnet Prefix Length	24	24
MTU	9000	9000
Send ICMP Redirect	Selected	Selected

i On the **Default Gateway Settings** page, deselect the **Configure Default Gateway** check box and click **Next**.

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

k On the **Ready to Complete** page, review the configuration settings you entered and click **Finish**.

6 Repeat this procedure to configure another NSX edge by using the settings for the second NSX Edge device.

7 Configure DRS affinity rules for the Edge Services Gateways.

a Go back to the **Home** page.

b In the **Navigator**, click **Hosts and Clusters** and expand the **lax01w01vc01.lax01.rainpole.local** tree.

c Select the **lax01-w01-comp01** cluster and click the **Configure** tab.

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

e Click **Add**.

f In the **lax01-w01-comp01 - Create VM/Host Rule** dialog box, enter the following settings and click **Add**.

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

g In the **Add Rule Member** dialog box, select the check box next to each of the two newly deployed NSX ESGs and click **OK**.

h In the **lax01-w01-comp01 - Create VM/Host Rule** dialog box, click **OK**.

Disable the Firewall Service in the Shared Edge and Compute Cluster in Region B

Disable the firewall of the two NSX Edge services gateways.

You repeat this procedure two times for each of the NSX Edge devices: lax01w01esg01 and lax01w01esg02.

Procedure

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

   a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 Under **Inventories**, click **Networking & Security**.

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

4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.

5 Double-click the **lax01w01esg01** NSX Edge device.

6 Click the **Manage** tab and click **Firewall**.

7 On the **Firewall** page, click the **Stop** button.

8 Click **Publish Changes**.

9 Repeat this procedure for the NSX Edge services gateway lax01w01esg02.

Enable and Configure Routing in the Shared Edge and Compute Cluster in Region B

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

Procedure

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

   a Open a Web browser and go to `https://lax01w01vc01.lax01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

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

2 Under **Inventories**, click **Networking Security**.

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

4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.

5 Double-click the **lax01w01esg01** NSX Edge device.

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

7 Configure settings on the **Global Configuration** page.

   a Click the **Start** button for **ECMP**.

   b To configure dynamic routing, click the **Edit** button next to **Dynamic Routing Configuration**.

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

   d Click **Publish Changes**.

8 On the **Routing** tab, select **Static Routes** to configure it.

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

Setting	Value
Network	*UDLR_Compute_Workload_Subnet*
Next Hop	192.168.100.3
Interface	sfo01w01udlr01
MTU	9000
Admin Distance	210

Note You must add all subnets that are behind the UDLR.

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

Setting	Value
Network	*DLR_Compute_Workload_Subnet*
Next Hop	192.168.102.3
Interface	lax01w01dlr01
MTU	9000
Admin Distance	210

Note You must add all subnets that are behind the DLR.

c Click **Publish Changes**.

9 On the **Routing** tab, select **BGP** to configure it.

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

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Enable Default Originate	Deselected
Local AS	65000

b Click the **Add** icon to add a Neighbor.

The **New Neighbor** dialog box appears. You add two neighbors: the first Top of Rack Switch and the second Top of Rack Switch.

c In the **New Neighbor** dialog box, enter the following values for the first Top of Rack Switch, and click **OK**.

Setting	Value
IP Address	172.17.35.1
Remote AS	65002
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.

e In the **New Neighbor** dialog box, enter the following values for the second Top of Rack Switch, and click **OK**.

Setting	Value
IP Address	172.27.21.1
Remote AS	65002
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	192.168.100.4
Remote AS	65000
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	*BGP_password*

h Click the **Add** icon to add another Neighbor.

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

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

Setting	Value
IP Address	192.168.102.4
Remote AS	65000
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	*BGP_password*

j Click **Publish Changes**.

The four neighbors you added are now visible in the **Neighbors** table.

10 On the **Routing** tab, select **Route Redistribution** to configure it.

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 Under **Route Redistribution** table, click the **Add** icon.

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 is now visible in the **Route Redistribution** table. Confirm that the configuration values you entered are correct.

11 Repeat this procedure for the NSX Edge device lax01w01esg02.

Verify Peering of Upstream Switches and Establishment of BGP in Shared Edge and Compute Cluster in Region B

The NSX Edge devices must establish a connection to each of their upstream BGP switches before BGP updates can be exchanged. Verify that the NSX Edges devices are successfully peering and that BGP routing has been established.

You repeat this procedure two times for each of the NSX Edge devices: lax01w01esg01 and lax01w01esg02.

Procedure

1 Log in to the NSX Edge device using a Secure Shell (SSH) client.

   a Open an SSH connection to the **lax01w01esg01** NSX Edge device.

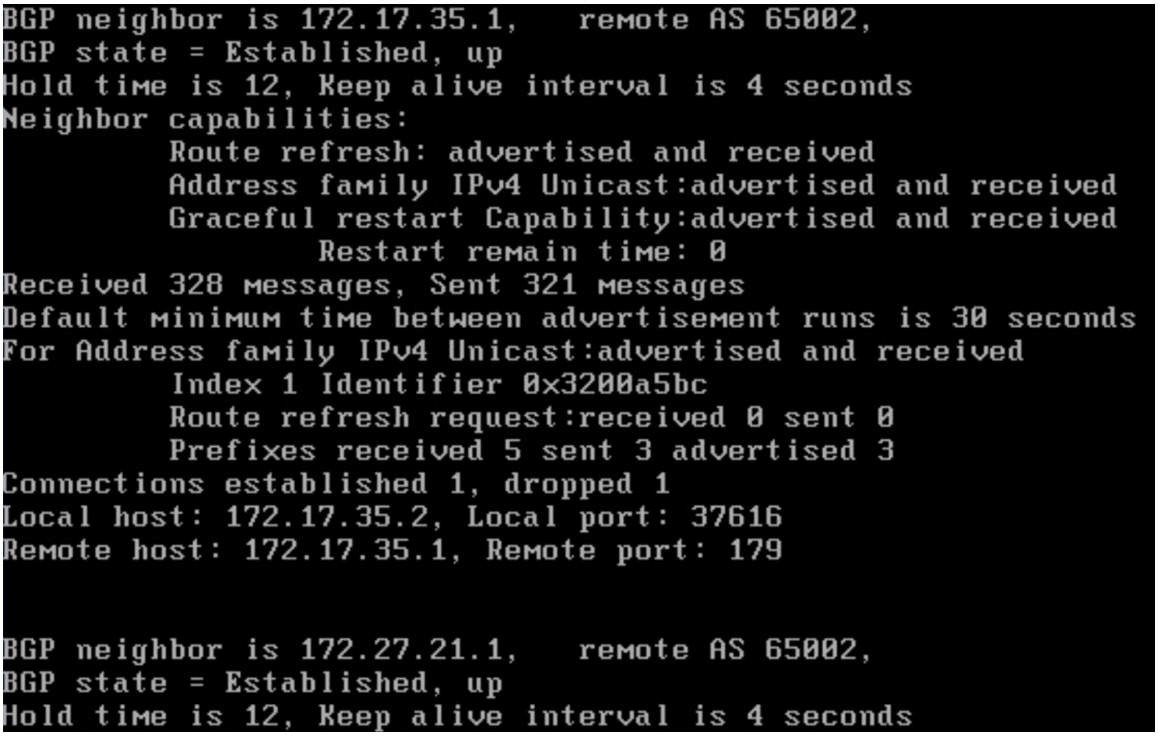
   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*edge_admin_password*

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

The BGP State displays `Established, UP` if you have peered with the upstream switches.

Note You have not yet configured the universal distributed logical router or distributed logical router, the BGP State does not display the `Established, UP` status message.

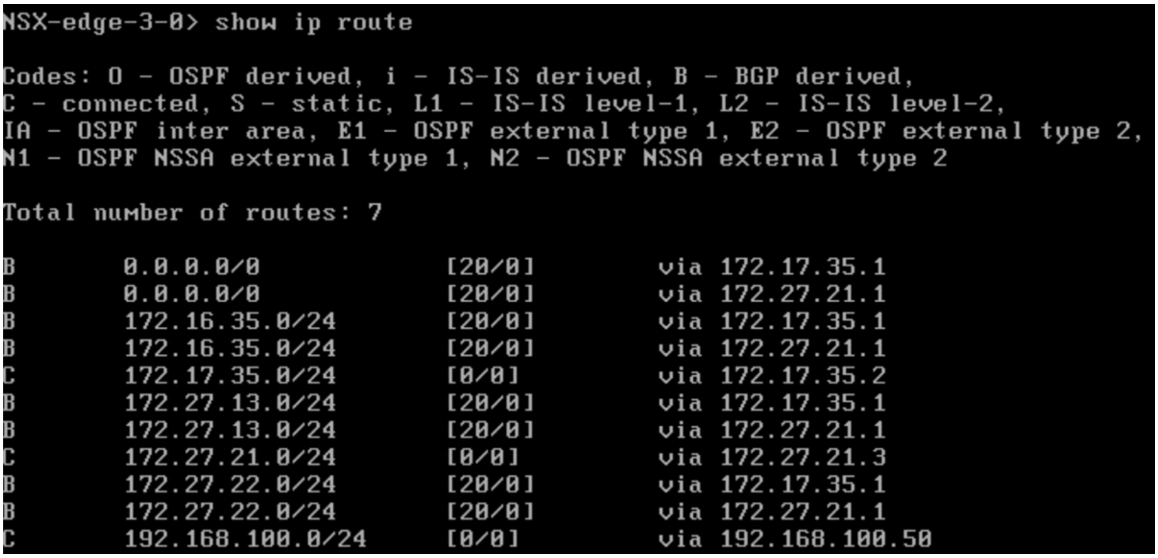


```
BGP neighbor is 172.17.35.1,   remote AS 65002,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
Neighbor capabilities:
         Route refresh: advertised and received
         Address family IPv4 Unicast:advertised and received
         Graceful restart Capability:advertised and received
                 Restart remain time: 0
Received 328 messages, Sent 321 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
         Index 1 Identifier 0x3200a5bc
         Route refresh request:received 0 sent 0
         Prefixes received 5 sent 3 advertised 3
Connections established 1, dropped 1
Local host: 172.17.35.2, Local port: 37616
Remote host: 172.17.35.1, Remote port: 179


BGP neighbor is 172.27.21.1,   remote AS 65002,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
```

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

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 following image there are two different routes to the following BGP networks: `0.0.0.0/0` and `172.27.22.0/24`. 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-3-0> 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: 7

B       0.0.0.0/0           [20/0]        via 172.17.35.1
B       0.0.0.0/0           [20/0]        via 172.27.21.1
B       172.16.35.0/24      [20/0]        via 172.17.35.1
B       172.16.35.0/24      [20/0]        via 172.27.21.1
C       172.17.35.0/24      [0/0]         via 172.17.35.2
B       172.27.13.0/24      [20/0]        via 172.17.35.1
B       172.27.13.0/24      [20/0]        via 172.27.21.1
C       172.27.21.0/24      [0/0]         via 172.27.21.3
B       172.27.22.0/24      [20/0]        via 172.17.35.1
B       172.27.22.0/24      [20/0]        via 172.27.21.1
C       192.168.100.0/24    [0/0]         via 192.168.100.50
```

4 Repeat this procedure for the NSX Edge device lax01w01esg02.

Configure Universal Distributed Logical Router for Dynamic Routing in the Shared Edge and Compute Cluster in Region B

Configure the universal distributed logical router (UDLR) in the shared edge and compute cluster to use dynamic routing.

Procedure

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

   a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 Under **Inventories**, click **Networking & Security**.

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

4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.

5 Configure the Universal Distributed Logical Router.

   a Double-click **sfo01w01udlr01**.

   b Click the **Manage** tab, click **Routing**, and select **BGP**.

   c On the **BGP** page, click the **Add Neighbor** icon.

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

Repeat two times to configure the UDLR for both NSX Edge devices: lax01w01esg01 and lax01w01esg02.

Setting	lax01w01esg01 Value	lax01w01esg02 Value
IP Address	192.168.100.50	192.168.100.51
Forwarding Address	192.168.100.3	192.168.100.3
Protocol Address	192.168.100.4	192.168.100.4
Remote AS	65000	65000
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	*bgp_password*	*bgp_password*

e Click **Publish Changes**.

Verify Establishment of BGP for the Universal Distributed Logical Router in the Shared Edge and Compute Cluster in Region B

The universal distributed logical router (UDLR) must establish a connection to Edge Services Gateway before BGP updates can be exchanged. Verify that the UDLR is successfully peering, and that BGP routing has been established.

Procedure

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

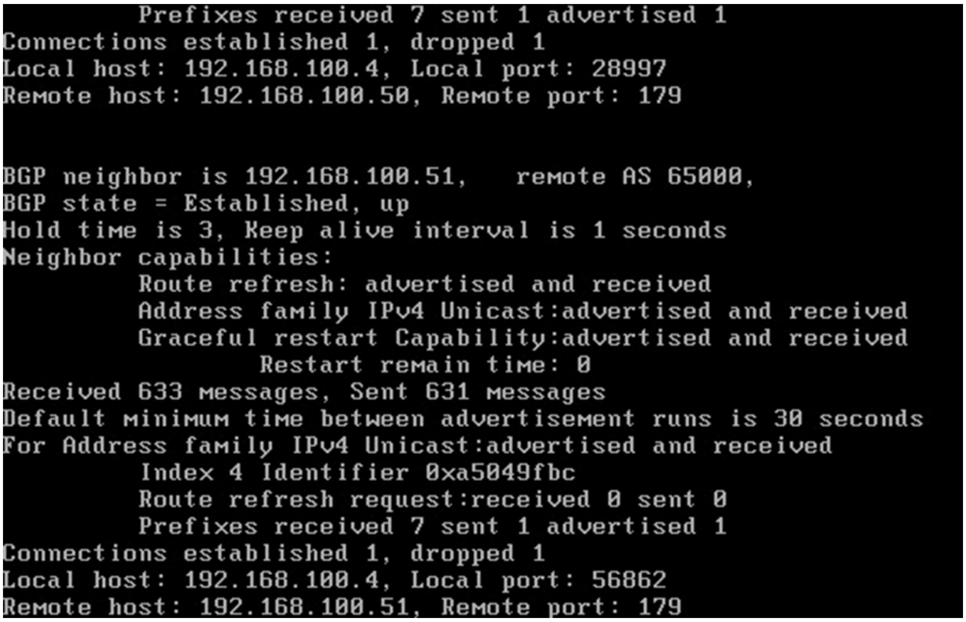
a Open an SSH connection to sfo01w01udlr01, the UDLR whose peering and BGP configuration you want to verify.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*udlr_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 Edge Service Gateway.

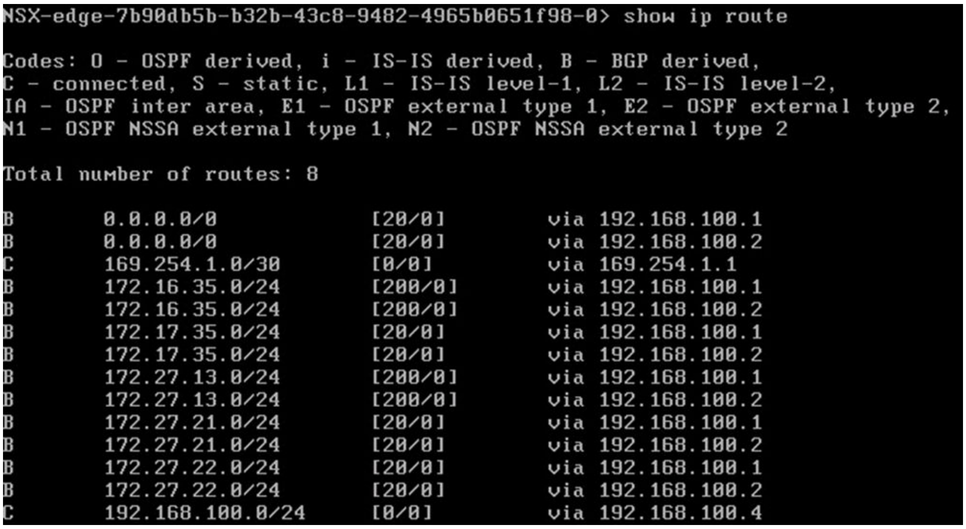


```
        Prefixes received 7 sent 1 advertised 1
Connections established 1, dropped 1
Local host: 192.168.100.4, Local port: 28997
Remote host: 192.168.100.50, Remote port: 179


BGP neighbor is 192.168.100.51,   remote AS 65000,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 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 633 messages, Sent 631 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
        Index 4 Identifier 0xa5049fbc
        Route refresh request:received 0 sent 0
        Prefixes received 7 sent 1 advertised 1
Connections established 1, dropped 1
Local host: 192.168.100.4, Local port: 56862
Remote host: 192.168.100.51, Remote port: 179
```

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

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 following image there are two different routes to the following BGP networks: `0.0.0.0/0`, `172.17.35.0/24`, `172.27.21.0/24`, and `172.27.22.0/24`. 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-7b90db5b-b32b-43c8-9482-4965b0651f98-0> 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: 8

B       0.0.0.0/0            [20/0]        via 192.168.100.1
B       0.0.0.0/0            [20/0]        via 192.168.100.2
C       169.254.1.0/30       [0/0]         via 169.254.1.1
B       172.16.35.0/24       [200/0]       via 192.168.100.1
B       172.16.35.0/24       [200/0]       via 192.168.100.2
B       172.17.35.0/24       [20/0]        via 192.168.100.1
B       172.17.35.0/24       [20/0]        via 192.168.100.2
B       172.27.13.0/24       [200/0]       via 192.168.100.1
B       172.27.13.0/24       [200/0]       via 192.168.100.2
B       172.27.21.0/24       [20/0]        via 192.168.100.1
B       172.27.21.0/24       [20/0]        via 192.168.100.2
B       172.27.22.0/24       [20/0]        via 192.168.100.1
B       172.27.22.0/24       [20/0]        via 192.168.100.2
C       192.168.100.0/24     [0/0]         via 192.168.100.4
```

Deploy the Distributed Logical Router in the Shared Edge and Compute Cluster in Region B

Deploy the distributed logical routers (DLR).

Procedure

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

   a Open a Web browser and go to `https://lax01w01vc01.lax01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

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

2 Under **Inventories**, click **Networking & Security**.

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

4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.

5 Click the **Add** icon to create a new DLR.

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

Setting	Value
Logical (Distributed) Router	Selected
Name	lax01w01dlr01
Deploy Edge Appliance	Selected
Enable High Availability	Selected

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

Setting	Value
User Name	admin
Password	*dlr_admin_password*
Enable SSH access	Selected
Enable FIPS mode	Deselected
Edge Control Level logging	INFO

8 On the **Configure deployment** page, click the **Add** icon.

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

Setting	Value
Cluster/Resource Pool	lax01-w01rp-sddc-edge
Datastore	*lax01_shared_edge_and_compute_datastore*
Folder	lax01-w01fd-nsx
Resource Reservation	System Managed

10 On the **Configure deployment** page, click the **Add** icon a second time to add a second NSX Edge device.

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

Setting	Value
Cluster/Resource Pool	lax01-w01rp-sddc-edge
Datastore	*lax01_shared_edge_and_compute_datastore*
Folder	lax01-w01fd-nsx

12 On the **Configure interfaces** page, under HA Interface Configuration, click **Select** and connect to **lax01-w01-vds01-management**.

13 On the **Configure interfaces** page, enter the following configuration settings and click **Next**.

a In the Add Interface dialog box, enter the following settings, click **OK** and click **Next**.

Setting	Value
Name	Uplink
Type	Uplink
Connected To	Global Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.102.3
Subnet Prefix Length	24
MTU	9000

14 In the **Default gateway settings** page, deselect **Configure Default Gateway** and click **Next**.

15 In the **Ready to complete** page, click **Finish**.

16 Allow SSH access in the Universal Distributed Logical Router firewall.

a Double click the device labeled **lax01w01dlr01**.

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

c Click **Add** icon to create a new firewall rule with the following settings.

Setting	Value
Name	enableSSH
Source	any
Destination	any
Service	SSH
Action	Accept

d Click **Publish Changes**.

Configure Distributed Logical Router for Dynamic Routing in Shared Edge and Compute Cluster in Region B

Configure the distributed logical router (DLR) in the shared edge and compute cluster to use dynamic routing.

Procedure

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

  a Open a Web browser and go to `https://lax01w01vc01.lax01.rainpole.local/vsphere-client`.

  b Log in using the following credentials.

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

2 Under **Inventories**, click **Networking & Security**.

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

4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.

5 Configure the routing for the Distributed Logical Router.

  a Double-click **lax01w01dlr01**.

  b Click the **Manage** tab and click **Routing**.

  c On the **Global Configuration** page, perform the following configuration steps.

  d Click the **Start** button for ECMP.

  e Click the **Edit** button under **Dynamic Routing Configuration**, select **Uplink** as the Router ID, and click **OK.**

  f Click **Publish Changes**.

6 On the left, select **BGP** to configure it.

  a On the **BGP** page, click the **Edit** button.

  The **Edit BGP Configuration** dialog box appears.

  b In the **Edit BGP Configuration** dialog box, enter the following settings and click **OK**.

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Local AS	65000

c Click the **Add** icon to add a Neighbor.

The **New Neighbor** dialog box appears.

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

You repeat this step two times to configure the DLR for both NSX Edge devices: lax01w01esg01 and lax01w01esg02.

Setting	lax01w01esg01 Value	lax01w01esg02 Value
IP Address	192.168.102.1	192.168.102.2
Forwarding Address	192.168.102.3	192.168.102.3
Protocol Address	192.168.102.4	192.168.102.4
Remote AS	65000	65000
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	*bgp_password*	*bgp_password*

e Click **Publish Changes**.

7 On the left, select **Route Redistribution**.

a Click the **Edit** button.

b In the **Change redistribution settings** dialog box, enter the following settings, and click **OK**.

Setting	Value
OSPF	Deselected
BGP	Selected

c On the **Route Redistribution** page, select the default **OSPF** entry and click the **Edit** button.

d Select **BGP** from the **Learner Protocol** drop-down menu, and click **OK**.

e Click **Publish Changes**.

Verify Establishment of BGP for the Distributed Logical Router in the Shared Edge and Compute Cluster in Region B

The distributed logical router (DLR) must establish a connection to Edge Services Gateway before BGP updates can be exchanged. Verify that the DLR is successfully peering, and that BGP routing has been established.

Procedure

1 Log in to the lax01w01dlr01 by using a Secure Shell (SSH) client.

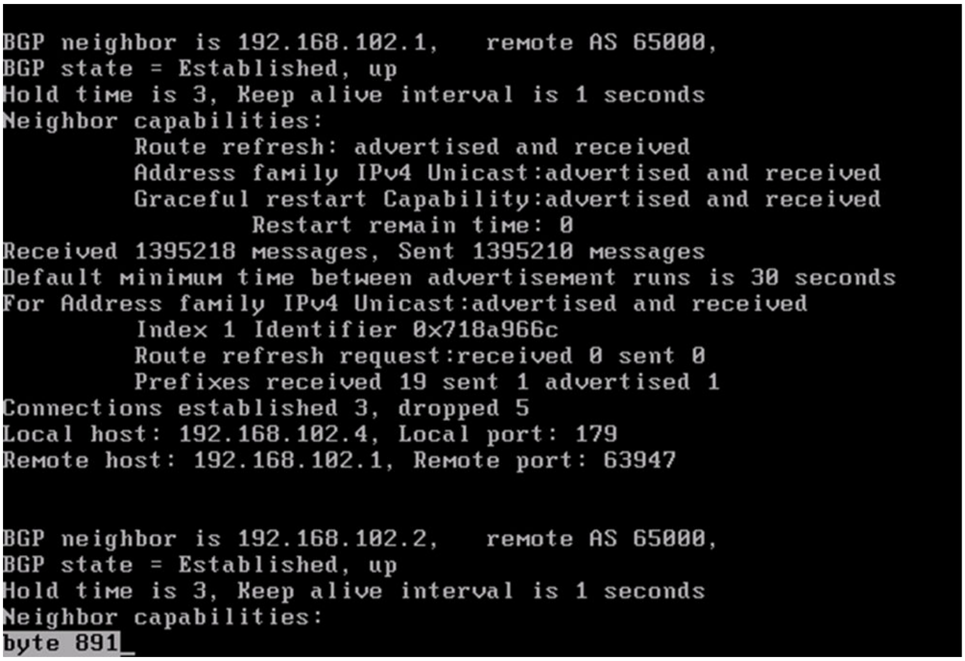
   a Open an SSH connection to lax01w01dlr01, the DLR whose peering and BGP configuration you want to verify.

   b Log in using the following credentials.

Options	Description
User name	admin
Password	*dlr_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 Edge Service Gateway.

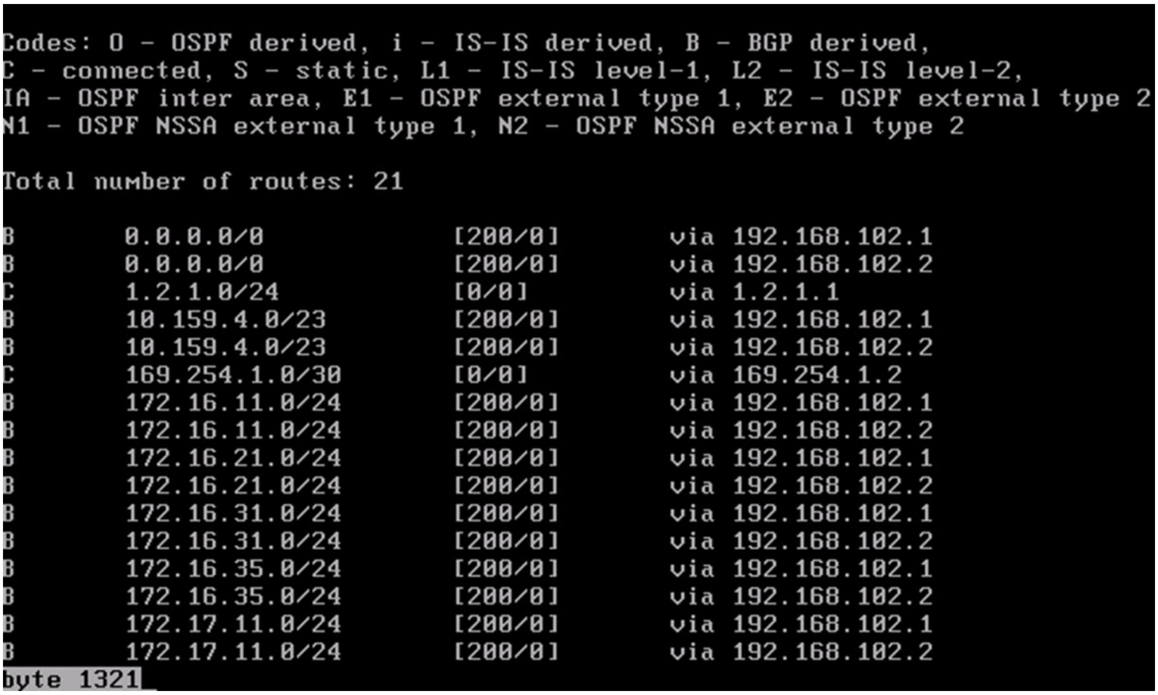


```
BGP neighbor is 192.168.102.1,   remote AS 65000,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
         Route refresh: advertised and received
         Address family IPv4 Unicast:advertised and received
         Graceful restart Capability:advertised and received
                 Restart remain time: 0
Received 1395218 messages, Sent 1395210 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
         Index 1 Identifier 0x718a966c
         Route refresh request:received 0 sent 0
         Prefixes received 19 sent 1 advertised 1
Connections established 3, dropped 5
Local host: 192.168.102.4, Local port: 179
Remote host: 192.168.102.1, Remote port: 63947


BGP neighbor is 192.168.102.2,   remote AS 65000,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
byte 891_
```

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

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 following image there are two different routes to the following BGP networks: 0.0.0.0/0, 10.159.4.0/23, 172.16.11.0/24, 172.16.21.0/24, 172.16.31.0/24, 172.16.35.0/24 and 172.17.11.0/24. You can identify BGP networks by the letter `B` in the left-side column. Lines beginning with `C` (connected) have only a single route.



```
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: 21

B       0.0.0.0/0           [200/0]       via 192.168.102.1
B       0.0.0.0/0           [200/0]       via 192.168.102.2
C       1.2.1.0/24          [0/0]         via 1.2.1.1
B       10.159.4.0/23       [200/0]       via 192.168.102.1
B       10.159.4.0/23       [200/0]       via 192.168.102.2
C       169.254.1.0/30      [0/0]         via 169.254.1.2
B       172.16.11.0/24      [200/0]       via 192.168.102.1
B       172.16.11.0/24      [200/0]       via 192.168.102.2
B       172.16.21.0/24      [200/0]       via 192.168.102.1
B       172.16.21.0/24      [200/0]       via 192.168.102.2
B       172.16.31.0/24      [200/0]       via 192.168.102.1
B       172.16.31.0/24      [200/0]       via 192.168.102.2
B       172.16.35.0/24      [200/0]       via 192.168.102.1
B       172.16.35.0/24      [200/0]       via 192.168.102.2
B       172.17.11.0/24      [200/0]       via 192.168.102.1
B       172.17.11.0/24      [200/0]       via 192.168.102.2
byte 1321
```

Test the Shared Edge and Compute Cluster NSX Configuration in Region B

Test the configuration of the NSX logical network.

Procedure

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

  a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`**.

  b Log in using the following credentials.

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

2 Use the Ping Monitor to test connectivity.

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

  b Under **Logical Switches**, double-click **Universal Transit Network**.

  c Click the **Monitor** tab.

  d Under **Test Parameters**, select **lax01w01esx01.lax01.rainpole.local** as the **Source** host.

e Under **Test Parameters**, select **lax01w01esx02.lax01.rainpole.local** as the **Destination** host, and click **Start Test**.

f There must be no error messages listed under **Results**.

Test the Shared Edge and Compute Clusters Routing Failover

After the clusters are fully configured in Region A and Region B, verify that the network connectivity between them works as expected.

Procedure

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

a Open a Web browser and go to **`https://lax01w01vc01.lax01.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 NSX Edge service gateways in Region A.

a In the **Navigator**, click **Hosts and Clusters**.

b Expand the entire **sfo01w01vc01.sfo01.rainpole.local** tree**.**

c Right-click **sfo01w01esg01-0** and select **Power > Shut Down Guest OS**.

d Right-click **sfo01w01esg02-0** and select **Power > Shut Down Guest OS**.

3 Log in to the universal distributed logical router by using a Secure Shell (SSH) client and verify the BGP routing state.

a Open an SSH connection to **`sfo01w01udlr01`**.

b Log in using the following credentials.

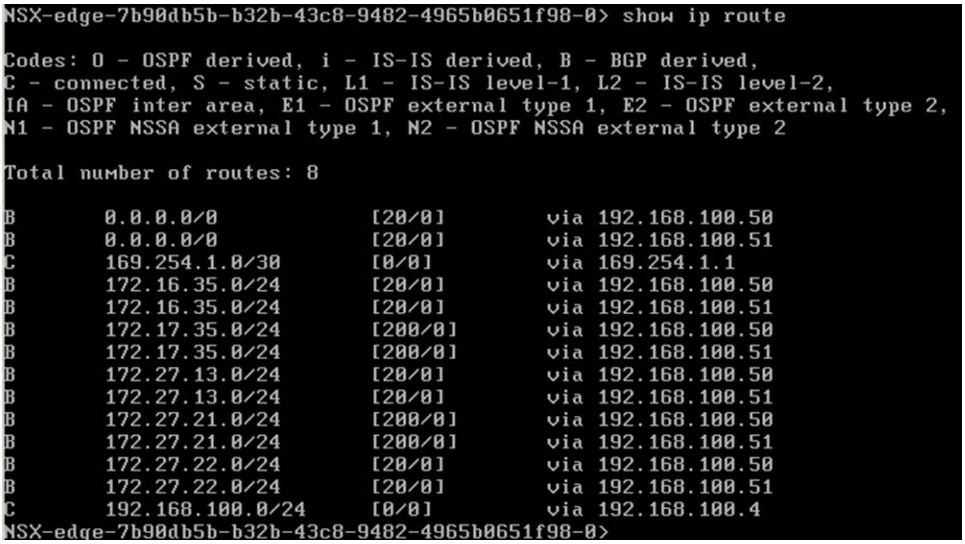
Setting	Value
User name	admin
Password	*udlr_admin_password*

c Run the `show ip route` command to verify you are receiving routes by way of BGP.

The letter `B` before the route indicates that BGP is used.

d Verify that multiple routes to BGP learned networks exist.

e Verify that routes come from Region B's ESGs.



```
NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0> 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: 8

B       0.0.0.0/0           [20/0]        via 192.168.100.50
B       0.0.0.0/0           [20/0]        via 192.168.100.51
C       169.254.1.0/30      [0/0]         via 169.254.1.1
B       172.16.35.0/24      [20/0]        via 192.168.100.50
B       172.16.35.0/24      [20/0]        via 192.168.100.51
B       172.17.35.0/24      [200/0]       via 192.168.100.50
B       172.17.35.0/24      [200/0]       via 192.168.100.51
B       172.27.13.0/24      [20/0]        via 192.168.100.50
B       172.27.13.0/24      [20/0]        via 192.168.100.51
B       172.27.21.0/24      [200/0]       via 192.168.100.50
B       172.27.21.0/24      [200/0]       via 192.168.100.51
B       172.27.22.0/24      [20/0]        via 192.168.100.50
B       172.27.22.0/24      [20/0]        via 192.168.100.51
C       192.168.100.0/24    [0/0]         via 192.168.100.4
NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0>
```

4 Power on the NSX Edge services gateways in Region A.

a In the **Navigator**, click **Hosts and Clusters**.

b Expand the entire **sfo01w01vc01.sfo01.rainpole.local** tree.

c Right-click **sfo01w01esg01-0** and select **Power > Power On**.

d Right-click **sfo01w01esg02-0** and select **Power > Power On**.

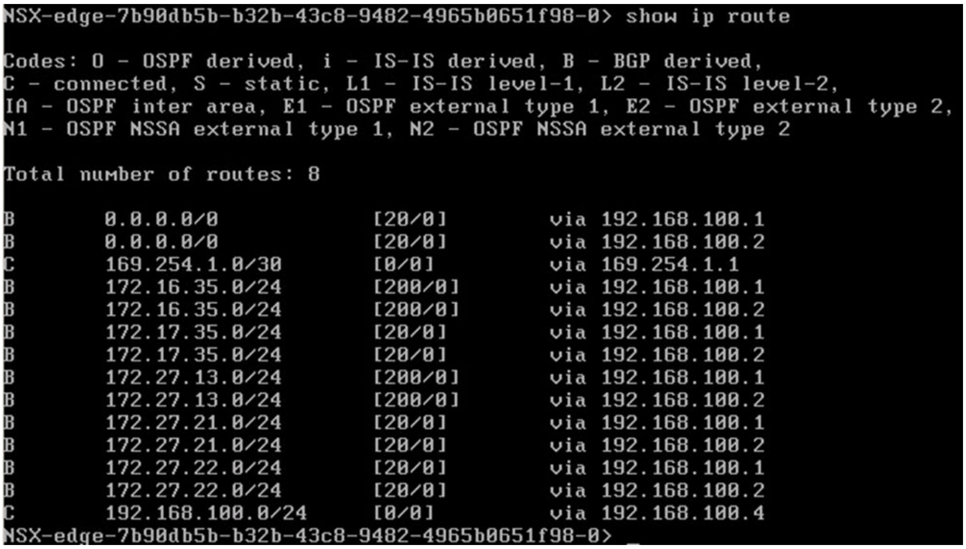
5 Verify the new state of the BGP routing.

a Go back to the SSH connection to sfo01w01udlr01 and run the `show ip route` command.

b Verify that you receive routes by way of BGP.

The letter `B` before the route indicates that BGP is used.

c Verify that you have multiple routes to BGP learned networks and that routes also come from the NSX Edge services gateways in Region A.



```
NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0> 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: 8

B       0.0.0.0/0           [20/0]        via 192.168.100.1
B       0.0.0.0/0           [20/0]        via 192.168.100.2
C       169.254.1.0/30      [0/0]         via 169.254.1.1
B       172.16.35.0/24      [200/0]       via 192.168.100.1
B       172.16.35.0/24      [200/0]       via 192.168.100.2
B       172.17.35.0/24      [20/0]        via 192.168.100.1
B       172.17.35.0/24      [20/0]        via 192.168.100.2
B       172.27.13.0/24      [200/0]       via 192.168.100.1
B       172.27.13.0/24      [200/0]       via 192.168.100.2
B       172.27.21.0/24      [20/0]        via 192.168.100.1
B       172.27.21.0/24      [20/0]        via 192.168.100.2
B       172.27.22.0/24      [20/0]        via 192.168.100.1
B       172.27.22.0/24      [20/0]        via 192.168.100.2
C       192.168.100.0/24    [0/0]         via 192.168.100.4
NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0> _
```

Region B Operations Management Implementation

3

You deploy the products for monitoring the SDDC, such as vRealize Operations Manager and vRealize Log Insight, on top of vSphere infrastructure and NSX networking setup, and connect them to the SDDC management products from all layers.

1 vRealize Operations Manager Implementation in Region B

   For a dual-region monitoring implementation, after you deploy the analytics cluster and the remote collectors in Region A, complete the installation and configuration of vRealize Operations Manager for Region B.

2 vRealize Log Insight Implementation in Region B

   Deploy vRealize Log Insight in a cluster configuration of 3 nodes in Region B. This configuration is set up with an integrated load balancer and uses one master and two worker nodes.

3 vSphere Update Manager Download Service Implementation in Region B

   Install the vSphere Update Manager Download Service (UMDS) on a Linux virtual machine to download and store binaries and metadata in a shared repository. Connect the UMDS instance to the vSphere Update Manager for each vCenter Server.

vRealize Operations Manager Implementation in Region B

For a dual-region monitoring implementation, after you deploy the analytics cluster and the remote collectors in Region A, complete the installation and configuration of vRealize Operations Manager for Region B.

Procedure

1 Deploy vRealize Operations Manager in Region B

   In Region B, deploy two remote collector nodes for vRealize Operations Manager to monitor the Management and Compute vCenter Server instances, NSX for vSphere, and storage components in SDDC.

2 Configure the Load Balancer for vRealize Operations Manager in Region B

   Configure load balancing for the analytics cluster on the dedicated lax01m01lb01 NSX Edge services gateway for Region B. Load balancing must be available if a failover of the analytics cluster from Region A occurs.

3 Add an Authentication Source for the Child Active Directory in Region B

Connect vRealize Operations Manager to the child Active Directory lax01.rainpole.local for central user management and access control in Region B.

4 Add vCenter Adapter Instances to vRealize Operations Manager for Region B

After you deploy the remote collector nodes of vRealize Operations Manager in Region B, pair a vCenter Adapter instance with each vCenter Server instance in the region.

5 Connect vRealize Operations Manager to the NSX Managers in Region B

Configure the vRealize Operations Management Pack for NSX for vSphere to monitor the NSX networking services deployed in each vSphere cluster in Region B and view the vSphere hosts in the NSX transport zones. You can also access end-to-end logical network topologies between any two virtual machines or NSX objects for better visibility into logical connectivity. Physical host and network device relationship in this view also helps in isolating problems in the logical or physical network.

6 Add Storage Devices Adapters in vRealize Operations Manager for Region B

Configure a Storage Devices adapter for Region B to collect monitoring data about the storage devices in the SDDC. Each adapter communicates with a vCenter Server instance to retrieve data about the storage devices from the vCenter Server inventory.

7 Enable vSAN Monitoring in vRealize Operations Manager in Region B

Configure the vRealize Operations Management Pack for vSAN to view the vSAN topology in Region B, and to monitor the capacity and problems.

8 Configure NTP Server on vRealize Operations Manager Cluster in Region B

To avoid misconfiguration of vRealize Opertions Manager analytics cluster in case of failover to Region B during disaster recovery, add the NTP server in Region B to the time synchronization settings of vRealize Operations Manager.

Deploy vRealize Operations Manager in Region B

In Region B, deploy two remote collector nodes for vRealize Operations Manager to monitor the Management and Compute vCenter Server instances, NSX for vSphere, and storage components in SDDC.

Deploying a separate group of remote collectors in Region B makes the data collection in each region independent from the location of the analytics cluster. If you fail over the analytics cluster, data collection continues for those nodes that are accessible in the active region.

Procedure

1 Prerequisites for Deploying the Remote Collectors in Region B

Before you deploy the remote collector nodes of vRealize Operations Manager in Region B, verify that your environment satisfies the requirements for this deployment.

2 Deploy the Remote Collector Virtual Appliances in Region B

After you deploy and configure the analytics and remote collector cluster nodes in Region A, use the vSphere Web Client to deploy the two virtual appliances for the remote collectors in Region B. You use remote collectors to forward data from the vCenter Server instances in Region B to the analytics cluster of vRealize Operations Manager.

3 Connect the Remote Collector Nodes to the Analytics Cluster in Region B

After you deploy the virtual appliances for the remote collector nodes on the Management vCenter Server in Region B, configure the settings of the remote collectors and connect them to the analytics cluster.

4 Configure a DRS Anti-Affinity Rule for vRealize Operations Manager Remote Collectors in Region B

To protect the vRealize Operations Manager virtual machines from a host-level failure, configure vSphere DRS to run the remote collector virtual machines on different hosts in the management cluster in Region B.

5 Group Remote Collector Nodes in Region B

After you configure the remote collector nodes for vRealize Operations Manager in Region B, join the remote collectors in a group for adapter resiliency in the cases where the collector experiences network interruption or becomes unavailable.

Prerequisites for Deploying the Remote Collectors in Region B

Before you deploy the remote collector nodes of vRealize Operations Manager in Region B, verify that your environment satisfies the requirements for this deployment.

IP Addresses and Host Names

Verify that static IP addresses and FQDNs for the vRealize Operations Manager application virtual network are available for Region B of the SDDC deployment.

