Deployment for Region B

Modified on 21 DEC 2017
VMware Validated Design 4.1
VMware Validated Design for Software-Defined Data Center 4.1
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
# Contents

1 About VMware Validated Design Deployment for Region B 4

Updated Information 5

2 Region B Virtual Infrastructure Implementation 6

Install and Configure ESXi Hosts in Region B 7

Deploy and Configure the Platform Services Controller and Virtual Center Components in Region B 13

Deploy and Configure the Management Cluster NSX Instance in Region B 45

Deploy and Configure the Shared Edge and Compute Cluster Components Region B 87

Deploy and Configure the Shared Edge and Compute Cluster NSX Instance in Region B 108

Deploy and Configure Site Recovery Manager 140

Deploy and Configure vSphere Replication 152

Deploy vSphere Data Protection in Region B 167

Replace Certificates in Region B 175

3 Region B Cloud Management Platform Implementation 185

Prerequisites for Cloud Management Platform Implementation in Region B 186

Configure Service Account Privileges in Region B 186

vRealize Automation Installation in Region B 191

Embedded vRealize Orchestrator Configuration in Region B 210

vRealize Business Installation in Region B 212

Create Anti-Affinity Rules for vRealize Automation Proxy Agent Virtual Machines in Region B 218

Content Library Configuration in Region B 219

Tenant Content Creation in Region B 220

4 Region B Operations Implementation 258

Region B vRealize Operations Manager Implementation 258

Region B vRealize Log Insight Implementation 285

Region B vSphere Update Manager Download Service Implementation 326
About VMware Validated Design Deployment for Region B

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.
Updated Information

This Deployment for Region B document is updated with each release of the product or when necessary.

This table provides the update history of the Deployment for Region B document.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
</table>
| 26 SEP 2017    | • Added step for configuring uplinks for the lax01-w01-vds01-uplink01 and lax01-w01-vds01-uplink02 port groups. Each uplink group is connected only to a single physical NIC. See Create a vSphere Distributed Switch for the Management Cluster in Region B.  
• Added step for configuring uplinks for the lax01-w01-vds01-uplink01 and lax01-w01-vds01-uplink02 port groups. Each uplink group is connected only to a single physical NIC. See Create a vSphere Distributed Switch for the Shared Edge and Compute Cluster in Region B. |
| 22 AUG 2017    | Initial release.                                                             |
Region B Virtual Infrastructure Implementation

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 Virtual Center Components in Region B
   Deploy and configure the management cluster components.

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.

6. 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.

7. 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.
8 **Deploy vSphere Data Protection in Region B**

Deploy vSphere Data Protection for backup and restore of SDDC management components in Region B.

9 **Replace Certificates in Region B**

By default, virtual infrastructure management components use TLS/SSL certificates that are signed by the VMware Certificate Authority (VMCA). These certificates are not trusted by end-user devices. For example, a certificate warning might appear when a user connects to a vCenter Server system by using the vSphere Web Client.

### 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 for each of your hosts in the management and the shared edge and compute clusters.

### 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

<table>
<thead>
<tr>
<th>FQDN</th>
<th>IP</th>
<th>Management VLAN</th>
<th>Default Gateway</th>
<th>NTP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01m01esx01.lax01.rainpole.local</td>
<td>172.17.11.101</td>
<td>1711</td>
<td>172.17.11.253</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ntp.sfo01.rainpole.local</td>
</tr>
<tr>
<td>lax01m01esx02.lax01.rainpole.local</td>
<td>172.17.11.102</td>
<td>1711</td>
<td>172.17.11.253</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ntp.sfo01.rainpole.local</td>
</tr>
<tr>
<td>lax01m01esx03.lax01.rainpole.local</td>
<td>172.17.11.103</td>
<td>1711</td>
<td>172.17.11.253</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ntp.sfo01.rainpole.local</td>
</tr>
<tr>
<td>lax01m01esx04.lax01.rainpole.local</td>
<td>172.17.11.104</td>
<td>1711</td>
<td>172.17.11.253</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ntp.sfo01.rainpole.local</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>FQDN</th>
<th>IP</th>
<th>Management VLAN</th>
<th>Default Gateway</th>
<th>NTP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01w01esx01.lax01.rainpole.local</td>
<td>172.17.31.101</td>
<td>1731</td>
<td>172.17.31.253</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ntp.sfo01.rainpole.local</td>
</tr>
<tr>
<td>lax01w01esx02.lax01.rainpole.local</td>
<td>172.17.31.102</td>
<td>1731</td>
<td>172.17.31.253</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ntp.sfo01.rainpole.local</td>
</tr>
<tr>
<td>lax01w01esx03.lax01.rainpole.local</td>
<td>172.17.31.103</td>
<td>1731</td>
<td>172.17.31.253</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ntp.sfo01.rainpole.local</td>
</tr>
<tr>
<td>lax01w01esx04.lax01.rainpole.local</td>
<td>172.17.31.104</td>
<td>1731</td>
<td>172.17.31.253</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ntp.sfo01.rainpole.local</td>
</tr>
</tbody>
</table>

### 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](image)

6 Select the keyboard layout, and press Enter.

7 Enter the `esxi_root_user_password`, enter the password a second time to confirm you are typing the correct password, and press Enter.

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

9 After the installation has completed 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  Enter root as login name, and esxi_root_user_password, and press Enter.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set static IPv4 address and network configuration</td>
<td>Selected</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>172.17.11.101</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>172.17.11.253</td>
</tr>
</tbody>
</table>

f Select DNS Configuration and press Enter.

g Configure the DNS using the following settings, and press Enter.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the following DNS Server address and hostname</td>
<td>Selected</td>
</tr>
<tr>
<td>Primary DNS Server</td>
<td>172.17.11.5</td>
</tr>
<tr>
<td>Alternate DNS Server</td>
<td>172.17.11.4</td>
</tr>
<tr>
<td>Hostname</td>
<td>lax01m01esx01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

h Select Custom DNS Suffixes and press Enter.

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

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

4 Repeat this procedure for all hosts in 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.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td><code>esxi_root_user_password</code></td>
</tr>
</tbody>
</table>

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, choose the VM Network port group, and click **Edit Settings**.
   b. On the Edit port group - VM Network window, input **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 for each of your hosts in the management and the shared edge and compute clusters.

**Procedure**

1. Log in to the lax01m01esx01.lax01.rainpole.local host by using the VMware Host Client.
   a. Open a Web browser and go to `http://lax01m01esx01.lax01.rainpole.local`.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td><code>esxi_root_user_password</code></td>
</tr>
</tbody>
</table>

2. Configure SSH options.
   a. In the Navigator, click **Manage**, click the **Services** tab, select the **TSM-SSH** service, and click the **Actions** menu. Choose **Policy** and click **Start and stop with host**.
   b. Click **Start** to start the service.

3. Configure the NTP Daemon (ntpd) options.
   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 choose **Start**.

## Deploy and Configure the Platform Services Controller and Virtual Center Components in Region B

Deploy and configure the management cluster components.

**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. 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. Once this has been done, the identity sources configured for the vSphere Domain will 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**
   
   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.

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 balancers 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 assign a license.

6. **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.

7. **Configure the Management Cluster in Region B**
   
   You must now create and configure the management cluster.

8. **Create a vSphere Distributed Switch for the Management Cluster in Region B**
   
   After you have added 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.

9. **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.
Enable vSphere HA on the Management Cluster in Region B

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

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 save space in the vSAN datastore.

Mount NFS Storage for the Management Cluster in Region B

You must mount a NFS datastore where vSphere Data Protection will later be deployed.

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.

Set Virtual SAN Policy on Management Virtual Machines in Region B

After you apply the host profile to all of the hosts, set the storage policy of the management virtual machines to the default Virtual SAN storage policy.

Create the VM and Template Folders in Region B

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

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.

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 ServerInstances in Region B

Two external Platform Services Controller instances must be deployed in Region B. 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.
   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FQDN or IP Address</td>
<td>lax01m01esx01.lax01.rainpole.local</td>
</tr>
<tr>
<td>HTTPS port</td>
<td>443</td>
</tr>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>esxi_root_user_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Management Value</th>
<th>Edge/Compute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM name</td>
<td>lax01m01psc01</td>
<td>lax01w01psc01</td>
</tr>
<tr>
<td>Root password</td>
<td>mgmtpsc_root_password</td>
<td>comppsc_root_password</td>
</tr>
<tr>
<td>Confirm root password</td>
<td>mgmtpsc_root_password</td>
<td>comppsc_root_password</td>
</tr>
</tbody>
</table>

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

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.

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

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**.
   
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time synchronization mode</td>
<td>Synchronize time with NTP servers</td>
</tr>
<tr>
<td>NTP servers (comma-separated list)</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td>SSH access</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
   
c  On the **SSO configuration** page, enter the following settings, and click **Next**.
   
<table>
<thead>
<tr>
<th>Setting</th>
<th>Management Value</th>
<th>Edge/Compute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO configuration</td>
<td>Join an existing SSO domain</td>
<td>Join an existing SSO domain</td>
</tr>
<tr>
<td>Platform Services Controller</td>
<td>sf01m01psc01.sf01.rainpole.local</td>
<td>lax01m01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>HTTPS port</td>
<td>443</td>
<td>443</td>
</tr>
<tr>
<td>SSO domain name</td>
<td>vsphere.local</td>
<td>vsphere.local</td>
</tr>
<tr>
<td>SSO password</td>
<td>sso_password</td>
<td>sso_password</td>
</tr>
</tbody>
</table>
   
d  On the **SSO Site Name** page, enter the following settings, and click **Next**.
   
<table>
<thead>
<tr>
<th>Setting</th>
<th>lax01m01psc01</th>
<th>lax01w01psc01</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO Site Creation</td>
<td>Create a new site</td>
<td>Join an existing site</td>
</tr>
<tr>
<td>Site name</td>
<td>LAX01</td>
<td>LAX01</td>
</tr>
</tbody>
</table>
   
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.

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

**Note**  Step 3h is performed only on the first deployment, during the second PSC deployment choose the existing vSAN datastore.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Server</td>
<td>sfo01w01psc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>mgmtpsc_root_password</td>
</tr>
</tbody>
</table>

   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 in the regions.