Allocate static IP addresses and host names for the 2 remote collector nodes.

Table 3-1. Application Virtual Network Names for vRealize Operations Manager

vRealize Operations Manager Component	Application Virtual Network
Analytics Cluster	Mgmt-xRegion01-VXLAN
Remote Collector Group	Mgmt-RegionB01-VXLAN

Table 3-2. IP Addresses and Host Names for the Remote Collector Nodes in Region B

Role	IP Address	FQDN
Remote collector node 1	192.168.32.31	lax01vropsc01a.lax01.rainpole.local
Remote collector node 2	192.168.32.32	lax01vropsc01b.lax01.rainpole.local
Default gateway	192.168.32.1	-
DNS server	172.17.11.5	-
Subnet mask	255.255.255.0	-

Deployment Prerequisites

Verify that your environment satisfies the following prerequisites for deployment of vRealize Operations Manager remote collector nodes.

Prerequisite	Value
Storage	■ Virtual disk provisioning. ■ Thin ■ Required storage per analytics cluster node to support replication and failover: 1TB ■ Required storage per remote collector group nodes. ■ Initial storage per node: 274GB
Software Features	■ Verify that vCenter Server is operational. ■ Verify that the vSphere cluster has DRS and HA enabled. ■ Verify that the NSX Manager is operational. ■ Verify that the application virtual networks are available. ■ Verify that the Load Balancer service is disabled on the NSX Edge service gateway. ■ Verify vRealize Operations Manager Analytics Cluster is operational. ■ Verify that vRealize Log Insight is operational. ■ Verify that vRealize Automation is operational. ■ Verify that vRealize Business for Cloud is operational. ■ Verify that Postman App is installed in your browser.
Installation Package	Download the `.ova` file of the vRealize Operations Manager virtual appliance on the machine where you use the vSphere Web Client.

Deploy the Remote Collector Virtual Appliances in Region B

After you deploy and configure the analytics and remote collector cluster nodes in Region A, use the vSphere Web Client to deploy the two virtual appliances for the remote collectors in Region B. You use remote collectors to forward data from the vCenter Server instances in Region B to the analytics cluster of vRealize Operations Manager.

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 Navigate to the lax01m01vc01.lax01.rainpole.local vCenter Server object.

3 Right-click the **lax01m01vc01.lax01.rainpole.local** object and select **Deploy OVF Template**.

4 On the **Select template** page, select **Local file**, browse to the location of the vRealize Operations Manager `.ova` file on your file system, and click **Next**.

5 On the **Select name and location** page, enter a node name, select the inventory folder for the virtual appliance, and click **Next**.

Setting	Value
Name of remote collector 1	lax01vropsc01a
Name of remote collector 2	lax01vropsc01b
vCenter Server	lax01m01vc01.lax01.rainpole.local
Data center	lax01-m01dc
Folder	lax01-m01fd-vropsrc

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

Setting	Value
Data center	lax01-m01dc
Cluster	lax01-m01-mgmt01

7 On the **Review details** page, examine the virtual appliance details, such as product, version, download and disk size, and click **Next**.

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

9 On the **Select configuration** page, from the **Configuration** drop-down menu, select **Remote Collector (Standard)** deployment configuration of the virtual appliance, and click **Next**.

10 On the **Select storage** page, select the following datastore, 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, select the distributed port group on the **lax01-m01-vds01** distributed switch that ends with `Mgmt-RegionB01-VXLAN` and click **Next**.

12 On the **Customize template** page, set the IPv4 settings and select the time zone for the virtual appliance, and click **Next**.

   a In the **Networking Properties** section, configure the following IPv4 settings.

Setting	Value
DNS server	172.17.11.5
Default gateway	192.168.32.1
Static IPv4 address	■ 192.168.32.31 for remote collector 1 ■ 192.168.32.32 for remote collector 2
Subnet mask	255.255.255.0
Timezone setting	Etc/UTC

13 On the **Ready to complete** page, verify that the settings for deployment are correct and click **Finish**.

14 After the virtual appliance is deployed, right-click the virtual appliance object and select **Power > Power On**.

15 Change the default empty password for the root user.

   a In the vSphere Web Client, right-click the remote collector virtual appliance and select **Open Console** to open the remote console to the appliance.

Name	Role
lax01vropsc01a	Remote collector 1
lax01vropsc01b	Remote collector 2

   b Press ALT+F1 to switch to the command prompt.

   c At the command prompt, log in as the **`root`** user using empty password.

   d At the command prompt, change the default empty password for the root user account with a new *vrops_root_password* password.

   e Close the virtual appliance console.

16 Repeat the procedure to deploy the second remote collector appliance.

Connect the Remote Collector Nodes to the Analytics Cluster in Region B

After you deploy the virtual appliances for the remote collector nodes on the Management vCenter Server in Region B, configure the settings of the remote collectors and connect them to the analytics cluster.

Procedure

1 Open a Web browser and go to the initial setup user interface of each remote collector node virtual appliance.

Remote Collector Node	URL for Setup Interface
Remote collector 1	https://lax01vropsc01a.lax01.rainpole.local
Remote collector 2	https://lax01vropsc01b.lax01.rainpole.local

2 On the **Get Started** page, click **Expand an Existing Installation**.

3 On the **Getting Started** page, review the steps for creating a cluster, and click **Next**.

4 On the **Node Settings And Cluster Info** page, configure the settings of the remote collector node.

   a Enter a node name, select a node type, and enter master node address.

Setting	Value
Node name	■ lax01vropsc01a for remote collector 1 ■ lax01vropsc01b for remote collector 2
Node type	Remote Collector
Master node IP address or FQDN	vrops01svr01a.rainpole.local

   b Click **Validate** next to the **Master node IP address or FQDN** text box.

   The certificate of the master node appears in the text box.

   c Validate that the master certificate is correct, and click **Accept this certificate**.

   d Click **Next**.

5 On the **Username And Password** page, select **Use cluster administrator user name and password**, enter the ***vrops_admin_password*** password for the admin user, and click **Next**.

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

   When the configuration process completes, the vRealize Operations Manager Administration console opens.

   The **System Status** page of vRealize Operations Manager appears. The cluster admin interface displays that the configuration of the node is in progress.

7 Repeat the procedure to configure the second remote collector node.

8 After the operation is complete, in the administration user interface of vRealize Operations Manager, click **Finish Adding New Node(s)** next to **Cluster Status**.

9 In the **Finish Adding New Node(s)** dialog box, click **OK** to confirm adding the nodes.

After the configuration of the remote collectors in Region B is complete, the cluster on the **System Status** page of the administration user interface consists of the following nodes:

- 3 nodes for the analytics cluster: vrops01svr01a, vrops01svr01b and vrops01svr01c
- Two remote collectors for Region A: sfo01vropsc01a and sfo01vropsc01b
- Two remote collectors for Region B: lax01vropsc01a and lax01vropsc01b

Configure a DRS Anti-Affinity Rule for vRealize Operations Manager Remote Collectors in Region B

To protect the vRealize Operations Manager virtual machines from a host-level failure, configure vSphere DRS to run the remote collector virtual machines on different hosts in the management cluster in Region B.

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 Navigate to the lax01m01vc01.lax01.rainpole.local vCenter Server object, and under the **lax01-m01dc** data center object select the **lax01-m01-mgmt01** cluster.

3 Click the **Configure** tab.

4 Under the **Configuration** group of settings, select **VM/Host Rules**.

5 Create the new anti-affinity rules for the vRealize Operations Manager analytics cluster and remote collectors using the following settings.

   a On the **VM/Host Rules** page, click the **Add** button above the rules list.

   b In the **Create VM/Host Rule** dialog box, add a new anti-affinity rule for the virtual machines of the two remote collectors using the following values, and click **OK**.

Setting	Value
Name	anti-affinity-rule-vropsr
Enable rule	Selected
Type	Separate Virtual Machines
Members	■ lax01vropsc01a ■ lax01vropsc01b

Group Remote Collector Nodes in Region B

After you configure the remote collector nodes for vRealize Operations Manager in Region B, join the remote collectors in a group for adapter resiliency in the cases where the collector experiences network interruption or becomes unavailable.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Management** and click **Collector Groups**.

4 Click **Add**.

5 In the **Add New Collector Group** dialog box, configure the following settings, and click **Save**.

Setting	Value
Name	lax01-remote-collectors
Description	Remote collector group for lax01
lax01vropsc01a	Selected
lax01vropsc01b	Selected

The lax01-remote-collectors collector group appears on the **Collector Groups** page under the **Administration** view of the user interface.

Configure the Load Balancer for vRealize Operations Manager in Region B

Configure load balancing for the analytics cluster on the dedicated lax01m01lb01 NSX Edge services gateway for Region B. Load balancing must be available if a failover of the analytics cluster from Region A occurs.

The remote collector cluster for Region B does not require load balancing.

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

The vSphere Web Client displays the **NSX Home** page.

3 On the **NSX Home** page, click **NSX Edges** and select **172.17.11.65** from the **NSX Manager** drop-down menu at the top of the **NSX Edges** page.

4 On the **NSX Edges** page, double-click the **lax01m01lb01** NSX edge.

5 Configure the load balancing VIP address for the analytics cluster.

a On the **Manage** tab, click the **Settings** tab and click **Interfaces**.

b Select the interface **OneArmLB** and click the **Edit**.

c In the **Edit NSX Edge Interface** dialog box, click the **Edit** and in the **Secondary IP Addresses** text box enter the `192.168.11.35` VIP address.

d Click **OK** to save the configuration.

6 Create an application profile.

a On the **Manage** tab for the lax01m01lb01 device, click the **Load Balancer** tab.

b Click **Application Profiles**, and click **Add**.

c In the **New Profile** dialog box, configure the profile using the following configuration settings, and click **OK**.

Setting	Value
Name	vrops-https
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	Source IP
Expires in (Seconds)	1800
Client Authentication	Ignore

7 Create a service monitoring entry.

   a On the **Load Balancer** tab of the lax01m01lb01 device, click **Service Monitoring** and click **Add**.

   b In the **New Service Monitor** dialog box, configure the health check parameters using the following configuration settings, and click **OK**.

Setting	Value
Name	vrops-443-monitor
Interval	3
Timeout	5
Max Retries	2
Type	HTTPS
Method	GET
URL	/suite-api/api/deployment/node/status
Receive	ONLINE (must be upper case)

8 Add a server pool.

   a On the **Load Balancer** tab of the lax01m01lb01 device, select **Pools**, and click **Add**.

   b In the **New Pool** dialog box, configure the load balancing profile using the following configuration settings.

Setting	Value
Name	vrops-svr-443
Algorithm	LEASTCONN
Monitors	vrops-443-monitor

   c Under **Members**, click **Add** to add the pool members.

d In the **New Member** dialog box, add one member for each node of the analytics cluster and click **OK**.

Setting	Value
Enable Member	Selected
Name	■ vrops01svr01a ■ vrops01svr01b ■ vrops01svr01c
IP Address	■ 192.168.11.31 ■ 192.168.11.32 ■ 192.168.11.33
State	Enable
Port	443
Monitor Port	443
Weight	1
Max Connections	8
Min Connections	8

e In the **New Pool** dialog box, click **OK**.

9 Add a virtual server.

a On the **Load Balancer** tab of the lax01m01lb01 device, select **Virtual Servers** and click **Add**.

b In the **New Virtual Server** dialog box, configure the settings of the virtual server for the analytics cluster and click **OK**.

Setting	Value
Enable Virtual Server	Selected
Application Profile	vrops-https
Name	vrops-svr-443
Description	vRealize Operations Manager Cluster
IP Address	192.168.11.35
Protocol	HTTPS
Port	443
Default Pool	vrops-svr-443
Connection Limit	0
Connection Rate Limit	0

10 Configure auto-redirect from HTTP to HTTPS requests.

The NSX Edge can redirect users from HTTP to HTTPS without entering another URL in the browser.

a On the **Load Balancer** tab of the `lax01m01lb01` device, select **Application Profiles** and click **Add**.

b In the **New Profile** dialog box, configure the application profile settings and click **OK**.

Setting	Value
Name	vrops-http-redirect
Type	HTTP
HTTP Redirect URL	https://vrops01svr01.rainpole.local/vcops-web-ent/login.action
Persistence	Source IP
Expires in (Seconds)	1800

c On the **Load Balancer** tab of the lax01m01lb01 device, select **Virtual Servers** and click **Add**.

d Configure the settings of the virtual server for HTTP redirects and click **OK**.

Setting	Value
Enable Virtual Server	Selected
Application Profile	vrops-http-redirect
Name	vrops-svr-80-redirect
Description	HTTP Redirect for vRealize Operations Manager
IP Address	192.168.11.35
Protocol	HTTP
Port	80
Default Pool	NONE
Connection Limit	0
Connection Rate Limit	0

Add an Authentication Source for the Child Active Directory in Region B

Connect vRealize Operations Manager to the child Active Directory lax01.rainpole.local for central user management and access control in Region B.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to `https://vrops01svr01.rainpole.local`.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Access** and click **Authentication Sources**.

4 On the **Authentication Sources** page, click **Add**.

5 In the **Add Source for User and Group Import** dialog box, enter the settings for the lax01.rainpole.local child Active Directory in Region B, and click **OK**.

Active Directory Setting	Value
Source Display Name	LAX01.RAINPOLE.LOCAL
Source Type	Active Directory
Integration Mode	Basic
Domain/Subdomain	LAX01.RAINPOLE.LOCAL
Use SSL/TLS	Deselected
User Name	svc-vrops@rainpole.local
Password	*svc-vrops_password*
Settings under the **Details** section	
Automatically synchronize user membership for configured groups	Selected
Host	dc51lax.lax01.rainpole.local
Port	389
Base DN	dc=LAX01,dc=RAINPOLE,dc=LOCAL
Common Name	userPrincipalName

6 Click the **Test** button to test the connection to the domain controller, and in the **Info** success message click **OK**.

7 In the **Add Source for User and Group Import** dialog box, click **OK**.

The users and user groups in the Active Directory domain are added to vRealize Operations Manager.

Add vCenter Adapter Instances to vRealize Operations Manager for Region B

After you deploy the remote collector nodes of vRealize Operations Manager in Region B, pair a vCenter Adapter instance with each vCenter Server instance in the region.

Procedure

1. Log in to vRealize Operations Manager by using the operations interface.
   a. Open a Web browser and go to `https://vrops01svr01.rainpole.local`.
   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2. On the main navigation bar, click **Administration**.
3. In the left pane of vRealize Operations Manager, click **Solutions**.
4. From the solution table on the **Solutions** page, select the **VMware vSphere** solution, and click the **Configure** icon at the top.

   The **Manage Solution - VMware vSphere** dialog box appears.
5. Under **Instance Settings**, enter the settings for connection to vCenter Server.
   a. If you already have added another vCenter Adapter, click the **Add** icon on the left side to add an adapter settings.
   b. Enter the display name, description and FQDN of vCenter Server instance.

Setting	Value for Management vCenter Server	Value for Compute vCenter Server
Display Name	vCenter Adapter - lax01m01vc01	vCenter Adapter - lax01w01vc01
Description	Management vCenter Server for lax01	Compute vCenter Server for lax01
vCenter Server	lax01m01vc01.lax01.rainpole.local	lax01w01vc01.lax01.rainpole.local

   c. Click the **Add** icon on the right side, configure the collection credentials for connection to the vCenter Server instances, and click **OK**.

Management vCenter Server Credentials Attribute	Value
Credential name	■ vCenter Adapter Credentials - lax01m01vc01 ■ vCenter Adapter Credentials - lax01w01vc01
User Name	svc-vrops-vsphere@rainpole.local
Password	*svc-vrops-vsphere-password*

d Leave **Enable Actions** set to **Enable** so that vCenter Adapter can run actions on objects in the vCenter Server from vRealize Operations Manager.

e Click **Test Connection** to validate the connection to vCenter Server instance.

The vCenter Server certificate appears.

f In the **Review and Accept Certificate** dialog box, verify the certificate information and click **Accept**.

g Click **OK** in the **Info** dialog box.

h Expand the **Advanced Settings** section of settings.

i From the **Collectors/Groups** drop-down menu, select the **lax01-remote-collectors** group.

j Specify a user account with administrator privileges to register vRealize Operations Manager with the vCenter Server instance.

Setting	Value
Registration user	administrator@vsphere.local
Registration password	*vsphere_admin_password*

6 Click **Define Monitoring Goals**.

7 In the **Define Monitoring Goals** dialog box, under **Enable vSphere Hardening Guide Alerts?**, select **Yes**, leave the default configuration for the other options, and click **Save**.

8 Click **OK** in the **Success** dialog box.

9 Click **Save Settings**.

10 In the **Info** dialog box, click **OK**.

11 Repeat Step 5 to Step 10 for the Compute vCenter Server.

12 In the **Manage Solution - VMware vSphere** dialog box, click **Close**.

13 On the **Solutions** page, select **VMware vSphere** from the solution table to view the collection state and the collection status of the adapters.

The **Collection State** of the adapters is `Collecting` and the **Collection Status** is `Data receiving.`

Connect vRealize Operations Manager to the NSX Managers in Region B

Configure the vRealize Operations Management Pack for NSX for vSphere to monitor the NSX networking services deployed in each vSphere cluster in Region B and view the vSphere hosts in the NSX transport zones. You can also access end-to-end logical network topologies between any two virtual machines or NSX objects for better visibility into logical connectivity. Physical host and network device relationship in this view also helps in isolating problems in the logical or physical network.

You configure only NSX-vSphere Adapters for collecting data from the NSX components in Region B. You can access the information about the networking device topology in your environment without creating Network Devices Adapter instances for Region B because this information is available from the Network Devices Adapter in Region A.

Procedure

1. Configure User Privileges in NSX Manager for Integration with vRealize Operations Manager for Region B

   Assign the permissions to the service account svc-vrops-nsx that are required to access monitoring data from the NSX Manager instances in the region in vRealize Operations Manager.

2. Add NSX-vSphere Adapter Instances to vRealize Operations Manager for Region B

   Configure the connection between vRealize Operations Manager and the NSX Manager instances in the region.

Configure User Privileges in NSX Manager for Integration with vRealize Operations Manager for Region B

Assign the permissions to the service account svc-vrops-nsx that are required to access monitoring data from the NSX Manager instances in the region in vRealize Operations Manager.

Procedure

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

   a. Open an SSH connection to the NSX Manager virtual machine.

NSX Manager	Host name
NSX Manager for the management cluster	lax01m01nsx01.lax01.rainpole.local
NSX Manager for the shared compute and edge cluster	lax01w01nsx01.lax01.rainpole.local

   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_admin_password*

2. Create the local service account svc-vrops-nsx on the NSX Manager instance.

   a. Run the following command to switch to Privileged mode of NSX Manager.

   ```
   enable
   ```

   b. Enter the admin password when prompted and press Enter.

   c. Switch to Configuration mode.

   ```
   configure terminal
   ```

d Create the service account svc-vrops-nsx.

```
user svc-vrops-nsx password plaintext svc-vrops-nsx_password
```

e Assign the svc-vrops-nsx user access to NSX Manager from the vSphere Web Client.

```
user svc-vrops-nsx privilege web-interface
```

f Commit these updates to NSX Manager.

```
write memory
```

g Exit the Configuration mode.

```
exit
```

3 Assign the **security_admin** role to the svc-vrops-nsx service account.

a Log in to the Windows host that has access to your data center.

b Start the Postman application and log in.

c Select **POST** from the drop-down menu that contains the HTTP request methods.

d In the URL text box next to the selected method, enter the following URL.

NSX Manager	POST URL
NSX Manager for the management cluster	https://lax01m01nsx01.lax01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true
NSX Manager for the shared edge and compute cluster	https://lax01w01nsx01.lax01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true

e On the **Authorization** tab, configure the following authorization settings and click **Update Request.**

Setting	Value
Type	Basic Auth
User name	admin
Password	*nsx_admin_password*

f On the **Headers** tab, enter the following header details.

Setting	Value
Key	Content-Type
Value	text/xml

g In the **Body** tab, select **raw** and paste the following request body in the **Body** text box and click **Send**.

```
<accessControlEntry>
  <role>security_admin</role>
  <resource>
    <resourceId>globalroot-0</resourceId>
  </resource>
</accessControlEntry>
```

The Status changes to `204 No Content`.

h Repeat the step for the other NSX Manager instance.

Add NSX-vSphere Adapter Instances to vRealize Operations Manager for Region B

Configure the connection between vRealize Operations Manager and the NSX Manager instances in the region.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Solutions**.

4 On the **Solutions** page, select **Management Pack for NSX-vSphere** from the solution table, and click **Configure**.

5 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, from the **Adapter Type** table at the top, select **NSX-vSphere Adapter**.

6 Under **Instance Settings**, enter the settings for connection to the NSX Manager instance.

   a If you already have added another NSX-vSphere Adapter, click the **Add** icon to add an adapter settings.

   b Enter the display name, the FQDN of the NSX Manager instance and the FQDN of the vCenter Server instance that is connected to NSX Manager.

Setting	Value for the NSX Manager for the Management Cluster	Value for the NSX Manager for the Shared Edge and Compute Cluster
Display Name	NSX Adapter - lax01m01nsx01	NSX Adapter - lax01w01nsx01
Description	Management NSX Manager for lax01	Compute NSX Manager for lax01
NSX Manager Host	lax01m01nsx01.lax01.rainpole.local	lax01w01nsx01.lax01.rainpole.local
VC Host	lax01m01vc01.lax01.rainpole.local	lax01w01vc01.lax01.rainpole.local
Enable Log Insight integration if configured	false	false

   c Click the **Add** icon next to the **Credential** text box, configure the credentials for the connection to NSX Manager and vCenter Server, and click **OK**.

Setting	Value for the NSX Manager for the Management Cluster	Value for the NSX Manager for the Shared Edge and Compute Cluster
Credential name	NSX Adapter Credentials - lax01m01nsx01	NSX Adapter Credentials - lax01w01nsx01
NSX Manager User Name	svc-vrops-nsx	svc-vrops-nsx
NSX Manager Password	*svc-vrops-nsx_password*	*svc-vrops-nsx_password*
vCenter User Name	svc-vrops-nsx@rainpole.local	svc-vrops-nsx@rainpole.local
vCenter Password	*svc-vrops-nsx-password*	*svc-vrops-nsx-password*

   d Click **Test Connection** to validate the connection to the NSX Manager instance.

   The NSX Manager certificate appears.

   e In the **Review and Accept Certificate** dialog box, verify the certificate information and click **Accept**.

   f Click **OK** in the **Info** dialog box.

   g Expand the **Advanced Settings** section of settings.

   h From the **Collectors/Groups** drop-down menu, select the **lax01-remote-collectors** remote collector group

   i Click **Save Settings.**

   j Click **OK** in the **Info** dialog box.

   k Repeat this procedure to create an NSX-vSphere Adapter for the other NSX Manager instance.

7 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, click **Close**.

The NSX-vSphere Adapters for Region B appear on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapters is `Collecting` and the **Collection Status** is `Data receiving`.

Add Storage Devices Adapters in vRealize Operations Manager for Region B

Configure a Storage Devices adapter for Region B to collect monitoring data about the storage devices in the SDDC. Each adapter communicates with a vCenter Server instance to retrieve data about the storage devices from the vCenter Server inventory.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

  a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

  b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Solutions**.

4 On the **Solutions** page, select **Management pack for Storage Devices** from solution table and click **Configure**.

  The **Manage Solution - Management Pack for Storage Devices** dialog box appears.

5 Under **Instance Settings**, enter the settings for connection to the vCenter Server instances.

  a If you already have added another Storage Devices adapter, click the **Add** icon on the left side to add an adapter settings.

  b Enter the display name, description, and FQDN of the vCenter Server instance.

Setting	Value for the Management Cluster	Value for the Shared Edge and Compute Cluster
Display Name	Storage Devices Adapter - lax01m01vc01	Storage Devices Adapter - lax01w01vc01
Description	Storage Devices in Management vCenter for lax01	Storage Devices in Compute vCenter for lax01
vCenter Server	lax01m01vc01.lax01.rainpole.local	lax01w01vc01.lax01.rainpole.local
SNMP Community Strings	-	-

c Click the **Add** icon on the right side, configure the collection credentials for connection to the vCenter Server instances, and click **OK**.

vCenter Server Credentials Attribute	Value
Credential name	■ Storage Devices Adapter Credentials - lax01m01vc01 ■ Storage Devices Adapter Credentials - lax01w01vc01
User Name	svc-vrops-mpsd@rainpole.local
Password	*svc-vrops-mpsd-password*

d Click **Test Connection** to validate the connection to the vCenter Server.

The vCenter Server certificate appears.

e In the **Review and Accept Certificate** dialog box, verify the vCenter Server certificate information and click **Accept**.

f Click **OK** in the **Info** dialog box.

g Expand the **Advanced Settings** section of settings

h From the **Collectors/Groups** drop-down menu, select the **lax01-remote-collectors** remote collector group.

i Click **Save Settings**.

j Click **OK** in the **Info** dialog box that appears.

k Repeat the procedure for the other vCenter Server instance.

6 In the **Manage Solution - Management Pack for Storage Devices** dialog box, click **Close**.

The Storage Devices adapters for Region B appear on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapters is `Collecting` and the **Collection Status** is `Data receiving`.

Enable vSAN Monitoring in vRealize Operations Manager in Region B

Configure the vRealize Operations Management Pack for vSAN to view the vSAN topology in Region B, and to monitor the capacity and problems.

Turn On vSAN Performance Service in Region B

When you create a vSAN cluster, the performance service is disabled. Turn on the vSAN performance service to monitor the performance of vSAN clusters, hosts, disks, and VMs.

When you turn on the performance service, vSAN places a Stats database object in the datastore to collect statistical data. The Stats database is a namespace object in the vSAN datastore of the cluster.

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**, expand the **lax01-m01dc** data center object.

3 Click the **lax01-m01-mgmt01** cluster object and click the **Configure** tab.

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

5 Next to the **Performance Service** settings, click **Edit**, configure the following settings and click **OK**.

Setting	Value
Turn ON vSAN performance service	Selected
Storage policy	vSAN Default Storage Policy

6 If you have vSAN configured in the shared edge and compute lax01-w01-comp01 cluster in Region B, repeat the procedure.

Add a vSAN Adapter in vRealize Operations Manager in Region B

Configure vSAN adapter to collect monitoring data in Region B about vSAN usage in the SDDC.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Solutions**.

4 On the **Solutions** page, select **VMware vSAN** from the solution table, and click **Configure**.

   The **Manage Solution - VMware vSAN** dialog box appears.

5 Under **Instance Settings**, enter the settings for connection to the Management vCenter Server instance.

a If you already have added another vSAN adapter, click the **Add** icon on the left side to add an adapter settings.

b Enter the settings for connection to the vCenter Server.

Setting	Value for the Management vCenter
Display Name	vSAN Adapter - lax01m01vc01
Description	Management vCenter Server VSAN Adapter for lax01
vCenter Server	lax01m01vc01.lax01.rainpole.local

c Click the **Add** icon, and configure the credentials for connection to vCenter Server, and click **OK**.

Setting	Value for the Management vCenter
Credential name	vSAN Adapter Credentials - lax01m01vc01
vCenter User Name	svc-vrops-vsan@rainpole.local
vCenter Password	*svc-vrops-vsan-password*

d Click **Test Connection** to validate the connection to vCenter Server.

The vCenter Server certificate appears.

e In the **Review and Accept Certificate** dialog box, verify the vCenter Server certificate information and click **Accept**.

f Click **OK** in the **Info** dialog box.

g Expand the **Advanced Settings** section of settings.

h From the **Collectors/Groups** drop-down menu, select the **lax01-remote-collectors** collector group.

i Make sure **Auto Discovery** is set to `true`.

j Click **Save Settings.**

k Click **OK** in the **Info** dialog box that appears.

6 Iif you have vSAN configured in the shared edge and compute cluster, repeat Step 5.

7 In the **Manage Solution - VMware vSAN** dialog box, click **Close**.

The vSAN Adapter appears on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is `Collecting` and the **Collection Status** is `Data receiving`.

Configure NTP Server on vRealize Operations Manager Cluster in Region B

To avoid misconfiguration of vRealize Opertions Manager analytics cluster in case of failover to Region B during disaster recovery, add the NTP server in Region B to the time synchronization settings of vRealize Operations Manager.

Procedure

1. Log in to vRealize Operations Manager by using the operations interface.
   a. Open a Web browser and go to `https://vrops01svr01.rainpole.local`.
   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2. On the main navigation bar, click **Administration**.
3. In the left pane of vRealize Operations Manager, expand **Management** and click **Cluster Management**.
4. Select **Network Time Protocol Settings** from **Actions** menu.
5. In **Global Network Time Protocol Settings** dialog box, enter `Region B NTP Server` in to **NTP Server Address** and click **Add**.
6. Click **OK**.

vRealize Log Insight Implementation in Region B

Deploy vRealize Log Insight in a cluster configuration of 3 nodes in Region B. This configuration is set up with an integrated load balancer and uses one master and two worker nodes.

Procedure

1. Deploy vRealize Log Insight in Region B

   Start the deployment of vRealize Log Insight in Region B by deploying the master and worker nodes and forming the vRealize Log Insight cluster.

2. Replace the Certificate to vRealize Log Insight in Region B

   After you generate the PEM certificate chain file that contains the own certificate, the signer certificate and the private key file by using the `CertGenVVD` utility, upload the certificate chain to vRealize Log Insight to support trusted connection to the vRealize Log Insight user interface.

3. Connect vRealize Log Insight to the vSphere Environment in Region B

   Start collecting log information about the ESXi and vCenter Server instances in the SDDC in Region B.

4 Connect vRealize Log Insight to vRealize Operations Manager in Region B

Connect vRealize Log Insight in Region B to vRealize Operations Manager so that you can use the Launch in Context functionality between the two applications, allowing for you to troubleshoot management nodes and vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.

5 Connect vRealize Log Insight to the NSX Instances in Region B

Install and configure the vRealize Log Insight Content Pack for NSX for vSphere for log visualization and alerting of the NSX for vSphere real-time operation in Region B. You can use the NSX-vSphere dashboards to monitor logs about installation and configuration, and about virtual networking services.

6 Collect Operating System Logs from the Management Virtual Appliances in vRealize Log Insight in Region B

Install and configure the vRealize Log Insight Content Pack for Linux to visualize and analyze operating system logs from the management virtual appliances.

7 Configure Log Retention and Archiving in Region B

In vRealize Log Insight in Region B, configure log retention for one week and archiving on storage sized for 90 days according to the *Architecture and Design* documentation.

8 Configure Event Forwarding Between Region A and Region B

According to vRealize Log Insight Design, vRealize Log Insight is not failed over to the recovery region. Use log event forwarding in vRealize Log Insight to retain real-time logs in the protected region if one region becomes unavailable.

Deploy vRealize Log Insight in Region B

Start the deployment of vRealize Log Insight in Region B by deploying the master and worker nodes and forming the vRealize Log Insight cluster.

Procedure

1 Prerequisites for Deploying vRealize Log Insight in Region B

Before you deploy vRealize Log Insight in Region B, verify that your environment satisfies the requirements for this deployment.

2 Deploy the Virtual Appliance for Each Node in the vRealize Log Insight Cluster in Region B

Use the vSphere Web Client to deploy each vRealize Log Insight node as a virtual appliance on the management cluster in Region B.

3 Configure a DRS Anti-Affinity Rule for vRealize Log Insight in Region B

To protect the vRealize Log Insight cluster in Region B from a host-level failure, configure vSphere DRS to run the worker virtual appliances on different hosts in the management cluster.

4 Start the vRealize Log Insight Instance in Region B

Configure and start the vRealize Log Insight master node in Region B. Before you form a cluster by adding the worker nodes, vRealize Log Insight must be running.

5 Join the Worker Nodes to vRealize Log Insight in Region B

After you deploy the virtual appliances for vRealize Log Insight and start the vRealize Log Insight instance on the master node in Region B, join the two worker nodes to form a cluster.

6 Enable the Integrated Load Balancer of vRealize Log Insight in Region B

After you join the master and the worker nodes to create a vRealize Log Insight cluster in Region B, enable the Integrated Load Balancer (ILB) to route incoming ingestion traffic of syslog data among the Log Insight nodes and for high availability.

7 Join vRealize Log Insight to the Active Directory in Region B

To propagate user roles in vRealize Log Insight that are maintained centrally and are inline with the other solutions in the SDDC, configure vRealize Log Insight in Region B to use the Active Directory (AD) domain as an authentication source.

Prerequisites for Deploying vRealize Log Insight in Region B

Before you deploy vRealize Log Insight in Region B, verify that your environment satisfies the requirements for this deployment.

IP Addresses and Host Names

Verify that static IP addresses and FQDNs for the vRealize Log Insight virtual application network are available for Region B of the SDDC deployment.

For the application virtual network, allocate 3 static IP addresses for the vRealize Log Insight nodes and one IP address for the integrated load balancer. Map host names to the IP addresses.

Note Region B must be routable via the vSphere management network.

Table 3-3. IP Addresses and Host Name for the vRealize Log Insight Cluster in Region B

Role	IP Address	FQDN
Integrated load balancer VIP address	192.168.32.10	lax01vrli01.lax01.rainpole.local
Master node	192.168.32.11	lax01vrli01a.lax01.rainpole.local
Worker node 1	192.168.32.12	lax01vrli01b.lax01.rainpole.local
Worker node 2	192.168.32.13	lax01vrli01c.lax01.rainpole.local
Default gateway	192.168.32.1	-
DNS servers	■ 172.17.11.5 ■ 172.17.11.4	-
Subnet mask	255.255.255.0	-
NTP servers	■ 172.16.11.251 ■ 172.16.11.252 ■ 172.17.11.251 ■ 172.17.11.252	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Deployment Prerequisites

Prerequisite	Value
Storage	■ Virtual disk provisioning ■ Thin ■ Required storage per node ■ Initial storage for node deployment: 510 GB ■ Required storage for cluster archiving ■ Initial storage for archiving: 400 GB
Software Features	■ Verify that the vCenter Server instances are operational. ■ Verify that the vSphere cluster has DRS and HA enabled. ■ Verify that the NSX Manager instances are operational. ■ Verify that vRealize Operations Manager is operational. ■ Verify that the application virtual network is available. ■ Verify that the Postman application is installed. ■ Verify the following NFS datastore requirements: ■ Create an NFS share of 400 GB in Region and export it as `/V2D_vRLI_MgmtA_400GB`. ■ Create an NFS share of 250 GB in Region and export it as `/V2D_vRLI_Consolidated_250GB`. ■ Verify that the NFS server supports NFS v3. ■ Verify that the NFS partition allows read and write operations for guest accounts. ■ Verify that the mount does not require authentication. ■ Verify that the NFS share is directly accessible to vRealize Log Insight ■ If using a Windows NFS server, allow unmapped user Unix access (by UID/GID).
Installation Package	Download the `.ova` file of the vRealize Log Insight virtual appliance on the machine where you use the vSphere Web Client.
License	Obtain a license that covers the use of vRealize Log Insight.
Active Directory	Verify that you have a parent and child Active Directory domain controllers configured with the role-specific SDDC users and groups for the rainpole.local domain.
Certificate Authority	Configure the Active Directory domain controller as a certificate authority for the environment.
E-mail account	Provide an email account to send vRealize Log Insight notifications from.

Deploy the Virtual Appliance for Each Node in the vRealize Log Insight Cluster in Region B

Use the vSphere Web Client to deploy each vRealize Log Insight node as a virtual appliance on the management cluster in Region B.

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 Navigate to the lax01m01vc01.lax01.rainpole.local vCenter Server object.

3 Right-click **lax01m01vc01.lax01.rainpole.local** and select **Deploy OVF Template**.

4 On the **Select source** page, select **Local file**, click **Browse** and browse to the location of the vRealize Log Insight `.ova` file on your local file system, and click **Next**.

5 On the **Select name and folder** page, make the following selections, and click **Next**.

   a Enter a name for the node according to its role.

Name	Role
lax01vrli01a	Master node
lax01vrli01b	Worker node 1
lax01vrli01c	Worker node 2

   b Select the inventory folder for the virtual appliance.

Object	Value
vCenter Server	lax01m01vc01.lax01.rainpole.local
Data center	lax01-m01dc
Folder	lax01-m01fd-vrli

6 On the **Select a resource** page, select the **lax01-m01-mgmt01** management cluster as the resource to run the virtual appliance on, and click **Next**.

Setting	Value
Data center	lax01-m01dc
Cluster	lax01-m01fd-mgmt01

7 On the **Review details** page, examine the virtual appliance details, such as product, version, download size, and disk size, and click **Next**.

8 On the **Accept License Agreements** page, click **Accept** to accept the end user license agreements and click **Next**.

9 On the **Select configuration** page, from the **Configuration** drop-down menu, select the **Medium** deployment configuration, and click **Next**.

10 On the **Select storage** page, select the following datastore, configure its 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, select the distributed port group on the lax01-m01-vds01 distributed switch that ends with `Mgmt-RegionB01-VXLAN`, and click **Next**.

12 On the **Customize template** page, set the networking settings and the root user credentials for the virtual appliance.

a In the **Networking Properties** section, configure the following networking settings.

Property	Value
DNS server	172.17.11.5,172.17.11.4
DNS domain	lax01.rainpole.local
DNS searchpath	lax01.rainpole.local,rainpole.local
Default gateway	192.168.32.1
Host name	■ lax01vrli01a.lax01.rainpole.local for the master node ■ lax01vrli01b.lax01.rainpole.local for the worker node 1 ■ lax01vrli01c.lax01.rainpole.local for the worker node 2
Static IPv4 address	■ 192.168.32.11 for the master node ■ 192.168.32.12 for the worker node 1 ■ 192.168.32.13 for the worker node 2
Subnet mask	255.255.255.0

b In the **Other Properties** section, enter and confirm a password for the root user and click **Next**.

The password must contain at least 8 characters, and must include:

- One uppercase character
- One lowercase character
- One digit
- One special character

Use this password if you log in to the console of the vRealize Log Insight virtual appliance.

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

The deployment of the virtual appliance starts.

14 Right-click the virtual appliance object and select the **Power > Power On** menu item.

15 Repeat the procedure to deploy the vRealize Log Insight virtual appliances for the remaining two nodes in the cluster.

Configure a DRS Anti-Affinity Rule for vRealize Log Insight in Region B

To protect the vRealize Log Insight cluster in Region B from a host-level failure, configure vSphere DRS to run the worker virtual appliances on different hosts in the management cluster.

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 Navigate to the **lax01m01vc01.lax01.rainpole.local** vCenter Server object, and under the **lax01-m01dc** data center object select the **lax01-m01-mgmt01** cluster.

3 On the **Configure** tab, select **VM/Host Rules**.

4 In the **VM/Host Rules** list, click the **Add** button above the rules list, add a new anti-affinity rule using the following details and click **OK**.

Rule Attribute	Value
Name	anti-affinity-rule-vrli
Enable rule	Yes
Type	Separate Virtual Machines
Members	■ lax01vrli01a ■ lax01vrli01b ■ lax01vrli01c

Start the vRealize Log Insight Instance in Region B

Configure and start the vRealize Log Insight master node in Region B. Before you form a cluster by adding the worker nodes, vRealize Log Insight must be running.

Procedure

1 Open a Web browser and go to **`https://lax01vrli01a.lax01.rainpole.local`**.

   The initial configuration wizard opens.

2 On the **Setup** page, click **Next**.

3 On the **Choose Deployment Type** page, click **Start New Deployment**.

4 After the deployment is launched, on the **Admin Credentials** page, set the email address and the password of the admin user, and click **Save and Continue**.

   The password must contain at least 8 characters, and contain one uppercase character, one lowercase character, one number, and one special character.

5 On the License page, enter the license key, click **Add New License Key**, and click **Continue**.

6 On the **General Configuration** page, enter the following settings and click **Save and Continue**.

Setting	Value
Email System Notifications to	*email address to receive system notifications*
Send HTTP Post System Notifications To	https://lax01vrli01.lax01.rainpole.local

7 On the **Time Configuration** page, enter the following settings, click **Test** and click **Save and Continue**.

Setting	Value
Sync Server Time With	NTP Server (recommended)
NTP Servers	ntp.lax01.rainpole.local, ntp.sfo01.rainpole.local

8 On the **SMTP Configuration** page, specify the properties of an SMTP server to enable outgoing alerts and system notification emails, and to test the email notification.

   a Set the connection setting for the SMTP server that will send the email messages from vRealize Log Insight.

   Contact your system administrator for details about the email server.

SMTP Option	Description
SMTP Server	*FQDN of the SMTP server*
Port	*Server port for SMTP requests*
SSL (SMTPS)	*Enable or disable encryption for the SMTP transport*
STARTTLS Encryption	*Enable or disable the STARTTLS encryption*
Sender	*Address that appears as the sender of the email*
Username	*User name on the SMTP server*
Password	*Password for the SMTP server you specified in Username*

   b To verify that the SMTP configuration is correct, enter a valid email address and click **Send > Test Email**.

   vRealize Log Insight sends a test email to the address that you provided.

9 On the **Setup Complete** page, click **Finish**.

vRealize Log Insight starts operating in standalone mode.

Join the Worker Nodes to vRealize Log Insight in Region B

After you deploy the virtual appliances for vRealize Log Insight and start the vRealize Log Insight instance on the master node in Region B, join the two worker nodes to form a cluster.

Procedure

1 For each worker node appliance, go to the initial setup UI in your Web browser.

Worker Node	HTTP URL
Worker node 1	https://lax01vrli01b.lax01.rainpole.local
Worker node 2	https://lax01vrli01c.lax01.rainpole.local

The initial configuration wizard opens.

2 Click the **Next** button on the **Welcome** page.

3 On the **Choose Deployment Type** page, click **Join Existing Deployment**.

4 On the **Join Existing Deployment** page, enter the master node FQDN `lax01vrli01a.lax01.rainpole.local` and click **Go**.

The worker node sends a request to the vRealize Log Insight master node to join the existing deployment.

5 After the worker node contacts the master node, click the **Click here to access the Cluster Management page** link.

The login page of the vRealize Log Insight user interface opens.

6 Log in to the vRealize Log Insight UI by using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

The **Cluster** page opens in the Log Insight user interface.

7 On the right of the notification message about adding the worker node, click **Allow**.

After you join the first worker node to the cluster, the user interface displays a warning message that another worker node must be added.

8 Repeat the steps to join the second worker node to the cluster.

After you add the second worker node, the **Cluster** page of the vRealize Log Insight UI contains the master and worker nodes as components of the cluster.

Enable the Integrated Load Balancer of vRealize Log Insight in Region B

After you join the master and the worker nodes to create a vRealize Log Insight cluster in Region B, enable the Integrated Load Balancer (ILB) to route incoming ingestion traffic of syslog data among the Log Insight nodes and for high availability.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://lax01vrli01a.lax01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 Click the configuration drop-down menu icon ☰ and select **Administration**.

3 Under **Management**, click **Cluster**.

4 Under **Integrated Load Balancer**, click **New Virtual IP Address**.

5 In the **New Virtual IP** dialog box, enter the following settings and click **Save**.

Setting	Value
IP	192.168.32.10
FQDN	lax01vrli01.lax01.rainpole.local

Join vRealize Log Insight to the Active Directory in Region B

To propagate user roles in vRealize Log Insight that are maintained centrally and are inline with the other solutions in the SDDC, configure vRealize Log Insight in Region B to use the Active Directory (AD) domain as an authentication source.

Figure 3-1. Procedure

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 On the **Authentication** page, select the check box to enable the support for Active Directory, then configure the Active Directory settings.

 a Configure the Active Directory connection settings according to the details from your IT administrator.

Setting	Value
Enable Active Directory support	Selected
Default Domain	RAINPOLE.LOCAL
Domain Controller(s)	dc51rpl.rainpole.local
User Name	svc-vrli
Password	*svc_vrli_password*
Connection Type	Standard
Require SSL	Yes or No according to the instructions from the IT administrator

 b Click **Test Connection** to verify the connection, and click **Save**.

Replace the Certificate to vRealize Log Insight in Region B

After you generate the PEM certificate chain file that contains the own certificate, the signer certificate and the private key file by using the `CertGenVVD` utility, upload the certificate chain to vRealize Log Insight to support trusted connection to the vRealize Log Insight user interface.

Procedure

1 Log in to the vRealize Log Insight user interface.

 a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

 b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 In the vRealize Log Insight UI, click the configuration drop-down menu icon ☰ and select **Administration**.

3 Under **Configuration**, click **SSL**.

4 On the **SSL Configuration** page, next to **New Certificate File (PEM format)** click **Choose File**, browse to the location of the PEM file on your computer, and click **Save**.

Certificate Generation Option	Certificate File
Using the CertGenVVD tool	vrli.lax01.2.chain.pem

The certificate is uploaded to vRealize Log Insight.

5. In a Web browser, go to **`https://lax01vrli01.lax01.rainpole.local`**.

   A warning message that the connection is not trusted appears.

6. To review the certificate, click the padlock icon in the address bar of the browser, and verify that the **Subject Alternative Name** contains the names of the vRealize Log Insight cluster nodes.

7. Import the certificate in your Web browser.

   For example, in Google Chrome under the **HTTPS/TLS** settings click the **Manage certificates** button, and in the **Certificates** dialog box import `vrli.lax01.2.chain.pem`.

   You can also use Certificate Manager on Windows or Keychain Access on MAC OS X.

Connect vRealize Log Insight to the vSphere Environment in Region B

Start collecting log information about the ESXi and vCenter Server instances in the SDDC in Region B.

Procedure

1. Connect vRealize Log Insight to vSphere in Region B

   After you configure the svc-vrli-vsphere Active Directory user with the vSphere privileges that are required for retrieving log information from the vCenter Server instances and ESXi hosts, connect vRealize Log Insight to vSphere.

2. Configure vCenter Server to Forward Log Events to vRealize Log Insight in Region B

   You can configure each vCenter Server and Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster. You can then view and analyze all syslog information in the vRealize Log Insight web interface.

3. Update the Host Profiles for the Management and Shared Edge and Compute Clusters with Syslog Settings in Region B

   To have a consistent logging configuration across all ESXi hosts in the clusters in Region B, update the host profile in each cluster to accommodate the syslog settings for connection to vRealize Log Insight.

Connect vRealize Log Insight to vSphere in Region B

After you configure the svc-vrli-vsphere Active Directory user with the vSphere privileges that are required for retrieving log information from the vCenter Server instances and ESXi hosts, connect vRealize Log Insight to vSphere.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to `https://lax01vrli01.lax01.rainpole.local`.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 Click the configuration drop-down menu icon ☰ and select **Administration**.

3 Under **Integration**, click **vSphere**.

4 In the **vCenter Servers** pane, enter the connection settings for the Management vCenter Server and for the Compute vCenter Server.

   a Enter the host name, user credentials, and collection options for the vCenter Server instances, and click **Test Connection**.

vCenter Server Option	Value
Hostname	■ lax01m01vc01.lax01.rainpole.local for Management vCenter Server ■ lax01w01vc01.lax01.rainpole.local for Compute vCenter Server
Username	svc-vrli-vsphere@rainpole.local
Password	*svc-vrli-vsphere_user_password*
Collect vCenter Server events, tasks and alarms	Selected
Configure ESXi hosts to send logs to Log Insight	Selected

   b Click **Advanced Options** and examine the list of ESXi hosts that are connected to the vCenter Server instance to verify that you connect to the correct vCenter Server.

   c In the **Advanced Options** configuration window, select **Configure all ESXi hosts**, select **UDP** under Syslog protocol, and click **OK**.

5 Click **Add vCenter Server** to add a new settings form and repeat the steps to add the settings for the second vCenter Server instance in Region B.

6 Click **Save**.

   A progress dialog box appears.

7 Click **OK** in the confirmation dialog box that appears after vRealize Log Insight contacts the vCenter Server instances.

You see the vSphere dashboards under the VMware - vSphere content pack dashboard category.

Configure vCenter Server to Forward Log Events to vRealize Log Insight in Region B

You can configure each vCenter Server and Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster. You can then view and analyze all syslog information in the vRealize Log Insight web interface.

In Region B, you configure the following vCenter Server and Platform Services Controller instances:

Appliance Type	Appliance Management Interface URL
vCenter Server instances	▪ https://lax01m01vc01.lax01.rainpole.local:5480 ▪ https://lax01w01vc01.lax01.rainpole.local:5480
Platform Services Controller instances	▪ https://lax01m01psc01.lax01.rainpole.local:5480 ▪ https://lax01w01psc01.lax01.rainpole.local:5480

Procedure

1. Redirect the log events from the appliance to vRealize Log Insight.

   a. Open a Web browser and go to **`https://lax01m01vc01.lax01.rainpole.local:5480`**.

   b. Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtvc_root_password*

   c. In the **Navigator**, click **Syslog Configuration**.

   d. On the **Syslog Configuration** page, click **Edit**, configure the following settings, and click **OK**.

Setting	Value
Common Log Level	*
Remote Syslog Host	lax01vrli01.lax01.rainpole.local
Remote Syslog Port	514
Remote Syslog Protocol	UDP

   e. Repeat the steps for the other vCenter Server Appliance and Platform Services Controller Appliances.

2. Verify that the appliances are forwarding their syslog traffic to vRealize Log Insight.

   a. Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

c In the vRealize Log Insight user interface, click **Dashboards** and select **VMware - vSphere** under **Content Pack Dashboards**.

d Verify that the vCenter Server nodes are presented on the **All vSphere events by hostname** widget of the **General Overview** dashboard.

Update the Host Profiles for the Management and Shared Edge and Compute Clusters with Syslog Settings in Region B

To have a consistent logging configuration across all ESXi hosts in the clusters in Region B, update the host profile in each cluster to accommodate the syslog settings for connection to vRealize Log Insight.

Setting	Value for the Management Cluster	Value for the Shared Edge and Computer Cluster
vCenter Server URL	https://lax01m01vc01.lax01.rainpole.local/vsphere-client/	https://lax01w01vc01.lax01.rainpole.local/vsphere-client/
Host Profiles	lax01-m01hp-mgmt01	lax01-w01hp-mgmt01
First ESXi host	lax01m01esx01.lax01.rainpole.local	lax01w01esx01.lax01.rainpole.local

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 Update the host profile to the management cluster.

a From the vSphere Web Client **Home** menu, select **Home**.

b In the **Navigator**, click **Policies and Profiles** and click **Host Profiles**.

c Right-click **lax01-m01hp-mgmt01** and select **Copy Settings** from **Host**.

d Select **lax01m01esx01.lax01.rainpole.local** and click **OK**.

3 Verify that the syslog host settings have been updated.

a On the **Host Profiles** page in the Navigator, click **lax01-m01hp-mgmt01**

b On the **Configure** tab, click **Settings**.

c In **Filter** search box, type in **Syslog.global.logHost**.

d Select the **Syslog.global.logHost** entry from the list and verify that value of the option is `udp://lax01vrli01.lax01.rainpole.local:514`

4 Verify compliance for the hosts in the management cluster.

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

   b Click the **lax01-m01-mgmt01** cluster, click the **Monitor** tab, and click **Profile Compliance**.

   c Click the **Check Compliance Now button**.

   d Verify all hosts are compliant.

5 Repeat the procedure with a host in the shared edge and compute cluster.

Connect vRealize Log Insight to vRealize Operations Manager in Region B

Connect vRealize Log Insight in Region B to vRealize Operations Manager so that you can use the Launch in Context functionality between the two applications, allowing for you to troubleshoot management nodes and vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.

Procedure

1 Enable the vRealize Log Insight Integration with vRealize Operations Manager in Region B

   Connect vRealize Log Insight in Region B with vRealize Operations Manager to send alerts to vRealize Operations Manager.

2 Connect vRealize Operations Manager to vRealize Log Insight in Region B

3 Configure the Log Insight Agent on vRealize Operations Manager to Forward Log Events to vRealize Log Insight in Region B

   After you install the content pack for vRealize Operations Manager, configure the Log Insight agent on the remote collector nodes of vRealize Operations Manager in Region B to send audit logs and system events to vRealize Log Insight.

Enable the vRealize Log Insight Integration with vRealize Operations Manager in Region B

Connect vRealize Log Insight in Region B with vRealize Operations Manager to send alerts to vRealize Operations Manager.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2. In the vRealize Log Insight user interface, click the configuration drop-down menu icon ☰ and select **Administration**.
3. Under **Integration**, click **vRealize Operations**.
4. On the **vRealize Operations Manager** pane, configure the integration settings for vRealize Operations Manager.

Setting	Value
Hostname	vrops01svr01.rainpole.local
Username	svc-vrli-vrops@rainpole.local
Password	*svc-vrli-vrops_password*
Enable alerts integration	Selected
Enable launch in context	Deselected

5. Click **Test Connection** to validate the connection and click **Save**.

   A progress dialog box appears.
6. Click **OK** to close the dialog.

Connect vRealize Operations Manager to vRealize Log Insight in Region B

Configure a vRealize Log Insight Adapter to integrate vRealize Log Insight in Region B with vRealize Operations Manager in your environment. You can access unstructured log data about any object in your environment by using Launch in Context in vRealize Operations Manager.

Procedure

1. Log in to vRealize Operations Manager by using the operations interface.

   a. Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2. On the main navigation bar, click **Administration**.
3. In the left pane of vRealize Operations Manager, click **Solutions**.
4. On the **Solutions** page, select **VMware vRealize Log Insight** from the solution table, and click **Configure**.

   The **Manage Solution - VMware vRelalize Log Insight** dialog box appears.
5. Click the **Add** icon above **Instance Name**

6 Under **Instance Settings**, enter the settings for connection to vRelalize Log Insight.

   a Enter the display name, description and the FQDN of the vRealize Log Insight instance.

Setting	Value for vRealize Log Insight
Display Name	Log Insight Adapter - lax01vrli01
Description	vRealize Log Insight for lax01
Log Insight server	lax01vrli01.lax01.rainpole.local

   b Click **Save Settings**.

   c Click **OK** in the **Info** box.

7 Validate the connection to vRelaize Log Insight.

   a Click **Test Connection** to validate the connection to vRelaize Log Insight.

   b Click **OK** in the **Info** box.

8 Expand the **Advanced Settings** pane and select **lax01-remote-collectors** from the **Collectors/Groups** drop-down menu.

9 Click **Save Settings** and click **OK** in the **Info** box. .

10 In the **Manage Solution - VMware vRealize Log Insight** dialog box, click **Close**.

11 The vRealize Log Insight Adapter is available on the Solutions page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is `Collecting` and the **Collection Status** is `Data receiving`.

Configure the Log Insight Agent on vRealize Operations Manager to Forward Log Events to vRealize Log Insight in Region B

After you install the content pack for vRealize Operations Manager, configure the Log Insight agent on the remote collector nodes of vRealize Operations Manager in Region B to send audit logs and system events to vRealize Log Insight.

Procedure

1 Enable SSH on each node of vRealize Operations Manager.

   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*

c Under the lax01m01vc01.lax01.rainpole.local vCenter Server, navigate to the virtual appliance for the node.

Virtual Appliance Name	Role
lax01vropsc01a	Remote collector 1
lax01vropsc01b	Remote collector 2

d Right-click the appliance node and select **Open Console** to open the remote console to the appliance.

e Press **ALT+F1** to switch to the command prompt.

f Log in using the following credentials.

Setting	Value
User name	root
Password	*vrops_root_password*

g Start the SSH service by running the command.

```
service sshd start
```

h Close the virtual appliance console.

i Repeat the step for other appliance nodes.

2 Configure the Log Insight agent in vRealize Operation Manager

a Open an SSH connection to the vRealize Operations Manager appliances using the following settings.

Setting	Value
Hostname	■ lax01vropsc01a.lax01.rainpole.local ■ lax01vropsc01b.lax01.rainpole.local
Username	root
Password	*vrops_root_password*

b Edit the `liagent.ini` file on each vRealize Operations Manager node using a text editor such as `vi`.

```
vi /var/lib/loginsight-agent/liagent.ini
```

c Locate the `[server]` section and uncomment the following parameters.

```
[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
hostname=lax01vrli01.lax01.rainpole.local
; Set protocol to use:
; cfapi – Log Insight REST API
; syslog – Syslog protocol
; If omitted the default value is cfapi
proto=cfapi
; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 512
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
port=9000
;ssl – enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is no.
ssl=no
; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30
```

d After the `[server]` section, add the following block on each vRealize Operations Manager node.

```
[common|filelog] tags={"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_clustername":"vrops01svr01",
"vmw_vr_ops_clusterrole":"Remote Collector", "vmw_vr_ops_nodename":"<Your vROPS Node Name
Here>", "vmw_vr_ops_hostname":"<Your vROPS Hostname Here>"}
```

Modify the following parameters specifically for each node.

Parameter	Description	Location in liagent.ini
vmw_vr_ops_nodename	IP address or FQDN of the vRealize Operations Manager node	Replace each **<Your VROPS Node Name Here>** with the following names: ■ lax01vropsc01a ■ lax01vropsc01b
vmw_vr_ops_hostname	Name of the vRealize Operations Manager node that is set during node initial configuration	Replace each **<Your VROPS Hostname Here>** with the following names: ■ lax01vropsc01a.lax01.rainpole.local ■ lax01vropsc01b.lax01.rainpole.local

e Modify the following parameters specifically for each node.

Parameter	Description	Location in liagent.ini
vmw_vr_ops_nodename	IP address or FQDN of the vRealize Operations Manager node	Replace each **<Your VROPS Node Name Here>** with the following names: ■ lax01vropsc01a ■ lax01vropsc01b
vmw_vr_ops_hostname	Name of the vRealize Operations Manager node that is set during node initial configuration	Replace each **<Your VROPS Hostname Here>** with the following names: ■ lax01vropsc01a.lax01.rainpole.local ■ lax01vropsc01b.lax01.rainpole.local

For example, on the first remote collector node you change the `[common|filelog]` section to add context to the logs that are sent to the vRealize Log Insight cluster:

```
[common|filelog]
tags={"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_clustername":"vrops01svr01",
"vmw_vr_ops_clusterrole":"Remote Collector", "vmw_vr_ops_nodename":"lax01vropsc01a",
"vmw_vr_ops_hostname":"lax01vropsc01a.lax01.rainpole.local"}
```

f Press Esc and enter `:wq!` to save the file.

g Restart the Log Insight agent on node by running the following console command.

```
/etc/init.d/liagentd restart
```

h Verify that the Log Insight agent is running.

```
/etc/init.d/liagentd status
```

i Stop the SSH service on the virtual appliance by running the following command.

```
service sshd stop
```

j Repeat the steps for the second remote collector node.

3 Configure the Agent Group for the vRealize Operations Manager components from the vRealize Log Insight Web user interface.

a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

c Click the configuration drop-down menu icon ☰ and select **Administration**.

d Under **Management**, click **Agents**.

e From the drop-down menu on the top, select **vRops 6.4 or higher - Sample** from the **Available Templates** section.

f Click **Copy Template**.

g In the **Copy Agent Group** dialog box, enter `vROPs – Appliance Agent Group` in the **Name** text box and click **Copy**.

h In the **agent filter** fields, enter the following values pressing Enter after each host name.

Filter	Operator	Value
Hostname	matches	■ lax01vropsc01a.lax01.rainpole.local ■ lax01vropsc01b.lax01.rainpole.local

i Click **Refresh** and verify that all the agents in the filter appear in the **Agents** list.

j Click **Save New Group** at the bottom of the page.

k Click the **Dashboard** tab and select the **VMware - vRops** link from the navigation menu on the left.

You see log information about the operation of the remote collectors of vRealize Operations Manager in Region B on the **VMware - vROps 6.x** Log Insight dashboards.

Connect vRealize Log Insight to the NSX Instances in Region B

Install and configure the vRealize Log Insight Content Pack for NSX for vSphere for log visualization and alerting of the NSX for vSphere real-time operation in Region B. You can use the NSX-vSphere dashboards to monitor logs about installation and configuration, and about virtual networking services.

Procedure

1 Install the vRealize Log Insight Content Pack for NSX for vSphere in Region B

Install the content pack for NSX for vSphere to add the dashboards for viewing log information in vRealize Log Insight in Region B.

2 Configure NSX Manager to Forward Log Events to vRealize Log Insight in Region B

Configure the NSX Manager for the management cluster and the NSX Manager for the shared edge and compute cluster to send audit logs and system events to vRealize Log Insight in Region B.

3 Configure the NSX Controllers to Forward Events to vRealize Log Insight in Region B

Configure the NSX Controller instances for the management cluster and shared compute and edge cluster to forward log information to vRealize Log Insight in Region B by using the NSX REST API. To enable log forwarding, you can use a REST client, such as the Postman application.

4 Configure the NSX Edge Instances to Forward Log Events to vRealize Log Insight in Region B

Configure the NSX Edge services gateways for vRealize Operations Manager, vRealize Log Insight, and vRealize Automation to forward log information to vRealize Log Insight in Region B.

Install the vRealize Log Insight Content Pack for NSX for vSphere in Region B

Install the content pack for NSX for vSphere to add the dashboards for viewing log information in vRealize Log Insight in Region B.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon ☰ and select **Content Packs**.

3 Under **Content Pack Marketplace**, select **Marketplace**.

4 In the list of content packs, locate the **VMware - NSX-vSphere** content pack and click its icon.

5 In the **Install Content Pack** dialog box, accept the **License Agreement** and click **Install**.

6 In the **VMware - NSX-vSphere Setup Instructions** dialog box, click **OK**.

After the installation is complete, the VMware - NSX-vSphere content pack appears in the **Installed Content Packs** list on the left.

Configure NSX Manager to Forward Log Events to vRealize Log Insight in Region B

Configure the NSX Manager for the management cluster and the NSX Manager for the shared edge and compute cluster to send audit logs and system events to vRealize Log Insight in Region B.

Procedure

1 On the Windows host that has access to the data center, log in to the NSX Manager Web interface.

a Open a Web browser and go to following URL.

NSX Manager	URL
NSX Manager for the management cluster	https://lax01m01nsx01.lax01.rainpole.local
NSX Manager for the shared compute and edge cluster	https://lax01w01nsx01.lax01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 On the main page of the appliance user interface, click **Manage Appliance Settings**.

3 Under **Settings**, click **General**, and in the **Syslog Server** pane, click **Edit**.

4 In the **Syslog Server** dialog box, configure vRealize Log Insight as a syslog server by specifying the following settings and click **OK**.

Syslog Server Setting	Value
Syslog Server	lax01vrli01.lax01.rainpole.local
Port	514
Protocol	UDP

5 Repeat the steps for the other NSX Manager instance.

Configure the NSX Controllers to Forward Events to vRealize Log Insight in Region B

Configure the NSX Controller instances for the management cluster and shared compute and edge cluster to forward log information to vRealize Log Insight in Region B by using the NSX REST API. To enable log forwarding, you can use a REST client, such as the Postman application.

Procedure

1 Log in to the Windows host that has access to your data center.

2 Start the Postman application and log in.

3 Specify the request headers for requests to NSX Manager.

   a On the **Authentication** tab, configure the following authorization settings and click **Update Request.**

Setting	Value
Type	Basic Auth
Username	admin
Password	*nsx_admin_password*

   The `Authorization:Basic XXX` header appears in the **Headers** pane.

   b On the **Headers** tab, enter the following header details.

Request Header Attribute	Value
Content-Type	application/xml

   The `Content-Type:application/xml` header appears in the **Headers** pane.

4 Contact the NSX Manager to retrieve the IDs of the associated NSX Controllers.

   a Select **GET** from the drop-down menu that contains the HTTP request methods.

   b In the **URL** text box next to the selected method, enter the following URL, and click **Send**.

NSX Manager	URL
NSX Manager for the management cluster	`https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller`
NSX Manager for the shared compute and edge cluster	`https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller`

   The Postman application sends a query to the NSX Manager about the installed NSX controllers.

   c After the NSX Manager sends a response back, click the **Body** tab in the response pane.

   The response body contains a root <controllers> XML element that groups the details about the three controllers that form the controller cluster.

   d Within the <controllers> element, locate the <controller> element for each controller and write down the content of the <id> element.

   Controller IDs have the `controller-`*`id`* format where *id* represents the sequence number of the controller in the cluster, for example, `controller-4`.

   e Repeat the steps for the other NSX Manager.

5 For each NSX Controller, send a request to configure vRealize Log Insight as a remote syslog server.

a In the request pane at the top, select **POST** from the drop-down menu that contains the HTTP request methods, and in the **URL** text box, enter the following URL.

Replace *controller-ID* with the controller IDs you have written down.

NSX Manager	NSX Controller in the Controller Cluster	POST URL
NSX Manager for the management cluster	NSX Controller 4	`https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/`**`controller-4`**`/syslog`
	NSX Controller 5	`https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/`**`controller-5`**`/syslog`
	NSX Controller 6	`https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/`**`controller-6`**`/syslog`
NSX Manager for the shared edge and compute cluster	NSX Controller 4	`https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/`**`controller-4`**`/syslog`
	NSX Controller 5	`https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/`**`controller-5`**`/syslog`
	NSX Controller 6	`https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/`**`controller-6`**`/syslog`

b In the **Request** pane, click the **Body** tab, select **Raw**, and using the drop-down menu, select **XML (Application/XML)**.

c Paste the following request body in the **Body** text box and click **Send**.

```
<controllerSyslogServer>
   <syslogServer>192.168.32.10</syslogServer>
   <port>514</port>
   <protocol>UDP</protocol>
   <level>INFO</level>
</controllerSyslogServer>
```

d Repeat the steps for the other NSX Controllers in the management cluster and in the shared edge and compute cluster.

6 Verify the syslog configuration on each NSX Controller.

   a In the **Request** pane, from the **Method** drop-down menu, select **GET**, in the **URL** text box, controller-specific syslog URL from Step 5 and click the **SEND** button.

   b After the NSX Manager sends a response back, click the **Body** tab under **Response**.

   The response body contains a root <controllerSyslogServer> element that represents the settings for the remote syslog server on the NSX Controller.

   c Verify that the value of the <syslogServer> element is `192.168.32.10`.

   d Repeat the steps for the other NSX Controllers to verify the syslog configuration.

Configure the NSX Edge Instances to Forward Log Events to vRealize Log Insight in Region B

Configure the NSX Edge services gateways for vRealize Operations Manager, vRealize Log Insight, and vRealize Automation to forward log information to vRealize Log Insight in Region B.

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

3 From the **Networking & Security** menu on the left, click **NSX Edges**.

4 On the **NSX Edges** page, select the NSX Manager instance from the **NSX Manager** drop-down menu.

NSX Manager Instance	IP Address
NSX Manager for the management cluster	172.17.11.65
NSX Manager for the shared edge and compute cluster	172.17.11.66

The edge devices in the scope of the NSX Manager appear.

5 Configure the log forwarding on each edge service gateway.

a Double-click the edge device to open its user interface.

Traffic	Management NSX Edge Service Gateway	Compute NSX Edge Service Gateway
North-South Routing	lax01m01esg01	lax01w01esg01
North-South Routing	lax01m01esg02	lax01w01esg02
East-West Routing	-	lax01w01dlr01
Load Balancer	lax01m01lb01	-
PSC Load Balancer	lax01psc01	-

b On the NSX edge device page, click the **Manage** tab, click **Settings** and click **Configuration**.

c In the **Details** panel, click **Change** next to **Syslog servers**.

d In the **Edit Syslog Servers Configuration** dialog box, configure the following settings and click **OK**.

Setting	Value
Syslog server 1	192.168.32.10
Protocol	udp

e Repeat the steps for the next NSX edge device.

The vRealize Log Insight user interface in Region B starts showing log data in the **NSX-vSphere-Overview** dashboard available under the VMware - NSX-vSphere group of content pack dashboards.

Collect Operating System Logs from the Management Virtual Appliances in vRealize Log Insight in Region B

Install and configure the vRealize Log Insight Content Pack for Linux to visualize and analyze operating system logs from the management virtual appliances.

Procedure

1 Install the vRealize Log Insight Content Pack for Linux and Configure the Virtual Appliance Agent Group for vRealize Log Insight for Region B

Install the content pack for VMware Linux to add the dashboards for viewing log information in vRealize Log Insight in Region B about the operating system of the management virtual appliances.

2 Configure a Log Insight Agent Grouper for the Management Virtual Appliances in Region B

After you install the content pack for Linux, to use dashboards for operating system logs from the management virtual appliances in the SDDC, configure an agent group to easily apply common settings to the agents on the appliances in the region.

Install the vRealize Log Insight Content Pack for Linux and Configure the Virtual Appliance Agent Group for vRealize Log Insight for Region B

Install the content pack for VMware Linux to add the dashboards for viewing log information in vRealize Log Insight in Region B about the operating system of the management virtual appliances.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon ☰ and select **Content Packs**.

3 Under **Content Pack Marketplace**, select **Marketplace**.

4 In the list of content packs, locate the **Linux** content pack and click its icon.

5 In the **Install Content Pack** dialog box, accept the License Agreement and click **Install**.

6 After the installation is complete, the **Linux** content pack appears in the **Installed Content Packs** list on the left.

Configure a Log Insight Agent Grouper for the Management Virtual Appliances in Region B

After you install the content pack for Linux, to use dashboards for operating system logs from the management virtual appliances in the SDDC, configure an agent group to easily apply common settings to the agents on the appliances in the region.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 Click the configuration drop-down menu icon ☰ and select **Administration**.

3 Under **Management**, click **Agents**.

4 From the drop-down at the top, select **Linux** from the **Available Templates** section.

5 Click **Copy Template**.

6 In the **Copy Agent Group** dialog box, enter `VA – Linux Agent Group` in the **Name** text box and click **Copy**.

7 In the agent filter fields, use the following selections.

Press ENTER to separate the host name values.

Filter	Operator	Values
Hostname	matches	■ lax01vropsc01a.lax01.rainpole.local ■ lax01vropsc01b.lax01.rainpole.local

8 Click **Refresh** and verify that all the agents listed in the filter appear in the **Agents** list.

9 Click **Save New Group** at the bottom of the page.

10 Verify that log data is showing up on the Linux dashboards.

a On the main navigation bar, click **Dashboards**.

b Expand **Linux** and click **Security - Overview**.

You see events that have occurred over the past 48 hours.

Configure Log Retention and Archiving in Region B

In vRealize Log Insight in Region B, configure log retention for one week and archiving on storage sized for 90 days according to the *Architecture and Design* documentation.

Procedure

1 Log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon ☰ and select **Administration**.

3 Configure retention threshold notification.

   Log Insight continually estimates how long data can be retained with the currently available pool of storage. If the estimation drops below the retention threshold of one week, Log Insight immediately notifies the administrator that the amount of searchable log data is likely to drop.

   a Under **Configuration**, click **General**.

   b On the **General Configuration** page, under the **Alerts** section select the **Send a notification when capacity drops below** check box next to the **Retention Notification Threshold** settings, and enter a 1-week period in the text box underneath.

   c Click **Save**.

4 Configure data archiving.

   a Under **Configuration**, click **Archiving**.

   b Select the **Enable Data Archiving** check box.

   c In the **Archive Location** text box, enter the path in the form of `nfs://nfs-server-address/V2D_vRLI_MgmtB_400GB` to an NFS partition where logs will be archived.

   d Click **Test** next to the **Archive Location** text box to verify that the share is accessible.

   e Click **Save**.

Configure Event Forwarding Between Region A and Region B

According to vRealize Log Insight Design, vRealize Log Insight is not failed over to the recovery region. Use log event forwarding in vRealize Log Insight to retain real-time logs in the protected region if one region becomes unavailable.

See *vRealize Log Insight Design* and *Logging Architecture* in the *VMware Validated Design Architecture and Design* documentation.

Procedure

1 Configure Event Forwarding in Region A

   You enable log forwarding from vRealize Log Insight in Region A to vRealize Log Insight in Region B to prevent lost of Region A related logs in the event of a disaster.

2 Configure Event Forwarding in Region B

   You enable log forwarding from vRealize Log Insight in Region B to vRealize Log Insight in Region A to prevent lost of Region B related logs in the event of a disaster.

3 Add a Log Filter in Region A

   Add a filter to avoid forwarding log events already forwarded to Region A back to their source Log Insight deployment in Region B. Using a filter prevents looping when the Log Insight deployments in Region A and Region B forward logs to each other.

Configure Event Forwarding in Region A

You enable log forwarding from vRealize Log Insight in Region A to vRealize Log Insight in Region B to prevent lost of Region A related logs in the event of a disaster.

You provide the following settings for log forwarding to vRealize Log Insight in Region B:

- Inject the vRealize Log Insight's SSL certificate for Region B into the Java keystore of vRealize Log Insight node in Region A.
- Target URL, protocol and tagging
- Disk cache

  Disk cache represents the amount of local disk space you can configure to reserve for buffering events to be forwarded. Buffering is used when the remote destination is unavailable or unable to process the events sent to it. If the local buffer becomes full while the remote destination is still unavailable, the oldest local events are dropped and not forwarded to the remote destination.

Procedure

1 Import the vRealize Log Insight's SSL certificate for Region B into the Java keystore of vRealize Log Insight node in Region A.

a Open an SSH session to the vRealize Log Insight node.

Name	Role
sfo01vrli01a.sfo01.rainpole.local	Master node
sfo01vrli01b.sfo01.rainpole.local	Worker node 1
sfo01vrli01c.sfo01.rainpole.local	Worker node 2

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrli_regionA_root_password*

c Create a working directory on the vRealize Log Insight node.

```
mkdir /tmp/ssl
cd /tmp/ssl
```

d Extract the root certificate from the destination vRealize Log Insight in the Region B.

```
echo "" | openssl s_client -showcerts -servername lax01vrli01a.lax01.rainpole.local -connect
lax01vrli01a.lax01.rainpole.local:443 -prexit 2>/dev/null | sed -n -e '/BEGIN\
CERTIFICATE/,/END\ CERTIFICATE/ p' > cert.pem
csplit -f individual- cert.pem '/-----BEGIN CERTIFICATE-----/' '{*}'
root_cert=$(ls individual-* | sort -n -t- | tail -1)
cp -f -- "$root_cert" root.crt
```

e Import the `root.crt` file in the Java keystore of the vRealize Log Insight node.

```
cd /usr/java/default/lib/security/

../../bin/keytool -import -alias loginsight -file /tmp/ssl/root.crt -keystore cacerts
```

f When prompted for a keystore password, type **changeit**

g When prompted to accept the certificate, type **yes**

h Reboot the vRealize Log Insight node by running the following command.

```
reboot
```

i Wait until the vRealize Log Insight node finished rebooting.

j Repeat this operation on all vRealize Log Insight nodes in Region A.

2 Log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

3 In the vRealize Log Insight user interface, click the configuration drop-down menu icon ☰ and select **Administration**.

4 Under **Management**, click **Event Forwarding**.

5 On the **Event Forwarding** page, click **New Destination** and enter the following forwarding settings in the **New Destination** dialog box.

Forwarding Destination Setting	Value
Name	SFO01 to LAX01
Host	lax01vrli01.lax01.rainpole.local
Protocol	Ingestion API
Use SSL	Selected

Forwarding Destination Setting	Value
Tags	site='SFO01'
Advanced Settings	
Port	9543
Disk Cache	2000 MB
Worker Count	8

6 In the **New Destination** dialog box, click **Test** to verify that the connection settings are correct.

7 Click **Save** to save the forwarding new destination.

The **Event Forwarding** page in the vRealize Log Insight user interface starts showing a summary of the forwarded events.

Configure Event Forwarding in Region B

You enable log forwarding from vRealize Log Insight in Region B to vRealize Log Insight in Region A to prevent lost of Region B related logs in the event of a disaster.

You provide the following settings for log forwarding to vRealize Log Insight in Region A:

- Inject the vRealize Log Insight's SSL certificate for Region A into the Java keystore of vRealize Log Insight node in Region B.
- Target URL, protocol and tagging
- Filtering

  Add a filter to avoid forwarding log events back to the Log Insight deployment in Region A. Using a filter prevents from looping when the Log Insight deployments in Region A and Region B forward logs to each other.

- Disk cache

  Disk cache represents the amount of local disk space you can configure to reserve for buffering events to be forwarded. Buffering is used when the remote destination is unavailable or unable to process the events sent to it. If the local buffer becomes full and the remote destination is still unavailable, the oldest local events are dropped and not forwarded to the remote destination.

Procedure

1 Import the root certificate in the Java keystore on each vRealize Log Insight node in Region B.

a Open an SSH session and go to the vRealize Log Insight node.

Name	Role
lax01vrli01a.lax01.rainpole.local	Master node
lax01vrli01b.lax01.rainpole.local	Worker node 1
lax01vrli01c.lax01.rainpole.local	Worker node 2

b Log in using the following credentials.

Name	Role
User name	root
Password	*vrli_regionB_root_password*

c Create a working directory on the vRealize Log Insight node.

```
mkdir /tmp/ssl
```

```
cd /tmp/ssl
```

d Extract the root certificate from the destination vRealize Log Insight in Region A.

```
echo "" | openssl s_client -showcerts -servername sfo01vrli01a.sfo01.rainpole.local -connect
sfo01vrli01a.sfo01.rainpole.local:443 -prexit 2>/dev/null | sed -n -e '/BEGIN\
CERTIFICATE/,/END\ CERTIFICATE/ p' > cert.pem
csplit -f individual- cert.pem '/-----BEGIN CERTIFICATE-----/' '{*}'
root_cert=$(ls individual-* | sort -n -t- | tail -1)
cp -f -- "$root_cert" root.crt
```

e Import the `root.crt` in the Java keystore of the vRealize Log Insight node.

```
cd /usr/java/default/lib/security/
../../bin/keytool -import -alias loginsight -file /tmp/ssl/root.crt -keystore cacerts
```

f When prompted for a keystore password, type **`changeit`**.

g When prompted to accept the certificate, type **`yes`**.

h Reboot the vRealize Log Insight node by performing the following command.

```
reboot
```

i Wait until the vRealize Log Insight node finished rebooting.

j Repeat this operation on all vRealize Log Insight nodes in Region B.

2. Log in to the vRealize Log Insight user interface.

   a. Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

3. In the vRealize Log Insight user interface, click the configuration drop-down menu icon ☰ and select **Administration**.

4. Under **Management**, click **Event Forwarding**.

5. On the **Event Forwarding** page, click **New Destination** and enter the following forwarding settings in the **New Destination** dialog box.

Forwarding Destination Option	Value
Name	LAX01 to SFO01
Host	sfo01vrli01.sfo01.rainpole.local
Protocol	Ingestion API
Use SSL	Selected
Tags	site='LAX01'
Filter	
Filter Type	site
Operator	does not match
Value	'SFO01'
Advanced Settings	
Port	9543
Disk Cache	2000 MB
Worker Count	8

6. In the **New Destination** dialog box, click **Test** to verify that the connection settings are correct.

7. Click **Save** to save the forwarding new destination.

The **Event Forwarding** page in the vRealize Log Insight user interface starts showing a summary of the forwarded events.

Add a Log Filter in Region A

Add a filter to avoid forwarding log events already forwarded to Region A back to their source Log Insight deployment in Region B. Using a filter prevents looping when the Log Insight deployments in Region A and Region B forward logs to each other.

Procedure

1. Log in to the vRealize Log Insight user interface.

   a. Open a Web browser and go to `https://sfo01vrli01.sfo01.rainpole.local`.

   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2. In the vRealize Log Insight user interface, click the configuration drop-down menu icon ☰ and select **Administration**.

3. Under **Management**, click **Event Forwarding**.

4. Add a filter to prevent forwarding loops.

   a. In the **Event Forwarding** page of the vRealize Log Insight user interface, click the **Edit** icon of the SFO01 to LAX01 destination.

   b. In the **Edit Destination** dialog box, click **Add Filter** and enter the following filter attributes.

Filter Attribute	Value
Filter Type	site
Operator	does not match
Value	'LAX01'

5. Click **Save**.

The **Event Forwarding** page in the vRealize Log Insight user interface shows a summary of the forwarded events.

vSphere Update Manager Download Service Implementation in Region B

Install the vSphere Update Manager Download Service (UMDS) on a Linux virtual machine to download and store binaries and metadata in a shared repository. Connect the UMDS instance to the vSphere Update Manager for each vCenter Server.

Procedure

1. Configure PostgreSQL Database on Your Linux-Based Host Operating System for UMDS in Region B

   In Region B, on a virtual machine with Ubuntu 14.04 Long Term Support (LTS) where you plan to install Update Manager Download Service (UMDS), install and configure a PostgreSQL database instance .

2 Install UMDS on Ubuntu OS in Region B

After you install the PostgreSQL database on the UMDS virtual machine, install the UMDS software.

3 Set Up the Data to Download Using UMDS in Region B

By default UMDS downloads patch binaries, patch metadata, and notifications for hosts. Disable the download of patches for all ESXi versions but the version that is used in this validated design.

4 Install and Configure the UMDS Web Server in Region B

The UMDS server downloads upgrades, patch binaries, patch metadata, and notifications to a directory that you must share to vSphere Update Manager by using a Web server.

5 Use the UMDS Shared Repository as the Download Source in Update Manager in Region B

Configure vSphere Update Manager to use the UMDS shared repository as a source for downloading ESXi patches, extensions, and notifications.

Configure PostgreSQL Database on Your Linux-Based Host Operating System for UMDS in Region B

In Region B, on a virtual machine with Ubuntu 14.04 Long Term Support (LTS) where you plan to install Update Manager Download Service (UMDS), install and configure a PostgreSQL database instance .

Prerequisites

- Create a virtual machine for UMDS. See *Virtual Machine Specifications* from the *Planning and Preparation* documentation.

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 vSphere Web Client, right-click the **`lax01umds01`** virtual machine and select **Open Console** to open the remote console to the virtual machine.

3 At the command prompt, log in as the **`svc-umds`** user using ***`svc-umds_password`***.

4 Install Secure Shell (SSH) server, and end the session.

```
sudo apt-get update
sudo apt-get -y install SSH
exit
```

5 Log back in to the UMDS virtual machine using Secure Shell (SSH) client and the `svc-umds` service account credentials.

6 Install and start PostgreSQL and its dependencies:

```
sudo apt-get -y install vim perl tar sed psmisc unixodbc postgresql postgresql-contrib odbc-
postgresql
sudo service postgresql start
```

The installation operation creates a user account called `postgres` that is associated with the default Postgres role. The **postgres** account is used to establish a service account for the Update Manager Download Service.

7 Log in as a PostgreSQL user, and create a database instance and a database user, by running the following commands.

When prompted, enter and confirm the *umds_db_user_password* password.

```
sudo su - postgres
createdb umds_db
createuser -d -e -r umds_db_admin -P
```

8 Enable password authentication for the database user.

a Navigate to the folder that contains the PostgreSQL configuration file `pg_hba.conf`.

Linux system	Default Location
Ubuntu 14.04	`/etc/postgresql/`*`postgres_version`*`/main`

```
cd /etc/postgresql/postgres_version/main
```

b In the PostgreSQL configuration file, enable password authentication for the database user by inserting the following line right above `local all all peer`.

You can use the `vi` editor to make and save the changes.

#TYPE	DATABASE	USER	ADDRESS	METHOD
local	umds_db	umds_db_admin		md5

c Log out as a PostgreSQL user by running the following command.

```
logout
```

9 Configure the PostgreSQL driver and the data source name (DSN) for connection to the UMDS database.

a Edit the ODBC configuration file.

```
sudo vi /etc/odbcinst.ini
```

b Replace the file with the following content and save the change using `:wq`.

```
[PostgreSQL]
Description=PostgreSQL ODBC driver (Unicode version)
Driver=/usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so
Debug=0
CommLog=1
UsageCount=1
```

c Edit the system file `/etc/odbc.ini`.

```
sudo vi /etc/odbc.ini
```

d Replace the file with the following content and save the change using `:wq`,

```
[UMDS_DSN]
;DB_TYPE = PostgreSQL
;SERVER_NAME = localhost
;SERVER_PORT = 5432
;TNS_SERVICE = <database_name>
;USER_ID = <database_username>
Driver = PostgreSQL
DSN = UMDS_DSN
ServerName = localhost
PortNumber = 5432
Server = localhost
Port = 5432
UserID = umds_db_admin
User = umds_db_admin
Database = umds_db
```

10 Create a symbolic link between UMDS and PostgreSQL by running the following command.

```
ln -s /var/run/postgresql/.s.PGSQL.5432 /tmp/.s.PGSQL.5432
```

11 Restart PostgreSQL.

```
sudo service postgresql restart
```

Install UMDS on Ubuntu OS in Region B

After you install the PostgreSQL database on the UMDS virtual machine, install the UMDS software.