   **Note**  The following 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. Once this has been done, the identity sources configured for the vSphere Domain will 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.

<table>
<thead>
<tr>
<th>Platform Services Controller</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Services Controller for the management cluster</td>
<td><a href="https://lax01m01psc01.lax01.rainpole.local">https://lax01m01psc01.lax01.rainpole.local</a></td>
</tr>
<tr>
<td>Platform Services Controller for the shared edge and compute cluster</td>
<td><a href="https://lax01w01psc01.lax01.rainpole.local">https://lax01w01psc01.lax01.rainpole.local</a></td>
</tr>
</tbody>
</table>
Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>lax01.rainpole.local</td>
</tr>
<tr>
<td>User name</td>
<td><a href="mailto:ad_admin_acct@lax01.rainpole.local">ad_admin_acct@lax01.rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>ad_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>psc_root_password</td>
</tr>
</tbody>
</table>
   c On the Summary page, click Reboot.
   d In the System Reboot dialog box, click Yes.
   e Wait for the reboot process to finish.

4 After the reboot process completes, log in to https://lax01m01psc01.lax01.rainpole.local/ using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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**

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.

You replace certificates twice: on the Platform Services Controller lax01m01psc01.lax01.rainpole.local, and then on the Platform Services Controller lax01w01psc01.lax01.rainpole.local.

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

<table>
<thead>
<tr>
<th>Platform Services Controller</th>
<th>Certificate File Name</th>
<th>Replacement Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01m01psc01.lax01.rainpole.local</td>
<td><em>lax01psc01.1.cer</em></td>
<td>First</td>
</tr>
<tr>
<td></td>
<td><em>lax01psc01.key</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Root64.cer</em></td>
<td></td>
</tr>
<tr>
<td>lax01w01psc01.lax01.rainpole.local</td>
<td><em>lax01psc01.1.cer</em></td>
<td>Second</td>
</tr>
<tr>
<td></td>
<td><em>lax01psc01.key</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Root64.cer</em></td>
<td></td>
</tr>
</tbody>
</table>

**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 Change the Platform Services Controller shell to the bash shell to allow SCP connections.
   a Open an SSH connection to lax01m01psc01.lax01.rainpole.local and log in with the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>mgmtpsc_root_password</td>
</tr>
</tbody>
</table>

   b Run the following command to enable Bash shell access for the root user.

   ```shell
csh -s "/bin/bash" root
```
2 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.
      Use `scp` software such as WinSCP.

3 Replace the certificate on the Platform Services Controller.
   a Start the vSphere Certificate Manager utility on the 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`.
   i The Platform Services Controller services automatically restart.

4 After Certificate Manager replaces the certificate, perform the following command to restart the vami-lighttp service and to remove certificate files.
   ```
   service vami-lighttp restart
cd /root/certs
rm lax01psc01.1.cer lax01psc01.key Root64.cer
   ```

5 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 balancers 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 setup 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 values below:

<table>
<thead>
<tr>
<th>FQDN</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01psc01.lax01.rainpole.local</td>
<td>172.17.11.61</td>
</tr>
</tbody>
</table>

   **Note** After the load balancer is configured the IP address will be 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>mgmtpsc_root_password</td>
</tr>
</tbody>
</table>

   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>comppsc_root_password</td>
</tr>
</tbody>
</table>

   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>mgmtpsc_root_password</td>
</tr>
</tbody>
</table>

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 assign a 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 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi host or vCenter Server name</td>
<td>lax01m01esx01.lax01.rainpole.local</td>
</tr>
<tr>
<td>HTTPS port</td>
<td>443</td>
</tr>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>esxi_root_user_password</td>
</tr>
</tbody>
</table>
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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance name</td>
<td>lax01m01vc01</td>
</tr>
<tr>
<td>OS password</td>
<td>mgmtvc_root_password</td>
</tr>
<tr>
<td>Confirm OS password</td>
<td>mgmtvc_root_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>VM Network</td>
</tr>
<tr>
<td>IP version</td>
<td>IPv4</td>
</tr>
<tr>
<td>IP assignment</td>
<td>static</td>
</tr>
<tr>
<td>System name</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>IP address</td>
<td>172.17.11.62</td>
</tr>
<tr>
<td>Subnet mask or prefix length</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default gateway</td>
<td>172.17.11.253</td>
</tr>
<tr>
<td>DNS servers</td>
<td>172.17.11.5,172.17.11.4</td>
</tr>
</tbody>
</table>

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

l  Once 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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Synchronization mode</td>
<td>Synchronize time with NTP servers</td>
</tr>
<tr>
<td>NTP servers (comma-separated list)</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td>SSH access</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
c On the **SSO configuration** page, enter the following settings and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Services Controller</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>HTTPS port</td>
<td>443</td>
</tr>
<tr>
<td>SSO domain name</td>
<td>vsphere.local</td>
</tr>
<tr>
<td>SSO password</td>
<td>sso_password</td>
</tr>
</tbody>
</table>

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

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

4 Add new licenses for this vCenter Server instance and the management cluster ESXi hosts if needed.

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

b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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

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

e Click the **Create New Licenses** icon to add license keys.

f On the **Enter license keys** page, enter license keys for vCenter Server, ESXi and vSAN, one per line and click **Next**.

g On the **Edit license name** page, enter a descriptive name for each license key and click **Next**.

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

5 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**.

6 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 field 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.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>config.SDDC.Deployed.Type</td>
<td>VVD</td>
</tr>
<tr>
<td>config.SDDC.Deployed.Flavor</td>
<td>Standard</td>
</tr>
<tr>
<td>config.SDDC.Deployed.Version</td>
<td>4.1.0</td>
</tr>
<tr>
<td>config.SDDC.Deployed.Method</td>
<td>DIY</td>
</tr>
</tbody>
</table>

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://lax01-m01vc01.lax01.rainpole.local/vsphere-client.
   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>esxi_root_user_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host 3</td>
<td>lax01m01esx03.lax01.rainpole.local</td>
</tr>
<tr>
<td>Host 4</td>
<td>lax01m01esx04.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>lax01.rainpole.local</td>
</tr>
<tr>
<td>Using credentials</td>
<td>Selected</td>
</tr>
<tr>
<td>User name</td>
<td><a href="mailto:ad_admin_acct@lax01.rainpole.local">ad_admin_acct@lax01.rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>ad_admin_lax_password</td>
</tr>
</tbody>
</table>

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 you have added 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of uplinks</td>
<td>2</td>
</tr>
<tr>
<td>Network I/O Control</td>
<td>Enabled</td>
</tr>
<tr>
<td>Create a default port group</td>
<td>Deselected</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Port Group Name</th>
<th>Port Binding</th>
<th>VLAN Type</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01-m01-vds01-management</td>
<td>Ephemeral - no binding</td>
<td>VLAN</td>
<td>1711</td>
</tr>
<tr>
<td>lax01-m01-vds01-vmotion</td>
<td>Static binding</td>
<td>VLAN</td>
<td>1712</td>
</tr>
<tr>
<td>lax01-m01-vds01-vsan</td>
<td>Static binding</td>
<td>VLAN</td>
<td>1713</td>
</tr>
<tr>
<td>lax01-m01-vds01-nfs</td>
<td>Static binding</td>
<td>VLAN</td>
<td>1715</td>
</tr>
<tr>
<td>lax01-m01-vds01-replication</td>
<td>Static binding</td>
<td>VLAN</td>
<td>1716</td>
</tr>
<tr>
<td>lax01-m01-vds01-ext-management</td>
<td>Static binding</td>
<td>VLAN</td>
<td>150</td>
</tr>
<tr>
<td>lax01-m01-vds01-uplink01</td>
<td>Static binding</td>
<td>VLAN</td>
<td>2714</td>
</tr>
<tr>
<td>lax01-m01-vds01-uplink02</td>
<td>Static binding</td>
<td>VLAN</td>
<td>2715</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Port Group</th>
<th>Port Properties</th>
<th>IPv4 Address</th>
<th>Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01-m01-vds01-replication</td>
<td>vSphere Replication traffic</td>
<td>172.17.16.101</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>vSphere Replication NFC traffic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lax01-m01-vds01-nfs</td>
<td>N/A</td>
<td>172.17.15.101</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source network</td>
<td>VM Network</td>
</tr>
<tr>
<td>Destination network</td>
<td>lax01-m01-vds01-management</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Physical Adapter Shares</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSAN Traffic</td>
<td>High</td>
</tr>
<tr>
<td>NFS Traffic</td>
<td>Low</td>
</tr>
<tr>
<td>vMotion Traffic</td>
<td>Low</td>
</tr>
<tr>
<td>vSphere Replication (VR) Traffic</td>
<td>Low</td>
</tr>
<tr>
<td>Management Traffic</td>
<td>Normal</td>
</tr>
<tr>
<td>vSphere Data Protection Backup Traffic</td>
<td>Low</td>
</tr>
<tr>
<td>Virtual Machine Traffic</td>
<td>High</td>
</tr>
<tr>
<td>Fault Tolerance Traffic</td>
<td>Low</td>
</tr>
<tr>
<td>iSCSI Traffic</td>
<td>Low</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2 In the Navigator, click Hosts and Clusters.
   a Expand the lax01m01vc01.lax01.rainpole.local inventory.
   b Select the lax01-m01-mgmt01 cluster.

3 Click the Configure tab, click vSphere Availability, and click Edit.

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

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Host Monitoring</td>
<td>Selected</td>
</tr>
<tr>
<td>Host Failure Response</td>
<td>Restart VMs</td>
</tr>
<tr>
<td>Response for Host Isolation</td>
<td>Power off and restart VMs</td>
</tr>
<tr>
<td>Datastore with PDL</td>
<td>Disabled</td>
</tr>
<tr>
<td>Datastore with APD</td>
<td>Disabled</td>
</tr>
<tr>
<td>VM Monitoring</td>
<td>VM Monitoring Only</td>
</tr>
</tbody>
</table>

6 Click Admission Control.
7 In the Admission Control page enter following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host failures cluster tolerates</td>
<td>1</td>
</tr>
<tr>
<td>Define host failover capacity by</td>
<td>Cluster resource percentage</td>
</tr>
<tr>
<td>Override calculated failover capacity</td>
<td>Deselected</td>
</tr>
<tr>
<td>Performance degradation VMs tolerate</td>
<td>100%</td>
</tr>
</tbody>
</table>

8 Click OK.

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 save 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 a NFS datastore where vSphere Data Protection will later be deployed.