Prerequisites

- Verify you have administrative privileges on the UMDS Ubuntu virtual machine.
- Mount the ISO file of the vCenter Server Appliance to the Linux machine.

Procedure

1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.

  a Open an SSH connection to lax01umds01.lax01.rainpole.local.

  b Log in using the following credentials.

Setting	Value
User name	svc-umds
Password	*svc-umds_password*

2 Mount the vCenter Server Appliance ISO to the UMDS virtual machine.

```
sudo mkdir -p /mnt/cdrom
sudo mount /dev/cdrom /mnt/cdrom
```

3 Extract the `VMware-UMDS-6.5.0.-`*`build_number`*`.tar.gz` file to the `/tmp` folder.

```
tar -xzvf /mnt/cdrom/umds/VMware-UMDS-6.5.0-build_number.tar.gz -C /tmp
```

4 Run the UMDS installation script.

```
sudo /tmp/vmware-umds-distrib/vmware-install.pl
```

5 Read and accept the EULA.

6 Press Enter to install UMDS in the default directory `/usr/local/vmware-umds` and enter **yes** to confirm directory creation.

7 Enter the UMDS proxy settings if needed according to the settings of your environment.

8 Press Enter to set the default patch location to `/var/lib/vmware-umds` and enter **yes** to confirm directory creation.

9 Provide the database details.

Option	Description
Provide the database DSN	UMDS_DSN
Provide the database username	umds_db_admin
Provide the database password	*umds_db_admin_password*

10 Type **yes** and press Enter to install UMDS.

Set Up the Data to Download Using UMDS in Region B

By default UMDS downloads patch binaries, patch metadata, and notifications for hosts. Disable the download of patches for all ESXi versions but the version that is used in this validated design.

Procedure

1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.

   a Open an SSH connection to lax01umds01.lax01.rainpole.local.

   b Log in using the following credentials.

Setting	Value
User name	svc-umds
Password	*svc-umds_password*

2 Navigate to the directory where UMDS is installed.

```
cd /usr/local/vmware-umds/bin
```

3 Disable the updates for older hosts and virtual appliances.

```
sudo ./vmware-umds -S -n
sudo ./vmware-umds -S -d embeddedEsx-5.5.0
sudo ./vmware-umds -S -d embeddedEsx-6.0.0
```

4 Configure automatic daily downloads by creating a cron job file.

```
cd /etc/cron.daily/
sudo touch umds-download
sudo chmod 755 umds-download
```

5 Edit the download command of the cron job.

```
sudo vi umds-download
```

6 Add the following lines to the file.

```
#!/bin/sh
/usr/local/vmware-umds/bin/vmware-umds -D
sudo chmod -R 755 /var/lib/vmware-umds
```

7 Test the UMDS Download cron job.

```
sudo ./umds-download
```

Install and Configure the UMDS Web Server in Region B

The UMDS server downloads upgrades, patch binaries, patch metadata, and notifications to a directory that you must share to vSphere Update Manager by using a Web server.

The default folder to which UMDS downloads patch binaries and patch metadata on a Linux machine is `/var/lib/vmware-umds`. You share this folder out to the vSphere Update Manager instances in the region using an Nginx Web server.

Procedure

1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.

a Open an SSH connection to lax01umds01.lax01.rainpole.local.

b Log in using the following credentials.

Setting	Value
User name	svc-umds
Password	*svc-umds_password*

2 Install the Nginx Web server with the following command.

```
sudo apt-get -y install nginx
```

3 Change the patch repository directory permissions by running the command.

```
sudo chmod -R 755 /var/lib/vmware-umds
```

4 Copy the default site configuration for use with the UMDS configuration.

```
sudo cp /etc/nginx/sites-available/default /etc/nginx/sites-available/umds
```

5 Edit the new `/etc/nginx/sites-available/umds` site configuration file and replace the `server {}` block with the following content.

```
server {
        listen 80 default_server;
        listen [::]:80 default_server ipv6only=on;

        root /var/lib/vmware-umds;
        index index.html index.htm;

        # Make site accessible from http://localhost/
        server_name localhost lax01umds01 lax01umds01.lax01.rainpole.local;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
                # Uncomment to enable naxsi on this location
                # include /etc/nginx/naxsi.rules
                autoindex on;
        }
}
```

6 Disable the existing default site.

```
sudo rm /etc/nginx/sites-enabled/default
```

7 Enable the new UMDS site.

```
sudo ln -s /etc/nginx/sites-available/umds /etc/nginx/sites-enabled/
```

8 Restart the Nginx Web service to apply the new configuration.

```
sudo service nginx restart
```

9 Ensure you can browse the files on the UMDS Web server by opening a Web browser to **`http://lax01umds01.lax01.rainpole.local`**.

Use the UMDS Shared Repository as the Download Source in Update Manager in Region B

Configure vSphere Update Manager to use the UMDS shared repository as a source for downloading ESXi patches, extensions, and notifications.

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 On the **Home** page of the vSphere Web Client, click the **Update Manager** icon.

3 On the **Objects** tab, click the **lax01m01vc01.lax01.rainpole.local** vCenter Server object.

   The **Objects** tab also displays all the vCenter Server systems to which an Update Manager instance is connected.

4 On the **Manage** tab, click **Settings** and select **Download Settings**.

5 On the **Download sources** page, click **Edit**.

   An **Edit Download Sources** dialog box opens.

6 Enter the following setting and click **OK**.

Setting	Value
Use a shared repository	Selected
URL	http://lax01umds01.lax01.rainpole.local

The vSphere Web Client performs validation of the URL.

7 In the **Download sources** page, click **Download Now** to run the download patch definitions.

Verify that a new task **Download Patch Definition** appears in the **Recent Tasks** pane and completes successfully.

8 Repeat the procedure to configure the http://lax01umds01.lax01.rainpole.local repository for the lax01w01vc01.lax01.rainpole.local vCenter Server.

Region B Cloud Management Implementation

4

The Cloud Management Platform (CMP) consists of integrated products that provide for the management of public, private and hybrid cloud environments. CMP consists of vRealize Automation, vRealize Orchestrator, and vRealize Business. vRealize Automation incorporates virtual machine provisioning and a self-service portal. vRealize Business enables billing and chargeback functions. vRealize Orchestrator provides workflow optimization.

The following procedures describe the validated flow of installation and configuration for the second site in the enterprise.

Procedure

1 Prerequisites for Cloud Management Platform Implementation in Region B

  Verify that the following configurations are established prior to beginning the Cloud Management Platform procedures in Region B.

2 Configure Service Account Privileges in Region B

  In order for you to provision virtual machines and logical networks, configure privileges for vRealize Automation for the service account svc-vra@rainpole.local on both the Compute vCenter Server and the Compute Cluster NSX Instance.

3 vRealize Automation Installation in Region B

  A vRealize Automation installation includes installing and configuring single sign-on (SSO) capabilities, the user interface portal, and Infrastructure as a Service (IaaS) components.

4 Embedded vRealize Orchestrator Configuration in Region B

  VMware Embedded vRealize Orchestrator provides a library of extensible workflows to allow you to create and run automated, configurable processes to manage your VMware vSphere infrastructure, as well as other VMware and third-party applications.

5 vRealize Business Installation in Region B

  vRealize Business is an IT financial management tool that provides transparency and control over the costs and quality of IT services, enabling alignment with the business and acceleration of IT transformation.

6 Create Anti-Affinity Rules for vRealize Automation Proxy Agent Virtual Machines in Region B

  After deploying the vRealize Automation proxy agents, set up anti-affinity rules.

7 Content Library Configuration in Region B

Content libraries are container objects for VM templates, vApp templates, and other types of files. vSphere administrators can use the templates in the library to deploy virtual machines and vApps in the vSphere inventory. Sharing templates and files across multiple vCenter Server instances in same or different locations brings out consistency, compliance, efficiency, and automation in deploying workloads at scale.

8 Tenant Content Creation in Region B

To provision virtual machines in the Compute vCenter Server instance, you configure the tenant to utilize vCenter Server compute resources.

9 Operations Management Configuration for Cloud Management in Region B

After you install the components of the Cloud Management Platform in Region B, enable their integration with the operations management layer. You can monitor and receive alerts and logs about the platform to a central location by using vRealize Operations Manager and vRealize Log Insight.

Prerequisites for Cloud Management Platform Implementation in Region B

Verify that the following configurations are established prior to beginning the Cloud Management Platform procedures in Region B.

DNS Entries and IP Address Mappings in Region B

Verify that the static IP addresses and FQDNs listed in the table below, are available for the vRealize Automation application virtual network for the second region of the SDDC deployment.

Table 4-1. IP Addresses and Host Name for the vRealize Automation Proxy Agents and vRealize Business Data Collector in Region B

Role	IP Address	FQDN
vRealize Automation Proxy Agents	192.168.32.52	lax01ias01a.lax01.rainpole.local
	192.168.32.53	lax01ias01b.lax01.rainpole.local
vRealize Business Data Collector	192.168.32.54	lax01vrbc01.lax01.rainpole.local
Default gateway	192.168.32.1	-
DNS server	172.17.11.5	-
Subnet mask	255.255.255.0	-
NTP	172.16.11.251 172.16.11.252	ntp.sfo01.rainpole.local
	172.17.11.251 172.17.11.252	ntp.lax01.rainpole.local

Configure Service Account Privileges in Region B

In order for you to provision virtual machines and logical networks, configure privileges for vRealize Automation for the service account svc-vra@rainpole.local on both the Compute vCenter Server and the Compute Cluster NSX Instance.

Procedure

1 Configure Service Account Privileges on the Compute vCenter Server in Region B

Configure Administrator privileges for the svc-vra and svc-vro users on the Compute vCenter Server in Region B.

2 Configure the Service Account Privilege on the Compute Cluster NSX Instance in Region B

Configure Enterprise Administrator privileges for the svc-vra@rainpole.local service account.

Configure Service Account Privileges on the Compute vCenter Server in Region B

Configure Administrator privileges for the svc-vra and svc-vro users on the Compute vCenter Server in Region B.

If you add more Compute vCenter Server instances in the future, perform this procedure on those instances as well.

Procedure

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

   a Open a Web browser and go to **`https://lax01w01vc01.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, select **Global Inventory Lists > vCenter Servers**.

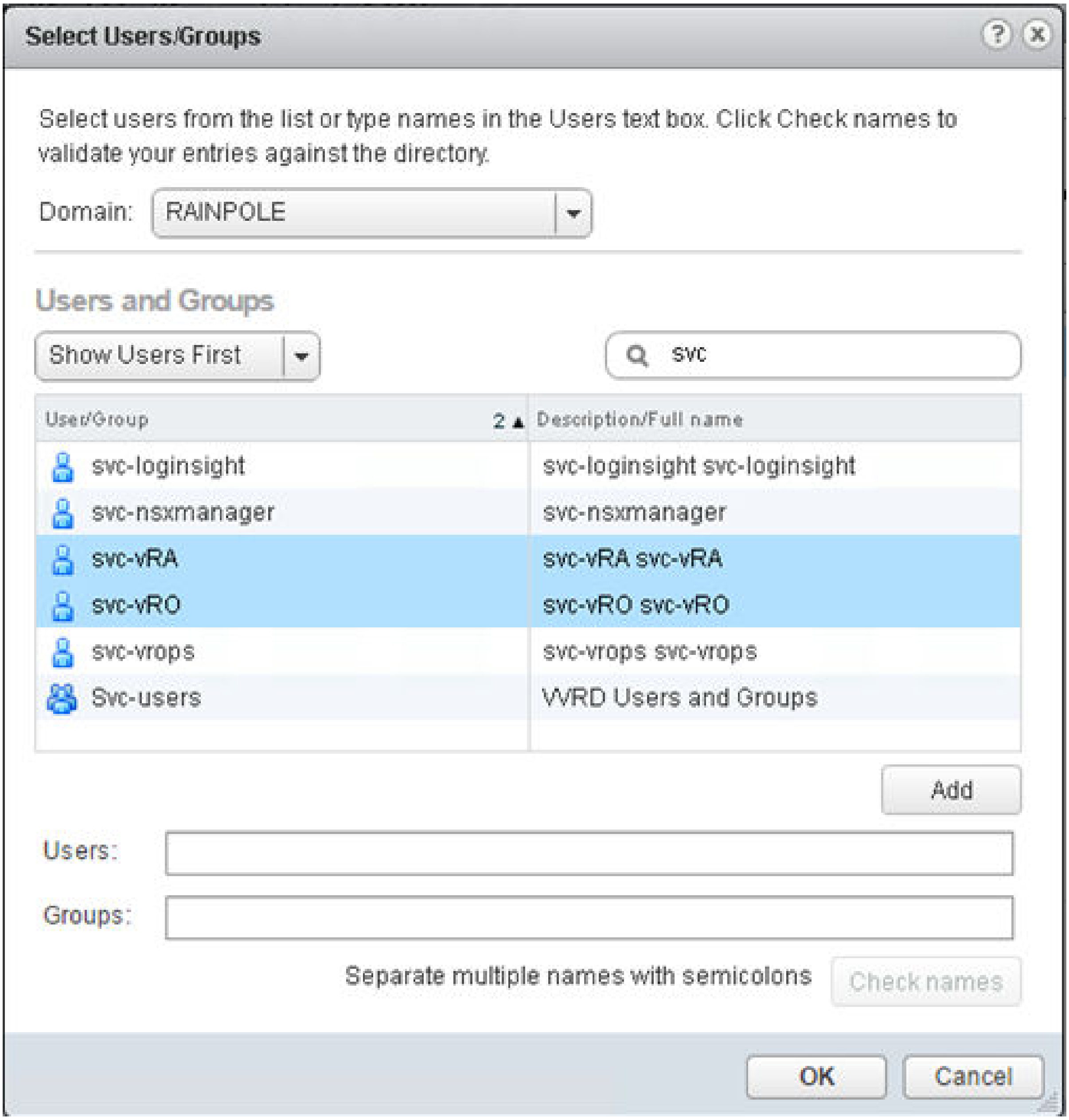
3 Right-click the **lax01w01vc01.lax01.rainpole.local** instance and select **Add Permissions**.

4 In the **Add Permission** dialog box, click the **Add** button.

The **Select Users/Groups** dialog box appears.

5 Select **RAINPOLE** from the **Domain** drop-down menu, and in the **Show Users First** text box enter **`svc`** to filter user and group names.

6 Select **svc-vra** and **svc-vro** from the **User/Group** list, click the **Add** button and click **OK**.



Select users from the list or type names in the Users text box. Click Check names to validate your entries against the directory.

Domain: RAINPOLE

Show Users First

svc

User/Group	Description/Full name
svc-loginsight	svc-loginsight svc-loginsight
svc-nsxmanager	svc-nsxmanager
svc-vRA	svc-vRA svc-vRA
svc-vRO	svc-vRO svc-vRO
svc-vrops	svc-vrops svc-vrops
Svc-users	VVRD Users and Groups

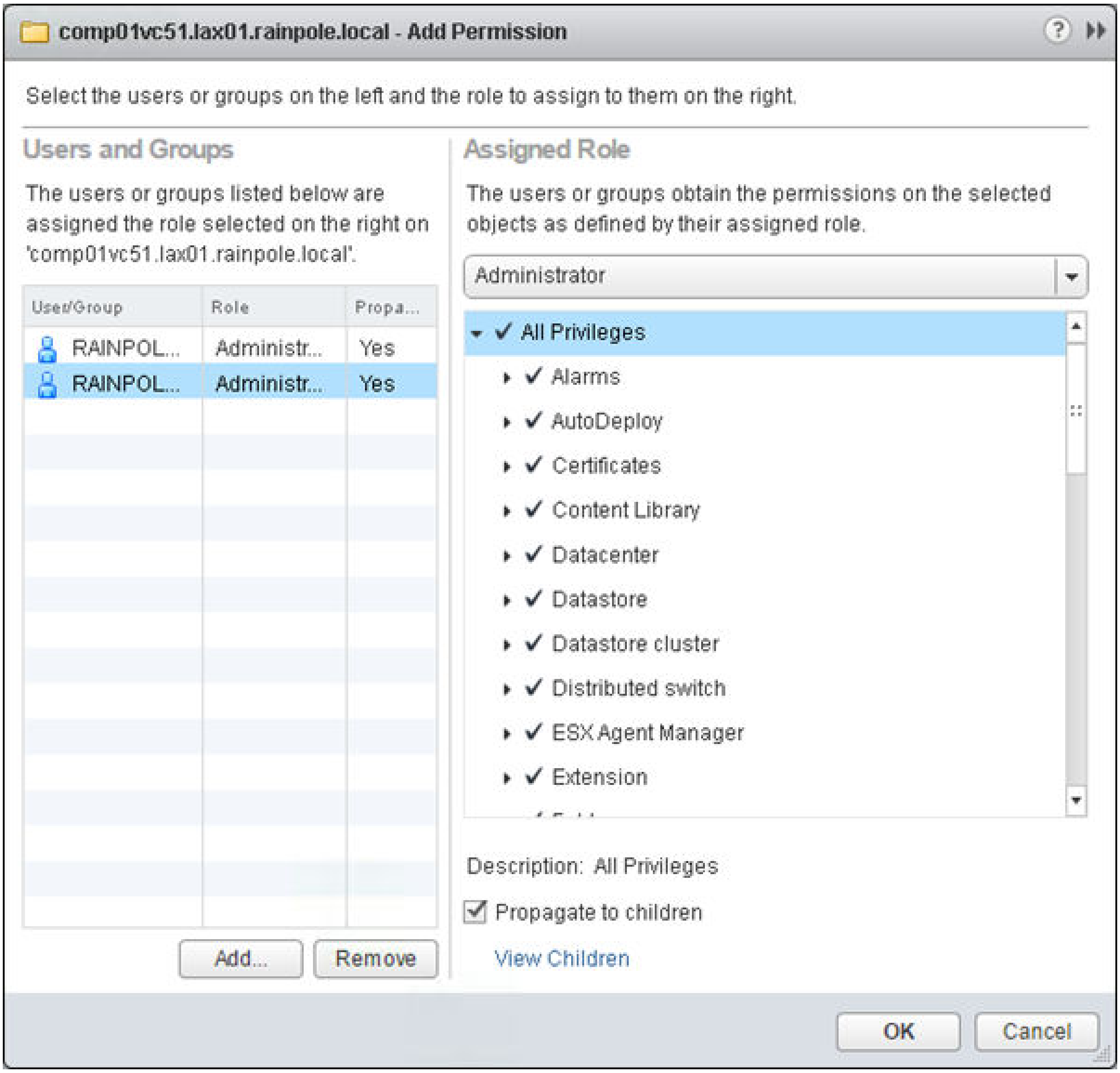
Users:

Groups:

Separate multiple names with semicolons

7 In the **Add Permission** dialog box, select **Administrator** from the **Assigned Role** drop-down menu and click **OK**.

The svc-vra and svc-vro users now have **Administrator** privilege on the Compute vCenter Server in Region A.



comp01vc51.lax01.rainpole.local - Add Permission

Select the users or groups on the left and the role to assign to them on the right.

Users and Groups

The users or groups listed below are assigned the role selected on the right on 'comp01vc51.lax01.rainpole.local'.

User/Group	Role	Propa...
RAINPOL...	Administr...	Yes
RAINPOL...	Administr...	Yes

Assigned Role

The users or groups obtain the permissions on the selected objects as defined by their assigned role.

Administrator

- ✓ All Privileges
  - ✓ Alarms
  - ✓ AutoDeploy
  - ✓ Certificates
  - ✓ Content Library
  - ✓ Datacenter
  - ✓ Datastore
  - ✓ Datastore cluster
  - ✓ Distributed switch
  - ✓ ESX Agent Manager
  - ✓ Extension

Description: All Privileges

☑ Propagate to children

Configure the Service Account Privilege on the Compute Cluster NSX Instance in Region B

Configure Enterprise Administrator privileges for the svc-vra@rainpole.local service account.

Procedure

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

a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

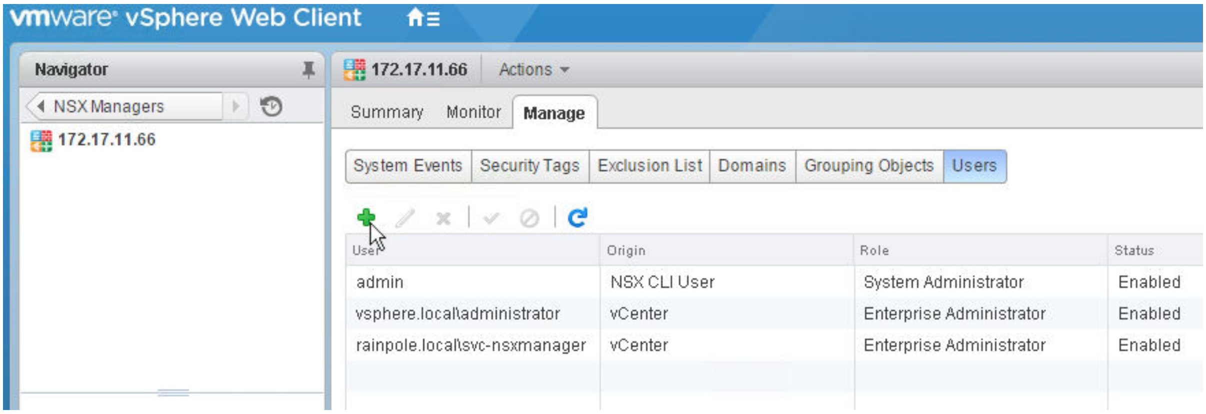
Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Navigator** pane, select **Networking & Security > NSX Managers**.

3 Double-click the **172.17.11.66** Compute NSX Manager.

4 Click **Manage**, click **Users**, and click the **Add** icon.

The **Assign Role** wizard appears.

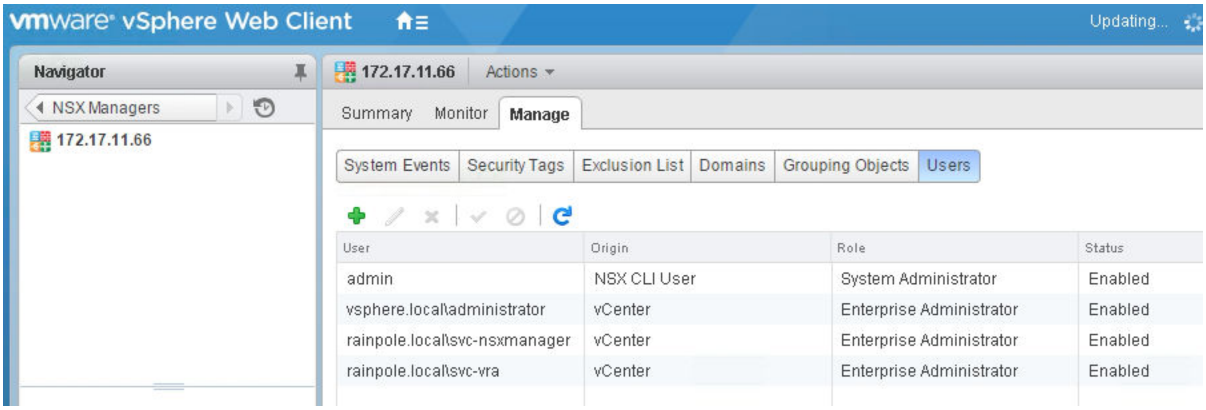


User	Origin	Role	Status
admin	NSX CLI User	System Administrator	Enabled
vsphere.local\administrator	vCenter	Enterprise Administrator	Enabled
rainpole.local\svc-nsxmanager	vCenter	Enterprise Administrator	Enabled

5 On the **Identify User** page, select the **Specify a vCenter User** radio button, enter **`svc-vra@rainpole.local`** in the **User** text box, and click **Next**.

6 On the **Select Roles** page, select the **Enterprise Administrator** radio button, and click **Finish**.

The svc-vra@rainpole.local user is now configured as an **Enterprise Administrator** for the compute cluster NSX instance, and appears in the lists of users and roles.



User	Origin	Role	Status
admin	NSX CLI User	System Administrator	Enabled
vsphere.local\administrator	vCenter	Enterprise Administrator	Enabled
rainpole.local\svc-nsxmanager	vCenter	Enterprise Administrator	Enabled
rainpole.local\svc-vra	vCenter	Enterprise Administrator	Enabled

vRealize Automation Installation in Region B

A vRealize Automation installation includes installing and configuring single sign-on (SSO) capabilities, the user interface portal, and Infrastructure as a Service (IaaS) components.

After installation you can customize the installation environment and configure one or more tenants, which sets up access to self-service provisioning and life-cycle management of cloud services. By using the secure portal Web interface, administrators, developers, or business users can request IT services and manage specific cloud and IT resources based on their roles and privileges. Users can request infrastructure, applications, desktops, and IT service through a common service catalog.

- Load Balancing the Cloud Management Platform in Region B

  You configure load balancing for all services and components related to vRealize Automation and vRealize Orchestrator by using an NSX Edge load balancer.

- Deploy Windows Virtual Machines for vRealize Automation in Region B

  vRealize Automation requires several Windows virtual machines to act as IaaS components in a distributed configuration. These redundant components provide high availability for the vRealize Automation infrastructure features.

- Install vRealize Automation Proxy Agents in Region B

  Proxy agents are required so vRealize Automation can communicate with vCenter Server instances. For every vCenter Server instance that will be a target for vRealize Automation, deploy at least two proxy agents.

Load Balancing the Cloud Management Platform in Region B

You configure load balancing for all services and components related to vRealize Automation and vRealize Orchestrator by using an NSX Edge load balancer.

You must configure the load balancer before you deploy the vRealize Automation appliance. This is because you need the virtual IP (VIP) addresses to deploy the vRealize Automation appliance.

Procedure

1 Add Virtual IP Addresses to the NSX Load Balancer in Region B

As the first step of configuring load balancing, you add virtual IP Addresses to the edge interfaces.

2 Create Application Profiles in Region B

Create an application profile to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

3 Create Service Monitoring in Region B

The service monitor defines health check parameters for the load balancer. You create a service monitor for each component.

4 Create Server Pools in Region B

A server pool consists of back-end server members. After you create a server pool, you associate a service monitor with the pool to manage and share the back-end servers flexibly and efficiently.

5 Create Virtual Servers in Region B

After load balancing is set up, the NSX load balancer distributes network traffic across multiple servers. When a virtual server receives a request, it chooses the appropriate pool to send traffic to. Each pool consists of one or more members. You create virtual servers for all of the configured server pools.

Add Virtual IP Addresses to the NSX Load Balancer in Region B

As the first step of configuring load balancing, you add virtual IP Addresses to the edge interfaces.

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 Click **Networking & Security**.

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

4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **lax01m01lb01** NSX Edge to edit its network settings.

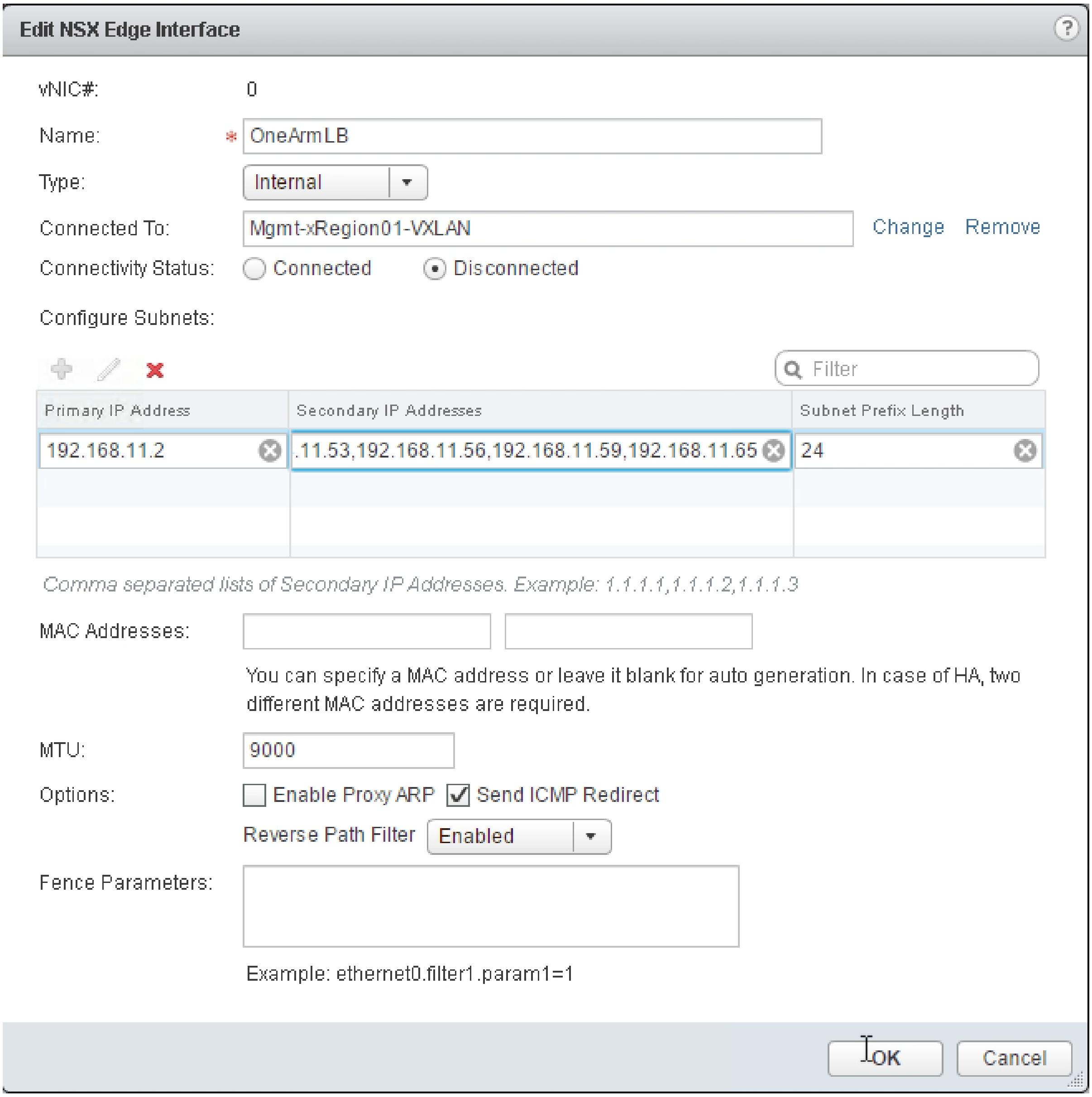
5 Click the **Manage** tab, click **Settings**, and select **Interfaces**.

6 Select the **OneArmLB** interface and click the **Edit** icon.

7 In the **Edit NSX Edge** Interface dialog box, add the VIP addresses of the vRealize Automation nodes in the **Secondary IP Addresses** text box.

Note The **Connectivity Status** should remain as **Disconnected**.

Setting	Value
Secondary IP Address	192.168.11.53,192.168.11.56,192.168.11.59,192.168.11.65



Edit NSX Edge Interface

vNIC#: 0

Name: * OneArmLB

Type: Internal

Connected To: Mgmt-xRegion01-VXLAN

Connectivity Status: ○ Connected ● Disconnected

Configure Subnets:

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
192.168.11.2	.11.53,192.168.11.56,192.168.11.59,192.168.11.65	24

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.1.2,1.1.1.3

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU: 9000

Options: □ Enable Proxy ARP ☑ Send ICMP Redirect

Reverse Path Filter: Enabled

Fence Parameters:

Example: ethernet0.filter1.param1=1

8 Click **OK** to save the configuration.

Create Application Profiles in Region B

Create an application profile to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

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 Click **Networking & Security**.

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

4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **lax01m01lb01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Application Profiles**.

6 Click the **Add** icon and in the New Profile dialog box, and configure the following values.

Setting	Value
Name	vra-https-persist
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	Source IP
Expires in (Seconds)	1800

7 Click **OK** to save the configuration.

8 Repeat this procedure to create the following application profile.

Setting	Value
Name	vra-https
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	None

Create Service Monitoring in Region B

The service monitor defines health check parameters for the load balancer. You create a service monitor for each component.

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 Click **Networking & Security**.

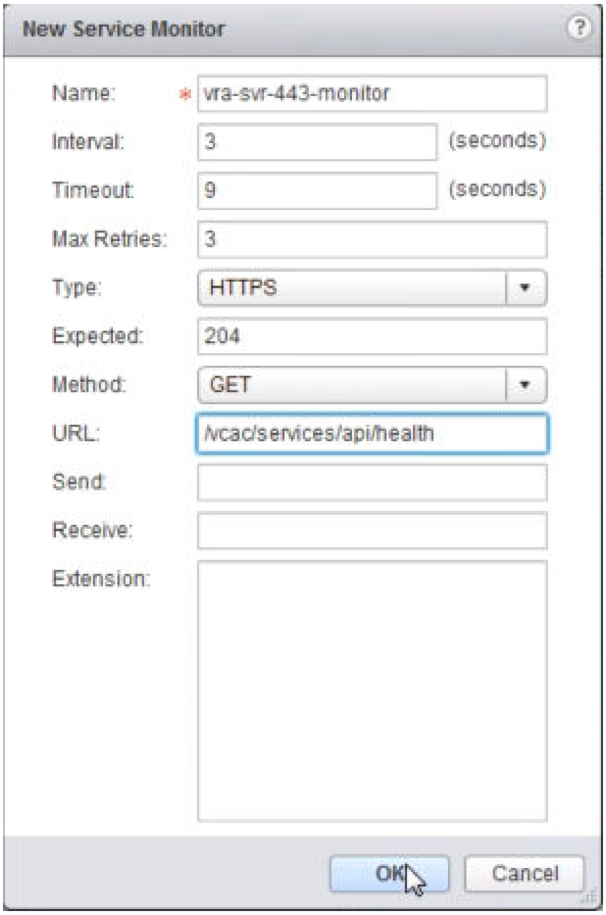
3 In the Navigator, click **NSX Edges**.

4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **lax01m01lb01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Service Monitoring**.

6 Click the **Add** icon and in the **New Service Monitor** dialog box, configure the values for the service monitor you are adding, and click **OK**.

Setting	vra-svr-443-monitor	vra-iaas-web-443-monitor	vra-iaas-mgr-443-monitor	vra-vro-8283-monitor
Name	vra-svr-443-monitor	vra-iaas-web-443-monitor	vra-iaas-mgr-443-monitor	vra-vro-8283-monitor
Interval	3	3	3	3
Timeout	10	10	10	10
Max Retries	3	3	3	3
Type	HTTPS	HTTPS	HTTPS	HTTPS
Expected	204			
Method	GET	GET	GET	GET
URL	/vcac/services/api/health	/wapi/api/status/web	/VMPSProvision	/vco-controlcenter/docs
Receive		REGISTERED	ProvisionService	



Name: * vra-svr-443-monitor

Interval: 3 (seconds)

Timeout: 9 (seconds)

Max Retries: 3

Type: HTTPS

Expected: 204

Method: GET

URL: /vcac/services/api/health

Send:

Receive:

Extension:

7 Repeat this procedure to create a service monitor for each component.

Create Server Pools in Region B

A server pool consists of back-end server members. After you create a server pool, you associate a service monitor with the pool to manage and share the back-end servers flexibly and efficiently.

Perform the procedure multiple times to configure five different server pools using the values shown in the following table.

Table 4-2. Server Pools for the Cloud Management Platform in Region B

			Members					
Pool Name	**Algorithm**	**Monitors**	**Enable Member**	**Member Name**	**IP address**	**Port**	**Monitor Port**	**Weight**
vra-svr-443	ROUND-ROBIN	vra-svr-443-monitor	Yes	vra01svr01a	192.168.11.51	443	-	1
			Yes	vra01svr01b	192.168.11.52			1
vra-iaas-web-443	ROUND-ROBIN	vra-iaas-web-443-monitor	Yes	vra01iws01a	192.168.11.54	443	-	1
			Yes	vra01iws01b	192.168.11.55			1

Table 4-2. Server Pools for the Cloud Management Platform in Region B (Continued)

			Members					
Pool Name	**Algorithm**	**Monitors**	**Enable Member**	**Member Name**	**IP address**	**Port**	**Monitor Port**	**Weight**
vra-iaas-mgr-443	ROUND-ROBIN	vra-iaas-mgr-443-monitor	Yes	vra01ims01a	192.168.11.57	443	-	1
			Yes	vra01ims01b	192.168.11.58			1
vra-svr-8444	ROUND-ROBIN	vra-svr-443-monitor	Yes	vra01svr01a	192.168.11.51	8444	443	1
			Yes	vra01svr01b	192.168.11.52			1
vra-vro-8283	ROUND-ROBIN	vra-vro-8283-monitor	Yes	vra01svr01a	192.168.11.51	8283	-	1
			Yes	vra01svr01b	192.168.11.52			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://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 Click **Networking & Security**.

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

4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **lax01m01lb01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.

6 Click the **Add** icon, and in the **New Pool** dialog box configure the following values.

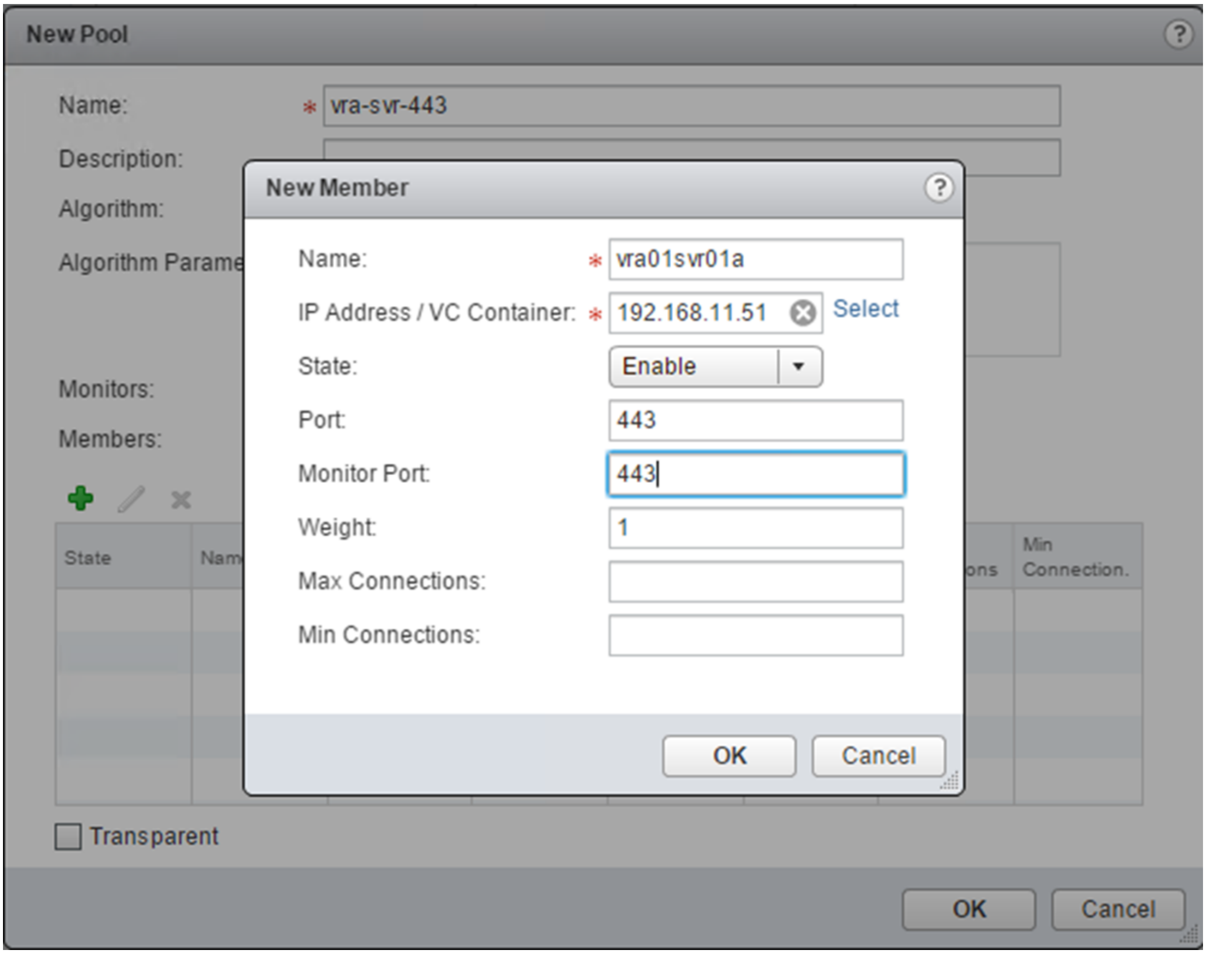
Setting	Value
Name	vra-svr-443
Algorithm	ROUND-ROBIN
Monitors	vra-svr-443-monitor

7 Under **Members**, click the **Add** icon to add the first pool member.

8 In the **New Member** dialog box configure the following values, and click **OK**.

Setting	Value
Name	vra01svr01a
IP Address/VC Container	192.168.11.51

Setting	Value
State	Enable
Port	443
Monitor Port	443
Weight	1



New Pool

Name: * vra-svr-443

New Member

Name: * vra01svr01a

IP Address / VC Container: * 192.168.11.51

State: Enable

Port: 443

Monitor Port: 443

Weight: 1

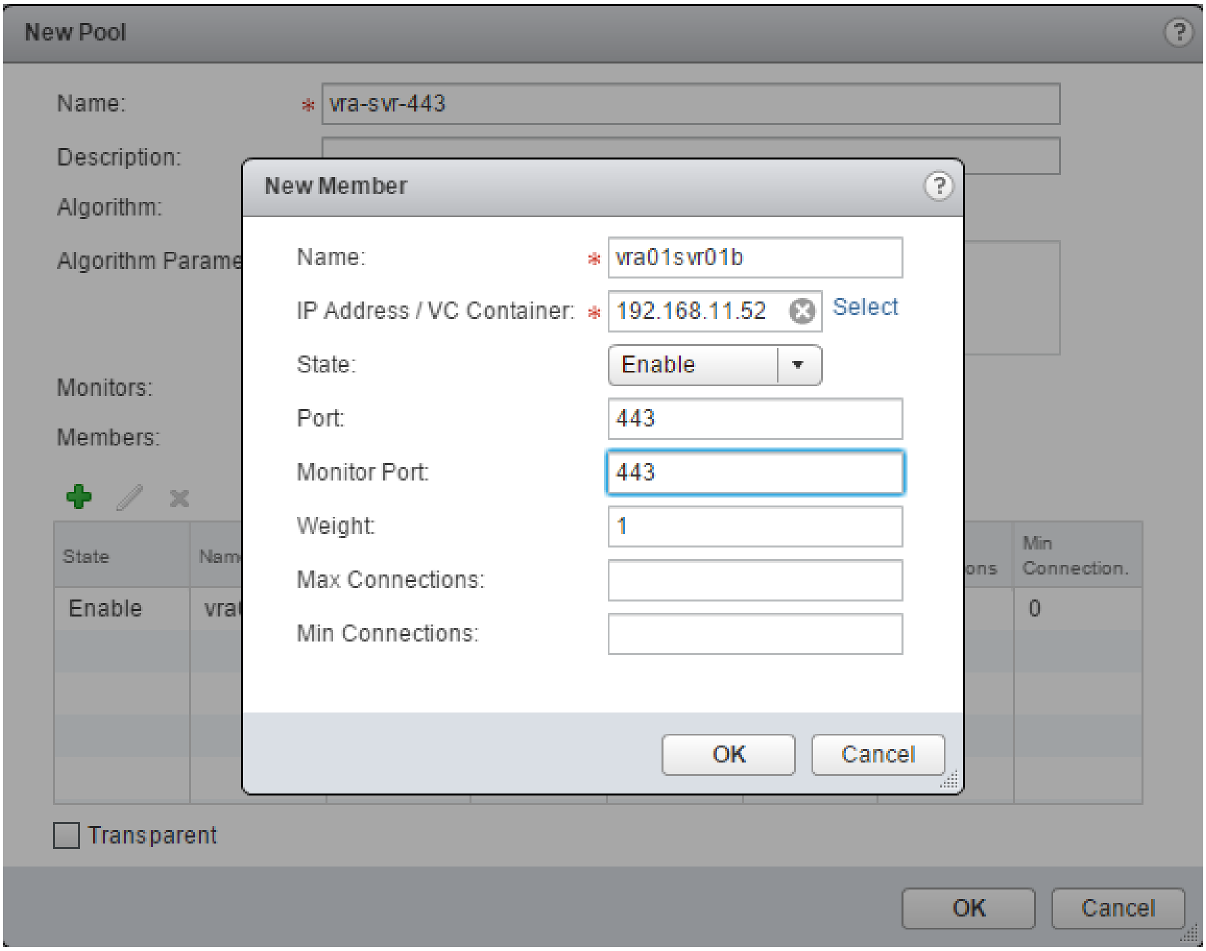
Max Connections:

Min Connections:

9 Under **Members**, click the **Add** icon to add the second pool member.

10 In the **New Member** dialog box, configure the following values, click **OK**, and click **OK** again to save the vRealize Automation server pool.

Setting	Description
Name	vra01svr01b
IP Address/VC Container	192.168.11.52
State	Enabled
Port	443
Monitor Port	443
Weight	1



New Pool

Name: * vra-svr-443

Description:

Algorithm:

Algorithm Parame

Monitors:

Members:

State	Nam	ons	Min Connection.
Enable	vra		0

☐ Transparent

New Member

Name: * vra01svr01b

IP Address / VC Container: * 192.168.11.52

State: Enable

Port: 443

Monitor Port: 443

Weight: 1

Max Connections:

Min Connections:

11 Repeat the procedure to create the remaining server pools.

Create Virtual Servers in Region B

After load balancing is set up, the NSX load balancer distributes network traffic across multiple servers. When a virtual server receives a request, it chooses the appropriate pool to send traffic to. Each pool consists of one or more members. You create virtual servers for all of the configured server pools.

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 Click **Networking & Security**.

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

4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **lax01m01lb01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Virtual Servers**.

6 Click the **Add** icon, and in the New Virtual Server dialog box configure the values for the virtual server you are adding, and click **OK**.

Setting	vra-svr-443	vra-iaas-web-443	vra-iaas-mgr-443	vra-svr-8444	vra-vro-8283
Enable Virtual server	Selected	Selected	Selected	Selected	Selected
Application Profile	vra-https-persist	vra-https-persist	vra-https	vra-https-persist	vra-https-persist
Name	vra-svr-443	vra-iaas-web-443	vra-iaas-mgr-443	vra-svr-8444	vra-vro-8283
Description	vRealize Automation Appliance UI	vRealize Automation IaaS Web UI	vRealize Automation IaaS Manager	vRealize Automation Remote Console Proxy	vRealize Orchestrator Control Center
IP Address	192.168.11.53	192.168.11.56	192.168.11.59	192.168.11.53	192.168.11.53
Protocol	HTTPS	HTTPS	HTTPS	HTTPS	HTTPS
Port	443	443	443	8444	8283
Default Pool	vra-svr-443	vra-iaas-web-443	vra-iaas-mgr-443	vra-svr-8444	vra-vro-8283

7 Repeat the previous step to create a virtual server for each component.

Deploy Windows Virtual Machines for vRealize Automation in Region B

vRealize Automation requires several Windows virtual machines to act as IaaS components in a distributed configuration. These redundant components provide high availability for the vRealize Automation infrastructure features.

Procedure

1 Create a Customization Specification for IaaS Proxy Agent Servers in Region B

Create a vSphere Image Customization template to use with your vRealize Automation IaaS Proxy Agent deployment.

2 Create Windows Virtual Machines for vRealize Automation in Region B

vRealize Automation requires several Windows virtual machines to act as IaaS components in a distributed configuration. These redundant components provide high availability for the vRealize Automation infrastructure features.

3 Install vRealize Automation Management Agent on Windows IaaS Virtual Machines in Region B

For each Windows virtual machine deployed as part of the vRealize Automation installation, a management agent must be deployed to facilitate the installation of the Windows dependencies and vRealize Automation components.

Create a Customization Specification for IaaS Proxy Agent Servers in Region B

Create a vSphere Image Customization template to use with your vRealize Automation IaaS Proxy Agent deployment.

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 From the **Home** page, click **Customization Specification Manager**.

3 Select **lax01m0101vc01.lax01.rainpole.local** from the **vCenter Server** drop-down menu.

4 Click the **Create a new specification** icon.

The **New VMGuest Customization Spec** wizard opens.

5 On the **Specify Properties** page, configure the following settings, and click **Next**.

Setting	Value
Target VM Operating System	Windows
Use custom SysPrep answer file	Deselected
Customization Spec Name	vra7-proxy-agent-template

6 On the **Set Registration Information** page, configure the following settings, and click **Next**.

Setting	Value
Name	Rainpole
Organization	Rainpole IT

7 On the **Set Computer Name** page, select the **Enter a name in the Clone/Deploy wizard** radio button, and click **Next**.

8 On the **Enter Windows License** page, enter the following settings, and click **Next**.

If you are using **Microsoft License Server**, or have multiple single license keys, leave the **Product Key** text box blank.

Setting	Value
Product Key	*volume_license_key*
Include Server License Information	Selected
Server License Mode	Per seat

9 On the **Set Administrator Password** page, configure the following settings, and click **Next**.

Setting	Value
Password	*local_administrator_pwd*
Confirm password	*local_administrator_pwd*
Automatically logon as Administrator	Selected
Number of times to logon automatically	1

10 On the **Time Zone** page, select **(GMT) Coordinated Universal Time** from the **Time Zone** drop down menu, and click **Next**.

11 On the **Run Once** page, type `net localgroup administrators rainpole\svc-vra /add` in the text box and click **Add**. This command will add service account rainpole\svc-vra into virtual machine's local administrators group. Click **Next**.

12 On the **Configure Network** page, select the **Manually select custom settings** radio button, select **NIC1** from the list of network interfaces in the virtual machine, and click **Edit**.

The **Network Properties** dialog box displays.

13 In the **Edit Network** dialog box, on the **IPv4** page, configure the following settings and click **DNS**.

Setting	Value
Prompt the user for an address when the specification is used	Selected
Subnet Mask	255.255.255.0
Default Gateway	192.168.32.1

14 On the **DNS** page, provide DNS servers and search suffixes.

a Configure the following DNS server settings.

Setting	Value
Use the following DNS server address	Selected
Preferred DNS Server	172.17.11.4
Alternate DNS Server	172.17.11.5

b Enter `rainpole.local` in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

c Enter `lax01.rainpole.local` in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

d Enter `sfo01.rainpole.local` in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

e Click **OK** to save settings and close the **Edit Network** dialog box, and click **Next**.

15 On the **Set Workgroup or Domain** page, enter credentials that have administrative privileges in the domain, and click **Next**.

Setting	Value
Windows Server Domain	lax01.rainpole.local
Username	svc-domain-join@rainpole.local
Password	*svc-domain-join_password*

16 On the **Set Operating System** options page, select the **Generate New Security ID (SID)** check box, and click **Next**.

17 On the **Ready to Complete** page, review the settings that you entered, and click **Finish**.

The customization specification you created is listed in the **Customization Specification Manager**, and can be used to customize virtual machine guest operating systems.

Create Windows Virtual Machines for vRealize Automation in Region B

vRealize Automation requires several Windows virtual machines to act as IaaS components in a distributed configuration. These redundant components provide high availability for the vRealize Automation infrastructure features.

To facilitate cloning, this design uses the vra7-proxy-agent-template image customization specification template and the windows-2012r2-64 VM template. Two virtual machines that run on Windows will be required to install vRealize Automation Proxy Agents in Region B. Repeat this procedure twice by using the information in the following table to create two VMs.

Name for Virtual Machines	NetBIOS name	vCenter Folder	IP	vCPU number	Memory Size	Image Customization Specification Template	Network
lax01ias01a	lax01ias01a	lax01-m01fd-vraias	192.168.32.52	2	4 GB	`vra7-proxy-agent-template`	vxw-dvs-xxxx-Mgmt-RegionB01-VXLAN
lax01ias01b	lax01ias01b	lax01-m01fd-vraias	192.168.32.53	2	4 GB	`vra7-proxy-agent-template`	vxw-dvs-xxxx-Mgmt-RegionB01-VXLAN

Prerequisites

Verify that you have created the Windows 2012 R2 VM template windows2012r2-template.

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, select **Global Inventory Lists** > **vCenter Servers**. Click the **lax01m01vc01.lax01.rainpole.local** instance.

3 Select **VM Templates in Folders**, and from the VM Templates in Folders pane, right-click the IaaS windows template **windows-2012r2-64** and select **New VM from this Template**.

4 On the **Select a name and folder** page of the **Deploy From Template** wizard, specify a name and location for the virtual machine.

   a Enter `lax01ias01a` in the **Enter a name for the virtual machine** text box.

   b In the **Select a location for the virtual machine** pane, select the **lax01-m01fd-vraias** folder in the **lax01-m01dc** datacenter under **lax01m01vc01.lax01.rainpole.local**, and click **Next**.

5 On the **Select a compute resource** page, select **lax01-m01-mgmt01** and click **Next**.

6 On the **Select storage** page, select the datastore on which to create the virtual machine's disks.

   a Select **vSAN Default Storage Policy** from the **VM Storage Policy** drop-down menu.

   b Select the **lax01-m01-vsan01** vSAN datastore from the datastore table and click **Next**.

7 On the **Select Clone options** page, select the **Customize the operating system** check box, and click **Next**.

8 On the **Customize guest OS** page, select the **vra7-proxy-agent-template** from the table, and click **Next**.

9 On the **User Settings** page, enter the following values, and click **Next**.

Setting	Value
NetBIOS name	lax01ias01a
IPv4 address	192.168.32.52
IPv4 subnet mask	255.255.255.0

10 On the **Ready to Complete** page, review your settings and click **Finish**.

When the deployment of the virtual machine completes, you can customize the virtual machine.

11 In the **Navigator**, select **VMs and Templates**.

12 Right-click the **lax01ias01a** virtual machine and select **Edit Settings**.

13 Click **Virtual Hardware** and configure the settings for **CPU**, **Memory**, and the **Network adapter 1**.

a Select **2** from the **CPU** drop-down menu.

b Set the **Memory** settings to **`4096 MB`**.

c Expand `Network adapter 1` and select **vxw-dvs-xxxx-Mgmt-RegionB01-VXLAN** from the drop-down menu and click **OK**.

14 Right-click the virtual machine **lax01ias01a**, and select **Power > Power on**.

15 From the Virtual Machine Console, verify that **lax01ias01a** reboots, and uses the configuration settings that you specified.

After the Windows customization process completes, a clean desktop appears.

16 Log in to the Windows operating system and perform final verification and customization.

a Verify that the IP address, computer name, and domain are correct.

b Verify the the vRealize Automation service account `svc-vra@rainpole.local` has been added to the Local Administrators Group.

17 Repeat this procedure to deploy and configure the remaining virtual machine.

Install vRealize Automation Management Agent on Windows IaaS Virtual Machines in Region B

For each Windows virtual machine deployed as part of the vRealize Automation installation, a management agent must be deployed to facilitate the installation of the Windows dependencies and vRealize Automation components.

Repeat this procedure twice to install the Management Agent on both of the Windows IaaS virtual machines. The host names of the Windows IaaS virtual machines are lax01ias01a.lax01.rainpole.local and lax01ias01b.lax01.rainpole.local.

Procedure

1 Log in to the Windows IaaS Proxy Agent virtual machine.

a Connect to **`lax01ias01a.lax01.rainpole.local`** over RDP.

b Log in using the local administrator credentials that you specified during the creation of the customization specification process.

2 Download the vRealize Management Agent.

a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480/installer`**.

b Download the `Management Agent Installer.msi` package.

3 Install the vRealize Management Agent.

   a Start the `vCAC–IaaSManagementAgent–Setup.msi` installer.

   b On the **Welcome** page, click **Next** to start the install process.

   c On the **EULA** page, select the **I accept the terms of this agreement** check box and click **Next**.

   d On the **Destination Folder** page, click **Next** to install in the default path.

   e On the **Management Site Service** page, enter the following settings and click **Load**.

Setting	Value
vRA Appliance Address	https://vra01svr01a.rainpole.local:5480
Root username	root
Password	*vra_appA_root_password*

   f Select the **I confirm the fingerprint matches the Management Site Service SSL certificate** check box, and click **Next**.

4 On the **Management Agent Account Configuration** page, configure the following credentials and click **Next**.

Setting	Value
Username	rainpole\svc-vra
Password	*svc-vra_password*

5 On the **Ready to install** page, click **Install**.

6 Repeat the procedure to install the Management Agent in virtual machine lax01ias02.lax01.rainpole.local.

Install vRealize Automation Proxy Agents in Region B

Proxy agents are required so vRealize Automation can communicate with vCenter Server instances. For every vCenter Server instance that will be a target for vRealize Automation, deploy at least two proxy agents.

Repeat this procedure twice to install the IaaS proxy Agent on the Windows virtual machines lax01ias01a.lax01.rainpole.local and lax01ias01b.lax01.rainpole.local.

Procedure

1 Log in to the **`lax01ias01a.lax01.rainpole.local`** virtual machine using the vRealize Automation service account.

Setting	Value
Username	rainpole\svc-vra
Password	*svc-vra_password*

2 Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480/installer`**.

3 Click the **IaaS Installer** link and save the installer with its default file name.

4 Right-click the installer file and select **Run as administrator**.

5 On the **Welcome** page, click **Next**.

6 On the **License** page, click **I accept the terms in the license agreement** and click **Next**.

7 On the **Log In** page, configure the following settings, and click **Next**.

Setting	Value
Appliance host name	vra01svr01a.rainpole.local:5480
User name	root
Password	*root_password*
Accept Certificate	Selected

8 On the **Installation Type** page, select **Custom Install**, select **Proxy Agents,** and click **Next**.

9 On the **Server and Account Settings** page, configure the following settings and click **Next**.

Setting	Value
Local server	Use the default host name
User name	rainpole\svc-vra
Password	*svc-vra_password*

10 On the **Install Proxy Agent** page, configure the following values, click **Test** to test the host connectivity, and click **Add**.

Note If the Root CA certificate was used to sign the vRealize Automation certificate, is not be trusted by Proxy Agent Windows virtual machines. The Root CA certificate must be imported as the Trusted Root Certification Authority before you begin installation of the Proxy Agent.

Setting	Value
Agent type	vSphere
Agent name	VSPHERE-AGENT-51
Manager Service Host	vra01ims01.rainpole.local
Model Manager Web Service Host	vra01iws01.rainpole.local
vSphere Endpoint	lax01w01vc01.lax01.rainpole.local

11 Click **Next**.

12 Verify the configuration, and click **Install** to install the proxy agent.

13 Click **Next** when the installation is completed, and click **Finish** to exit the wizard.

14 Repeat the procedure for virtual machine `lax01ias01b.lax01.rainpole.local` to install another proxy agent for redundancy, using the following values.

Setting	Value
Agent Type	vSphere
Agent Name	VSPHERE-AGENT-51
Manager Service Host name	vra01ims01.rainpole.local
Model Manager Web Service Host name	vra01iws01.rainpole.local
vSphere Endpoint	lax01w01vc01.lax01.rainpole.local

Embedded vRealize Orchestrator Configuration in Region B

VMware Embedded vRealize Orchestrator provides a library of extensible workflows to allow you to create and run automated, configurable processes to manage your VMware vSphere infrastructure, as well as other VMware and third-party applications.

vRealize Orchestrator is composed of three distinct layers: an orchestration platform that provides the common features required for an orchestration tool, a plug-in architecture to integrate control of subsystems, and a library of workflows. vRealize Orchestrator is an open platform that you can extend with new plug-ins and libraries, and that can be integrated into larger architectures through the use of its REST API.

Add Compute vCenter Server Instance to vRealize Orchestrator in Region B

Add each vCenter Server instance that contributes resources to vRealize Automation and uses vRealize Orchestrator workflows to allow communication.

Procedure

1 Log in to the vRealize Orchestrator Client.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local`**

   b Click **vRealize Orchestrator Client**.

   c On the VMware vRealize Orchestrator login page, log in to the Embedded vRealize Orchestrator Host by using the following host name and credentials.

Setting	Value
Host name	vra01svr01.rainpole.local:443
User name	svc-vra
Password	*svc-vra_password*

2 In the left pane, click **Workflows**, and navigate to **Library > vCenter > Configuration**.

3 Right-click the **Add a vCenter Server instance** workflow and click **Start Workflow**.

   a On the **Set the vCenter Server Instance** page, configure the following settings and click **Next**.

Setting	Value
IP or hostname of the vCenter Server instance to add	lax01w01vc01.lax01.rainpole.local
HTTPS port of the vCenter Server instance	443
Location of SDK that you use to connect	/sdk
Will you orchestrate this instance	Yes
Do you want to ignore certificate warnings	Yes

   b On the **Set the connection properties** page, configure the following settings, and click **Submit**.

Setting	Value
Use a session per user	No
vCenter Server user name	rainpole.local\svc-vro
vCenter Server user password	*svc-vro_password*

4 To verify that the workflow completed successfully, click the **Inventory** tab and expand the **vSphere vCenter Plug-in** tree control.

The vCenter Server instance you added will be visible in the inventory.

vRealize Business Installation in Region B

vRealize Business is an IT financial management tool that provides transparency and control over the costs and quality of IT services, enabling alignment with the business and acceleration of IT transformation.

Install vRealize Business and integrate it with vRealize Automation to continuously monitor the cost of each individual virtual machine and the cost of the corresponding data center.

Procedure

1 Deploy the vRealize Business Data Collector in Region B

VMware vRealize Business for Cloud allows users to gain greater visibility into financial aspects of their cloud infrastructure and lets them optimize and improve associated operations.

2 Configure NTP for vRealize Business in Region B

Configure the network time protocol (NTP) on vRealize Business Data Collector virtual appliance from the virtual appliance management interface (VAMI).

3 Register the vRealize Business Data Collector with the Server in Region B

As part of vRealize Business installation in Region B, you connect the Region B vRealize Business Data Collector with the vRealize Business Server previously deployed in Region A.

4 Connect vRealize Business with the Compute vCenter Server in Region B

vRealize Business requires communication with the Compute vCenter Server to collect data from the entire cluster. You perform this operation by using the vRealize Business Data Collector console.

Deploy the vRealize Business Data Collector in Region B

VMware vRealize Business for Cloud allows users to gain greater visibility into financial aspects of their cloud infrastructure and lets them optimize and improve associated operations.

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 Click **Hosts and Clusters** and navigate to the **lax01m01vc01.lax01.rainpole.local** vCenter Server object.

3 Right-click the **lax01m01vc01.lax01.rainpole.local** object and select **Deploy OVF Template**.

4 On the **Select template** page, select **Local file**, browse to the location of the vRealize Business virtual appliance `.ova` file on your file system, and click **Next**.

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

Setting	Value
Name	lax01vrbc01.lax01.rainpole.local
Select a folder or datacenter	lax01-m01fd-vraias

6 On the **Select a resource** page, select the **lax01-m01-mgmt01** cluster and click **Next**.

7 On the **Review details** page, examine the virtual appliance details, such as product, version, download and disk size, and click **Next**.

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

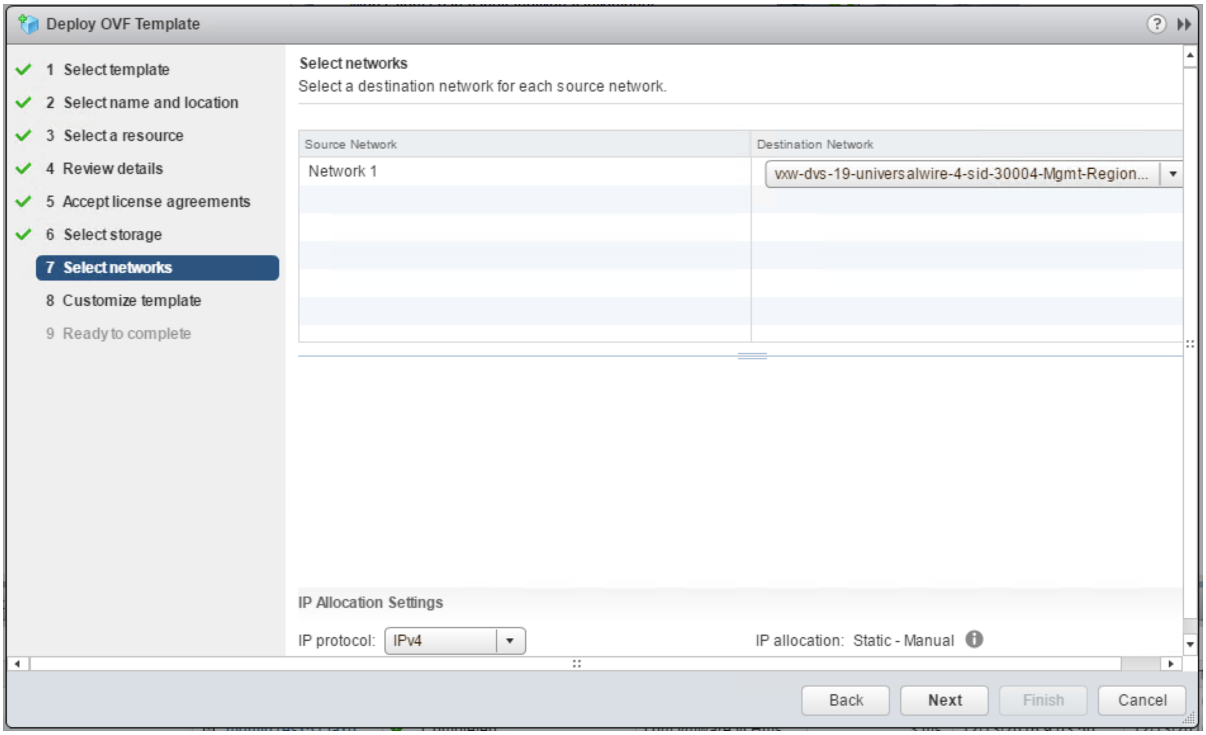
9 On the **Select storage** page, select the datastore.

   a Select **Thin provision** from the **Select virtual disk format** drop-down menu.

   b Select **vSAN Default Storage Policy** from the **VM storage policy** drop-down menu.

   c From the datastore table, select the **lax01-m01-vsan01** vSAN datastore and click **Next**.

10 On the **Select networks** page, select the distributed port group that ends with `Mgmt-RegionB01-VXLAN` from the **Destination** drop-down menu and click **Next**.



Select networks
Select a destination network for each source network.

Source Network	Destination Network
Network 1	vxw-dvs-19-universalwire-4-sid-30004-Mgmt-Region...

IP Allocation Settings

IP protocol: IPv4

IP allocation: Static - Manual

11 On the **Customize template** page, configure the following values and click **Next**.

Setting	Value
Currency	USD
Enable SSH service	Deselected
Enable Server	Deselected
Join the VMware Customer Experience Improvement Program	Selected
Root user password	*vrb_collector_root_password*
Default gateway	192.168.32.1
Domain Name	lax01vrbc01.lax01.rainpole.local
Domain Name Servers	172.17.11.5,172.17.11.4
Domain Search Path	lax01.rainpole.local
Network 1 IP Address	192.168.32.54
Network 1 Netmask	255.255.255.0

12 On the **Ready to complete** page, review the configuration settings that you specified and click **Finish**.

13 Change the vRealize Business Remote Collector virtual appliance memory size.

   a Right-click the **lax01vrbc01.lax01.rainpole.local** virtual machine and select **Edit Settings**.

   b Click **Virtual Hardware**, enter `2GB` for **Memory**, and click **OK**.

14 Navigate to the new appliance and power on the VM.

Configure NTP for vRealize Business in Region B

Configure the network time protocol (NTP) on vRealize Business Data Collector virtual appliance from the virtual appliance management interface (VAMI).

Procedure

1 Log in to the vRealize Business Data Collector appliance management console.

   a Open a Web browser and go to **`https://lax01vrbc01.lax01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_collector_root_password*

2 Configure the appliance to use a time server.

   a Click the **Administration** tab and click **Time Settings**.

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

Setting	Description
Time Sync. Mode	Use Time Server
Time Server #1	ntp.lax01.rainpole.local
Time Server #2	ntp.sfo01.rainpole.local

Register the vRealize Business Data Collector with the Server in Region B

As part of vRealize Business installation in Region B, you connect the Region B vRealize Business Data Collector with the vRealize Business Server previously deployed in Region A.

Because the tenant is configured in vRealize Automation, you register the vRealize Business Data Collector appliance with the vRealize Business Server using the following procedure.

- Generate a one-time key from vRealize Automation.
- Register the Data Collector to the vRealize Business Server.

Procedure

1. Log in to the vRealize Automation Rainpole portal.

   a. Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b. Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

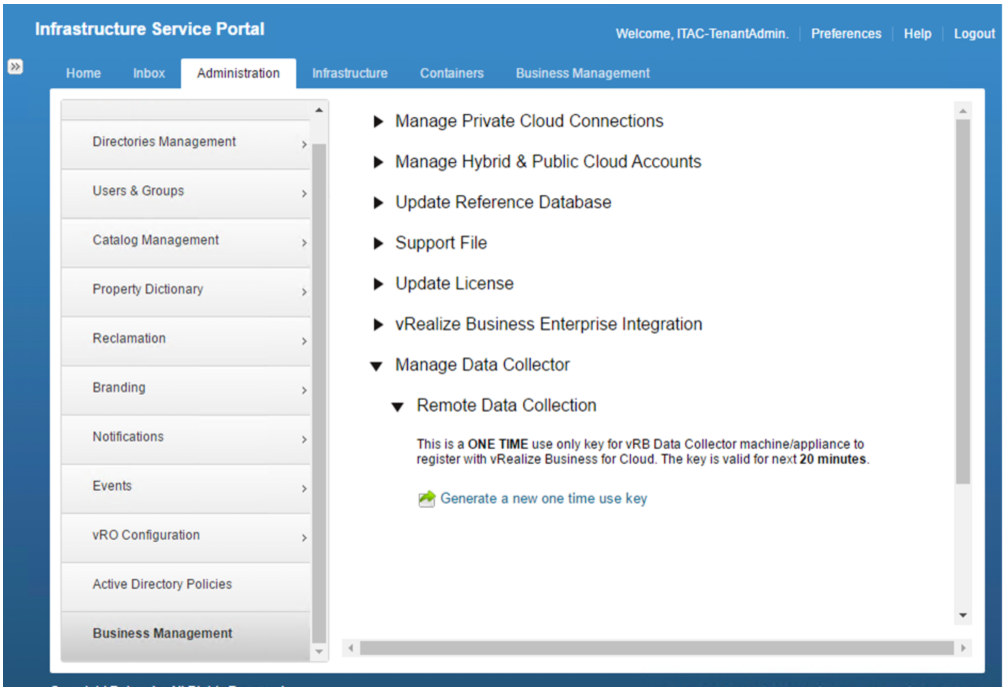
2. Generate a one-time use key for connecting vRealize Business Data Collector.

   a. Navigate to **Administration > Business Management**.

   b. Expand the **Manage Data Collector > Remote Data Collection** section.

   c. Click **Generate a new one time use key**.

   d. Save the one time use key as you need it later.



This is a **ONE TIME** use only key for vRB Data Collector machine/appliance to register with vRealize Business for Cloud. The key is valid for next **20 minutes**.

3 Log in to the vRealize Business Data Collector console.

   a Open a Web browser and go to **`https://lax01vrbc01.lax01.rainpole.local:9443/dc-ui`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_collector_root_password*

4 Register the Data Collector with the vRealize Business Server.

   a Expand the **Registration with the vRealize Business Server** section.

   b Enter the following values and click **Register**.

   After you click **Register**, a warning message informs you that the certificate is not trusted.

Setting	Value
Enter the vRB Server Url:	https://vrb01svr01.rainpole.local
Enter the One Time Key:	*one_time_use_key*

   c Click **Install** and click **OK**.

vRealize Business Data Collector is now connected to vRealize Business Server.

Connect vRealize Business with the Compute vCenter Server in Region B

vRealize Business requires communication with the Compute vCenter Server to collect data from the entire cluster. You perform this operation by using the vRealize Business Data Collector console.

Procedure

1 Log in to the vRealize Business Data Collector console.

   a Open a Web browser and go to **`https://lax01vrbc01.lax01.rainpole.local:9443/dc-ui`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_collector_root_password*

2 Click **Manage Private Cloud Connections**, select **vCenter Server**, and click the **Add** icon.

3 In the **Add vCenter Server Connection** dialog box, enter the following settings and click **Save**.

Setting	Value
Name	lax01w01vc01.lax01.rainpole.local
vCenter Server	lax01w01vc01.lax01.rainpole.local

Setting	Value
Username	svc-vra@rainpole.local
Password	*svc_vra_password*

4 In the **SSL Certificate warning** dialog box, click **Install**.

5 In the **Success** dialog box, click **OK**.

Create Anti-Affinity Rules for vRealize Automation Proxy Agent Virtual Machines in Region B

After deploying the vRealize Automation proxy agents, set up anti-affinity rules.

A VM-Host anti-affinity (or affinity) rule specifies a relationship between a group of virtual machines and a group of hosts. Anti-affinity rules force specified virtual machines to remain apart during failover actions, and are a requirement for high availability.

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 From the **Home** page, click **Hosts and Clusters**.

3 Under **lax01m01vc01.lax01.rainpole.local**, click **lax01-m01dc**, and click **lax01-m01-mgmt01**.

4 Click the **Configure** tab and under **Configuration**, select **VM/Host Rules**.

5 Under **VM/Host Rules**, click **Add** to create a virtual machine anti-affinity rule.

6 In the **Create VM/Host Rule** dialog box, specify the first rule for the vRealize Automation virtual appliances.

   a In the **Name** text box, enter `anti-affinity-rule-vra-ias`.

   b Select the **Enable rule** check box.

   c Select **Separate Virtual Machines** from the **Type** drop-down menu.

   d Click **Add**, select the **lax01ias01a** and **lax01ias01b** virtual machines, click **OK**, and click **OK**.

Content Library Configuration in Region B

Content libraries are container objects for VM templates, vApp templates, and other types of files. vSphere administrators can use the templates in the library to deploy virtual machines and vApps in the vSphere inventory. Sharing templates and files across multiple vCenter Server instances in same or different locations brings out consistency, compliance, efficiency, and automation in deploying workloads at scale.

You create and manage a content library from a single vCenter Server instance, but you can share the library items to other vCenter Server instances if HTTP(S) traffic is allowed between them.

Connect to Content Library of the Compute vCenter Server Instance in Region B

Connect to content library in Region A to synchronize templates among different Compute vCenter Server instances so that all of the templates in your environment are consistent.

There is only one Compute vCenter Server in this VMware validated design. If you deploy more instances for use by the compute cluster they can also use this content library.

Procedure

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

   a. Open a Web browser and go to **`https://sfo01w01vc01.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** page, click **Content Libraries** and click content library **sfo01-w01cl-vra01** that was created in the Compute vCenter Server in Region A.

3. Select the **Configure** tab and click **Copy Link**.

   A subscription URL is saved to the clipboard.

4. Log out from the vSphere Web Client session to log back in to the Region B Compute vCenter Server.

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

   a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

6 From the **Home** page, click **Content Libraries**, and click the **Create new content library** icon.

The **New Content Library** wizard opens.

7 On the **Name and location** page, specify the following settings and click **Next**.

Setting	Value
Name	lax01-w01cl-vra01
vCenter Server	lax01w01vc01.lax01.rainpole.local

8 On the **Configure content library** page, select **Subscribed content library** specify the following settings, and click **Next**.

Setting	Value
Subscribed content library	Selected
Subscription URL	*sfo01-w01cl-vra01_subscription_URL*
Enable authentication	Selected
Password	*sfo01-w01cl-vra01_password*
Download all library content immediately	Selected

9 On the **Add storage** page, click the **Select a datastore** radio button, select the **lax01-w01-lib01** datastore to store the content library, and click **Next**.

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

Tenant Content Creation in Region B

To provision virtual machines in the Compute vCenter Server instance, you configure the tenant to utilize vCenter Server compute resources.

Prerequisites

- Verify that a vCenter Server compute cluster has been deployed and configured. See "Deploy and Configure the Compute and Edge Clusters Components in Region A."
- Verify that an NSX instance has been configured for use by the vCenter Server compute cluster. See "Deploy and Configure the Compute and Edge Clusters NSX Instance in Region A."

- Proxy agents have been deployed.

Procedure

1. Create Fabric Groups in Region B

   IaaS administrators can organize virtualization compute resources and cloud endpoints into fabric groups by type and intent. One or more fabric administrators manage the resources in each fabric group. Fabric administrators are responsible for creating reservations on the compute resources in their groups to allocate fabric to specific business groups. Fabric groups are created in a specific tenant, but their resources can be made available to users who belong to business groups in all tenants.

2. Create Reservation Policies in Region B

   You use reservation policies to group similar reservations together. Create the reservation policy tag first, then add the policy to reservations to allow a tenant administrator or business group manager to use the reservation policy in a blueprint.

3. Create a vSphere Endpoint in vRealize Automation in Region B

   To allow vRealize Automation to manage the infrastructure, IaaS administrators create endpoints and configure user-credentials for those endpoints. When you create a vSphere Endpoint, vRealize Automation can to communicate with the vSphere environment and discover compute resources that are managed by vCenter Server, collect data, and provision machines.

4. Add Compute Resources to a Fabric Group in Region B

   You allocate compute resources to fabric groups so that vRealize Automation can use the resources in that compute resource for that fabric group when provisioning virtual machines.

5. Create Reservations for the Compute Cluster in Region B

   Before members of a business group can request machines, fabric administrators must allocate resources to them by creating a reservation. Each reservation is configured for a specific business group to grant them access to request machines on a specified compute resource.

6. Create Reservations for the User Edge Resources in Region B

   Before members of a business group can request virtual machines, fabric administrators must allocate resources to that business group by creating a reservation. Each reservation is configured for a specific business group to grant them access to request virtual machines on a specified compute resource.

7. Create Blueprint Customization Specifications in Compute vCenter Server in Region B

   Create two customization specifications, one for Linux and one for Windows, for use by the virtual machines you deploy. Customization specifications are XML files that contain system configuration settings for the guest operating systems used by virtual machines. When you apply a specification to a guest operating system during virtual machine cloning or deployment, you prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names.

8 Create Virtual Machines Using VM Templates in the Content Library in Region B

vRealize Automation cannot directly access virtual machine templates in the content library. You must create a virtual machine using the virtual machine templates in the content library, then convert the template in vCenter Server. Perform this procedure on all vCenter Servers compute clusters you add to vRealize Automation, including the first vCenter Server compute instance.

9 Convert Virtual Machines to VM Templates in Region B

You can convert a virtual machine directly to a template instead of making a copy by cloning.

10 Configure Single Machine Blueprints in Region B

Virtual machine blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

11 Configure Unified Single Machine Blueprints for Cross-Region Deployment in Region B

To provision blueprints from a specific vRealize Automation deployment to multiple regions, you define the additional regions in vRealize Automation, and associate the blueprints with those locations.

Create Fabric Groups in Region B

IaaS administrators can organize virtualization compute resources and cloud endpoints into fabric groups by type and intent. One or more fabric administrators manage the resources in each fabric group. Fabric administrators are responsible for creating reservations on the compute resources in their groups to allocate fabric to specific business groups. Fabric groups are created in a specific tenant, but their resources can be made available to users who belong to business groups in all tenants.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Select **Infrastructure > Endpoints > Fabric Groups**.

3 Click **New Fabric Group**, enter the following settings and click **OK**.

Setting	Value
Name	LAX Fabric Group
Fabric administrators	ug-vra-admins-rainpole@rainpole.local

You have not configured a vCenter Endpoint yet. A compute resource is currently available for you to select. You configure the vCenter Endpoint later.

4 Log out of the vRealize Automation portal.

Create Reservation Policies in Region B

You use reservation policies to group similar reservations together. Create the reservation policy tag first, then add the policy to reservations to allow a tenant administrator or business group manager to use the reservation policy in a blueprint.

When you request a machine, it can be provisioned on any reservation of the appropriate type that has sufficient capacity for the machine. You can apply a reservation policy to a blueprint to restrict the machines provisioned from that blueprint to a subset of available reservations. A reservation policy is often used to collect resources into groups for different service levels, or to make a specific type of resource easily available for a particular purpose. You can add multiple reservations to a reservation policy, but a reservation can belong to only one policy. You can assign a single reservation policy to more than one blueprint. A blueprint can have only one reservation policy. A reservation policy can include reservations of different types, but only reservations that match the blueprint type are considered when selecting a reservation for a particular request.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > Reservation > Reservation Polices**.

3 Click the **New** icon, configure the following settings, and click **OK**.

Setting	Value
Name	LAX-Production-Policy
Description	Reservation policy for Production Business Group in LAX

4 Click the **New** icon, configure the following settings, and click **OK**.

Setting	Value
Name	LAX-Development-Policy
Description	Reservation policy for Development Business Group in LAX

5 Click the **New** icon, configure the following settings, and click **OK**.

Setting	Value
Name	LAX-Edge-Policy
Description	Reservation policy for Tenant Edge resources in LAX

Create a vSphere Endpoint in vRealize Automation in Region B

To allow vRealize Automation to manage the infrastructure, IaaS administrators create endpoints and configure user-credentials for those endpoints. When you create a vSphere Endpoint, vRealize Automation can to communicate with the vSphere environment and discover compute resources that are managed by vCenter Server, collect data, and provision machines.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > Endpoints > Endpoints** and click **New > Virtual > vSphere (vCenter)**.

3 On the **New Endpoint - vSphere (vCenter)** page, create a vSphere Endpoint with the following settings, and click **Test Connection**.

Setting	Value
Name	lax01w01vc01.lax01.rainpole.local
Address	https://lax01w01vc01.lax01.rainpole.local/sdk
User Name	rainpole\svc-vra
Password	*svc-vra_password*

Note The Name in the table above must be identical to the vSphere Endpoint from Step 10 in Install vRealize Automation Proxy Agents in Region B.

4 If a **Security Alert** window appears, click **OK**.

5 Click **OK** to create the Endpoint.

6 Remain on the page and click **New > Network and Security > NSX**.

7 On the General page, configure the vRealize Automation Endpoint with the following settings.

Setting	Value
Name	LAX-NSXEndpoint
Address	https://lax01w01nsx01.lax01.rainpole.local
User Name	rainpole\svc-vra
Password	*svc-vra_password*

8 Click **Test Connection**.

9 Click on the **Associations** tab, click **New**, choose **lax01w01vc01.lax01.rainpole.local** from the **Name** drop-down menu, and click **OK**.