Create 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](https://lax01m01vc01.lax01.rainpole.local/vsphere-client).

   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore Name</td>
<td>lax01-m01-vdp01</td>
</tr>
<tr>
<td>Folder</td>
<td>/V2D_vDP_MgmtB_6TB</td>
</tr>
<tr>
<td>Server</td>
<td>172.17.15.251</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 choose 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.
Edit the Excel file to include the following values.

<table>
<thead>
<tr>
<th>ESXi Host</th>
<th>Active Directory Configuration Password</th>
<th>Active Directory Configuration Username</th>
<th>NetStack Instance DefaultTcpipStack-DNS Configuration Name for this host</th>
<th>NetStack Instance Vmotion-DNS Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01m01esx01.lax01.rainpole.local</td>
<td>ad_admin_password</td>
<td><a href="mailto:ad_admin_acct@lax01.rainpole.local">ad_admin_acct@lax01.rainpole.local</a></td>
<td>lax01m01esx01</td>
<td></td>
</tr>
<tr>
<td>lax01m01esx02.lax01.rainpole.local</td>
<td>ad_admin_password</td>
<td><a href="mailto:ad_admin_acct@lax01.rainpole.local">ad_admin_acct@lax01.rainpole.local</a></td>
<td>lax01m01esx02</td>
<td></td>
</tr>
<tr>
<td>lax01m01esx03.lax01.rainpole.local</td>
<td>ad_admin_password</td>
<td><a href="mailto:ad_admin_acct@lax01.rainpole.local">ad_admin_acct@lax01.rainpole.local</a></td>
<td>lax01m01esx03</td>
<td></td>
</tr>
<tr>
<td>lax01m01esx04.lax01.rainpole.local</td>
<td>ad_admin_password</td>
<td><a href="mailto:ad_admin_acct@lax01.rainpole.local">ad_admin_acct@lax01.rainpole.local</a></td>
<td>lax01m01esx04</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ESXi Host</th>
<th>Host virtual NIC lax01-m01-mgmt01:mgmt01:mgmt01-management:management-&gt;IP address settings Host IPv4 address</th>
<th>Host virtual NIC lax01-m01-mgmt01:mgmt01:mgmt01-management:management-&gt;IP address settings SubnetMask</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01m01esx01.lax01.rainpole.local</td>
<td>172.17.11.101</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>lax01m01esx02.lax01.rainpole.local</td>
<td>172.17.11.102</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>lax01m01esx03.lax01.rainpole.local</td>
<td>172.17.11.103</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>lax01m01esx04.lax01.rainpole.local</td>
<td>172.17.11.104</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ESXi Host</th>
<th>Host virtual NIC lax01-m01-mgmt01-mgmt01-nfs:&lt;UNRESOLVED&gt;-&gt;IP address settings Host IPv4 address</th>
<th>Host virtual NIC lax01-m01-mgmt01-mgmt01-nfs:&lt;UNRESOLVED&gt;-&gt;IP address settings SubnetMask</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01m01esx01.lax01.rainpole.local</td>
<td>172.17.15.101</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>lax01m01esx02.lax01.rainpole.local</td>
<td>172.17.15.102</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>lax01m01esx03.lax01.rainpole.local</td>
<td>172.17.15.103</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>lax01m01esx04.lax01.rainpole.local</td>
<td>172.17.15.104</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ESXi Host</th>
<th>Host virtual NIC lax01-m01-mgmt01-replication:vsphereReplication,vsphereReplication:NFC-&gt;IP address settings Host IPv4 address</th>
<th>Host virtual NIC lax01-m01-mgmt01-replication:vsphereReplication,vsphereReplication:NFC-&gt;IP address settings SubnetMask</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01m01esx01.lax01.rainpole.local</td>
<td>172.17.16.101</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>lax01m01esx02.lax01.rainpole.local</td>
<td>172.17.16.102</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>lax01m01esx03.lax01.rainpole.local</td>
<td>172.17.16.103</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>lax01m01esx04.lax01.rainpole.local</td>
<td>172.17.16.104</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>ESXi Host</td>
<td>Host virtual NIC lax01-m01-mgmt01:mgmt01-mgmt01-vmotion:vmotion-IP address settings</td>
<td>Host virtual NIC lax01-m01-mgmt01:mgmt01-mgmt01-vmotion:vmotion-IP address settings</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lax01m01esx01.lax01.rainpole.local</td>
<td>172.17.12.101</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>lax01m01esx02.lax01.rainpole.local</td>
<td>172.17.12.102</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>lax01m01esx03.lax01.rainpole.local</td>
<td>172.17.12.103</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>lax01m01esx04.lax01.rainpole.local</td>
<td>172.17.12.104</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

- **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** Click the **Browse** button to use a customization file, locate the `lax01-m01hp-mgmt01_host_customizations.csv` file saved earlier and select it and click **Open** then 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 should 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 sub-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-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 of the 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 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 a 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.

You repeat this procedure eight times to create all of the management application folders listed in the following table.

<table>
<thead>
<tr>
<th>Management Applications</th>
<th>Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server + Platform Services Controllers</td>
<td>lax01-m01fd-mgmt</td>
</tr>
<tr>
<td>vRealize Log Insight</td>
<td>lax01-m01fd-vrfi</td>
</tr>
<tr>
<td>vRealize Automation + vRealize Orchestrator + vRealize Business</td>
<td>lax01-m01fd-vra</td>
</tr>
<tr>
<td>vRealize Automation (Proxy Agent) + vRealize Business (Data Collector)</td>
<td>lax01-m01fd-vraias</td>
</tr>
<tr>
<td>vRealize Operations Manager</td>
<td>lax01-m01fd-vrops</td>
</tr>
<tr>
<td>vRealize Operations Manager (Remote Collectors)</td>
<td>lax01-m01fd-vropsrc</td>
</tr>
<tr>
<td>NSX Manager + Controllers + Edges</td>
<td>lax01-m01fd-nsx</td>
</tr>
<tr>
<td>VMware Site Recovery Manager + vSphere Data Protection</td>
<td>lax01-m01fd-bcdr</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2  Create a folder for the vRealize Log Insight management application.
   a  In the Navigator, click VMs and Templates.
   b  Expand the lax01m01vc01.lax01.rainpole.local tree.
   c  Right-click the lax01-m01dc data center, and select New Folder > New VM and Template Folder.
   d  In the New Folder dialog box enter lax01-m01fd-mgmt as the name to label the folder, and click OK.
   e  Repeat this step to create the remaining folders.
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 choose 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2 In the Navigator select Hosts and Clusters and expand the mgm01vc51.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 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.
   
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. In the Navigator select Hosts and Clusters and expand the mgm01vc51.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 the Enable rule check box is selected, 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. You must install the NSX kernel modules on the management cluster ESXi hosts to be able to use NSX.

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 exclusion list. The default rule in Region b also needs to 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>lax01-m01-mgmt01</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select virtual disk format</td>
<td>Thin provision</td>
</tr>
<tr>
<td>VM storage policy</td>
<td>vSAN Default Storage Policy</td>
</tr>
<tr>
<td>Datastore</td>
<td>lax01-m01-vsan01</td>
</tr>
</tbody>
</table>

10 On the **Setup networks** page, under Destination Network, select `la01-m01-vds01-management` and click **Next**.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Server List</td>
<td>172.17.11.5,172.17.11.4</td>
</tr>
<tr>
<td>Domain Search List</td>
<td>lax01.rainpole.local</td>
</tr>
<tr>
<td>Default IPv4 Gateway</td>
<td>172.17.11.253</td>
</tr>
<tr>
<td>Hostname</td>
<td>lax01m01nsx01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Network 1 IPv4 Address</td>
<td>172.17.11.65</td>
</tr>
<tr>
<td>Network 1 Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Enable SSH</td>
<td>Selected</td>
</tr>
<tr>
<td>NTP Server List</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td>CLI &quot;admin&quot; User Password / enter</td>
<td>mgmtnsx_admin_password</td>
</tr>
<tr>
<td>CLI &quot;admin&quot; User Password / confirm</td>
<td>mgmtnsx_admin_password</td>
</tr>
<tr>
<td>CLI Privilege Mode Password / enter</td>
<td>mgmtnsx_privilege_password</td>
</tr>
<tr>
<td>CLI Privilege Mode Password / confirm</td>
<td>mgmtnsx_privilege_password</td>
</tr>
</tbody>
</table>

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.

**Connect NSX Manager to the Management vCenter Server in Region B**

After you deploy the NSX Manager virtual appliance for the management cluster, you connect the NSX Manager to the Management vCenter Server.
Procedure

1. Connect the NSX Manager to the Management vCenter Server for Region B.
   a. Open a Web browser and go to https://lax01m01nsx01.lax01.rainpole.local.
   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>nsx_manager_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup Service Host</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Lookup Service Port</td>
<td>443</td>
</tr>
<tr>
<td>SSO Administrator User Name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>vCenter User Name</td>
<td><a href="mailto:svc-nsxmanager@rainpole.local">svc-nsxmanager@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-nsxmanager_password</td>
</tr>
</tbody>
</table>

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 in Region B

Assign the administrator@vsphere.local account access to NSX.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:svc-nsxmanager@rainpole.local">svc-nsxmanager@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-nsxmanager_password</td>
</tr>
</tbody>
</table>

2 In the Navigator, click Networking & Security and click NSX Managers.

3 Under NSX Managers, click the 172.17.11.65 instance.

4 Click the Manage tab, click Users and click the Add icon.

5 On the Identify User page, enter administrator@vsphere.local in the User text field 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.
   c On the Management tab, select the primary 172.16.11.65 instance.
   d Select Actions > Add Secondary NSX Manager.
In the **Add secondary NSX Manager** dialog box, enter the following settings and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager</td>
<td>172.17.11.65</td>
</tr>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>mgmtnsx_admin_password</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>mgmtnsx_admin_password</td>
</tr>
</tbody>
</table>

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

3 Empty Step

### 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. You must install the NSX kernel modules on the management cluster ESXi hosts to be able to use NSX.