10 If a **Security Alert** window appears, click **OK**.

11 Click **OK** to create the Endpoint.

Add Compute Resources to a Fabric Group in Region B

You allocate compute resources to fabric groups so that vRealize Automation can use the resources in that compute resource for that fabric group when provisioning virtual machines.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

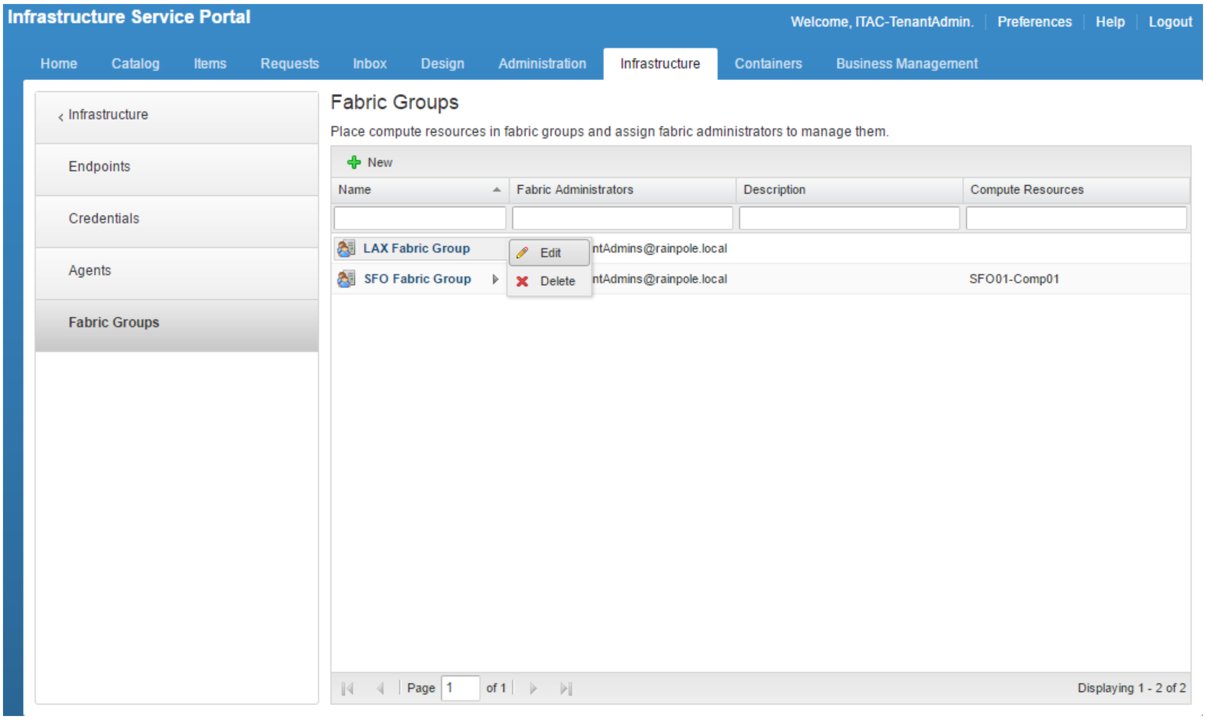
a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > End Points > Fabric Groups**.

3 In the **Name** column, point the mouse over the fabric group name **LAX Fabric Group**, and click **Edit**.



Name	Fabric Administrators	Description	Compute Resources
LAX Fabric Group	ntAdmins@rainpole.local		
SFO Fabric Group	ntAdmins@rainpole.local		SFO01-Comp01

4 On the **Edit Fabric Group** page, select **lax01-w01-comp01** from the **Compute resources** table, and click **OK**.

Note It might take several minutes for vRealize Automation to connect to the Compute vCenter Server system and associated clusters. If you still do not see the shared edge and compute cluster after some time, try to restart both proxy agent services in the virtual machines lax01ias01a.lax01.rainpole.local and lax01ias01b.lax01.rainpole.local.

5 Navigate to **Infrastructure > Compute Resources > Compute Resources**.

6 In the **Compute Resource** column, point the mouse over the shared edge and compute cluster **lax01-w01-comp01**, and click **Data Collection**.

7 Click on the **Request now** buttons in each field on the page.

Wait a few seconds for the data collection process to complete.

8 Click **Refresh**, and verify that the **Status** for both **Inventory** and **Network and Security Inventory** shows **Succeeded**.

Create Reservations for the Compute Cluster in Region B

Before members of a business group can request machines, fabric administrators must allocate resources to them by creating a reservation. Each reservation is configured for a specific business group to grant them access to request machines on a specified compute resource.

Perform this procedure twice to create compute resource reservations for both the Production and Development business groups.

Table 4-3. Business Group Names

Group	Name
Production	LAX01-Comp01-Prod-Res01
Development	LAX01-Comp01-Dev-Res01

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > Reservations > Reservations** and select **New > vSphere (vCenter)**.

3 On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values for each group.

Setting	Production Group Value	Development Group Value
Name	LAX01-Comp01-Prod-Res01	LAX01-Comp01-Dev-Res01
Tenant	rainpole	rainpole
Business Group	Production	Development
Reservation Policy	LAX-Production-Policy	LAX-Development-Policy
Priority	100	100
Enable This Reservation	Selected	Selected

4 On the **New Reservation - vSphere (vCenter)** page, click the **Resources** tab.

   a Select **lax01-w01-comp01 (lax01w01vc01.lax01.rainpole.local)** from the **Compute Resource** drop-down menu.

   b In the **This Reservation** column of the **Memory (GB)** table, enter **`200`**.

   c In the **Storage (GB)** table, select the check box for your primary datastore, for example, **lax01-w01-vsan01**, enter **`2000`** in the **This Reservation Reserved** text box, enter **`1`** in the **Priority** text box, and click **OK**.

   d Select **lax01-w01rp-user-vm** from the **Resource pool** drop-down menu.

5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.

6 On the **Network** tab, select the following network path from the **Network Paths** list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.

   a Configure the Production Business Group with the following values.

Production Network Path	Production Group Network Profile
vxw-dvs-xxxxx-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxw-dvs-xxxxx-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxw-dvs-xxxxx-Production-App-VXLAN	Ext-Net-Profile-Production-App

   b Configure the Development Business Group with the following values.

Development Network Path	Development Group Network Profile
vxw-dvs-xxxxx-Development-Web-VXLAN	Ext-Net-Profile-Development-Web
vxw-dvs-xxxxx-Development-DB-VXLAN	Ext-Net-Profile-Development-DB
vxw-dvs-xxxxx-Development-App-VXLAN	Ext-Net-Profile-Development-App

7 Click **OK** to save the reservation.

8 Repeat this procedure to create a reservation for the Development Business Group.

Create Reservations for the User Edge Resources in Region B

Before members of a business group can request virtual machines, fabric administrators must allocate resources to that business group by creating a reservation. Each reservation is configured for a specific business group to grant them access to request virtual machines on a specified compute resource.

Perform this procedure twice to create Edge reservations for both the Production and Development business groups.

Table 4-4. Business Group Names

Group	Name
Production	LAX01-Edge01-Prod-Res01
Development	LAX01-Edge01-Dev-Res01

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > Reservations > Reservations**, and click **New vSphere (vCenter)**.

3 On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values for your business group.

Setting	Production Group Value	Development Group Value
Name	LAX01-Edge01-Prod-Res01	LAX01-Edge01-Dev-Res01
Tenant	rainpole	rainpole
Business Group	Production	Development
Reservation Policy	LAX-Edge-Policy	LAX-Edge-Policy
Priority	100	100
Enable This Reservation	Selected	Selected

4 On the **New Reservation - vSphere (vCenter)** page, click the **Resources** tab.

a Select **lax01-w01-comp01(lax01w01vc01.lax01.rainpole.local)** from the **Compute resource** drop-down menu.

b Enter `200` in the **This Reservation** column of the **Memory (GB)** table.

c In the **Storage (GB)** table, select the check box for your primary datastore, for example, **lax01-w01-vsan01**, enter `2000` in the **This Reservation Reserved** text box, enter `1` in the **Priority** text box, and click **OK**.

d Select **lax01-w01rp-user-edge** from the **Resource pool** drop-down menu.

5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.

6 On the **Network** tab, select the network path check boxes listed in the table below from the **Network Paths** list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.

Production Business Group

Production Port Group	Production Network Profile
vxw-dvs-xxxxx-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxw-dvs-xxxxx-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxw-dvs-xxxxx-Production-App-VXLAN	Ext-Net-Profile-Production-App

Development Business Group

Development Port Group	Development Network Profile
vxw-dvs-xxxxx-Development -Web-VXLAN	Ext-Net-Profile-Development -Web
vxw-dvs-xxxxx-Development -DB-VXLAN	Ext-Net-Profile-Development -DB
vxw-dvs-xxxxx-Development -App-VXLAN	Ext-Net-Profile-Development -App

7 Click **OK** to save the reservation.

8 Repeat the procedure to create an Edge reservation for the Development Business Group.

Create Blueprint Customization Specifications in Compute vCenter Server in Region B

Create two customization specifications, one for Linux and one for Windows, for use by the virtual machines you deploy. Customization specifications are XML files that contain system configuration settings for the guest operating systems used by virtual machines. When you apply a specification to a guest operating system during virtual machine cloning or deployment, you prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names.

You use the customization specifications that you create when you produce blueprints for use with vRealize Automation.

Procedure

1 Create a Customization Specification for Linux in Region B

Create a Linux guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

2 Create a Customization Specification for Windows in Region B

Create a Windows guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

Create a Customization Specification for Linux in Region B

Create a Linux guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

Procedure

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

a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

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

2 Navigate to **Home > Policies and Profiles > Customization Specification Manager**.

3 Select the vCenter Server **lax01w01vc01.lax01.rainpole.local** from the drop-down menu.

4 Click the **Create a new specification** icon.

   The **New VM Guest Customization Spec** wizard appears.

5 On the **Specify Properties** page, select **Linux** from the **Target VM Operating System** drop-down menu, enter `os-linux-custom-spec` for the **Customization Spec Name**, and click **Next**.

6 On the **Set Computer Name** page, select **Use the virtual machine name**, enter `lax01.rainpole.local` in the **Domain Name** text box and click **Next**.

7 On the **Time Zone** page, specify the time zone as shown in the table below for the virtual machine, and click **Next**.

Setting	Value
Area	America
Location	Los Angeles
Hardware Clock Set To	Local Time

8 On the **Configure Network** page, click **Next**.

9 On the **Enter DNS and domain settings** page, leave the default settings, and click **Next**.

10 Click **Finish** to save your changes.

   The customization specification that you created is listed in the **Customization Specification Manager**.

Create a Customization Specification for Windows in Region B

Create a Windows guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

Procedure

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

   a Open a Web browser and go to `https://lax01w01vc01.lax01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

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

2 Navigate to **Home > Policies and Profiles > Customization Specification Manager**.

3 Select the vCenter Server **lax01w01vc01.lax01.rainpole.local** from the drop-down menu.

4 Click the **Create a new specification** icon.

   The **New VM Guest Customization Spec** wizard appears.

5 On the **Specify Properties** page, select **Windows** from the **Target VM Operating System** drop-down menu, enter **`os-windows-joindomain-custom-spec`** for the **Customization Spec Name**, and click **Next**.

6 On the **Set Registration Information** page, enter **`Rainpole`** for the virtual machine owner's **Name** and **Organization**, and click **Next**.

7 On the **Set Computer Name** page, select **Use the virtual machine name**, and click **Next**.

The operating system uses this name to identify itself on the network.

8 On the **Enter Windows License** page, provide licensing information for the Windows operating system, enter the ***volume_license_key*** license key, and click **Next**.

9 Specify the administrator password for use with the virtual machine, and click **Next**.

10 On the **Time Zone** page, select **(GMT-08:00) Pacific Time(US & Canada)**, and click **Next**.

11 On the **Run Once** page, click **Next**.

12 On the **Configure Network** page, click **Next**.

13 On the **Set Workgroup or Domain** page, select **Windows Server Domain**, configure the following settings, and click **Next**.

Setting	Value
Domain	lax01.rainpole.local
User name	svc-domain-join@rainpole.local
Password	*svc-domain-join_password*

14 On the **Set Operating System Options** page, select **Generate New Security ID (SID)**, and click **Next**.

15 Click **Finish** to save your changes.

The customization specification that you created is listed in the **Customization Specification Manager**.

Create Virtual Machines Using VM Templates in the Content Library in Region B

vRealize Automation cannot directly access virtual machine templates in the content library. You must create a virtual machine using the virtual machine templates in the content library, then convert the template in vCenter Server. Perform this procedure on all vCenter Servers compute clusters you add to vRealize Automation, including the first vCenter Server compute instance.

Repeat this procedure three times for each VM Template in the content library. The table below lists the VM Templates and the guest OS each template uses to create a virtual machine.

Table 4-5. VM Templates and their Guest Operating Systems

VM Template Name	Guest OS
redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)
windows-2012r2-64	Windows Server 2012 R2 (64-bit)
windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)

Procedure

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

   a Open a Web browser and go to `https://lax01w01vc01.lax01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

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

2 Navigate to **Home > VMs and Templates**.

3 Expand the **lax01w01vc01.lax01.rainpole.local** vCenter Server.

4 Right-click the **lax01-w01dc** data center and select **New Folder > New VM and Template Folder**.

5 Create a new folder and label it `VM Templates`.

6 Navigate to **Home > Content Libraries**.

7 Click **lax01-w01cl-vra01 > Templates**.

8 Right-click the VM Template **redhat6-enterprice-64** and click **New VM from This Template**.

   The **New Virtual Machine from Content Library** wizard opens.

9 On the **Select name and location** page, use the same template name.

   Note Use the same template name to create a common service catalog that works across different vCenter Server instances within your datacenter environment.

10 Select **VM Templates** as the folder for this virtual machine, and click **Next**.

11 On the **Select a resource** page, expand cluster **lax01-w01-comp01** and select resource pool **lax01-w01rp-user-vm**.

12 On the **Review details** page, verify the template details, and click **Next**.

13 On the **Select storage** page, select the **lax01-w01-lib01** datastore and **Thin Provision** from the **Select virtual disk format** drop-down menu.

14 On the **Select networks** page, select **lax01-w01-vds01-management** for the **Destination Network**, and click **Next**.

Note vRealize Automation will change the network according to the blueprint configuration.

15 On the **Ready to complete** page, review the configurations you made for the virtual machine, and click **Finish**.

A new task for creating the virtual machine appears in the **Recent Tasks** pane. After the task is complete, the new virtual machine is created.

16 Repeat this procedure for all of the VM Templates in the content library.

Convert Virtual Machines to VM Templates in Region B

You can convert a virtual machine directly to a template instead of making a copy by cloning.

Repeat this procedure three times for each of the VM Templates in the content library. The table below lists the VM Templates and the guest OS each template uses to create a virtual machine.

Table 4‑6. VM Templates and their Guest Operating Systems

VM Template Name	Guest OS
redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)
windows-2012r2-64	Windows Server 2012 R2 (64-bit)
windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)

Procedure

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

a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

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

2 Navigate to **Home > VMs and Templates**.

3 In the **Navigator** pane, expand **lax01w01vc01.lax01.rainpole.local > lax01-w01dc > VM Templates**.

4 Right-click the **redhat6-enterprise-64** virtual machine located in the `VM Templates` folder, and click **Template > Convert to Template**.

5 Click **Yes** to confirm the template conversion.

Configure Single Machine Blueprints in Region B

Virtual machine blueprints determine a machine’s attributes, the manner in which it is provisioned, and its policy and management settings.

Procedure

1 Create a Service Catalog in Region B

A service catalog provides a common interface for consumers of IT services to request services, track their requests, and manage their provisioned service items.

2 Create a Single Machine Blueprint in Region B

Create a blueprint for cloning the windows-2012r2-64 virtual machine using the specified resources on the Compute vCenter Server. Tenants can later use this blueprint for automatic provisioning. A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

3 Configure Entitlements of Blueprints in Region B

You entitle users to the actions and items that belong to the service catalog by associating each blueprint with an entitlement.

4 Test the Deployment of a Single Machine Blueprint in Region B

Test your environment and confirm the successful provisioning of virtual machines using the blueprints that have been created. If multiple availability zones have been configured, you must manually place all the virtual machines provisioned by vRealize Automation into the appropriate VM group for the availability zone.

Create a Service Catalog in Region B

A service catalog provides a common interface for consumers of IT services to request services, track their requests, and manage their provisioned service items.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Administration** tab, click **Catalog Management > Services**, and click **New**.

The **New Service** page appears.

3 In the **New Service** page, configure the following settings, and click **OK**.

Setting	Value
Name	LAX Service Catalog
Description	Default setting (blank)
Icon	Default setting (blank)
Status	Active
Hours	Default setting (blank)
Owner	Default setting (blank)
Support Team	Default setting (blank)
Change Window	Default setting (blank)

Create a Single Machine Blueprint in Region B

Create a blueprint for cloning the windows-2012r2-64 virtual machine using the specified resources on the Compute vCenter Server. Tenants can later use this blueprint for automatic provisioning. A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

Repeat this procedure to create six blueprints.

Blueprint Name	VM Template	Customization Specification	Reservation Policy
Windows Server 2012 R2 - LAX Prod	windows-2012r2-64 (lax01w01vc01.lax01.rainpole.local)	os-windows-joindomain-custom-spec	LAX-Production-Policy
Windows Server 2012 R2 - LAX Dev	windows-2012r2-64 (lax01w01vc01.lax01.rainpole.local)	os-windows-joindomain-custom-spec	LAX-Development-Policy
Windows Server 2012 R2 With SQL2012 - LAX Prod	windows-2012r2-64-sql2012(lax01w01vc01.lax01.rainpole.local)	os-windows-joindomain-custom-spec	LAX-Production-Policy
Windows Server 2012 R2 With SQL2012 - LAX Dev	windows-2012r2-64-sql2012(lax01w01vc01.lax01.rainpole.local)	os-windows-joindomain-custom-spec	LAX-Development-Policy
Redhat Enterprise Linux 6 - LAX Prod	redhat6-enterprise-64(lax01w01vc01.lax01.rainpole.local)	os-linux-custom-spec	LAX-Production-Policy
Redhat Enterprise Linux 6 - LAX Dev	redhat6-enterprise-64(lax01w01vc01.lax01.rainpole.local)	os-linux-custom-spec	LAX-Development-Policy

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Design > Blueprints**.

3 Click **New**.

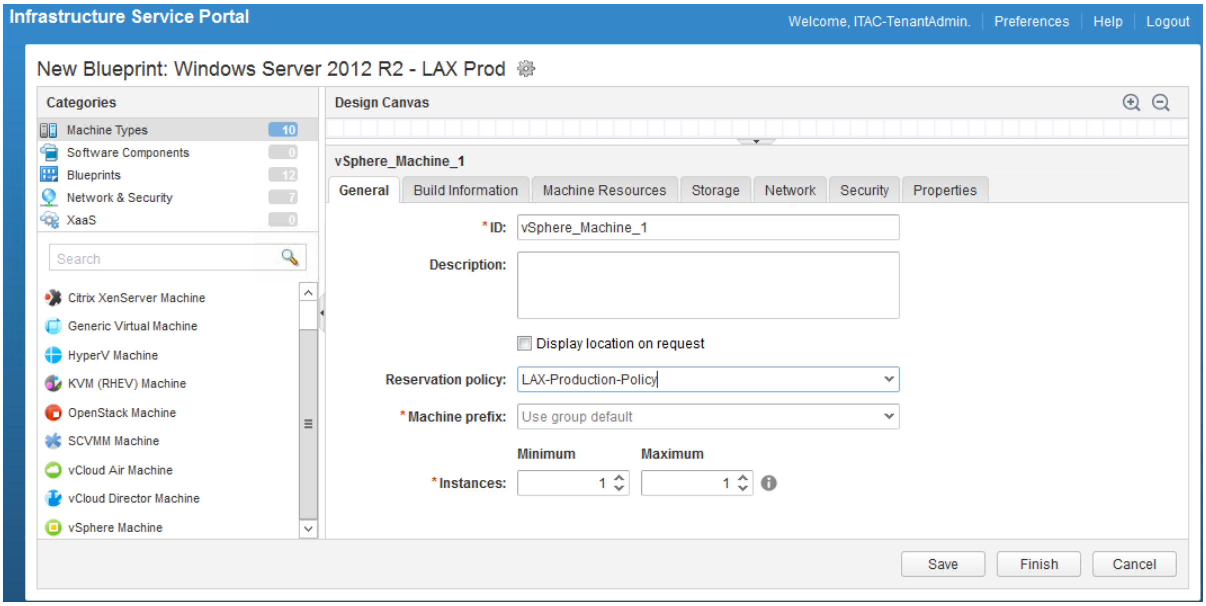
4 In the **New Blueprint** dialog box, configure the following settings on the **General** tab, and click **OK**.

Setting	Value
Name	Windows Server 2012 R2 - LAX Prod
Deployment limit	Default setting (blank)
Minimum	30
Maximum	270
Archive (days)	15

5 Select and drag the **vSphere (vCenter) Machine** icon to the **Design Canvas**.

6 Click the **General** tab, configure the following settings, and click **Save**.

Setting	Default
ID	Default setting (vSphere_vCenter_Machine_1)
Description	Default setting (blank)
Display location on request	Deselected
Reservation policy	LAX-Production-Policy
Machine prefix	Default setting (blank)
Minimum	Default setting (blank)
Maximum	Default setting (blank)



New Blueprint: Windows Server 2012 R2 - LAX Prod

vSphere_Machine_1

*ID: vSphere_Machine_1

Description:

□ Display location on request

Reservation policy: LAX-Production-Policy

*Machine prefix: Use group default

*Instances: Minimum 1 Maximum 1

7 Click the **Build Information** tab, configure the following settings, and click **Save**.

Setting	Value
Blueprint type	Server
Action	Clone
Provisioning workflow	CloneWorkflow
Clone from	windows-2012r2-64
Customization spec	os-windows-joindomain-custom-spec

Note If the value of the **Clone from** setting does not list **windows-2012r2-64 template**, you must perform a data collection on the **sfo01-w01-comp01** Compute Resource.

8 Click the **Machine Resources** tab, configure the following settings, and click **Save**.

Setting	Minimum	Maximum
CPU	2	4
Memory (MB):	4096	16384
Storage	Default setting (blank)	Default setting (50)

9 In the **Categories** section of the page, select **Network & Security** to display the list of available network and security components.

   a Select the **Existing Network** component and drag it onto the **Design Canvas**.

   b Click in the **Existing network** text box and select the **Ext-Net-Profile-Production-Web** network profile.

Blueprint Name	Existing network
Windows Server 2012 R2 - LAX Prod	Ext-Net-Profile-Production-Web
Windows Server 2012 R2 - LAX Dev	Ext-Net-Profile-Development-Web
Windows Server 2012 R2 With SQL2012 - LAX Prod	Ext-Net-Profile-Production-DB
Windows Server 2012 R2 With SQL2012 - LAX Dev	Ext-Net-Profile-Development-DB
Redhat Enterprise Linux 6 - LAX Prod	Ext-Net-Profile-Production-App
Redhat Enterprise Linux 6 - LAX Dev	Ext-Net-Profile-Development-App

   c Click **Save**.

   d Select **vSphere_vCenter_Machine_1** properties from the design canvas.

   e Select the **Network** tab, click **New**, configure the following settings, and click **OK**.

Network	Assignment Type	Address
ExtNetProfileProductionWeb	Static IP	Default setting (blank)
ExtNetProfileDevelopmentWeb	Static IP	Default setting (blank)
ExtNetProfileProductionDB	Static IP	Default setting (blank)
ExtNetProfileDevelopmentDB	Static IP	Default setting (blank)
ExtNetProfileProductionApp	Static IP	Default setting (blank)
ExtNetProfileDevelopmentApp	Static IP	Default setting (blank)

   f Click **Finish** to save the blueprint.

10 Select the blueprint **Windows Server 2012 R2 - LAX Prod** and click **Publish**.

11 Repeat this procedure to create additional blueprints.

Configure Entitlements of Blueprints in Region B

You entitle users to the actions and items that belong to the service catalog by associating each blueprint with an entitlement.

Repeat this procedure to associate the six blueprints with their entitlement.

Blueprint Name	VM Template	Reservation Policy	Service Catalog	Add to Entitlement
Windows Server 2012 R2 - LAX Prod	windows-2012r2-64 (lax01w01vc01.lax01.rainpole.local)	LAX-Production-Policy	LAX Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 - LAX Dev	windows-2012r2-64 (lax01w01vc01.lax01.rainpole.local)	LAX-Development-Policy	LAX Service Catalog	Dev-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - LAX Prod	windows-2012r2-64-sql2012(lax01w01vc01.lax01.rainpole.local)	LAX-Production-Policy	LAX Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - LAX Dev	windows-2012r2-64-sql2012(lax01w01vc01.lax01.rainpole.local)	LAX-Development-Policy	LAX Service Catalog	Dev-SingleVM-Entitlement
Redhat Enterprise Linux 6 - LAX Prod	redhat6-enterprise-64(lax01w01vc01.lax01.rainpole.local)	LAX-Production-Policy	LAX Service Catalog	Prod-SingleVM-Entitlement
Redhat Enterprise Linux 6 - LAX Dev	redhat6-enterprise-64(lax01w01vc01.lax01.rainpole.local)	LAX-Development-Policy	LAX Service Catalog	Dev-SingleVM-Entitlement

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

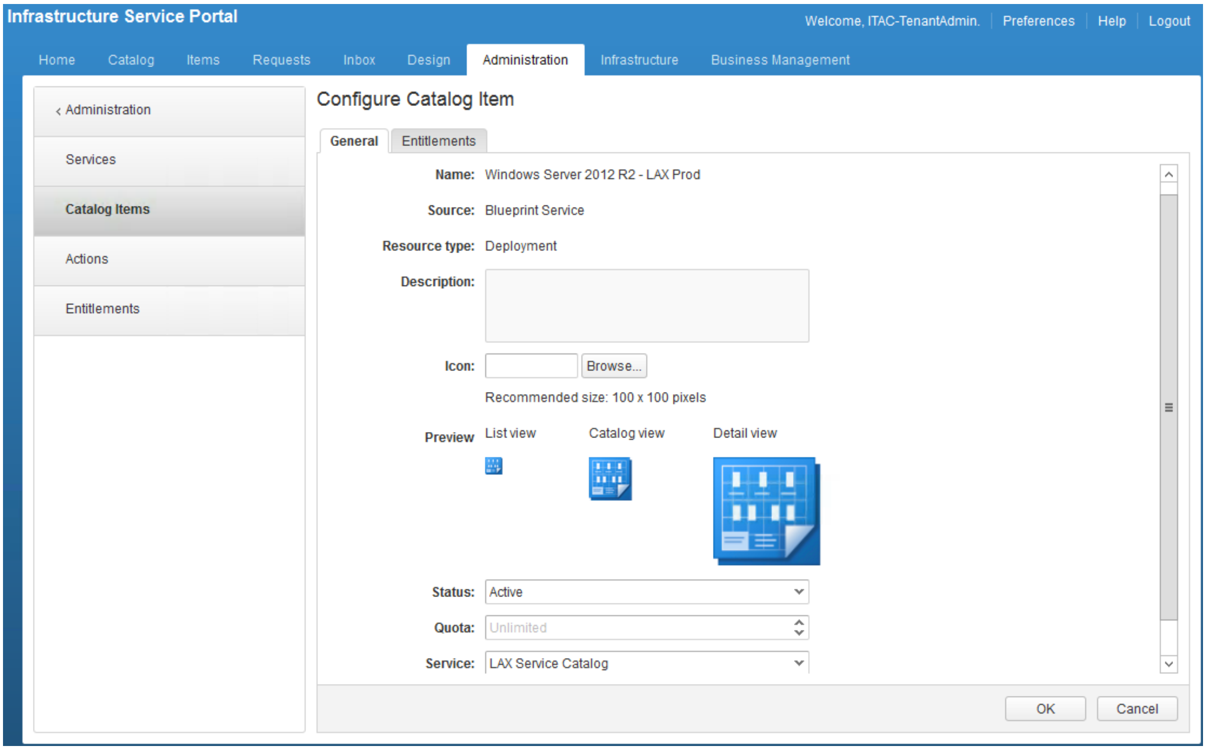
   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Select the **Administration** tab and navigate to **Catalog Management > Catalog Items**.

3 On the **Catalog Items** pane, select the **Windows Server 2012 R2 - LAX Prod** blueprint in the **Catalog Items** list and click **Configure**.

4 On the **General** tab of the **Configure Catalog Items** dialog box, select **LAX Service Catalog** from the **Service** drop-down menu, and click **OK**.



Configure Catalog Item

Name: Windows Server 2012 R2 - LAX Prod

Source: Blueprint Service

Resource type: Deployment

Description:

Icon:

Recommended size: 100 x 100 pixels

Status: Active

Quota: Unlimited

Service: LAX Service Catalog

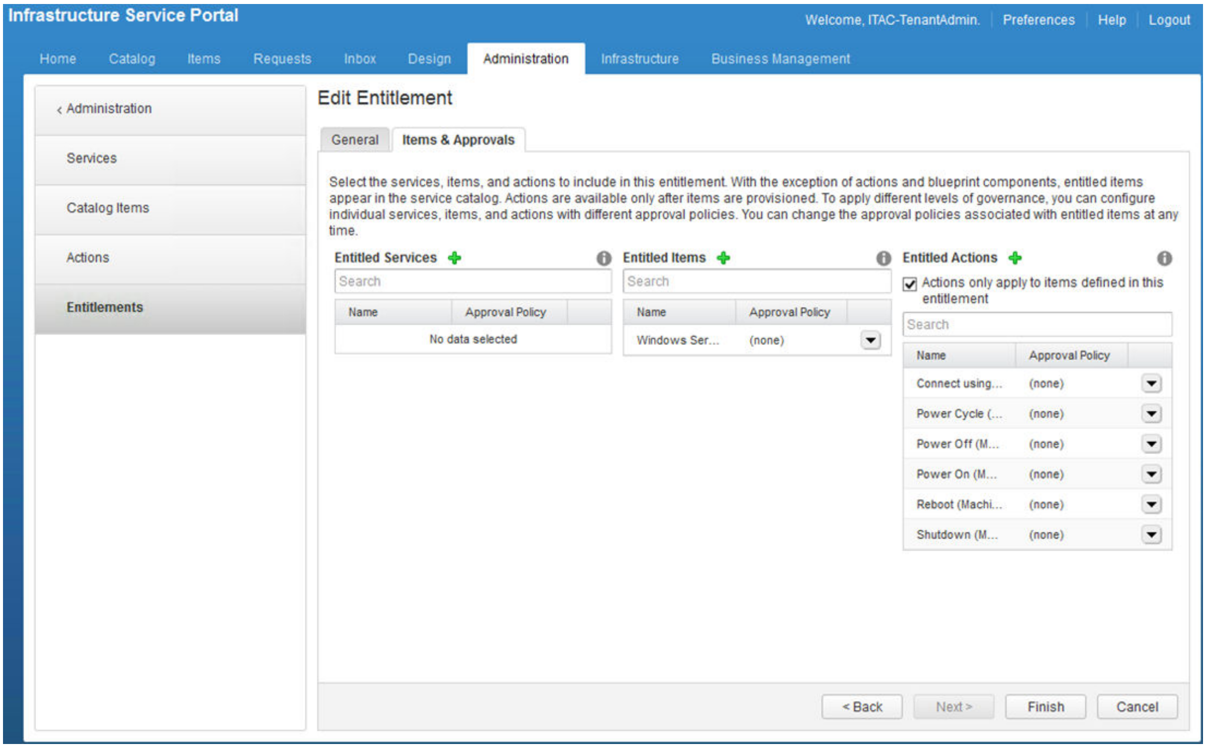
5 Associate the blueprint with the **Prod-SingleVM-Entitlement** entitlement.

a Click **Entitlements** and select **Prod-SingleVM-Entitlement**.

The **Edit Entitlement** pane appears.

b Select the **Items & Approvals** tab and add the **Windows Server 2012 R2 - LAX Prod** blueprint to the **Entitled Items** list.

c Click **Finish**.



Edit Entitlement

Select the services, items, and actions to include in this entitlement. With the exception of actions and blueprint components, entitled items appear in the service catalog. Actions are available only after items are provisioned. To apply different levels of governance, you can configure individual services, items, and actions with different approval policies. You can change the approval policies associated with entitled items at any time.

Entitled Services

Name	Approval Policy
No data selected	

Entitled Items

Name	Approval Policy
Windows Ser...	(none)

Entitled Actions

☑ Actions only apply to items defined in this entitlement

Name	Approval Policy
Connect using...	(none)
Power Cycle (...	(none)
Power Off (M...	(none)
Power On (M...	(none)
Reboot (Machi...	(none)
Shutdown (M...	(none)

6 Repeat this procedure to associate all of the blueprints with their entitlement.

Test the Deployment of a Single Machine Blueprint in Region B

Test your environment and confirm the successful provisioning of virtual machines using the blueprints that have been created. If multiple availability zones have been configured, you must manually place all the virtual machines provisioned by vRealize Automation into the appropriate VM group for the availability zone.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

  a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

  b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Select the **Catalog** tab, and click **LAX Service Catalog** from the catalog of available services.

3 Click the **Request** button for the **Windows Server 2012 R2 - LAX Prod** blueprint.

4 Click **Submit**.

5 Verify the request finishes successfully.

  a Select the **Requests** tab.

  b Select the request you submitted and wait several minutes for the request to complete.

  Click the **Refresh** icon every few minutes until a Successful message appears under **Status**.

  c Click **View Details**.

  d Under **Status Details**, verify that the virtual machine successfully provisioned.

6 Verify the virtual machine provisions in the consolidated cluster.

  a Open a Web browser and go to `https://lax01w01vc01.lax01.rainpole.local`.

  b Log in as the vCenter Server administrator using the following credentials.

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

  c Select **Home > VMs and Templates**.

  d In the Navigator panel, expand the vCenter Server cluster **lax01w01vc01.lax01.rainpole.local > lax01-w01-comp01 > lax01-w01rp-user-vm**, and verify the existence of the virtual machine.

Configure Unified Single Machine Blueprints for Cross-Region Deployment in Region B

To provision blueprints from a specific vRealize Automation deployment to multiple regions, you define the additional regions in vRealize Automation, and associate the blueprints with those locations.

Procedure

1 Add Data Center Locations to the Compute Resource Menu

You can configure new data center locations and resources in the Compute Resource menu of the vRealize Automation deployment selection screen, allowing you to more easily select new compute resources for deployment. To add a new location to the Compute Resource menu, you edit an XML file on the vRealize Automation server.

2 Associate Compute Resources with a Location in Region B

Each data center location has its own compute resources, which you associate with that site for its dedicated use.

3 Add a Property Group and a Property Definition for Data Center Location in Region B

Property definitions let you more easily control which location to deploy a blueprint, and based upon that choice, which storage and network resources to use with that blueprint.

4 Create a Reservation Policy for the Unified Blueprint in Region B

When tenant administrators and business group managers create a blueprint, the option to add a reservation policy become available. To add a reservation policy to an existing blueprint, edit the blueprint.

5 Specify Reservation Information for the Unified Blueprint in Region B

Each reservation is configured for a specific business group to grant them access to request specific physical machines.

6 Create a Service Catalog for the Unified Blueprint in Region B

The service catalog provides a common interface for consumers of IT services to request and manage the services and resources they need. Users can browse the catalog to request services, track their requests, and manage their provisioned service items.

7 Create an Entitlement for the Unified Blueprint Catalog in Region B

Entitle all blueprints in the Unified Blueprint Catalog to the Production business group. Entitlements determine which users and groups can request specific catalog items or perform specific actions. Entitlements are specific to a business group, and allow users in different business groups to access the blueprint catalog.

8 Create Unified Single Machine Blueprints in Region B

A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings. Create three blueprints from which to clone the virtual machine for your environment using pre-configured resources on the vCenter Server compute cluster in both Region A and Region B. Tenants use these blueprints to automatically provision virtual machines.

9 Test the Cross-Region Deployment of the Single Machine Blueprints in Region B

The data center environment is now ready for the multi-site deployment of virtual machines using vRealize Automation. Test your environment and confirm the successful provisioning of virtual machines using the blueprints you created to both Region A and Region B.

Add Data Center Locations to the Compute Resource Menu

You can configure new data center locations and resources in the Compute Resource menu of the vRealize Automation deployment selection screen, allowing you to more easily select new compute resources for deployment. To add a new location to the Compute Resource menu, you edit an XML file on the vRealize Automation server.

Perform this procedure for both IaaS Web server virtual machines: `vra01iws01a`.rainpole.local and `vra01iws01b`.rainpole.local.

Procedure

1. Log in to 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.

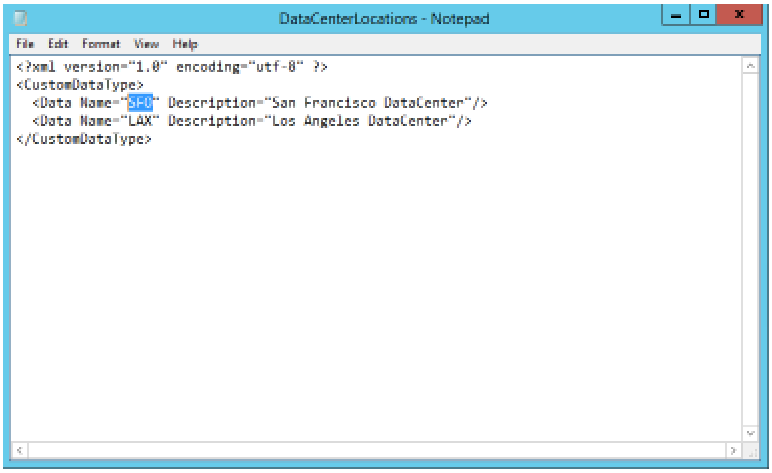
Setting	Value
User name	administrator@vsphere.local
Password	*vcenter_admin_password*

2. Open a VM console to the IaaS Web server virtual machine **`vra01iws01a.rainpole.local`**, and log in using administrator credentials.

    a. Open the file `C:\Program Files (x86)\VMware\VCAC\Server\Website\XmlData\DataCenterLocations.xml` in a text editor.

    b. Update the `Data Name` and `Description` attributes to use the following settings.

Data Name	Description
SFO	San Francisco DataCenter
LAX	Los Angeles DataCenter



```
<?xml version="1.0" encoding="utf-8" ?>
<CustomDataType>
  <Data Name="SFO" Description="San Francisco DataCenter"/>
  <Data Name="LAX" Description="Los Angeles DataCenter"/>
</CustomDataType>
```

3 Save and close the file.

4 Restart the IaaS Web server virtual machine `vra01iws01a`.rainpole.local.

Wait until the virtual machine restarts and is successfully running.

5 Repeat this procedure for the IaaS web server virtual machine `vra01iws01b`.rainpole.local.

Associate Compute Resources with a Location in Region B

Each data center location has its own compute resources, which you associate with that site for its dedicated use.

Repeat this procedure twice, once for each vCenter Server compute cluster and region.

Location	vCenter Server Compute Cluster
SFO	sfo01-w01-comp01
LAX	lax01-w01-comp01

Procedure

1 Log in to the vRealize Automation Rainpole portal.

  a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

  b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Select **Infrastructure > Compute Resources > Compute Resources**.

3 Using the mouse pointer, point to the compute resource **sfo01-w01-comp01** and click **Edit**.

4 Select the **SFO** data center location from the **Locations** drop-down menu.

This will be the data center location for the **sfo01-w01-comp01** compute cluster.

5 Click **OK**.

6 Repeat this to set data center location for **lax01-w01-comp01** compute cluster.

Add a Property Group and a Property Definition for Data Center Location in Region B

Property definitions let you more easily control which location to deploy a blueprint, and based upon that choice, which storage and network resources to use with that blueprint.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Select **Administration > Property Dictionary > Property Definitions**.

3 Click **New** to create a property definition.

   a Enter `Vrm.DataCenter.Location` in the **Name** text box.

   Note The property definition name is case sensitive, and must exactly match the property name used in the blueprint or build profile.

   b Enter `Select a Region` in the **Label** text box.

   c In the **Visibility** section, select the **All tenants** radio button and specify to which tenant the property is available.

   d (Optional) Enter a property description in the **Description** text box.

   Describe the intent of the property and any information that might help the consumer best use the property.

   e Leave default setting for **Display order**.

   f Select **String** from the **Data type** drop-down menu.

   g Select **Yes** from the **Required** drop-down menu.

   h Select **Dropdown** from the **Display as** drop-down menu.

   i Select **Static list** radio button for **Values**.

   j Deselect **Enable custom value entry**.

   k Click **New** in the **Static list** area and enter a property name and value from the following table.

Name	Value
San Francisco	SFO
Los Angeles	LAX

   l Click **OK** to save both predefined values.

   m Click **OK** to save the property definition.

   The property is created and available on the **Property Definitions** page.

4 Select **Administration > Property Dictionary > Property Groups**. Click **New**.

5 Enter `Select Location` in the **Name** text box.

6 If you enter the **Name** value first, the **ID** text box is populated with the same value.

7 In the **Visibility** section, select the **All tenants** radio button to specify with which tenant the property is to be available.

8 (Optional) Enter a description of the property group.

9 Add a property to the group by using the **Properties** box.

   a Click **New**.

   b Select **Vrm.DataCenter.Location** as the property name.

   c Deselect the **Encrypted** check box.

   d Select the **Show in Request** check box.

   e Click **OK** to add the property to the group.

10 Click **OK** to save the property group.

Create a Reservation Policy for the Unified Blueprint in Region B

When tenant administrators and business group managers create a blueprint, the option to add a reservation policy become available. To add a reservation policy to an existing blueprint, edit the blueprint.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > Reservations > Reservation Polices**.

   a Click **New**.

   b Type `UnifiedBlueprint-Policy` in the **Name** text box.

   c Select **Reservation Policy** from the **Type** drop-down menu.

   d Type **`Reservation policy for Unified Blueprint`** in the **Description** text box.

   e Click **OK**.

Specify Reservation Information for the Unified Blueprint in Region B

Each reservation is configured for a specific business group to grant them access to request specific physical machines.

Before members of a business group can request machines, fabric administrators must allocate resources for them by creating a reservation. Each reservation is configured for a specific business group, and grants access to request machines on a specified compute resource.

Repeat this procedure twice to create reservations on both of the Region A and Region B Compute vCenter Clusters for the Production business group.