**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](https://lax01m01vc01.lax01.rainpole.local/vsphere-client).
   
b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>
2 Install the NSX kernel modules on the management cluster ESXi hosts.
   a In the Navigator, click Networking & Security.
   b Click Installation and click the Host Preparation tab.
   c Select 172.17.11.65 from the NSX Manager drop-down menu.
   d Under Installation Status, click Install for the lax01-m01-mgmt01 cluster, and click Yes in the confirmation dialog box.
3 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>
2 Configure the Segment ID allocation.
   a In the Navigator, click Networking & Security.
   b Click Installation, click the Logical Network Preparation tab, 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.

**Note** Universal Segment ID pool populates automatically from the primary NSX Manager.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment ID pool</td>
<td>6000-6200</td>
</tr>
<tr>
<td>Enable Multicast addressing</td>
<td>Selected</td>
</tr>
<tr>
<td>Multicast addresses</td>
<td>239.5.0.0-239.5.255.255</td>
</tr>
</tbody>
</table>

3 Configure the VXLAN networking.

a Click the Host Preparation tab.

b Under VXLAN, click Not Configured, enter the following values, and click OK.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>lax01-m01-vds01</td>
</tr>
<tr>
<td>VLAN</td>
<td>3019</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
</tr>
<tr>
<td>VMKNic IP Addressing</td>
<td>Use DHCP</td>
</tr>
<tr>
<td>VMKNic Teaming Policy</td>
<td>Load Balance - SRCID</td>
</tr>
<tr>
<td>VTEP</td>
<td>2</td>
</tr>
</tbody>
</table>

4 Configure the transport zone.

a On the Installation 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Type</td>
<td>Edge Services Gateway</td>
</tr>
<tr>
<td>Name</td>
<td>lax01psc01</td>
</tr>
<tr>
<td>Hostname</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Deploy NSX EDGE</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable High Availability</td>
<td>Selected</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>edge_admin_password</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource pool</td>
<td>lax01-m01-mgmt01</td>
</tr>
<tr>
<td>Datastore</td>
<td>lax01-m01-vsan01</td>
</tr>
<tr>
<td>Folder</td>
<td>lax01-m01fd-nsx</td>
</tr>
</tbody>
</table>

   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource pool</td>
<td>lax01-m01-mgmt01</td>
</tr>
<tr>
<td>Datastore</td>
<td>lax01-m01-vsan01</td>
</tr>
<tr>
<td>Folder</td>
<td>lax01-m01fd-nsx</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>lax01psc01</td>
</tr>
<tr>
<td>Type</td>
<td>Internal</td>
</tr>
<tr>
<td>Connected To</td>
<td>lax01-m01-vds01-management</td>
</tr>
<tr>
<td>Connectivity Status</td>
<td>Connected</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>172.17.11.71</td>
</tr>
<tr>
<td>Subnet Prefix Length</td>
<td>24</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
</tr>
<tr>
<td>Send ICMP Redirect</td>
<td>Selected</td>
</tr>
</tbody>
</table>

10 On the Default gateway settings page, enter the following settings and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway IP</td>
<td>172.17.11.253</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
</tr>
</tbody>
</table>
11 On the **Firewall and HA** page, select the following settings and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Firewall default policy</td>
<td>Selected</td>
</tr>
<tr>
<td>Default Traffic Policy</td>
<td>Accept</td>
</tr>
<tr>
<td>Logging</td>
<td>Disable</td>
</tr>
<tr>
<td>vNIC</td>
<td>any</td>
</tr>
<tr>
<td>Declare Dead Time</td>
<td>15</td>
</tr>
</tbody>
</table>

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 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value 1</th>
<th>Value 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>psc-tcp</td>
<td>psc-https</td>
</tr>
<tr>
<td>Type</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Enable SSL Passthrough</td>
<td>Deselected</td>
<td>Selected</td>
</tr>
<tr>
<td>Persistence</td>
<td>Source IP</td>
<td>Source IP</td>
</tr>
<tr>
<td>Expires in (Seconds)</td>
<td>60</td>
<td>60</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>psc-https-443</td>
</tr>
<tr>
<td>Algorithm</td>
<td>ROUND-ROBIN</td>
</tr>
<tr>
<td>Monitors</td>
<td>default-tcp-monitor</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Values for First Server Pool</th>
<th>Values for Second Server Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>lax01m01psc01</td>
<td>lax01m01psc01</td>
</tr>
<tr>
<td>IP Address/VC Container</td>
<td>lax01m01psc01</td>
<td>lax01m01psc01</td>
</tr>
<tr>
<td>Monitor Port</td>
<td>443</td>
<td>389</td>
</tr>
<tr>
<td>Weight</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Values for First Server Pool</th>
<th>Values for Second Server Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Member</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>Name</td>
<td>lax01w01psc01</td>
<td>lax01w01psc01</td>
</tr>
<tr>
<td>IP Address/VC Container</td>
<td>lax01w01psc01</td>
<td>lax01w01psc01</td>
</tr>
<tr>
<td>Port</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
11 Repeat the procedure to create the remaining server pool.

**CreatePlatform Services ControllerVirtual 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Virtual server</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>Application Profile</td>
<td>psc-tcp</td>
<td>psc-https</td>
</tr>
<tr>
<td>Name</td>
<td>psc-tcp -389</td>
<td>psc-https-443</td>
</tr>
<tr>
<td>Description</td>
<td>389-LDAP,2012-Control Interface,2014-RPC Port,2020-Authentication,636-SSL LDAP</td>
<td>Data from the vSphere Web Client</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.17.11.71</td>
<td>172.17.11.71</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Default Pool</td>
<td>psc-tcp</td>
<td>psc-https</td>
</tr>
</tbody>
</table>
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 LoadBalancer 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully Qualified domain name (FQDN)</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.17.11.71</td>
</tr>
<tr>
<td>Update Associated Pointer (PTR) record</td>
<td>Selected</td>
</tr>
</tbody>
</table>

**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.
3. **Enable and Configure Routing in Region B**
   
   The Border Gateway Protocol (BGP) is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems (AS).
4 Verify Peering of Upstream Switches and Establishment of BGP in Region B
   The NSX Edge devices need to 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 two times to deploy two identical NSX Edge devices. Enter name and IP addresses for the respective device by using the values in the tables.

Table 2-5. NSX Edge Settings

<table>
<thead>
<tr>
<th>NSX Edge Device</th>
<th>Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Edge Device 1</td>
<td>lax01m01esg01</td>
</tr>
<tr>
<td>NSX Edge Device 2</td>
<td>lax01m01esg02</td>
</tr>
</tbody>
</table>

Table 2-6. NSX Edge Interfaces Settings

<table>
<thead>
<tr>
<th>Interface</th>
<th>NSX Edge 1</th>
<th>NSX Edge 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uplink01</td>
<td>172.27.14.2</td>
<td>172.27.14.3</td>
</tr>
<tr>
<td>Uplink02</td>
<td>172.27.15.3</td>
<td>172.27.15.2</td>
</tr>
<tr>
<td>sfo01m01udlr01</td>
<td>192.168.10.50</td>
<td>192.168.10.51</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Type</td>
<td>Edge Service Gateway</td>
</tr>
<tr>
<td>Name</td>
<td>lax01m01esg01</td>
</tr>
<tr>
<td>Deploy NSX Edge</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable High Availability</td>
<td>Deselected</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>edge_admin_password</td>
</tr>
<tr>
<td>Enable SSH access</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable FIPS mode</td>
<td>Deselected</td>
</tr>
<tr>
<td>Enable auto rule generation</td>
<td>Selected</td>
</tr>
<tr>
<td>Edge Control Level logging</td>
<td>INFO</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster/Resource Pool</td>
<td>lax01-m01-mgmt01</td>
</tr>
<tr>
<td>Datastore</td>
<td>lax01-m01-vsan01</td>
</tr>
<tr>
<td>Folder</td>
<td>lax01-m01fd-nsx</td>
</tr>
</tbody>
</table>
e On the Configure Interfaces page, click the Add icon to configure the Uplink01 interface, enter the following settings, and click OK.

<table>
<thead>
<tr>
<th>Setting</th>
<th>lax01m01esg01</th>
<th>lax01m01esg02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Uplink01</td>
<td>Uplink01</td>
</tr>
<tr>
<td>Type</td>
<td>Uplink</td>
<td>Uplink</td>
</tr>
<tr>
<td>Connected To</td>
<td>lax01-m01-vds01-uplink01</td>
<td>lax01-m01-vds01-uplink01</td>
</tr>
<tr>
<td>Connectivity Status</td>
<td>Connected</td>
<td>Connected</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>172.27.14.2</td>
<td>172.27.14.3</td>
</tr>
<tr>
<td>Subnet Prefix Length</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
<td>9000</td>
</tr>
<tr>
<td>Send ICMP Redirect</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>lax01m01esg01</th>
<th>lax01m01esg02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Uplink02</td>
<td>Uplink02</td>
</tr>
<tr>
<td>Type</td>
<td>Uplink</td>
<td>Uplink</td>
</tr>
<tr>
<td>Connected To</td>
<td>lax01-m01-vds01-uplink02</td>
<td>lax01-m01-vds01-uplink02</td>
</tr>
<tr>
<td>Connectivity Status</td>
<td>Connected</td>
<td>Connected</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>172.27.15.2</td>
<td>172.27.15.2</td>
</tr>
<tr>
<td>Subnet Prefix Length</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
<td>9000</td>
</tr>
<tr>
<td>Send ICMP Redirect</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>lax01m01esg01</th>
<th>lax01m01esg02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>sfo01m01udlr01</td>
<td>sfo01m01udlr01</td>
</tr>
<tr>
<td>Type</td>
<td>Internal</td>
<td>Internal</td>
</tr>
<tr>
<td>Connected To</td>
<td>Universal Transit Network</td>
<td>Universal Transit Network</td>
</tr>
<tr>
<td>Connectivity Status</td>
<td>Connected</td>
<td>Connected</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>192.168.10.50</td>
<td>192.168.10.51</td>
</tr>
<tr>
<td>Subnet Prefix Length</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
<td>9000</td>
</tr>
<tr>
<td>Send ICMP Redirect</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>

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.

Upon repeating the procedure to configure lax01m01esg02, the Ready to Complete page in the New NSX Edge wizard must display the following values.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>anti-affinity-rule-ecmpedges</td>
</tr>
<tr>
<td>Enable rule</td>
<td>Selected</td>
</tr>
<tr>
<td>Type</td>
<td>Separate Virtual Machine</td>
</tr>
</tbody>
</table>

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 twice for each of the NSX Edge devices lax01m01esg01 and lax01m01esg02.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 Disable button.

8 Click the Publish Changes button.

9 Repeat this procedure for the NSX Edge device lax01m01esg02.

Enable and Configure Routing in Region B

The Border Gateway Protocol (BGP) is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems (AS).

Repeat this procedure two times to enable BGP for both NSX Edge devices: lax01m01esg01 and lax01m01esg02.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 **Enable** button for **ECMP**.
   b. Click the **Edit** button for **Dynamic Routing Configuration**.
   c. Choose **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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>192.168.11.0/24</td>
</tr>
<tr>
<td>Next Hop</td>
<td>192.168.10.3</td>
</tr>
<tr>
<td>Interface</td>
<td>sfo01m01udlr01</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
</tr>
<tr>
<td>Admin Distance</td>
<td>210</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>192.168.31.0/24</td>
</tr>
<tr>
<td>Next Hop</td>
<td>192.168.10.3</td>
</tr>
<tr>
<td>Interface</td>
<td>sfo01m01udlr01</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
</tr>
<tr>
<td>Admin Distance</td>
<td>210</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>192.168.32.0/24</td>
</tr>
<tr>
<td>Next Hop</td>
<td>192.168.10.3</td>
</tr>
<tr>
<td>Interface</td>
<td>sfo01m01udlr01</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
</tr>
<tr>
<td>Admin Distance</td>
<td>210</td>
</tr>
</tbody>
</table>

   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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable BGP</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable Graceful Restart</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable Default Originate</td>
<td>Deselected</td>
</tr>
<tr>
<td>Local AS</td>
<td>65003</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>172.27.14.1</td>
</tr>
<tr>
<td>Remote AS</td>
<td>65002</td>
</tr>
<tr>
<td>Weight</td>
<td>60</td>
</tr>
<tr>
<td>Keep Alive Time</td>
<td>4</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>12</td>
</tr>
<tr>
<td>Password</td>
<td><em>BGP_password</em></td>
</tr>
</tbody>
</table>

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 172.27.12.1.
In the New Neighbor dialog box, enter the following values for the second Top of Rack Switch, and click OK.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>172.27.15.1</td>
</tr>
<tr>
<td>Remote AS</td>
<td>65002</td>
</tr>
<tr>
<td>Weight</td>
<td>60</td>
</tr>
<tr>
<td>Keep Alive Time</td>
<td>4</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>12</td>
</tr>
<tr>
<td>Password</td>
<td>BGP_password</td>
</tr>
</tbody>
</table>

Click the Add icon to add another Neighbor.

The New Neighbor dialog box appears. Configure the universal distributed logical router (lax01m01udlr01) as a neighbor.
In the **New Neighbor** dialog box, enter the following values, and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.10.4</td>
</tr>
<tr>
<td>Remote AS</td>
<td>65003</td>
</tr>
<tr>
<td>Weight</td>
<td>10</td>
</tr>
<tr>
<td>Keep Alive Time</td>
<td>1</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>3</td>
</tr>
<tr>
<td>Password</td>
<td><code>BGP_password</code></td>
</tr>
</tbody>
</table>

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 Under Route Redistribution table, click the Add icon.
   d In the New Redistribution Criteria dialog box, enter the following settings and click OK.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>Any</td>
</tr>
<tr>
<td>Learner Protocol</td>
<td>BGP</td>
</tr>
<tr>
<td>OSPF</td>
<td>Deselected</td>
</tr>
<tr>
<td>Static routes</td>
<td>Selected</td>
</tr>
<tr>
<td>Connected</td>
<td>Selected</td>
</tr>
<tr>
<td>Action</td>
<td>Permit</td>
</tr>
</tbody>
</table>

   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 need to 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>edge_admin_password</td>
</tr>
</tbody>
</table>

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

   The BGP State will display Established, UP if you have peered with the upstream switches.

   **Note** You have not yet created the universal distributed logical router (UDLR), so it will not display the Established, UP status message.

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 image below 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.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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`.

<table>
<thead>
<tr>
<th>Setting</th>
<th>lax01m01esg01 Value</th>
<th>lax01m01esg02 Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.10.50</td>
<td>192.168.10.51</td>
</tr>
<tr>
<td>Forwarding Address</td>
<td>192.168.10.3</td>
<td>192.168.10.3</td>
</tr>
<tr>
<td>Protocol Address</td>
<td>192.168.10.4</td>
<td>192.168.10.4</td>
</tr>
<tr>
<td>Remote AS</td>
<td>65003</td>
<td>65003</td>
</tr>
<tr>
<td>Weight</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Keep Alive Time</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Password</td>
<td><code>BGP_password</code></td>
<td><code>BGP_password</code></td>
</tr>
</tbody>
</table>

   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><code>admin</code></td>
</tr>
<tr>
<td>Password</td>
<td><code>udlr_admin_password</code></td>
</tr>
</tbody>
</table>

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

The BGP State will display `Established, UP` if you have successfully peered with the Edge Service Gateway.
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.
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.
   a. Open a Web browser and go to https://lax01m01vc01.lax01.rainpole.local/vsphere-client.
   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. Configure the Universal Distributed Logical Router static routes.
   b. In the Navigator, click NSX Edges.
   c. Select 172.16.11.65 from the NSX Manager drop-down menu.
   d. Double-click sfo01m01udlr01.
   e. Click the Manage tab, click Routing, and select Static Routes.
   f. On the Static Routes page, click the Add button.
g In the **Add Static Route** dialog box, enter the following values and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>172.17.11.0/24</td>
</tr>
<tr>
<td>Next Hop</td>
<td>192.168.10.50, 192.168.10.51</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
</tr>
<tr>
<td>Admin Distance</td>
<td>1</td>
</tr>
</tbody>
</table>

h Click **Publish Changes**.

**Update Distributed Firewall for Region B**

After deploying the vCenter Server you must add it to the exclusion list. The default rule in Region b also needs to 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. Exclude vCenter Server in Region B from firewall protection.
   a. Click NSX Managers and select the 172.17.11.65 instance.
   b. Click Manage and click Exclusion List.
   c. Click the Add button.
   d. 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>
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 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 `show ip route` to verify 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 ESG's.

```
NSX-edge-7b98db5b-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
B    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  [20/0]    via 192.168.100.50
B    172.27.21.0/24  [20/0]    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  [10/0]    via 192.168.100.4
```

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.

![Show ip route command output]

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Mgmt-RegionB01-VXLAN</td>
</tr>
<tr>
<td>Transport Zone</td>
<td>Mgmt Universal Transport Zone</td>
</tr>
<tr>
<td>Replication Mode</td>
<td>Hybrid</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Mgmt-RegionB01-VXLAN</td>
</tr>
<tr>
<td>Type</td>
<td>Internal</td>
</tr>
<tr>
<td>Connectivity Status</td>
<td>Connected</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>192.168.32.1</td>
</tr>
<tr>
<td>Subnet Prefix Length</td>
<td>24</td>
</tr>
</tbody>
</table>

e On the Ready to Complete page click **Finish**.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>


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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Type</td>
<td>Edge Services Gateway</td>
</tr>
<tr>
<td>Name</td>
<td>lax01m01lb01</td>
</tr>
<tr>
<td>Hostname</td>
<td>lax01m01lb01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Deploy NSX Edge</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable High Availability</td>
<td>Selected</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>edge_admin_password</td>
</tr>
<tr>
<td>Enable SSH access</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable FIPS mode</td>
<td>Deselected</td>
</tr>
<tr>
<td>Enable auto rule generation</td>
<td>Selected</td>
</tr>
<tr>
<td>Edge Control Level logging</td>
<td>INFO</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource pool</td>
<td>lax01-m01-mgmt01</td>
</tr>
<tr>
<td>Datastore</td>
<td>lax01-m01-vsan01</td>
</tr>
<tr>
<td>Folder</td>
<td>lax01-m01fd-nsx</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>OneArmLB</td>
</tr>
<tr>
<td>Type</td>
<td>Internal</td>
</tr>
<tr>
<td>Connected To</td>
<td>Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>Connectivity Status</td>
<td>Connected</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>192.168.11.2</td>
</tr>
<tr>
<td>Subnet Prefix Length</td>
<td>24</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
</tr>
<tr>
<td>Send ICMP Redirect</td>
<td>Selected</td>
</tr>
</tbody>
</table>
On the Default Gateway Settings page, enter the following settings and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway IP</td>
<td>192.168.11.1</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
</tr>
</tbody>
</table>
11 On the **Firewall and HA** page, select the following settings and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Firewall default policy</td>
<td>Selected</td>
</tr>
<tr>
<td>Default Traffic Policy</td>
<td>Accept</td>
</tr>
<tr>
<td>Logging</td>
<td>Disable</td>
</tr>
<tr>
<td>vNIC</td>
<td>any</td>
</tr>
<tr>
<td>Declare Dead Time</td>
<td>15</td>
</tr>
</tbody>
</table>

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 **tax01m01lb01**.
   d Click the **Manage** tab and click the **Settings** tab.
14 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.

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 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 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.

3 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 may add new licenses for this vCenter Server instance if needed.

4 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.
5 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.

6 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.

7 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.

8 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.

9 Change Advanced Options on the ESXi Hosts in the Shared Edge and Compute Cluster in Region B
   Change the default ESX Admins group to achieve greater levels of security by removing a known
   administrative access point.

10 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.

11 Create and Apply the Host Profile for the Shared Edge and Compute Cluster in Region B
    Host Profiles ensure all hosts in the cluster have the same configuration.