Region	Business Group	Reservation Name	Reservation Policy	Compute Resource
Region A	Production	SFO01-Comp01-Prod-UnifiedBlueprint	UnifiedBlueprint-Policy	sfo01-w01-comp01(sfo01w01vc01.sfo01.rainpole.local)
Region B	Production	LAX01-Comp01-Prod-UnifiedBlueprint	UnifiedBlueprint-Policy	lax01-w01-comp01(lax01w01vc01.lax01.rainpole.local)

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > Reservations > Reservations** and click **New > vSphere (vCenter)**.

3 On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values.

Setting	Production Business Group Value
Name	SFO01-Comp01-Prod-UnifiedBlueprint
Tenant	rainpole
Business Group	Production
Reservation Policy	UnifiedBlueprint-Policy
Priority	100
Enable This Reservation	Selected

4 On the **New Reservation - vSphere** page, click the **Resources** tab.

   a Select **sfo01-w01-comp01(sfo01w01vc01.sfo01.rainpole.local)** from the **Compute Resource** drop-down menu.

   b Enter `200` in the **This Reservation** column of the **Memory (GB)** table.

   c In the **Storage (GB)** table, select your primary datastore, for example, **sfo01-w01-vsan01,** enter `2000` in the **This Reservation Reserved** text box, enter `1` in the **Priority** text box, and click **OK**.

   d Select **sfo01-w01rp-user-vm** from the **Resource Pool** drop-down menu.

5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.

6 On the **Network** tab, select the network path check boxes listed in the table below from the **Network Paths** list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.

   Production Business Group

Production Network Path	Production Group Network Profile
vxw-dvs-xxxxx-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxw-dvs-xxxxx-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxw-dvs-xxxxx-Production-App-VXLAN	Ext-Net-Profile-Production-App

7 Click **OK** to save the reservation.

Create a Service Catalog for the Unified Blueprint in Region B

The service catalog provides a common interface for consumers of IT services to request and manage the services and resources they need. Users can browse the catalog to request services, track their requests, and manage their provisioned service items.

After the service catalog is created, business group managers can create entitlements for services, catalog items, and resource actions to groups of users. The entitlement allows members of a particular business group, for example, the Production business group, to use the blueprint. Without an entitlement, users cannot use the blueprint.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Click the **Administration** tab, and select **Catalog Management > Services** .

3 Click **New**.

   a In the **New Service** dialog box type `Unified Single Machine Catalog` in the **Name** text box.

   b Select **Active** from the **Status** drop-down menu.

   c Click **OK**.

Create an Entitlement for the Unified Blueprint Catalog in Region B

Entitle all blueprints in the Unified Blueprint Catalog to the Production business group. Entitlements determine which users and groups can request specific catalog items or perform specific actions. Entitlements are specific to a business group, and allow users in different business groups to access the blueprint catalog.

Perform this procedure to associate the Unified Blueprint Catalog with the Prod-SingleVM-Entitlement entitlement.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Associate the **Unified Blueprint Catalog** with the **Prod-SingleVM-Entitlement entitlement** that you created earlier.

   a Select **Administration** > **Catalog Management** > **Entitlements**.

   b Click **Prod-SingleVM-Entitlement**.

   The **Edit Entitlement** pane appears.

   c Select the **Items & Approvals** tab.

   d Navigate to **Entitled Services** and click the **Add** icon.

   e Check the box next to **Unified Single Machine Catalog** and click **OK**.

   f Click **Finish** to save your changes.

Create Unified Single Machine Blueprints in Region B

A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings. Create three blueprints from which to clone the virtual machine for your environment using pre-configured resources on the vCenter Server compute cluster in both Region A and Region B. Tenants use these blueprints to automatically provision virtual machines.

Repeat this procedure to create three Unified Single Machine blueprints, one for each blueprint name listed in the following table.

Blueprint Name	VM Template	Reservation Policy	Customization Specification	Service Catalog
Windows Server 2012 R2 - Unified Prod	windows-2012r2-64 (sfo01w01vc01.sfo01.rainpole.local)	UnifiedBlueprint-Policy	os-windows-joindomain-custom-spec	Unified Single Machine Catalog
Windows Server 2012 R2 With SQL2012 - Unified Prod	windows-2012r2-64-sql2012(sfo01w01vc01.sfo01.rainpole.local)	UnifiedBlueprint-Policy	os-windows-joindomain-custom-spec	Unified Single Machine Catalog
Redhat Enterprise Linux 6 - Unified Prod	redhat6-enterprise-64(sfo01w01vc01.sfo01.rainpole.local)	UnifiedBlueprint-Policy	os-linux-custom-spec	Unified Single Machine Catalog

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Design > Blueprints**.

3 Click **New**.

4 In the **New Blueprint** dialog box, configure the following settings on the **General** tab.

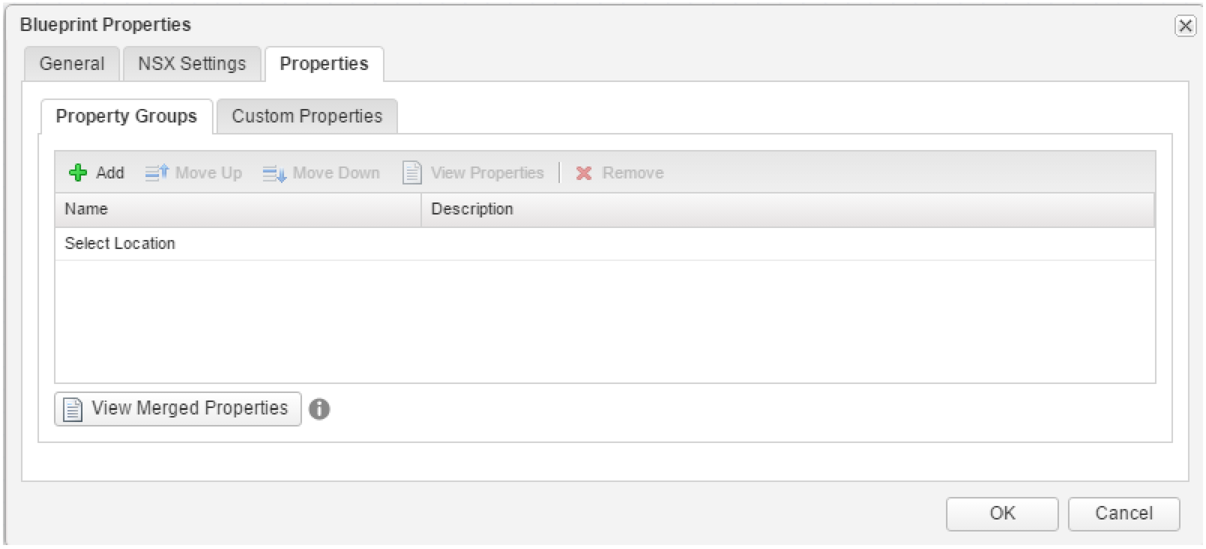
Setting	Value
Name	Windows Server 2012 R2 - Unified
Archive (days)	15
Deployment limit	Default setting (blank)

Setting	Value
Minimum	30
Maximum	270

5 Click the **Properties** tab.

a Click **Add** on the **Property Groups** tab.

b Select the property group **Select Location** and click **OK**.



Blueprint Properties

Name	Description
Select Location	

6 Click **OK**.

7 Select and drag the **vSphere Machine** icon to the Design Canvas.

8 Click the **General** tab, configure the following settings, and click **Save**.

Setting	Value
ID	Default setting (vSphere_vCenter_Machine_1)
Reservation Policy	UnifiedBlueprint-Policy
Machine Prefix	Use group default
Minimum	Default setting
Maximum	Default setting

9 Click the **Build Information** tab, configure the following settings, and click **Save**.

Setting	Value
Blueprint Type	Server
Action	Clone
Provisioning Workflow	CloneWorkflow
Clone from	windows-2012r2-64
Customization spec	os-windows-joindomain-custom-spec

10 Click the **Machine Resources** tab, configure the following settings, and click **Save**.

Setting	Minimum	Maximum
CPU	1	4
Memory (MB):	4096	16384
Storage	50	60

11 Click the **Network** tab.

a Select **Network & Security** in the **Categories** section to display the list of available network and security components.

b Select the **Existing Network** component and drag it onto the design canvas.

c Click in the **Existing network** text box and select the **Ext-Net-Profile-Production-Web** network profile.

Blueprint Name	Existing Network
Windows Server 2012 R2 - Unified	Ext-Net-Profile-Production-Web
Windows Server 2012 R2 with SQL2012 - Unified	Ext-Net-Profile-Production-DB
Redhat Enterprise Linux 6 - Unified	Ext-Net-Profile-Production-App

d Click **Save**.

e Select **vSphere_Machine** properties from the design canvas.

f Select the **Network** tab, click New, and configure the following settings. Click **OK**.

Setting	Value
Network	ExtNetProfileProductionWeb
Assignment Type	Static IP
Address	Default setting (blank)

12 Click **Finish** to save the blueprint.

13 Select the blueprint **Windows Server 2012 R2 - Unified** and click **Publish**.

14 Navigate to **Administration > Catalog Management > Catalog Items** and add the blueprint to the **Unified Single Machine Catalog**.

a In the **Catalog Items** list, click the blueprint labelled **Windows Server 2012 R2 - Unified**.

b In the **Configure Catalog Items** dialog box, set **Service** to **Unified Single Machine Catalog**, and click **OK**.

Test the Cross-Region Deployment of the Single Machine Blueprints in Region B

The data center environment is now ready for the multi-site deployment of virtual machines using vRealize Automation. Test your environment and confirm the successful provisioning of virtual machines using the blueprints you created to both Region A and Region B.

Repeat this procedure twice to provision virtual machines in both the Region A and Region B Compute vCenter Server instances.

Region	Compute vCenter Server
San Francisco	sfo01w01vc01.sfo01.rainpole.local
Los Angeles	lax01w01vc01.lax01.rainpole.local

Procedure

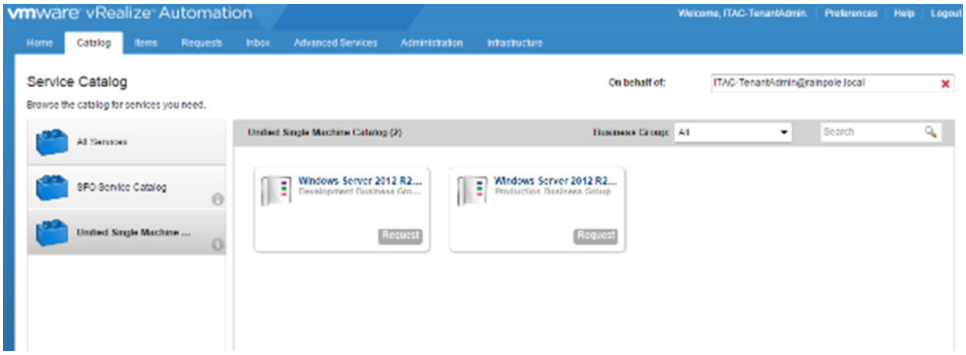
1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

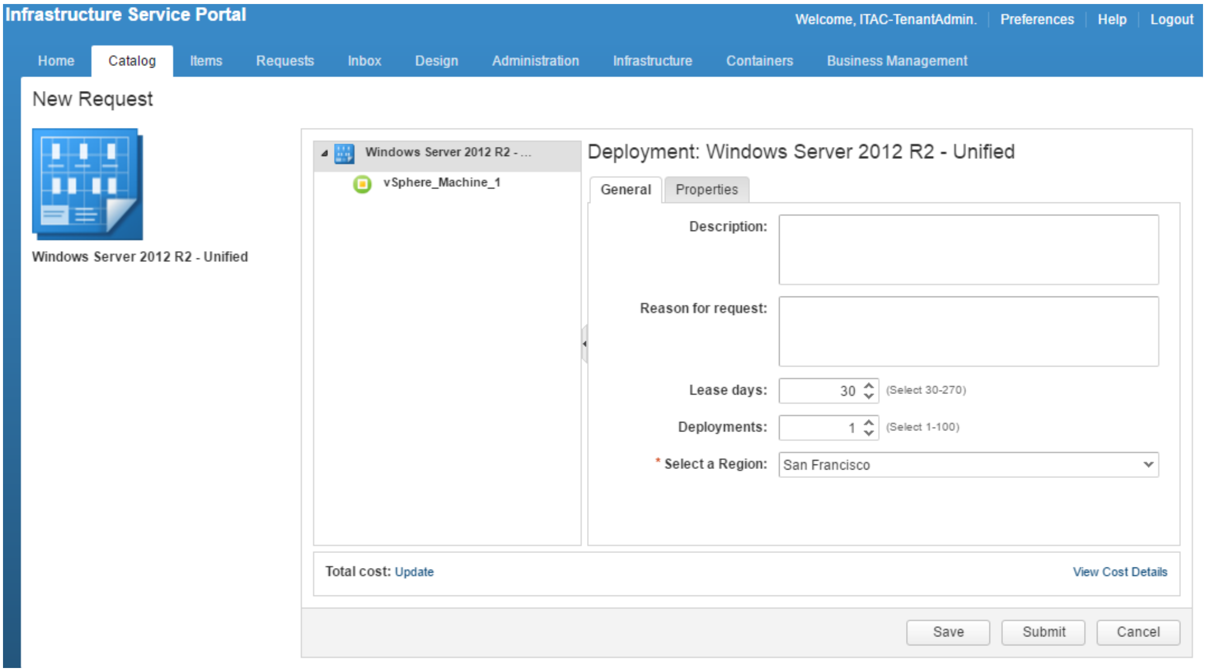
2 Select the **Catalog** tab, and click **Unified Single Machine Catalog** from the catalog of available services.


vmware vRealize Automation
Welcome, ITAC-TenantAdmin
Preferences
Help
Logout
Home
Catalog
Items
Requests
Inbox
Advanced Services
Administration
Infrastructure
Service Catalog
Browse the catalog for services you need.
On behalf of:
ITAC-TenantAdmin@rainpole.local
All Services
SFO Service Catalog
Unified Single Machine ...
Unified Single Machine Catalog (2)
Business Group:
All
Search
Windows Server 2012 R2...
Development Business Gro...
Request
Windows Server 2012 R2...
Production Business Group
Request

3 Click the **Request** button for the Windows Server 2012 R2 - Unified blueprint.

   The **New Request** window appears.

4 Select **San Francisco** from the **Select a Region** drop-down menu, and click **Submit**.



Infrastructure Service Portal

Welcome, ITAC-TenantAdmin. | Preferences | Help | Logout

Home | Catalog | Items | Requests | Inbox | Design | Administration | Infrastructure | Containers | Business Management

New Request

Windows Server 2012 R2 - Unified

Windows Server 2012 R2 - ...

vSphere_Machine_1

Deployment: Windows Server 2012 R2 - Unified

General | Properties

Description:

Reason for request:

Lease days: 30 (Select 30-270)

Deployments: 1 (Select 1-100)

* Select a Region: San Francisco

Total cost: Update

View Cost Details

Save | Submit | Cancel

5 Verify the request finishes successfully.

a Select the **Requests** tab.

b Select the request you submitted and wait several minutes for the request to complete.

Click the **Refresh** icon every few minutes until a `Successful` message appears under **Status**.

c Click **View Details**.

d Under **Status Details**, verify that the virtual machine successfully provisioned.

6 Verify the virtual machine provisions in the Region A vCenter Server compute cluster.

a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.

b Log in as the vCenter Server administrator using the following credentials.

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

c Select **Home > VMs and Templates**.

d In the **Navigator** panel, expand the vCenter Server compute cluster **sfo01w01vc01.sfo01.rainpole.local > sfo01-w01dc > VRM**, and verify the existence of the virtual machine.

7 Repeat this procedure for Region B.

   a Provision virtual machines to the Region B vCenter Server compute cluster.

   b Verify the request finishes successfully and that the virtual machine is provisioned in the Region B vCenter Server compute cluster.

You have successfully performed a cross-region deployment of vRealize Automation single machine blueprints, provisioning virtual machines in both Region A and Region B.

Operations Management Configuration for Cloud Management in Region B

After you install the components of the Cloud Management Platform in Region B, enable their integration with the operations management layer. You can monitor and receive alerts and logs about the platform to a central location by using vRealize Operations Manager and vRealize Log Insight.

Procedure

1 Configure Service Account Privileges for Integration between vRealize Operations Manager and vRealize Automation in Region B

   Configure the rights of the service accounts that vRealize Automation and vRealize Operations Manager use to communicate with each other.

2 Connect vRealize Log Insight to vRealize Automation in Region B

   Connect vRealize Log to vRealize Automation to receive log information from the components of vRealize Automation in Region B in the vRealize Log Insight UI.

Configure Service Account Privileges for Integration between vRealize Operations Manager and vRealize Automation in Region B

Configure the rights of the service accounts that vRealize Automation and vRealize Operations Manager use to communicate with each other.

You use these service accounts in the following cases:

- When vRealize Operations Manager collects statistics about the tenant workloads in vRealize Automation in Region B.
- When vRealize Automation collects metrics to identify tenant workloads for reclamation in Region B. Such workloads have low use of CPU, memory use, or disk space.

Configure User Privileges on vRealize Automation for Integration with vRealize Operations Manager in Region B

Assign the permissions that are required to access monitoring data from vRealize Automation in vRealize Operations Manager to the svc-vrops-vra operations service account.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > Endpoints > Fabric Groups** to assign the fabric administrator role to the svc-vrops-vra service account.

   a On the **Fabric Groups** page, click **LAX Fabric Group**.

   b On the **Edit Fabric Group** page, enter `svc-vrops-vra` in **Fabric administrators** search text box and click the **Search** icon.

   c Click **svc-vrops-vra@rainpole.local** in the search result list to assign the fabric administrator role to the account, and click **OK**.

Configure User Privileges on vRealize Operations Manager for Tenant Workload Reclamation in Region B

Configure read-only privileges for the svc-vra-vrops@rainpole.local service account on vRealize Operations Manager. You configure these privileges so that vRealize Automation can pull metrics from vRealize Operations Manager for reclamation of tenant workloads in Region B.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to `https://vrops01svr01.rainpole.local`.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, expand **Access**, and click **Access Control**.

4 On the **Access Control** page, click the **User Accounts** tab.

5 Select the **svc-vra-vrops@rainpole.local** service account, and click **Edit**.

6 On the **Edit Permissions** page, to assign the `ReadOnly` role to the svc-vra-vrops@rainpole.local service account, click the **Objects** tab, configure the following settings and click **Finish.**

Setting	Value
Select Role	ReadOnly
Assign this role to the user	Selected
Select Object	vCenter Adapter > vCenter Adapter - lax01w01vc01

Connect vRealize Log Insight to vRealize Automation in Region B

Connect vRealize Log to vRealize Automation to receive log information from the components of vRealize Automation in Region B in the vRealize Log Insight UI.

Procedure

1 Install the vRealize Log Insight Content Pack for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server in Region B

Install the content packs for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server to add the dashboards for viewing log information in vRealize Log Insight.

2 Install Log Insight Windows Agents on the vRealize Automation Proxy Agents in Region B

Install the vRealize Log Insight agent to collect and forward events to vRealize Log Insight in Region B on the Windows virtual machines for the vSphere proxy agents.

3 Create Log Insight Agent Groups for vRealize Automation Windows Agents in Region B

Create agent groups for the vRealize Automation IaaS components and for Microsoft SQL Server. By using the agent groups you can configure Log Insight Windows Agents centrally from the vRealize Log Insight user interface.

4 Configure the vRealize Log Insight Linux Agent on vRealize Business in Region B

vRealize Log Insight Agent comes pre-installed on the vRealize Business virtual appliances. Configure the `liagent.ini` configuration file on each virtual appliance.

5 Add the Cloud Management Components to the Agent Group for Management Virtual Appliances in Region B

After you deploy the Cloud Management Platform and configure the Log Agent agents on its components, add the virtual appliance of the platform to the agent group for the management virtual appliances. You use this agent group to centrally configure collection of logs from the operating system of the appliances.

Install the vRealize Log Insight Content Pack for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server in Region B

Install the content packs for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server to add the dashboards for viewing log information in vRealize Log Insight.

You install the following content packs:

- VMware - vRA 7
- VMware - Orchestrator 7.0.1+
- Microsoft - SQL Server

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon ☰ and select **Content Packs**.

3 Under **Content Pack Marketplace**, select **Marketplace**.

4 In the list of content packs, locate the **VMware - vRA 7** content pack and click its icon.

5 In the **Install Content Pack** dialog box, click **Install**.

6 Repeat the procedure to install the VMware - Orchestrator 7.0.1+ and Microsoft - SQL Server content pack

After the installation is complete, the VMware - vRA 7, VMware - Orchestrator and Microsoft - SQL Server content packs appear in the **Installed Content Packs** list on the left.

Install Log Insight Windows Agents on the vRealize Automation Proxy Agents in Region B

Install the vRealize Log Insight agent to collect and forward events to vRealize Log Insight in Region B on the Windows virtual machines for the vSphere proxy agents.

Procedure

1 Log in to the Windows virtual machines of the vRealize Automation component.

   a Open a Remote Desktop Protocol (RDP) connection to each of the following vRealize Automation virtual machines.

vRealize Automation Component	Host Name/VM Name
vSphere Proxy Agent	lax01ias01a.lax01.rainpole.local
vSphere Proxy Agent	lax01ias01b.lax01.rainpole.local

   b Log in using the following credentials.

Setting	Value
User name	Rainpole\svc-vra
Password	*svc-vra-user-password*

2 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

3 Click the configuration drop-down menu icon ☰ and select **Administration**.

4 Under **Management**, click **Agents**.

5 On the **Agents** page, click the **Download Log Insight Agent Version** link.

6 In the **Download Log Insight Agent Version** dialog box, click **Windows MSI (32-bit/64-bit)** and save the `.msi` file on the vRealize Automation virtual machine.

7 Open an administrative command prompt window, and navigate to the directory to where you saved the `.msi` file.

8 Run the the following command to install the vRealize Log Insight agent with custom values.

```
VMware-Log-Insight-Agent-4.5.0-5626690_192.168.32.10.msi SERVERPORT=9000 AUTOUPDATE=yes
LIAGENT_SSL=no
```

9 In the **VMware vRealize Log Insight Agent Setup** wizard, accept the license agreement and click **Next**.

10 With the Log Insight host name lax01vrli01.lax01.rainpole.local selected in the **Host** text box, click **Install**.

11 After the installation is complete, click **Finish**.

12 Repeat the steps for the other vRealize Automation virtual machines.

All VMware vRA 7 dashboards become available on the home page of vRealize Log Insight.

Create Log Insight Agent Groups for vRealize Automation Windows Agents in Region B

Create agent groups for the vRealize Automation IaaS components and for Microsoft SQL Server. By using the agent groups you can configure Log Insight Windows Agents centrally from the vRealize Log Insight user interface.

Procedure

1 Log in to the vRealize Log Insight user interface.

  a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

  b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 Click the configuration drop-down menu icon ☰ and select **Administration**.

3 Under **Management**, click **Agents**.

4 Create an agent group for the IaaS components of vRealize Automation.

  a From the drop-down at the top, select **vRealize Automation 7 - Windows** from the **Available Templates** section.

  b Click **Copy Template**.

  c In the **Copy Agent Group** dialog box, enter **`vRA – Windows Agent Group`** in the name text box and click **Copy**.

  d In the agent filter fields, use the following selections.

  Use Enter to separate the host name values.

Filter	Operator	Values
Hostname	matches	lax01ias01a.lax01.rainpole.local lax01ias01b.lax01.rainpole.local

  e Under **Agent Configuration**, click **Edit**

  f In the `[filelog|vra-agent-vcenter-70x]` section, locate `directory=C:\Program Files (x86)\VMware\vCAC\Agents\vCenter\logs\` and change it to **`directory=C:\Program Files (x86)\VMware\vCAC\Agents\VSPHERE-AGENT-51\logs`**

  g Click **Refresh** and verify that all the agents that are listed in the filter appear in the Agents list.

  h Click **Save New Group** at the bottom of the page.

Configure the vRealize Log Insight Linux Agent on vRealize Business in Region B

vRealize Log Insight Agent comes pre-installed on the vRealize Business virtual appliances. Configure the `liagent.ini` configuration file on each virtual appliance.

Procedure

1 Enable Secure Shell (SSH) on the vRealize Business data collector appliance.

   a Open a Web browser and go to the following URLs,

vRealize Business node	Virtual Appliance Management Interface URL
vRealzie Business Data Collector	https://lax01vrbc01.lax01.rainpole.local:5480

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_collector_root_password*

   The appliance management interface of the appliance opens.

   c Click the **Administration** tab and click **Administration**.

   d Under the **Actions** section, click **Toggle SSH setting**.

   e Verify that the **SSH service status** reports **`Enabled`**.

2 Configure the Log Insight agent on the vRealize Business appliance.

   a Open an SSH connection to the vRealize Business appliance using the following settings.

Setting	Value
Hostname	lax01vrbc01.lax01.rainpole.local
User name	root
Password	*vrb_server_appliance_root_password*

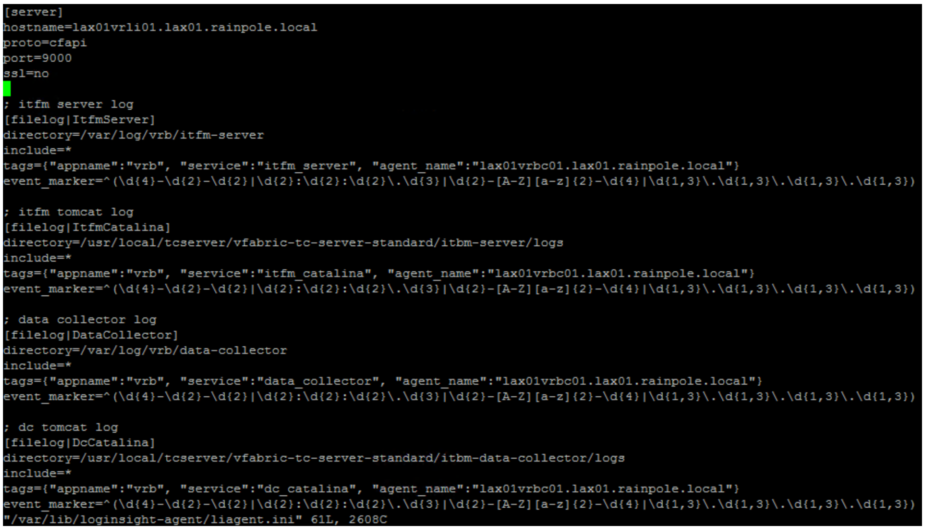
   b Edit the `liagent.ini` file using a text editor such as `vi`.

   ```
   vi /var/lib/loginsight-agent/liagent.ini
   ```

   c Add the following information under `[server]` section.

   ```
   [server]
   hostname=lax01vrli01.lax01.rainpole.local
   proto = cfapi
   port = 9000
   ssl = no
   ```

d Replace all instances of `FQDN_localhost` parameter located after `agent_name` with **`lax01vrbc01.lax01.rainpole.local`**.



```
[server]
hostname=lax01vrli01.lax01.rainpole.local
proto=cfapi
port=9000
ssl=no

; itfm server log
[filelog|ItfmServer]
directory=/var/log/vrb/itfm-server
include=*
tags={"appname":"vrb", "service":"itfm_server", "agent_name":"lax01vrbc01.lax01.rainpole.local"}
event_marker=^(\d{4}-\d{2}-\d{2}|\d{2}:\d{2}:\d{2}\.\d{3}|\d{2}-[A-Z][a-z]{2}-\d{4}|\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})

; itfm tomcat log
[filelog|ItfmCatalina]
directory=/usr/local/tcserver/vfabric-tc-server-standard/itbm-server/logs
include=*
tags={"appname":"vrb", "service":"itfm_catalina", "agent_name":"lax01vrbc01.lax01.rainpole.local"}
event_marker=^(\d{4}-\d{2}-\d{2}|\d{2}:\d{2}:\d{2}\.\d{3}|\d{2}-[A-Z][a-z]{2}-\d{4}|\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})

; data collector log
[filelog|DataCollector]
directory=/var/log/vrb/data-collector
include=*
tags={"appname":"vrb", "service":"data_collector", "agent_name":"lax01vrbc01.lax01.rainpole.local"}
event_marker=^(\d{4}-\d{2}-\d{2}|\d{2}:\d{2}:\d{2}\.\d{3}|\d{2}-[A-Z][a-z]{2}-\d{4}|\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})

; dc tomcat log
[filelog|DcCatalina]
directory=/usr/local/tcserver/vfabric-tc-server-standard/itbm-data-collector/logs
include=*
tags={"appname":"vrb", "service":"dc_catalina", "agent_name":"lax01vrbc01.lax01.rainpole.local"}
event_marker=^(\d{4}-\d{2}-\d{2}|\d{2}:\d{2}:\d{2}\.\d{3}|\d{2}-[A-Z][a-z]{2}-\d{4}|\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})
"/var/lib/loginsight-agent/liagent.ini" 61L, 2608C
```

e Press ESC and enter `:wq!` to save the file.

f Start the Log Insight agent.

```
/etc/init.d/liagentd start
```

g Verify that the Log Insight agent is running.

```
/etc/init.d/liagentd status
```

h Turn on auto-run by default for the Log Insight agent.

```
chkconfig liagentd on
```

3 In the vRealize Log Insight Web interface, verify that the Log Insight agent is working.

a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

c Click the configuration drop-down menu icon ☰ and select **Administration**.

d Under **Management**, click **Agents**.

e Verify that lax01vrbc01.lax01.rainpole.local appear on the page.

Add the Cloud Management Components to the Agent Group for Management Virtual Appliances in Region B

After you deploy the Cloud Management Platform and configure the Log Agent agents on its components, add the virtual appliance of the platform to the agent group for the management virtual appliances. You use this agent group to centrally configure collection of logs from the operating system of the appliances.

Procedure

1 In the **All Agents** drop-down menu, select **VA - Linux Agent Group** from the **Active Groupes** section.

2 In the agent filter fields, add the host name of the vRealize Business data collector appliance to the list of management virtual appliances in the region pressing Enter after each host name.

Filter	Operator	Values
Hostname	matches	■ lax01vropsc01a.lax01.rainpole.local ■ lax01vropsc01b.lax01.rainpole.local ■ **lax01vrbc01.lax01.rainpole.local**

3 Click **Refresh** and verify that all the agents listed in the filter appear in the **Agents** list.

4 Click **Save New Group** at the bottom of the page.

Region B Business Continuity Implementation

5

The business continuity layer provides continuous operation of the management components of the SDDC if hardware failure or disaster occurs. Install Site Recovery Manager in Region A and Region B, and pair the two instances to provide disaster recovery support in the two regions.

This chapter includes the following topics:

- Deploy and Configure Site Recovery Manager
- Deploy and Configure vSphere Replication
- Configure Operations Management for the Business Continuity Components

Deploy and Configure Site Recovery Manager

You deploy Site Recovery to enable fail over of management applications from Region A to Region B in the cases of disaster or planned migration.

Procedure

1 Prerequisites for Installing Site Recovery Manager

Before you install two Site Recovery Manager instances, one in the protected site (Region A), and one in the recovery site (Region B), in each region you must provide a Windows Server 2012 R2 virtual machine that has a certain configuration.

2 Configure User Privileges in vSphere for Integration with Site Recovery Manager

Assign vCenter Single Sign-On administrative global permissions to the operations service account svc-srm so that you can manage, pair and perform orchestrated disaster recovery operations between the management vCenter Server instances by using Site Recovery Manager.

3 Install Site Recovery Manager in Region A

Install the first Site Recovery Manager instance on the dedicated virtual machine in Region A.

4 Install Site Recovery Manager in Region B

Install the second Site Recovery Manager instance on the dedicated virtual machine in Region B.

5 Configure the Site Recovery Manager Instances

After both Site Recovery Manager Instances are deployed, assign the appropriate licensing. Using the svc-srm service account, pair the Region A and Region B instances and configure the mappings between them to support disaster recovery.

Prerequisites for Installing Site Recovery Manager

Before you install two Site Recovery Manager instances, one in the protected site (Region A), and one in the recovery site (Region B), in each region you must provide a Windows Server 2012 R2 virtual machine that has a certain configuration.

Software Requirements

Before you install Site Recovery Manager, make sure that you have the following virtual machines and environment configuration available in your environment.

Table 5-1. Software and Configuration Requirements for Site Recovery Manager VMs

Component	Requirement
Operating System	Windows Server 2012 R2
Active Directory	Join each VM to the domain in Region A or Region B (sfo01.rainpole.local or lax01.rainpole.local).
Network interface	Connect the VMs to the management port group on the distributed switch (sfo01-m01-vds01-management and lax01-m01-vds01-management).
Time synchronization	Synchronize both VMs with the NTP servers ntp.sfo01.rainpole.local and ntp.lax01.rainpole.local.
vSphere cluster configuration	Provide a cluster for hosting management application with enabled vSphere DRS and vSphere HA.
Site Recovery Manager installation file	Download Site Recovery Manager installer to both VMs.
Email address of Site Recovery Manager administrators	Get the email addresses of the Site Recovery Manager site administrators.
Certificate Authority	■ Configure the root Active Directory domain controller as a certificate authority for the environment. ■ Download the `CertGenVVD` tool and generate the signed certificate for the analytics cluster. See the *VMware Validated Design Planning and Preparation* documentation.

IP Addresses, Host Names, and Network Configuration

In each region, allocate a static IP address and FQDN for Site Recovery Manager, and map the host name to the IP address.

Table 5-2. Network Configuration of Site Recovery Manager in Region A

Setting	Value
Host name	sfo01m01srm01
Static IPv4 address	172.16.11.124
Subnet mask	255.255.255.0
Default gateway	172.16.11.253
DNS server	172.16.11.5

Table 5-2. Network Configuration of Site Recovery Manager in Region A (Continued)

Setting	Value
FQDN	sfo01m01srm01.sfo01.rainpole.local
Used ports	■ 9086 ■ 5678
NTP servers	■ Configure the VM with the following NTP servers: ■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local ■ Verify that time synchronization is successful

Table 5-3. Network Configuration of Site Recovery Manager in Region B

Setting	Value
Host name	lax01m01srm01
Static IPv4 address	172.17.11.124
Subnet mask	255.255.255.0
Default gateway	172.17.11.253
DNS server	172.17.11.5
FQDN	lax01m01srm01.lax01.rainpole.local
Used ports	■ 9086 ■ 5678
NTP servers	■ Configure the VM with the following NTP servers: ■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local ■ Verify that time synchronization is successful

Configure User Privileges in vSphere for Integration with Site Recovery Manager

Assign vCenter Single Sign-On administrative global permissions to the operations service account svc-srm so that you can manage, pair and perform orchestrated disaster recovery operations between the management vCenter Server instances by using Site Recovery Manager.

Prerequisites

- Verify that the Management Platform Services Controllers for Region A and Region B are connected to the Active Directory domain.
- Verify that the users and groups from the rainpole.local domain are available in Region A and Region B.

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.

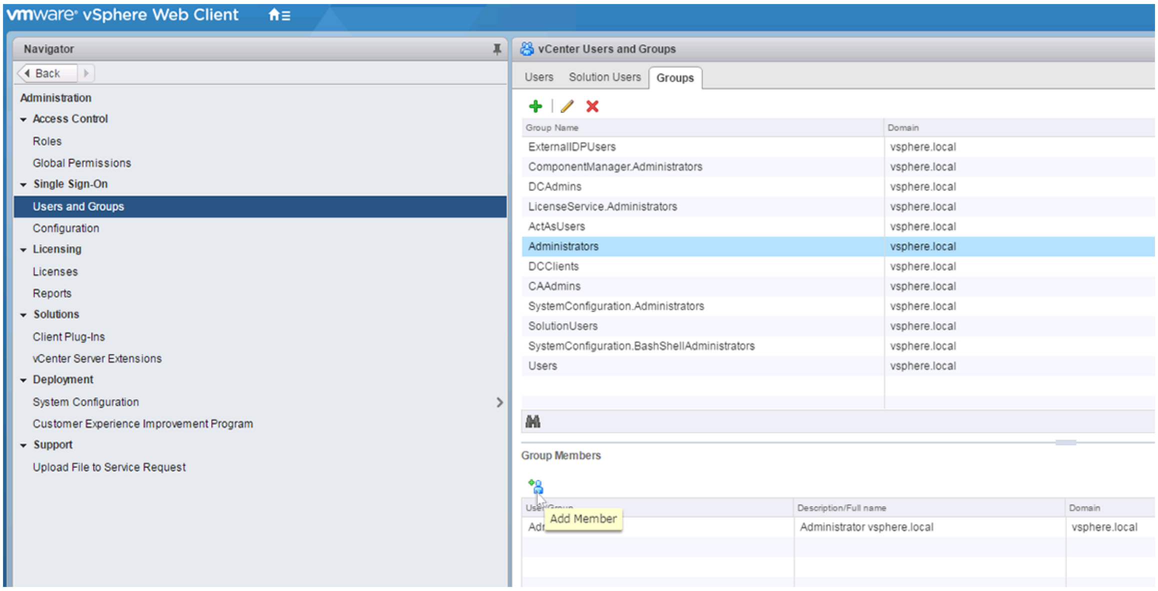
Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Administration**.

3 Add the service account svc-srm@rainpole.local to the Single Sign-On administrators group.

  a In the vSphere Web Client, select **Administration** from the **Home** menu and click **Users and Groups** under **Single Sign-On**.

  b On the **Groups** tab under **vCenter Users and Groups** page, click the **Administrators** group and click the **Add Member** icon under **Group Members**.

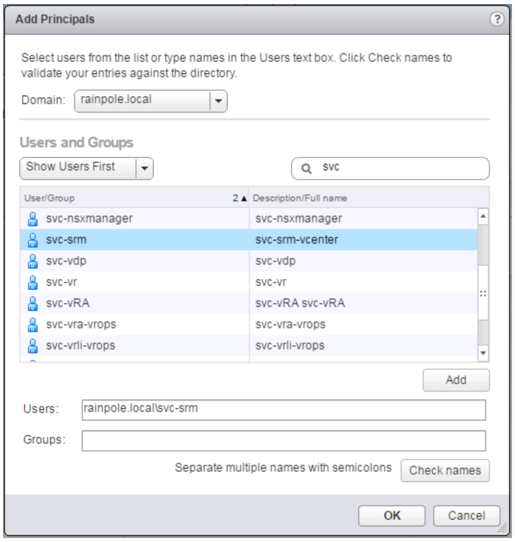


Group Name	Domain
ExternalIDPUsers	vsphere.local
ComponentManager.Administrators	vsphere.local
DCAdmins	vsphere.local
LicenseService.Administrators	vsphere.local
ActAsUsers	vsphere.local
Administrators	vsphere.local
DCClients	vsphere.local
CAAdmins	vsphere.local
SystemConfiguration.Administrators	vsphere.local
SolutionUsers	vsphere.local
SystemConfiguration.BashShellAdministrators	vsphere.local
Users	vsphere.local

User/Group	Description/Full name	Domain
Adı	Administrator vsphere.local	vsphere.local

c In the **Add Principals** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.

d From the **User/Group** list, select the **svc-srm** user, click **Add**, and click **OK**.



Add Principals

Select users from the list or type names in the Users text box. Click Check names to validate your entries against the directory.

Domain: rainpole.local

Users and Groups

Show Users First

svc

User/Group	Description/Full name
svc-nsxmanager	svc-nsxmanager
svc-srm	svc-srm-vcenter
svc-vdp	svc-vdp
svc-vr	svc-vr
svc-vRA	svc-vRA svc-vRA
svc-vra-vrops	svc-vra-vrops
svc-vrli-vrops	svc-vrli-vrops

Users: rainpole.local\svc-srm

Groups:

Separate multiple names with semicolons

The global vCenter Single Sign-On administrative permissions of the svc-srm account propagate to all other linked vCenter Server instances.

Install Site Recovery Manager in Region A

Install the first Site Recovery Manager instance on the dedicated virtual machine in Region A.

Use the following certificate files to replace the default certificate on Site Recovery Manager:

Site Recovery Manager	Certificate Files
sfo01m01srm01.sfo01.rainpole.local	■ sfo01m01srm01.5.p12 ■ Root64.cer

Procedure

1 Log in to the Site Recovery Manager virtual machine by using a Remote Desktop Protocol (RDP) client.

a Open an RDP connection to the sfo01m01srm01.sfo01.rainpole.local virtual machine.

b Log in using the following credentials.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

2 Install the CA certificates in the Windows trusted root certificate store of the Site Recovery Manager virtual machine.

   a Create a folder on the C drive (`C:\certs`) and copy `sfo01m01srm01.5.p12` and `Root64.cer` to the `C:\certs` folder

   b Double-click the `Root64.cer` file in the `C:\certs` folder to open **Certificate** import dialog box.

   c In the **Certificate** dialog box, select the **Install Certificate** option.

   The **Certificate Import Wizard** appears.

   d Select the **Local Machine** option for **Store Location** and click **Next**.

   e Select **Place all certificates in the following store** option, click **Browse**, select the **Trusted Root Certificate Authorities** store, and click **OK**.

   f On the **Certificate Import Wizard** page, click **Next**.

   g On the **Completing the Certificate Import Wizard** page, click **Finish**.

3 Navigate to the folder where you downloaded the VMware Site Recovery Manager installer, and open the file to start the installation wizard.

4 In the **Select Language** dialog box click **OK**.

5 On the **Welcome** page click **Next**.

6 On the **VMware Patents** page click **Next**.

7 On the **End User License Agreement** page, select the **I agree to the terms in the license agreement** radio button, and click **Next**.

8 On the **Installation Prerequisites** page click **Next**.

9 On the **Destination Folder** page click **Next**.

10 On the **vSphere Platform Services Controller** page, enter the following settings, and click **Next**.

Setting	Value
Address	sfo01psc01.sfo01.rainpole.local
HTTPS Port	443
Username	svc-srm@rainpole.local
Password	*svc-srm_password*

11 If prompted, in the **Platform Services Controller Certificate** dialog box, click **Accept**.

12 On the **VMware vCenter Server** page, select **sfo01m01vc01.sfo01.rainpole.local** from the drop-down menu, and click **Next**.