12 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.

**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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi host or vCenter Server name</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>HTTPS port</td>
<td>443</td>
</tr>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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

g  On the **Select folder** page choose **lax01-m01fd-mgmt**.

h  On the **Select compute resource** page choose the **lax01-m01-mgmt01** cluster.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance name</td>
<td>lax01w01vc01</td>
</tr>
<tr>
<td>OS password</td>
<td>compvc_root_password</td>
</tr>
<tr>
<td>Confirm OS password</td>
<td>compvc_root_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>lax01-m01-vds01-management</td>
</tr>
<tr>
<td>IP version</td>
<td>IPv4</td>
</tr>
<tr>
<td>IP assignment</td>
<td>Static</td>
</tr>
<tr>
<td>System name</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>IP address</td>
<td>172.17.11.64</td>
</tr>
<tr>
<td>Subnet mask or prefix length</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default gateway</td>
<td>172.17.11.253</td>
</tr>
<tr>
<td>DNS servers</td>
<td>172.17.11.5,172.17.11.4</td>
</tr>
</tbody>
</table>

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

n  Once 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Synchronization mode</td>
<td>Synchronize time with NTP servers</td>
</tr>
<tr>
<td>NTP servers (comma-separated list)</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td>SSH access</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Services Controller</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>HTTPS port</td>
<td>443</td>
</tr>
<tr>
<td>SSO domain name</td>
<td>vsphere.local</td>
</tr>
<tr>
<td>SSO password</td>
<td>sso_password</td>
</tr>
</tbody>
</table>

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

e Click OK on the Warning.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>config.SDDC.Deployed.Type</td>
<td>VVD</td>
</tr>
<tr>
<td>config.SDDC.Deployed.Flavor</td>
<td>Standard</td>
</tr>
<tr>
<td>config.SDDC.Deployed.Version</td>
<td>4.1.0</td>
</tr>
<tr>
<td>config.SDDC.Deployed.Method</td>
<td>DIY</td>
</tr>
</tbody>
</table>

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 may 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](https://lax01w01vc01.lax01.rainpole.local/vsphere-client).
   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2 Click the **Home** icon above the **Navigator** and choose 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. In the Navigator, click Networking & Security.

3. Click NSX Managers and select the 172.17.11.65 instance.

4. Click Manage and then click Exclusion List.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>lax01-w01-comp01</td>
</tr>
<tr>
<td>DRS</td>
<td>Turn ON Selected</td>
</tr>
<tr>
<td>Other DRS options</td>
<td>Default values</td>
</tr>
<tr>
<td>vSphere HA</td>
<td>Turn ON Deselected</td>
</tr>
<tr>
<td>EVC</td>
<td>Set EVC mode to the lowest available setting supported for the hosts in the cluster</td>
</tr>
<tr>
<td>vSAN</td>
<td>Turn ON Deselected</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>esxi_root_user_password</td>
</tr>
</tbody>
</table>

   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host 2</td>
<td>lax01w01esx02.lax01.rainpole.local</td>
</tr>
<tr>
<td>Host 3</td>
<td>lax01w01esx03.lax01.rainpole.local</td>
</tr>
<tr>
<td>Host 4</td>
<td>lax01w01esx04.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>lax01.rainpole.local</td>
</tr>
<tr>
<td>User name</td>
<td><code>ad_admin_acct@lax01.rainpole.local</code></td>
</tr>
<tr>
<td>Password</td>
<td><code>ad_admin_lax_password</code></td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td><code>lax01-w01rp-sddc-edge</code></td>
</tr>
<tr>
<td>CPU-Shares</td>
<td>High</td>
</tr>
<tr>
<td>CPU-Reservation</td>
<td>0</td>
</tr>
<tr>
<td>CPU-Reservation Type</td>
<td>Expandable selected</td>
</tr>
<tr>
<td>CPU-Limit</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Memory-Shares</td>
<td>Normal</td>
</tr>
<tr>
<td>Memory-Reservation</td>
<td>16 GB</td>
</tr>
<tr>
<td>Memory-Reservation type</td>
<td>Expandable selected</td>
</tr>
<tr>
<td>Memory-Limit</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

9. Repeat step Step 8 to add two more additional resource pools.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Resource Pool 2</th>
<th>Resource Pool 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td><code>lax01-w01rp-user-edge</code></td>
<td><code>lax01-w01rp-user-vm</code></td>
</tr>
<tr>
<td>CPU-Shares</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>CPU-Reservation</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CPU-Reservation Type</td>
<td>Expandable selected</td>
<td>Expandable selected</td>
</tr>
<tr>
<td>CPU-Limit</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Memory-Shares</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>Memory-Reservation</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Memory-Reservation type</td>
<td>Expandable selected</td>
<td>Expandable selected</td>
</tr>
<tr>
<td>Memory-Limit</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of uplinks</td>
<td>2</td>
</tr>
<tr>
<td>Network I/O Control</td>
<td>Enabled</td>
</tr>
<tr>
<td>Create a default port group</td>
<td>Deselected</td>
</tr>
</tbody>
</table>

   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.

<table>
<thead>
<tr>
<th>Port Group Name</th>
<th>Port Binding</th>
<th>VLAN Type</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01-w01-vds01-management</td>
<td>Static binding</td>
<td>VLAN</td>
<td>1731</td>
</tr>
<tr>
<td>lax01-w01-vds01-vmotion</td>
<td>Static binding</td>
<td>VLAN</td>
<td>1732</td>
</tr>
<tr>
<td>lax01-w01-vds01-vsan</td>
<td>Static binding</td>
<td>VLAN</td>
<td>1733</td>
</tr>
<tr>
<td>lax01-w01-vds01-nfs</td>
<td>Static binding</td>
<td>VLAN</td>
<td>1725</td>
</tr>
<tr>
<td>lax01-w01-vds01-uplink01</td>
<td>Static binding</td>
<td>VLAN</td>
<td>1735</td>
</tr>
<tr>
<td>lax01-w01-vds01-uplink02</td>
<td>Static binding</td>
<td>VLAN</td>
<td>2721</td>
</tr>
</tbody>
</table>

**Note** You create the VXLAN port group at a later time during the configuration of NSX Manager.

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**.
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 and 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 and 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.

Under System Traffic, edit each of the following traffic types with the values from the table.

<table>
<thead>
<tr>
<th>Traffic Types</th>
<th>Shares</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSAN Traffic</td>
<td>Low</td>
</tr>
<tr>
<td>NFS Traffic</td>
<td>Low</td>
</tr>
<tr>
<td>vMotion Traffic</td>
<td>Low</td>
</tr>
<tr>
<td>vSphere Replication Traffic</td>
<td>Low</td>
</tr>
<tr>
<td>Management Traffic</td>
<td>Normal</td>
</tr>
<tr>
<td>vSphere Data Protection Backup Traffic</td>
<td>Low</td>
</tr>
<tr>
<td>Virtual Machine Traffic</td>
<td>High</td>
</tr>
<tr>
<td>Fault Tolerance Traffic</td>
<td>Low</td>
</tr>
<tr>
<td>iSCSI Traffic</td>
<td>Low</td>
</tr>
</tbody>
</table>

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 only 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 Select Enabled for VLAN and MTU and Teaming and failover 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  Click on lax01w01esx01.lax01.rainpole.local and then click on Configure.
   c  On the Configure page select Virtual Switches.
   d  On the Virtual Switches page, select vSwitch0 and then 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Host Monitoring</td>
<td>Selected</td>
</tr>
<tr>
<td>Host Failure Response</td>
<td>Restart VM's</td>
</tr>
<tr>
<td>Response for Host Isolation</td>
<td>Power off and restart VM's</td>
</tr>
<tr>
<td>Datastore with PDL</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
7 Click **Admission Control**.

8 Under the **Admission Control** settings, enter the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host failures cluster tolerates</td>
<td>1</td>
</tr>
<tr>
<td>Define host failover capacity by</td>
<td>Cluster resource percentage</td>
</tr>
<tr>
<td>Override calculated failover capacity</td>
<td>Deselected</td>
</tr>
<tr>
<td>Performance degradation VMs tolerate</td>
<td>100%</td>
</tr>
</tbody>
</table>

9 Click **OK**.

### Change Advanced Options on the ESXi Hosts in the Shared Edge and Compute Cluster in Region B

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](https://lax01w01vc01.lax01.rainpole.local/vsphere-client).
   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2 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**.
3 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 filer 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore Name</td>
<td>lax01-w01-lib01</td>
</tr>
<tr>
<td>Folder</td>
<td>/V2D_vRA_ComputeB_1TB</td>
</tr>
<tr>
<td>server</td>
<td>172.17.25.251</td>
</tr>
</tbody>
</table>
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 all hosts in the cluster have the same configuration.

**Procedure**

1. Log in to the Compute vCenter Server by using the vSphere Web Client.
   - Open a Web browser and go to `https://lax01w01vc01.lax01.rainpole.local/vsphere-client`.
   - 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`
   - In the **Navigator** select **Hosts and Clusters** and expand the `lax01w01vc01.lax01.rainpole.local` tree.
   - Right Click the ESXi host `lax01w01esx01.lax01.rainpole.local` and choose **Host Profiles > Extract Host Profile**.
   - In the **Extract Host Profile** window enter `lax01-w01hp-comp01` for the **Name** and click **Next**.
   - In the **Ready to complete** window click **Finish**.

3. Attach the Host Profile to the shared edge and compute cluster.
   - In the **Navigator** select **Hosts and Clusters** and expand the `lax01w01vc01.lax01.rainpole.local` tree.
   - Right Click on the `lax01-w01-comp01` cluster and choose **Host Profiles > Attach Host Profile**.
   - 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.
   - In the **Navigator** select **Policies and Profiles**.
   - Click on **Host Profiles** then right click on `lax01-w01hp-comp01` and choose **Export Host Customizations**.
   - In the dialog box click **Save**.
   - Choose a file location to save the `lax01-w01hp-comp01_host_customizations.csv` file.
   - Open the `lax01-w01hp-comp01_host_customizations.csv` in Excel.
f  Edit the file using the following configuration value.

<table>
<thead>
<tr>
<th>ESXi Host</th>
<th>Active Directory Configuration Password</th>
<th>Active Directory Configuration Username</th>
<th>NetStack Instance DefaultTcpipStack-&gt;DNS Configuration Name for this host</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01w01esx01.lax01.rainpole.local</td>
<td>ad_admin_password</td>
<td><a href="mailto:ad_admin_acct@lax01.rainpole.local">ad_admin_acct@lax01.rainpole.local</a></td>
<td>lax01w01esx01</td>
</tr>
<tr>
<td>lax01w01esx02.lax01.rainpole.local</td>
<td>ad_admin_password</td>
<td><a href="mailto:ad_admin_acct@lax01.rainpole.local">ad_admin_acct@lax01.rainpole.local</a></td>
<td>lax01w01esx02</td>
</tr>
<tr>
<td>lax01w01esx03.lax01.rainpole.local</td>
<td>ad_admin_password</td>
<td><a href="mailto:ad_admin_acct@lax01.rainpole.local">ad_admin_acct@lax01.rainpole.local</a></td>
<td>lax01w01esx03</td>
</tr>
<tr>
<td>lax01w01esx04.lax01.rainpole.local</td>
<td>ad_admin_password</td>
<td><a href="mailto:ad_admin_acct@lax01.rainpole.local">ad_admin_acct@lax01.rainpole.local</a></td>
<td>lax01w01esx04</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ESXi Host</th>
<th>Host virtual NIC lax01-w01-vds01:management:management-&gt;IP address settings</th>
<th>IPv4 address</th>
<th>SubnetMask</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01w01esx01.lax01.rainpole.local</td>
<td>172.17.31.101</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>lax01w01esx02.lax01.rainpole.local</td>
<td>172.17.31.102</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>lax01w01esx03.lax01.rainpole.local</td>
<td>172.17.31.103</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>lax01w01esx04.lax01.rainpole.local</td>
<td>172.17.31.104</td>
<td>255.255.255.0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ESXi Host</th>
<th>Host virtual NIC lax01-w01-vds01:nfs:&lt;UNRESOLVED&gt;-&gt;IP address settings</th>
<th>IPv4 address</th>
<th>SubnetMask</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01w01esx01.lax01.rainpole.local</td>
<td>172.17.25.101</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>lax01w01esx02.lax01.rainpole.local</td>
<td>172.17.25.102</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>lax01w01esx03.lax01.rainpole.local</td>
<td>172.17.25.103</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>lax01w01esx04.lax01.rainpole.local</td>
<td>172.17.25.104</td>
<td>255.255.255.0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ESXi Host</th>
<th>Host virtual NIC lax01-w01-vds01:vmotion:vmotion-&gt;IP address settings</th>
<th>IPv4 address</th>
<th>SubnetMask</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01w01esx01.lax01.rainpole.local</td>
<td>172.17.32.101</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>lax01w01esx02.lax01.rainpole.local</td>
<td>172.17.32.102</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>lax01w01esx03.lax01.rainpole.local</td>
<td>172.17.32.103</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>lax01w01esx04.lax01.rainpole.local</td>
<td>172.17.32.104</td>
<td>255.255.255.0</td>
<td></td>
</tr>
</tbody>
</table>


Once the file has been 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  Click the **Browse** button to use a customization file, locate the *lax01-w01hp-comp01_host_customizations.csv* file saved earlier and select it and click **Open** then click **Finish**.

5  Remediating 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 should now 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 then click the **Scheduled Tasks** tab.

   b  Click **Schedule a New Task** then 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** 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.

### 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 table below lists all of the hosts.
### Table 2-7. Hosts in the data center

<table>
<thead>
<tr>
<th>Host</th>
<th>FQDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management host 1</td>
<td>lax01m01esx01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Management host 2</td>
<td>lax01m01esx02.lax01.rainpole.local</td>
</tr>
<tr>
<td>Management host 3</td>
<td>lax01m01esx03.lax01.rainpole.local</td>
</tr>
<tr>
<td>Management host 4</td>
<td>lax01m01esx04.lax01.rainpole.local</td>
</tr>
<tr>
<td>Shared Edge and Compute host 1</td>
<td>lax01w01esx01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Shared Edge and Compute host 2</td>
<td>lax01w01esx02.lax01.rainpole.local</td>
</tr>
<tr>
<td>Shared Edge and Compute host 3</td>
<td>lax01w01esx03.lax01.rainpole.local</td>
</tr>
<tr>
<td>Shared Edge and Compute host 4</td>
<td>lax01w01esx04.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

### Procedure

1. **Log in to the Compute vCenter Server by using the vSphere Web Client.**
   - Open a Web browser and go to https://lax01w01vc01.lax01.rainpole.local/vsphere-client.
   - Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

### 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
   You must first deploy the NSX Manager virtual appliance. After the NSX Manager is successfully deployed you must connect it to the Compute vCenter Server instance.
2  Join the Shared Edge and Compute Cluster NSX Manager to the Primary NSX Instance in Region B
   This validated design instructs that you join the secondary Shared Edge and Compute 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
   You must install the NSX kernel modules on the compute and edge clusters ESXi hosts to be able to use NSX.
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

You must first deploy the NSX Manager virtual appliance. After the NSX Manager is successfully deployed you must connect it to the Compute vCenter Server instance.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

VMware, Inc.  109
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**.

3. Use the **Deploy OVF Template** wizard to deploy the NSX Manager virtual appliance.
   a. On the **Select Source** page, click the **Browse** button, select the VMware NSX Manager `.ova` file, and click **Next**.
   b. On the **Select Name and location** page, enter the following settings, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td><code>lax01m01nsx01</code></td>
</tr>
<tr>
<td>Folder or Datacenter</td>
<td><code>lax01-m01fd-nsx</code></td>
</tr>
</tbody>
</table>

c. On the **Select Resource** page, select the following values, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datacenter</td>
<td><code>lax01-m01dc</code></td>
</tr>
<tr>
<td>Cluster</td>
<td><code>lax01-m01-mgmt01</code></td>
</tr>
</tbody>
</table>

d. On the **Review Details** page, select the **Accept extra configuration option** check box, and click **Next**.

e. On the **Accept License Agreements** page, click **Accept**, and click **Next**.

f. On the **Select Storage** page, enter the following settings and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Storage Policy</td>
<td>vSAN Default Storage Policy</td>
</tr>
<tr>
<td>Datastore</td>
<td><code>lax01-m01-vsxn01</code></td>
</tr>
</tbody>
</table>

g. On the **Setup Networks** page, under **Destination**, select `lax01-m01-vds01-management`, and click **Next**.
h On the **Customize Template** page, expand the different options, enter the following settings, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Server List</td>
<td>172.17.11.5, 172.17.11.4</td>
</tr>
<tr>
<td>Domain Search List</td>
<td>lax01.rainpole.local</td>
</tr>
<tr>
<td>Default IPv4 Gateway</td>
<td>172.17.11.253</td>
</tr>
<tr>
<td>Hostname</td>
<td>lax01w01nsx01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Network 1 IPv4 Address</td>
<td>172.17.11.66</td>
</tr>
<tr>
<td>Network 1 Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Enable SSH</td>
<td>Selected</td>
</tr>
<tr>
<td>NTP Server List</td>
<td>ntp.lax01.rainpole.local, ntp.sfo01.rainpole.local</td>
</tr>
<tr>
<td>CLI &quot;admin&quot; User Password / enter</td>
<td>compnsx_admin_password</td>
</tr>
<tr>
<td>CLI &quot;admin&quot; User Password / confirm</td>
<td>compnsx_admin_password</td>
</tr>
<tr>
<td>CLI Privilege Mode Password / enter</td>
<td>compnsx_privilege_password</td>
</tr>
<tr>
<td>CLI Privilege Mode Password / confirm</td>
<td>compnsx_privilege_password</td>
</tr>
</tbody>
</table>

i On the **Ready to Complete** page click **Finish**.

j In the **Navigator**, expand the **lax01w01vc01.lax01.rainpole.local** control tree, select the **lax01w01nsx01** virtual machine, and click the **Power on** button.

4 Connect the NSX Manager to the Compute vCenter Server.

a Open a Web browser and go to **https://lax01w01nsx01.lax01.rainpole.local**.

b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>compnsx_admin_password</td>
</tr>
</tbody>
</table>

c Click **Manage vCenter Registration**.

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

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup Service IP</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Lookup Service Port</td>
<td>443</td>
</tr>
<tr>
<td>SSO Administrator User Name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

f In the **Trust Certificate?** dialog box, click **Yes**.
g. Under vCenter Server, click the Edit button.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>vCenter User Name</td>
<td><a href="mailto:svc-nsxmanager@rainpole.local">svc-nsxmanager@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-nsxmanager_password</td>
</tr>
</tbody>
</table>

i. In the Trust Certificate? dialog box, click Yes.

j. Wait until the Status indicators for the Lookup Service and vCenter Server change to Connected.

5. Log out from the vCenter Server session in the vSphere Web Client.

6. 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:svc-nsxmanager@rainpole.local">svc-nsxmanager@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-nsxmanager_password</td>
</tr>
</tbody>
</table>

7. Assign the administrator@vsphere.local account access to NSX.

   a. In the Navigator, click Network & Security.

   b. Select NSX Managers.

   c. Select 172.17.11.66 from the tree.

   d. Click the Manage tab and click Users.

   e. Click the Add icon.

   f. In the Assign Role dialog box enter administrator@vsphere.local and click Next.

   g. Click Enterprise Administrator and click Finish.

8. Log out from the vCenter Server session in the vSphere Web Client.

Join the Shared Edge and Compute Cluster NSX Manager to the Primary NSX Instance in Region B

This validated design instructs that you join the secondary Shared Edge and Compute 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.
   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager</td>
<td>172.17.11.66</td>
</tr>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>mgmtnsx_admin_password</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>mgmtnsx_admin_password</td>
</tr>
</tbody>
</table>

   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

You must install the NSX kernel modules on the compute and edge clusters ESXi hosts to be able to use 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. Install the NSX kernel modules on the shared edge and compute cluster ESXi hosts.
   a. In the Navigator, click Networking & Security, click Installation, and click the Host Preparation tab.
   b. Change the NSX Manager that you edit to 172.17.11.66.
   c. Under Installation Status, click Install for the lax01-w01-comp01 cluster and click Yes in the confirmation dialog box.