13 If prompted, in the **vCenter Server Certificate** dialog box, click **Accept**.

14 On the **Site Recovery Manager Extension** page, enter the following settings, and click **Next**.

Setting	Value
Local Site Name	sfo01m01vc01.sfo01.rainpole.local
Administrator E-mail	*srm_admin_sfo_email_address*
Local Host	172.16.11.124
Listener Port	9086

15 On the **Site Recovery Manager Plug-in ID** page, select **Default Site Recovery Manager Plug-in Identifier**, and click **Next**.

16 On the **Certificate Type** page, select the **Use a PKCS#12 certificate file** option and click **Next**.

17 Browse to the `C:\certs` folder, select the `sfo01m01srm01.5.p12` file, and enter the certificate password that you specified when generating the PKCS#12 file.

18 Click **Yes** in the certificate warning dialog box.

19 On the **Database Server Selection** page, select **Use the embedded database server**, and click **Next**.

20 On the **Embedded Database Configuration** page, enter the following settings, and click **Next**.

Setting	Value
Data Source Name	SRM_SITE_SFO01
Database User Name	srm_db_admin
Database Password	*srm_db_admin_sfo_password*
Database Port	5678
Connection Count	5
Max. Connections	20

21 On the **Site Recovery Manager Service Account** page, enter the following credentials, and click **Next**.

Setting	Value
Use Local System account	Deselected
Username	SFO01M01SRM01\Administrator
Password	*sfo01m01srm01_admin_password*

22 On the **Ready to Install the Program** page click **Install**.

23 Click **Finish** to complete the installation.

Install Site Recovery Manager in Region B

Install the second Site Recovery Manager instance on the dedicated virtual machine in Region B.

Use the following certificate files to replace the default certificate on Site Recovery Manager:

Site Recovery Manager	Certificate Files
lax01m01srm01.lax01.rainpole.local	■ lax01m01srm01.5.p12 ■ Root64.cer

Procedure

1 Log in to the Site Recovery Manager virtual machine by using a Remote Desktop Protocol (RDP) client.

  a Open an RDP connection to the lax01m01srm01.lax01.rainpole.local virtual machine.

  b Log in using the following credentials.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

2 Install the CA certificates in the Windows trusted root certificate store of the Site Recovery Manager virtual machine.

  a Create a folder on the C drive (`C:\certs`) and copy `lax01m01srm01.5.p12` and `Root64.cer` to the `C:\certs` folder

  b Double-click the `Root64.cer` file in the `C:\certs` folder to open **Certificate** import dialog box.

  c In the **Certificate** dialog box, select the **Install Certificate** option.

  The **Certificate Import Wizard** appears.

  d Select the **Local Machine** option for **Store Location** and click **Next**.

  e Select **Place all certificates in the following store** option, click **Browse**, select the **Trusted Root Certificate Authorities** store, and click **OK**.

  f On the **Certificate Import Wizard** page, click **Next**.

  g On the **Completing the Certificate Import Wizard** page, click **Finish**.

3 Navigate to the folder where you downloaded the VMware Site Recovery Manager installer, and open the file to start the installation wizard.

4 In the **Select Language** dialog box click **OK**.

5 On the **Welcome** page click **Next**.

6 On the **VMware Patents** page click **Next**.

7 On the **End User License Agreement** page, select the **I agree to the terms in the license agreement** radio button, and click **Next.**

8 On the **Installation Prerequisites** page click **Next**.

9 On the **Destination Folder** page click **Next**.

10 On the **vSphere Platform Services Controller** page, enter the following settings, and click **Next**.

Setting	Value
Address	lax01psc01.lax01.rainpole.local
HTTPS Port	443
Username	svc-srm@rainpole.local
Password	*svc-srm_password*

11 If prompted, in the **Platform Services Controller Certificate** dialog box, click **Accept**.

12 On the **VMware vCenter Server** page, select **lax01m01vc01.lax01.rainpole.local** from the drop-down menu, and click **Next**.

13 If prompted, in the **vCenter Server Certificate** dialog box, click **Accept**.

14 On the **Site Recovery Manager Extension** page, enter the following settings, and click **Next**.

Setting	Value
Local Site Name	lax01m01vc01.lax01.rainpole.local
Administrator E-mail	*srm_admin_lax_email_address*
Local Host	172.17.11.124
Listener Port	9086

15 On the **Site Recovery Manager Plug-in ID** page, select **Default Site Recovery Manager Plug-in Identifier**, and click **Next**.

16 On the **Certificate Type** page, select the **Use a PKCS#12 certificate file** option and click **Next**.

17 Browse to the `C:\certs` folder, select the `lax01m01srm01.5.p12` file, and enter the certificate password that you specified when generating the PKCS#12 file.

18 Click **Yes** in the certificate warning dialog box.

19 On the **Database Server Selection** page, select **Use the embedded database server**, and click **Next**.

20 On the **Embedded Database Configuration** page, enter the following settings, and click **Next**.

Setting	Value
Data Source Name	SRM_SITE_LAX01
Database User Name	srm_db_admin
Database Password	*srm_admin_lax_password*
Database Port	5678
Connection Count	5
Max. Connections	20

21 On the **Site Recovery Manager Service Account** page, enter the following credentials, and click **Next**.

Setting	Value
Use Local System account	Deselected
Username	LAX01M01SRM01\Administrator
Password	*lax01m01srm01_admin_password*

22 On the **Ready to Install the Program** page click **Install**.

23 Click **Finish** to complete the installation.

Configure the Site Recovery Manager Instances

After both Site Recovery Manager Instances are deployed, assign the appropriate licensing. Using the svc-srm service account, pair the Region A and Region B instances and configure the mappings between them to support disaster recovery.

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 Add new license for the Site Recovery Manager instances.

a From the **Home** menu, select **Administration**.

b In the **Navigator**, under **Licensing**, click **Licenses**.

c Under **Licenses** page click the**Licenses** tab.

d Click the **Create New Licenses** icon to add license keys.

e On the **Enter license keys** page, enter license keys for Site Recovery Manager, and click **Next**.

f On the **Edit license name** page, enter a descriptive name for the license key, and click **Next**.

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

3 Assign the newly added license to the Site Recovery Manager assets.

a From the **Home** menu, select **Administration**.

b In the **Navigator**, under **Licensing**, click **Licenses**.

c Under **Licenses** page, click the **Assets** tab, and click **Solutions**.

d Select the **sfo01m01vc01.sfo01.rainpole.local** instance and click the **Assign License** icon.

e Select the available license from the list and click **OK**.

f Select the **lax01m01vc01.lax01.rainpole.local** instance and click the **Assign License** icon.

g Select the available license from the list and click **OK**.

4 Pair the two Site Recovery Manager sites.

a From the **Home** menu, select **Site Recovery**.

b In the **Navigator**, under **Sites**, click **Sites**.

c In **Sites** page, click the **sfo01m01vc01.sfo01.rainpole.local** site.

d On the **Summary** tab, under **Guide to configuring SRM**, click **1. Pair sites**.

e On the **Select site** page, enter `lax01psc01.lax01.rainpole.local` in the **PSC address** text box, leave the port value, and click **Next**.

f On the **Select vCenter Server** page, select **lax01m01vc01.lax01.rainpole.local**, enter the following credentials, and click **Finish.**

Setting	Value
User name	svc-srm@rainpole.local
Password	*svc-srm_password*

g In the **Security Alert** dialog box that appears twice, click **Yes** and wait until a new pane, **Paired Site**, appears on the **Summary** tab.

5 Configure resource mappings.

a On the **sfo01m01vc01.sfo01.rainpole.local** page, on the **Summary** tab, under **Guide to configuring SRM**, click **2.1 Create resource mappings**.

The **Create Resource Mapping** wizard appears.

b On the **Prepare Mappings** page, select the clusters underneath the vCenter Server instances for Region A and Region B to create a mapping between the resource in the clusters, click **Add mappings**, and click **Next**.

Setting	Protected Region	Recovery Region
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
Data center	sfo01-m01dc	lax01-m01dc
Cluster	sfo01-m01-mgmt01	lax01-m01-mgmt01
Inventory path	**sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01-mgmt01**	**lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01-mgmt01**

c On the **Prepare Reverse Mappings** page, click **Select all applicable** and click **Finish**.

Site Recovery Manager selects the following reverse resource mapping from Region B to Region A:

Setting	Recovery Region	Protected Region
vCenter Server	lax01m01vc01.lax01.rainpole.local	sfo01m01vc01.sfo01.rainpole.local
Data center	lax01-m01dc	sfo01-m01dc
Cluster	lax01-m01-mgmt01	sfo01-m01-mgmt01

6 Configure folder mappings.

a Under **Guide to configuring SRM**, click **2.2 Create folder mappings**.

The **Create Folder Mapping** wizard appears.

b On the **Select Creation Mode** page, select **Prepare mappings manually** and click **Next**.

c On the **Prepare Mappings** page, select the folders of the vRealize Operations Manager components and click **Add mappings**.

Setting	Protected Region	Recovery Region
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
Data center	sfo01-m01dc	lax01-m01dc
Folder	sfo01-m01fd-vrops	lax01-m01fd-vrops
Inventory path	**sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vrops**	**lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01fd-vrops**

d On the **Prepare Mappings** page, select the folders of vRealize Automation core components, click **Add mappings**, and click **Next**.

Setting	Protected Region	Recovery Region
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
Data center	sfo01-m01dc	lax01-m01dc
Folder	sfo01-m01fd-vra	lax01-m01fd-vra
Inventory path	**sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra**	**lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01fd-vra**

e On the **Prepare Reverse Mappings** page, click **Select all applicable**, and click **Finish**.

Site Recovery Manager selects the following reverse folder mappings from Region B to Region A:

Setting	Recovery Region	Protected Region
vCenter Server	lax01m01vc01.lax01.rainpole.local	sfo01m01vc01.sfo01.rainpole.local
Data center	lax01-m01dc	sfo01-m01dc
Folder for vRealize Operations Manager	lax01-m01fd-vrops	sfo01-m01fd-vrops
Folder for vRealize Automation	lax01-m01fd-vra	sfo01-m01fd-vra

7 Configure network mappings to enable failover of vRealize Operations Manager and vRealize Automation.

a Under **Guide to configuring SRM**, click **2.3 Create network mappings**.

The **Create Network Mapping** wizard appears.

b On the **Select Creation Mode** page, select **Prepare mappings manually** and click **Next**.

c On the **Prepare Mappings** page, expand the object trees, select the distributed port groups to map, click **Add mappings**, and click **Next**.

Setting	Protected Region	Recovery Region
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
Data center	sfo01-m01dc	lax01-m01dc
Distributed switch	sfo01-m01-vds01	lax01-m01-vds01
Port group	*port_group_prefix*-xRegion01-VXLAN	*port_group_prefix*-xRegion01-VXLAN

d On the **Select Test Networks** page, keep the default values and click **Next**.

e On the **Prepare Reverse Mappings** page, click **Select all applicable** and click **Finish**.

Site Recovery Manager selects the following reverse network mapping from Region B to Region A:

Setting	Recovery Region	Protected Region
vCenter Server	lax01m01vc01.lax01.rainpole.local	sfo01m01vc01.sfo01.rainpole.local
Data center	lax01-m01dc	sfo01-m01dc
Folder	lax01-m01fd-vra	sfo01-m01fd-vra
Distributed switch	lax01-m01-vds01	sfo01-m01-vds01
Port group	*port_group_prefix*-xRegion01-VXLAN	*port_group_prefix*-xRegion01-VXLAN

8 Configure placeholder datastore.

a Under **Guide to configuring SRM**, click **3. Configure placeholder datastore**.

b In the **Configure Placeholder Datastore** dialog box, select the **sfo01-m01-vsan01** datastore and click **OK**.

c Under **Sites**, click the **lax01m01vc01.lax01.rainpole.local** site.

d Under **Guide to configuring SRM**, click **3. Configure placeholder datastore**.

e In the **Configure Placeholder Datastore** dialog box, select the **lax01-m01-vsan01** datastore and click **OK**.

Deploy and Configure vSphere Replication

You deploy and configure vSphere Replication to enable replication of critical virtual machine data from Region A to Region B for failover by using Site Recovery Manager in the cases of disaster or planned migration.

Procedure

1 Prerequisites for the vSphere Replication Deployment

To deploy the two vSphere Replication virtual appliances, one in the protected region, and one in the recovery region, your environment must satisfy certain hardware and software requirements.

2 Configure User Privileges in vSphere for Integration with vSphere Replication

Assign vCenter Single Sign-On administrative, global permissions to the operations service account svc-vr so that you can manage and configure virtual machine replication for disaster recovery operations between the management vCenter Server instances by using vSphere Replication.

3 Deploy vSphere Replication in Region A

Deploy vSphere Replication in Region to enable replication of virtual machines from Region A.

4 Deploy vSphere Replication in Region B

After you deploy vSphere Replication in Region A, deploy it in Region B to complete the support for replication of virtual machines between the two regions.

5 Connect the vSphere Replication Instances

To use vSphere Replication between Region A and Region B, you must configure a connection between the two vSphere Replication appliances because each region is managed by a different vCenter Server instance.

6 Isolate the Network Traffic of vSphere Replication

vSphere Replication can consume a lot of bandwidth during initial replication, and when virtual machines are added or destroyed.

Prerequisites for the vSphere Replication Deployment

To deploy the two vSphere Replication virtual appliances, one in the protected region, and one in the recovery region, your environment must satisfy certain hardware and software requirements.

Software Requirements

Before you install vSphere Replication, make sure that you have the following configuration available in your environment.

Component	Requirement
Installation package	Download the vSphere Replication `.iso` image and mount it on the machine that you use to access the vSphere Web Client.
Email address of the vSphere Replication site administrators	Get the email addresses of the vSphere Replication site administrators.
Certificate Authority	■ Configure the root Active Directory domain controller as a certificate authority for the environment. ■ Download the `CertGenVVD` tool and generate the signed certificate for vSphere Replication. See the *VMware Validated Design Planning and Preparation* documentation.

IP Addresses, Host Names, and Network Configuration

In each region, allocate a static IP address and FQDN for vSphere Replication, and map the host name to the IP address.

Table 5-4. Network Configuration of vSphere Replication in Region A

Setting	Value
Host name	sfo01m01vrms01
Static IPv4 address	172.16.11.123
Subnet mask	255.255.255.0
Default gateway	172.16.11.253
DNS servers	172.16.11.5

Table 5-4. Network Configuration of vSphere Replication in Region A (Continued)

Setting	Value
FQDN	sfo01m01vrms01.sfo01.rainpole.local
Used ports	5480
NTP servers	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Table 5-5. Network Configuration of vSphere Replication in Region B

Setting	Value
Host name	lax01m01vrms01
Static IPv4 address	172.17.11.123
Subnet mask	255.255.255.0
Default gateway	172.17.11.253
DNS servers	172.17.11.5
FQDN	lax01m01vrms01.lax01.rainpole.local
Used ports	5480
NTP servers	■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local

Table 5-6. VLAN and IP Requirements for vSphere Replication Traffic

Requirement	Region A	Region B
VLAN ID	1616	1716
Static IPv4 address	172.16.16.71	172.17.16.71
Subnet mask	255.255.255.0	255.255.255.0
Gateway	172.16.16.253	172.17.16.253

Deployment Prerequisites

Verify that your environment satisfies the following prerequisites for the deployment of vSphere Replication.

Prerequisite	Value
Active Directory	Verify that you have a parent active directory with the SDDC user roles configured for the rainpole.local domain. The users and groups must be available in Region A and Region B.
Software Features	Verify that the Platform Services Controller instances for Region A and Region B are connected to the Active Directory domain.

Configure User Privileges in vSphere for Integration with vSphere Replication

Assign vCenter Single Sign-On administrative, global permissions to the operations service account svc-vr so that you can manage and configure virtual machine replication for disaster recovery operations between the management vCenter Server instances by using vSphere Replication.

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. From the **Home** menu, select **Administration**.
3. Assign the service account svc-vr@rainpole.local to the vCenter Single Sign-On administrators group
   a. In the **Navigator**, click **Users and Groups**, and click the **Groups** tab.
   b. Click the **Administrators** group and click the **Add Member** icon under **Group Members**.
   c. In the **Add Principals** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.
   d. From the list of users and groups, select the **svc-vr** user, click **Add**, and click **OK**.

The global vCenter Single Sign-On administrative permissions of the svc-vr account propagate to all other linked vCenter Server instances.

Deploy vSphere Replication in Region A

Deploy vSphere Replication in Region to enable replication of virtual machines from Region A.

Deploy the vSphere Replication Application in Region A

Deploy the vSphere Replication appliance on the protected region.

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 In the **Navigator**, click **Hosts and Clusters**.

3 Right-click **sfo01m01vc01.sfo01.rainpole.local** and select **Deploy OVF Template**.

4 On the **Select template** page, click the **Browse** button, use a multiple selection to select the following files from the `bin` folder of the `.iso` mount for vSphere Replication on your computer, click **Open**, and click **Next**.

   - vSphere_Replication_OVF10.ovf
   - vSphere_Replication-support.vmdk
   - vSphere_Replication-system.vmdk

5 On the **Select name and location** page, enter a node name, select the inventory folder for the virtual appliance, and click **Next**.

Setting	Value
Name	sfo01m01vrms01
vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Data center	sfo01-m01dc
Folder	sfo01-m01fd-bcdr

6 On the **Select a resource** page, select the **sfo01-m01-mgmt01** cluster and click **Next**.

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, leave the default **4 vCPU** configuration selected and click **Next**.

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	sfo01-m01-vsan01

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

Setting	Value
Management Network Destination	sfo01-m01-vds01-management
IP protocol	IPv4
IP allocation	Static - Manual

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

Setting	Value
DNS servers	172.16.11.5,172.16.11.4
Domain name	sfo01.rainpole.local
Gateway	172.16.11.253
Netmask	255.255.255.0
DNS search path	sfo01.rainpole.local
Management Network IP Address	172.16.11.123
NTP Servers	ntp.sfo01.rainpole.local,ntp.lax01.rainpole.local
Enter password	*vr_sfo_root_password*
Confirm password	*vr_sfo_root_password*

13 On the **vService bindings** page, click **Next**.

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

15 In the **Navigator**, expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree, select the **sfo01m01vrms01** VM and click the **Power On** button.

Replace the CA-Signed Certificate on vSphere Replication in Region A

In a dual-region SDDC, replace the default certificate on vSphere Replication in Region A with a custom one for improved security.

Table 5-7. PKCS#12 Files for vSphere Replication in Region A

vSphere Replication	PKCS#12 File Name from the CertGenVVD Tool
sfo01m01vrms01.sfo01.rainpole.local	sfo01m01vrms01.5.p12

Procedure

1 Upload the PKCS#12 file to vSphere Replication by using the vSphere Replication appliance management interface (VAMI).

   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*

   c On the **VR** tab, click the **Configuration** tab.

   d Click **Choose File** next to **Upload PKCS#12 (*.pfx) file** and locate the `sfo01m01vrms01.5.p12` file on your local file system.

   e Click the **Upload and Install** button and enter the certificate password when prompted.

   After you apply the SSL certificate, the VAMI session of vSphere Replication will be disconnected.

2 Log in again by using the root credential.

3 On the **VR** tab, click the **Security** tab.

4 Verify that the **Current SSL Certificate** shows the updated certificate information.

Register vSphere Replication with vCenter Single Sign-On in Region A

After you deploy the vSphere Replication appliance on the protected region, register vSphere Replication with the Platform Services Controller pair by using the vSphere Replication appliance management interface.

Procedure

1 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*

2 On the **VR** tab, click **Configuration**, enter the following settings, and click **Save and Restart Service**.

Setting	Value
Configuration Mode	Configure using the embedded database
LookupService Address	sfo01psc01.sfo01.rainpole.local

Setting	Value
SSO Administrative Account	svc-vr@rainpole.local
Password	*svc-vr_password*
VRM Host	172.16.11.123
VRM Site Name	sfo01m01vc01.sfo01.rainpole.local
vCenter Server Address	sfo01m01vc01.sfo01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	*vcenter_server_admin_email*

3 In the **Confirm SSL Certificate** dialog box, click **Accept**.

4 Wait for the vSphere Replication Management (VRM) server to save the configuration.

5 Under **Service Status**, verify that the status of the VRM service is `running`.

6 Log out from the vSphere Replication appliance management interface.

Deploy vSphere Replication in Region B

After you deploy vSphere Replication in Region A, deploy it in Region B to complete the support for replication of virtual machines between the two regions.

Deploy the vSphere Replication Appliance in Region B

After you deploy vSphere Replication on the protected region, deploy the vSphere Replication appliance on the recovery region to complete replication deployment.

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**, click **Hosts and Clusters**.

3 Right-click **lax01m01vc01.lax01.rainpole.local** and select **Deploy OVF Template**.

4 On the **Select template** page, click the **Browse** button, use a multiple selection to select the following files from the `bin` folder of the `.iso` mount for vSphere Replication on your computer, click **Open**, and click **Next**.

- vSphere_Replication_OVF10.ovf
- vSphere_Replication-support.vmdk

- vSphere_Replication-system.vmdk

5 On the **Select name and location** page, enter a node name, select the inventory folder for the virtual appliance, and click **Next**.

Setting	Value
Name	lax01m01vrms01
vCenter Server	lax01m01vc01.lax01.rainpole.local
Data center	lax01-w01dc
Folder	lax01-m01fd-bcdr

6 On the **Select a resource** page, select the **lax01-m01-mgmt01** cluster, and click **Next**.

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, leave the default **4 vCPU** configuration selected and click **Next**.

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, select the following settings and click **Next**.

Setting	Value
Management Network Destination	lax01-m01-vds01-management
IP protocol	IPv4
IP allocation	Static - Manual

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

Setting	Value
DNS servers	172.17.11.5,172.17.11.4
Domain name	lax01.rainpole.local
Gateway	172.17.11.253
Netmask	255.255.255.0
DNS search path	lax01.rainpole.local
Management Network IP Address	172.17.11.123
NTP Servers	ntp.lax01.rainpole.local,ntp.sfo01.rainpole.local
Enter password	*vr_lax_root_password*
Confirm password	*vr_lax_root_password*

13 On the **vService bindings** page, click **Next**.

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

15 In the **Navigator**, expand the entire **lax01m01vc01.lax01.rainpole.local** tree, select the **lax01m01vrms01** VM, and click the **Power On** button.

Replace the CA-Signed Certificate on vSphere Replication in Region B

Replace the certificates on vSphere Replication in Region B so that vSphere Replication can communicate with connected management solutions over a secure connection.

Table 5-8. PKCS#12 Files for vSphere Replication in Region B

vSphere Replication FQDN	PKCS#12 File Name from the CertGenVVD Tool
lax01m01vrms01.lax01.rainpole.local	lax01m01vrms01.5.p12

Prerequisites

- CA-signed certificate files generated by using VMware Validated Design Certificate Generation Utility (`CertGenVVD`). See the *VMware Validated Design Planning and Preparation* documentation.

Procedure

1 Upload the PKCS#12 file to vSphere Replication by using the vSphere Replication appliance management interface (VAMI).

a Open a Web browser and go to **`https://lax01m01vrms01.lax01.rainpole.local:5480`**.

b Log in using the following credentials.

Settings	Value
User name	root
Password	*vr_sfo_root_password*

c On the **VR** tab, click the **Configuration** tab.

d Enter the password of the service account svc-vr@rainpole.local.

e Click **Choose File** next to **Upload PKCS#12 (*.pfx)** file and locate the `lax01m01vrms01.5.p12` file on your local file system.

f Click the **Upload and Install** button and enter the certificate password when prompted.

After you apply the SSL certificate, the VAMI session of vSphere Replication will be disconnected.

2 Log in again by using the root credential.

3 On the **VR** tab, click the **Security** tab.

4 Verify that the **Current SSL Certificate** shows the updated certificate information.

Register vSphere Replication with vCenter Single Sign-On in Region B

After you deploy the vSphere Replication appliance on the recovery region, register vSphere Replication with the Platform Services Controller pair by using the vSphere Replication appliance management interface.

Procedure

1 Log in to the management interface of the vSphere Replication appliance.

a Open a Web browser and go to **`https://lax01m01vrms01.lax01.rainpole.local:5480`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vr_lax_root_password*

2 On the **VR** tab, click **Configuration**, enter the following settings, and click **Save and Restart Service**.

Setting	Value
Configuration Mode	Configure using the embedded database
LookupService Address	lax01psc01.lax01.rainpole.local
SSO Administrative Account	svc-vr@rainpole.local
Password	*svc-vr_password*
VRM Host	172.17.11.123
VRM Site Name	lax01m01vc01.lax01.rainpole.local
vCenter Server Address	lax01m01vc01.lax01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	*vcenter_server_admin_email*

3 In the **Confirm SSL Certificate** dialog box, click **Accept**.

4 Wait for the vSphere Replication Management (VRM) server to save the configuration.

5 Under **Service Status**, verify that the status of the VRM service is `running`.

6 Log out from the vSphere Replication appliance management interface.

Connect the vSphere Replication Instances

To use vSphere Replication between Region A and Region B, you must configure a connection between the two vSphere Replication appliances because each region is managed by a different vCenter Server instance.

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 Connect the two vSphere Replication instances.

a On the vSphere Web Client **Home** page, click **Hosts and Clusters**.

b In the **Navigator**, select the **sfo01m01vc01.sfo01.rainpole.local** instance, click the **Configure** tab, and click **Target Sites** under **vSphere Replication**.

c Click the **Connect to target site to configure replications** icon.

d In the **Connect to Target Site** dialog box, select **Connect to a remote site**, enter the following settings, and click the **Log In** button.

Setting	Value
PSC address of the remote site	lax01psc01.lax01.rainpole.local
User name	svc-vr@rainpole.local
Password	*svc-vr_password*

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

The **Connect to Target site** dialog box shows lax01m01vc01.lax01.rainpole.local selected.

f In the **Connect to Target Site** dialog box, click **OK**.

3 On the **Target Sites** page, verify that the value under **Status** is `Connected`.

Isolate the Network Traffic of vSphere Replication

vSphere Replication can consume a lot of bandwidth during initial replication, and when virtual machines are added or destroyed.

To avoid network problems in the data center, isolate replication traffic from other network traffic. Isolating the vSphere Replication traffic also enhances network performance in the data center by reducing the impact of this traffic on other traffic types.

You isolate the network traffic to the vSphere Replication Server by dedicating a VMkernel network adapter on each management ESXi host that sends data to the vSphere Replication Server and using a dedicated network adapter on the vSphere Replication Server VM.

By default, the vSphere Replication appliance has one virtual machine network adapter that is used by the vSphere Replication Server for both replication traffic and by vCenter Server for virtual machine management. To isolate the replication traffic, you add a second adapter to the appliances in both regions and configure them for replication traffic.

You configure isolation of the replication traffic on the management cluster in each region.

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	sfo01-m01hp-mgmt01	lax01-m01hp-mgmt01
Template ESXi host	sfo01m01esx01.sfo01.rainpole.local	lax01m01esx01.lax01.rainpole.local
Filter value	172.16.16.253	172.17.16.253
IP Next Hop	172.16.16.253	172.17.16.253
Destination network address	172.17.16.0	172.16.16.0
Device name	vmk2	vmk2
Host/Cluster	sfo01-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 appliance to allow changes in the hardware configuration.

  a In the **Navigator**, click **Hosts and Clusters**.

  b 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** to proceed.

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

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

  b In the **Edit Settings** dialog box, click **Yes** to proceed.

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

d From the **New Network** device drop-down menu, select **sfo01-m01-vds01-replication** and click **OK**.

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

f In the **Confirm Power On** dialog box, click **Yes** to proceed 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 `eth1`.

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

b Under **eth1 info**, enter the following settings and click **Save Settings**.

Setting	Value
IPv4 Address Type	Static
IPv4 Address	172.16.16.71
Netmask	255.255.255.0
IPv6 Address Type	Auto

c Click the **VR** tab and click **Configuration**.

d In the **IP Address for Incoming Storage Traffic** text box, enter **`172.16.16.71`** and click **Apply Network Setting**.

172.16.16.71 is the IP address of the new network adapter that will handle replication traffic.

6 Repeat the steps to reconfigure the lax01m01vrms01 vSphere Replication appliance in Region B, using the values from the following table.

Setting	Value
Object to configure	lax01m01vrms01
Connect New Network Adapter To	lax01-m01-vds01-replication
URL of vSphere Replication Appliance	https://lax01m01vrms01.lax01.rainpole.local:5480
IPv4 Address Type	Static
IPv4 Address	172.17.16.71

Setting	Value
Netmask	255.255.255.0
IP Address For Incoming Storage Traffic	172.17.16.71

7 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*

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

Appliance Host Name	Source Gateway	Target Network
sfo01m01vrms01.sfo01.rainpole.local	172.16.16.253	172.17.16.0/24
lax01m01vrms01.lax01.rainpole.local	172.17.16.253	172.16.16.0/24

a In the **Navigator**, click **Hosts and Clusters**.

b 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 Press ALT+F2 to switch to the command prompt.

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 Add the following line after the default gateway 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, and save the file.

Region of the vSphere Replication Appliance	Value
Region A	172.17.16.0/24 172.16.16.253 dev eth1
Region B	172.16.16.0/24 172.17.16.253 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 vSphere Replication appliance in the other region.

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

Region	Host Name	Source Gateway	Target Network
Region A	sfo01m01esx01.sfo01.rainpole.local	172.16.16.253	172.17.16.0/24
Region B	lax01m01esx01.lax01.rainpole.local	172.17.16.253	172.16.16.0/24

a Open an SSH session to the sfo01m01esx01.sfo01.rainpole host in the sfo01-m01-mgmt01 cluster in Region A and log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

b Run the following command 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.

Region of the ESXi Host	Command
Region A	esxcli network ip route ipv4 add --gateway 172.16.16.253 --network 172.17.16.0/24
Region B	esxcli network ip route ipv4 add --gateway 172.17.16.253 --network 172.16.16.0/24

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.

10 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*

11 Update the host profile of the management cluster.

a From the vSphere Web Client **Home** menu, select **Home**.

b In the **Navigator**, click **Policies and Profiles** and click **Host Profiles**.

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

   d Select **sfo01m01esx01.sfo01.rainpole.local** and click **OK**.

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

   a On the **Host Profiles** page in the **Navigator**, click **sfo01-m01hp-mgmt01**.

   b On the **Configure** tab, click **Settings**.

   c In **Filter** search box, type in `172.16.16.253`.

   You locate the **Network Configuration > NetStack Instance > defaultTcpipStack > IP route Configuration > IP route config** profile property.

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

Settings	Value
IP Next Hop	172.16.16.253
Destination Network address	172.17.16.0
Device Name	vmk2

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

   a On the **Policies and Profiles** page, select **sfo01-m01hp-mgmt01**.

   b On the **Monitor** tab, click the **Compliance** tab.

   c Select **sfo01-m01-mgmt01** in the **Host/Cluster** column and click **Check Host Profile Compliance**.

   This compliance test shows that the first host is `Compliant`, and that the other hosts are `Not Compliant`.

   d Select each of the non-compliant hosts, click **Remediate Hosts Based on its Host Profile** and click **Next** in the **Remediate Hosts Based on its Host Profile** wizard.

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

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

14 Repeat Step 10 to Step 13 on the management cluster in Region B.

Configure Operations Management for the Business Continuity Components

After you install Site Recovery Manager in Region A and Region B, enable its integration with the operations management layer. You can monitor and receive alerts and logs about site protection and disaster recovery in a central location by using vRealize Operations Manager and vRealize Log Insight.

Procedure

1. Connect vRealize Operations Manager to Site Recover Manager

   Install and configure the vRealize Operations Management Pack for Site Recovery Manager to monitor the health and configuration of the Site Recovery Manager instances, and the status of the protection groups and recovery plans for failing over the management components of the SDDC.

2. Connect vRealize Log Insight to Site Recovery Manager

   Monitor Site Recovery Manager operation by tracking its logs in vRealize Log Insight. In each region, install the content pack for Site Recovery Manager in vRealize Log Insight and install the Log Insight Agent on the Windows virtual machine of the Site Recovery Manager instance.

Connect vRealize Operations Manager to Site Recover Manager

Install and configure the vRealize Operations Management Pack for Site Recovery Manager to monitor the health and configuration of the Site Recovery Manager instances, and the status of the protection groups and recovery plans for failing over the management components of the SDDC.

Procedure

1. Configure User Privileges for Site Recovery Manager Adapters in vRealize Operations Manager

   Assign read-only permissions to the service account svc-vrops-srm on the sites that are required for collecting data about Site Recovery Manager instances in vRealize Operations Manager.

2. Install the vRealize Operations Manager Management Pack for Site Recovery Manager

   Install the `.pak` file for the management pack for Site Recovery Manager to add the management pack as a solution to vRealize Operations Manager.

3. Add SRM Adapter Instances to vRealize Operations Manager

   In a dual-region SDDC, configure SRM Adapters to collect monitoring data in vRealize Operations Manager about the Site Recovery Manager instances and failover objects.

Configure User Privileges for Site Recovery Manager Adapters in vRealize Operations Manager

Assign read-only permissions to the service account svc-vrops-srm on the sites that are required for collecting data about Site Recovery Manager instances in vRealize Operations Manager.

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 On the **Home** page of the vSphere Web Client, select **Site Recovery.**

3 In the **Navigator**, under **Sites**, click **Sites**.

4 In **Sites** page, click the **sfo01m01vc01.sfo01.rainpole.local** site.

5 On the **Manage** tab, click **Permissions** tab.

6 On the **Permissions** tab, click **Add permission**.

7 In the **Add Permission** dialog box, click **Add** .

8 Add the service account.

   a In the **Select Users/Groups** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type `svc-vrops-srm`, and press Enter.

   b From the list of users and groups, select **svc-vrops-srm**, click **Add**, and click **OK.**

9 Associate the service account with the read-only role.

   a In the **Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **Read-only**.

   b Verify that **Propogate to children** is selected and click **OK.**

10 Repeat the steps to assign read-only permissions to the svc-vrops-srm service account on the site instance for Region B.

Install the vRealize Operations Manager Management Pack for Site Recovery Manager

Install the `.pak` file for the management pack for Site Recovery Manager to add the management pack as a solution to vRealize Operations Manager.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Solutions**.

4 On the **Solutions** page, click the **Add** icon.

5 On the **Select Solution** page from the **Add Solution** wizard, browse to the `.pak` file of the vRealize Operations Manager Management Pack for Site Recovery Manager and click **Upload**.

   After the management pack file has been uploaded, you see details about the management pack.

6 After the upload is complete, click **Next**.

7 On the **End User License Agreement** page, accept the license agreement and click **Next**.

   The installation of the management pack starts. You see its progress on the **Install** page.

8 After the installation is complete, click **Finish** on the **Install** page.

The Srm Adapter solution appears on the **Solutions** page of the vRealize Operations Manager user interface.

Add SRM Adapter Instances to vRealize Operations Manager

In a dual-region SDDC, configure SRM Adapters to collect monitoring data in vRealize Operations Manager about the Site Recovery Manager instances and failover objects.

You

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the main navigation bar, click **Administration**.

3 In the left pane of vRealize Operations Manager, click **Solutions**.

4 On the **Solutions** page, select **Srm Adapter** from the solution table, and click **Configure**.

The **Manage Solution - Srm Adapter** dialog box appears.

5 Under **Instance Settings**, enter the settings for the connection to Site Recovery Manager instances.

a If you already have added another Srm Adapter, click the **Add** icon on the left side to add an adapter settings.

b Enter the settings for connection to Site Recovery Manager.

Setting	Value for Site Recovery Manager in Region A	Value for Site Recovery Manager in Region B
Display Name	SRM Adapter - sfo01m01srm01	SRM Adapter - lax01m01srm01
Description	Site Recovery Manager Adapter for sfo01	Site Recovery Manager Adapter for lax01
SRM Host	sfo01m01srm01.sfo01.rainpole.local	lax01m01srm01.lax01.rainpole.local
SRM Port	9086	9086

c Click the **Add** icon next to the **Credential** text box, configure the credentials for connection to Site Recovery Manager instances, and click **OK.**

Setting	Value for Site Recovery Manager in Region A	Value for Site Recovery Manager in Region B
Credential name	SRM Adapter Credentials - sfo01m01srm01	SRM Adapter Credentials - lax01m01srm01
Username	svc-vrops-srm@rainpole.local	svc-vrops-srm@rainpole.local
Password	*svc-vrops-srm_password*	*svc-vrops-srm_password*

d Click **Test Connection** to validate the connection to Site Recovery Manager.

The Site Recovery Manager certificate appears.

e In the **Review and Accept Certificate** dialog box, verify the Site Recovery Manager certificate information and click **Accept**.

f Click **OK** in the **Info** dialog box.

g Expand the **Advanced Settings** section of settings.

h From the **Collectors/Groups** drop-down menu, select the collector group for the region.

Site Recovery Manager Instance	Remote Collector Group
Site Recovery Manager in Region A	sfo01-remote-collectors
Site Recovery Manager in Region B	lax01-remote-collectors

i Click **Save Settings**.

   j Click **OK** in the **Info** dialog box that appears.

   k Repeat the steps for the Site Recovery Manager in Region B.

6 In the **Manage Solution - Srm Adapter** dialog box, click **Close**.

The SRM Adapter instances appear on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is `Collecting` and the **Collection Status** is `Data receiving`.

Connect vRealize Log Insight to Site Recovery Manager

Monitor Site Recovery Manager operation by tracking its logs in vRealize Log Insight. In each region, install the content pack for Site Recovery Manager in vRealize Log Insight and install the Log Insight Agent on the Windows virtual machine of the Site Recovery Manager instance.

Procedure

1 Install the vRealize Log Insight Content Pack for Site Recovery Manager

   Install the content pack for Site Recovery Manager to add the dashboards for viewing log information in vRealize Log Insight in Region A and Region B.

2 Configure Site Recovery Manager to Forward Log Events to vRealize Log Insight

   Install the vRealize Log Insight agent on the Site Recovery Manager instances in Region A and Region B to collect and forward events to vRealize Log Insight.

Install the vRealize Log Insight Content Pack for Site Recovery Manager

Install the content pack for Site Recovery Manager to add the dashboards for viewing log information in vRealize Log Insight in Region A and Region B.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon ☰ and select **Content Packs**.

3 Under **Content Pack Marketplace**, select **Marketplace**.

4 In the list of content packs, locate the **VMware - SRM** content pack and click its icon.

5 In the **Install Content Pack** dialog box, accept the **License Agreement** and click **Install**.

6 In the **VMware - SRM Content Pack Setup Instructions** dialog box, click **OK**.

7 Repeat the steps on vRealize Log Insight in Region B lax01vrli01.lax01.rainpole.local

After the installation is complete, the VMware - SRM content pack appears in the **Installed Content Packs** list on the left in vRealize Log Insight.

Configure Site Recovery Manager to Forward Log Events to vRealize Log Insight

Install the vRealize Log Insight agent on the Site Recovery Manager instances in Region A and Region B to collect and forward events to vRealize Log Insight.

In each region, you perform the following operations:

1 Install the Windows Log Insight Agent on the Site Recovery Manager virtual machine and connect it to the vRealize Log Insight instance in the region.

2 Create an agent group for central configuration of the Log Insight Agent on the Site Recovery Manager instance.

Table 5-9. Settings for Forwarding Events from Site Recovery Manager to vRealize Log insight

Setting	Value for Site Recovery Manager in Region A	Value for Site Recovery Manager in Region B
FQDN of the Site Recovery Manager virtual machine	sfo01m01srm01.sfo01.rainpole.local	lax01m01srm01.lax01.rainpole.local
vRealize Log Insight URL	https://sfo01vrli01.sfo01.rainpole.local	https://lax01vrli01.lax01.rainpole.local
Host names in the agent group in vRealize Log Insight	sfo01m01srm01.sfo01.rainpole.local	lax01m01srm01.lax01.rainpole.local

Procedure

1 Install Log Insight Windows agents in the virtual machines of the Site Recovery Manager nodes.

a Open a Remote Desktop Protocol (RDP) connection to **`sfo01m01srm01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	*windows_administrator_user*

c On the Windows host, open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

d Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

e Click the **Configuration** drop-down menu icon ☰ and select **Administration**.

f Under **Management**, click **Agents**.

g On the **Agents** page, click the **Download Log Insight Agent Version** link.

h In the **Download Log Insight Agent Version** dialog box, click **Windows MSI (32-bit/64-bit)** and save the `.msi` file to the vRealize Automation virtual machine.

i Open an administrative command prompt window, and navigate to the directory where you saved the `.msi` file.

j Run the following command to install the vRealize Log Insight agent with custom values.

```
VMware-Log-Insight-Agent-4.5.0-5626690_192.168.32.10.msi SERVERPORT=9000 AUTOUPDATE=yes
LIAGENT_SSL=no
```

k In the **VMware vRealize Log Insight Agent Setup** wizard, accept the license agreement and click **Next**.

l With the Log Insight host name **`sfo01m01srm01.sfo01.rainpole.local`** selected in the **Host** text box, click **Install**.

m After the installation is complete, click **Finish**.

2 Create an agent group for Site Recovery Manager in the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

c Click the configuration drop-down menu icon ☰ and select **Administration**.

d Under **Management**, click **Agents**.

e From the drop-down on the top, select **vSphere - SRM** from the **Available Templates** section.

f Click **Copy Template**.

g In the **Copy Agent Group** dialog box, enter **`SRM – Agent Group`** in the name text box and click **Copy**.

h Configure the following agent filter.

  Press Enter to separate the host names.

Filter	Operator	Values
Hostname	matches	sfo01m01srm01.sfo01.rainpole.local

i Click **Refresh** and verify that all the agents listed in the filter appear in the **Agents** list.

j Click **Save New Group** at the bottom of the page.

3 Repeat the procedure on Site Recovery Manager and vRealize Log Insight in Region B.

All VMware Site Recovery Manager dashboards become available on the vRealize Log Insight Home page.