3. 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>
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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment ID pool</td>
<td>10000-14000</td>
</tr>
<tr>
<td>Enable Multicast addressing</td>
<td>Selected</td>
</tr>
<tr>
<td>Multicast addresses</td>
<td>239.6.0.0-239.6.255.255</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>lax01-w01-vds01</td>
</tr>
<tr>
<td>VLAN</td>
<td>1734</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
</tr>
<tr>
<td>VMKNic IP Addressing</td>
<td>Use DHCP</td>
</tr>
<tr>
<td>VMKNic Teaming Policy</td>
<td>Load Balance - SRCID</td>
</tr>
<tr>
<td>VTEP</td>
<td>2</td>
</tr>
</tbody>
</table>

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 In the **Navigator**, click the **Logical Network Preparation** tab and click **Transport Zones**.
   b From the **NSX Manager** drop-down menu, select `172.16.11.66`.
   c Right-click the **Comp Global Transport Zone**, and choose **Disable CDO Mode**.

   **Note** In order to successfully create the Global transport zone, CDO Mode must be temporarily disabled from the Primary NSX Manager. CDO Mode is re-enabled after creating the Global transport zone.
   d From the **NSX Manager** drop-down menu, select `172.17.11.66`. 
e Click the Add New Transport zone icon, enter the following settings, and click OK.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Comp Global Transport Zone</td>
</tr>
<tr>
<td>Replication mode</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Select clusters part of the</td>
<td>lax01-w01-comp01</td>
</tr>
<tr>
<td>Transport Zone</td>
<td></td>
</tr>
</tbody>
</table>

f From the NSX Manager drop-down menu, select 172.16.11.66.

g Right-click the Comp Global Transport Zone, and choose Enable CDO Mode.

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2 Update the Host Profile for the management cluster.
   a In the Navigator select Policies and Profiles.
   b Click on Host Profiles then 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 Click the Monitor tab and click Compliance.
   b Select lax01-w01-comp01 and click the Check Host Profile Compliance button.
      All hosts should show the status Compliant.

**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).
Deployment for Region B

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 need to 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.

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) needs to 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) needs to 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         |

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Global Transit Network</td>
</tr>
<tr>
<td>Transport Zone</td>
<td>Comp Global Transport Zone</td>
</tr>
<tr>
<td>Replication Mode</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Enable IP Discovery</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable MAC Learning</td>
<td>Deselected</td>
</tr>
</tbody>
</table>

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: lax01w01esg01 and lax01w01esg02.

Table 2-8. NSX Edge Devices

<table>
<thead>
<tr>
<th>NSX Edge Device</th>
<th>Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Edge Device 1</td>
<td>lax01w01esg01</td>
</tr>
<tr>
<td>NSX Edge Device 2</td>
<td>lax01w01esg02</td>
</tr>
</tbody>
</table>
Table 2-9. NSX Edge Interface Settings

<table>
<thead>
<tr>
<th>Interface</th>
<th>Primary IP Address lax01w01esg01</th>
<th>Primary IP Address lax01w01esg02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uplink01</td>
<td>172.17.35.2</td>
<td>172.17.35.3</td>
</tr>
<tr>
<td>Uplink02</td>
<td>172.27.21.3</td>
<td>172.27.21.2</td>
</tr>
<tr>
<td>sfo01w01udlr01</td>
<td>192.168.100.50</td>
<td>192.168.100.51</td>
</tr>
<tr>
<td>lax01w01dir01</td>
<td>192.168.102.1</td>
<td>192.168.102.2</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>


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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Type</td>
<td>Edge Service Gateway</td>
</tr>
<tr>
<td>Name</td>
<td>lax01w01esg01</td>
</tr>
<tr>
<td>Deploy NSX Edge</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable High Availability</td>
<td>Deselected</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>edge_admin_password</td>
</tr>
<tr>
<td>Enable SSH access</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable FIPS mode</td>
<td>Deselected</td>
</tr>
<tr>
<td>Enable auto rule generation</td>
<td>Selected</td>
</tr>
<tr>
<td>Edge Control Level logging</td>
<td>INFO</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster/Resource Pool</td>
<td>lax01-w01rp-sddc-edge</td>
</tr>
<tr>
<td>Datastore</td>
<td>lax01_shared_edge_and_compute_datastore</td>
</tr>
</tbody>
</table>
e Click the **Add** icon to configure the Uplink01 interface, enter the following settings and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>lax01w01esg01</th>
<th>lax01w01esg02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Uplink01</td>
<td>Uplink01</td>
</tr>
<tr>
<td>Type</td>
<td>Uplink</td>
<td>Uplink</td>
</tr>
<tr>
<td>Connected To</td>
<td>lax01-w01-vds01-uplink01</td>
<td>lax01-w01-vds01-uplink01</td>
</tr>
<tr>
<td>Connectivity Status</td>
<td>Connected</td>
<td>Connected</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>172.17.35.2</td>
<td>172.17.35.3</td>
</tr>
<tr>
<td>Subnet Prefix Length</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
<td>9000</td>
</tr>
<tr>
<td>Send ICMP Redirect</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>lax01w01esg01</th>
<th>lax01w01esg02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Uplink02</td>
<td>Uplink02</td>
</tr>
<tr>
<td>Type</td>
<td>Uplink</td>
<td>Uplink</td>
</tr>
<tr>
<td>Distributed Portgroup</td>
<td>lax01-w01-vds01-uplink02</td>
<td>lax01-w01-vds01-uplink02</td>
</tr>
<tr>
<td>Connectivity Status</td>
<td>Connected</td>
<td>Connected</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>172.27.21.3</td>
<td>172.27.21.2</td>
</tr>
<tr>
<td>Subnet Prefix Length</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
<td>9000</td>
</tr>
<tr>
<td>Send ICMP Redirect</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>

g Click the **Add** icon to configure the sfo01w01udlr01 interface, enter the following settings, click **OK**, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>lax01w01esg01</th>
<th>lax01w01esg02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>sfo01w01udlr01</td>
<td>sfo01w01udlr01</td>
</tr>
<tr>
<td>Type</td>
<td>Internal</td>
<td>Internal</td>
</tr>
<tr>
<td>Connected To</td>
<td>Universal Transit Network</td>
<td>Universal Transit Network</td>
</tr>
<tr>
<td>Connectivity Status</td>
<td>Connected</td>
<td>Connected</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>192.168.100.50</td>
<td>192.168.100.51</td>
</tr>
<tr>
<td>Subnet Prefix Length</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
<td>9000</td>
</tr>
<tr>
<td>Send ICMP Redirect</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>
Click the **Add** icon to configure the lax01w01dlr01 interface, enter the following settings, click **OK**, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>lax01w01esg01</th>
<th>lax01w01esg02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>lax01w01dlr01</td>
<td>lax01w01dlr01</td>
</tr>
<tr>
<td>Type</td>
<td>Internal</td>
<td>Internal</td>
</tr>
<tr>
<td>Connected To</td>
<td>Global Transit Network</td>
<td>Global Transit Network</td>
</tr>
<tr>
<td>Connectivity Status</td>
<td>Connected</td>
<td>Connected</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>192.168.102.1</td>
<td>192.168.102.2</td>
</tr>
<tr>
<td>Subnet Prefix Length</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
<td>9000</td>
</tr>
<tr>
<td>Send ICMP Redirect</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>

On the **Default Gateway Settings** page, deselect the **Configure Default Gateway** check box and click **Next**.

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

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

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

Configure DRS affinity rules for the Edge Services Gateways.

Go back to the **Home** page.

In the **Navigator**, click **Hosts and Clusters**, and expand the `lax01w01vc01.lax01.rainpole.local` tree.

Select the `lax01-w01-comp01` cluster, and click the **Configure** tab.

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

Click **Add**.

In the `lax01-w01-comp01 - Create VM/Host Rule` dialog box, enter the following settings and click **Add**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>anti-affinity-rule-ecmpedges</td>
</tr>
<tr>
<td>Enable rule</td>
<td>Selected</td>
</tr>
<tr>
<td>Type</td>
<td>Separate Virtual Machine</td>
</tr>
</tbody>
</table>

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

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 Disable 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.

Repeat this procedure two times to enable BGP for both 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 On the Global Configuration page.
   a Click the Enable 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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>UDLR_Compute_Workload_Subnet</td>
</tr>
<tr>
<td>Next Hop</td>
<td>192.168.100.3</td>
</tr>
<tr>
<td>Interface</td>
<td>sfo01w01udlr01</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
</tr>
<tr>
<td>Admin Distance</td>
<td>210</td>
</tr>
</tbody>
</table>

   **Note**  You must add all subnets that are behind the UDLR.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>DLR_Compute_Workload_Subnet</td>
</tr>
<tr>
<td>Next Hop</td>
<td>192.168.102.3</td>
</tr>
<tr>
<td>Interface</td>
<td>lax01w01dlr01</td>
</tr>
<tr>
<td>MTU</td>
<td>9000</td>
</tr>
<tr>
<td>Admin Distance</td>
<td>210</td>
</tr>
</tbody>
</table>

   **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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable BGP</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable Graceful Restart</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable Default Originate</td>
<td>Deselected</td>
</tr>
<tr>
<td>Local AS</td>
<td>65000</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>172.17.35.1</td>
</tr>
<tr>
<td>Remote AS</td>
<td>65002</td>
</tr>
<tr>
<td>Weight</td>
<td>60</td>
</tr>
<tr>
<td>Keep Alive Time</td>
<td>4</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>12</td>
</tr>
<tr>
<td>Password</td>
<td>BGP_password</td>
</tr>
</tbody>
</table>

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 172.27.21.1.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>172.27.21.1</td>
</tr>
<tr>
<td>Remote AS</td>
<td>65002</td>
</tr>
<tr>
<td>Weight</td>
<td>60</td>
</tr>
<tr>
<td>Keep Alive Time</td>
<td>4</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>12</td>
</tr>
<tr>
<td>Password</td>
<td>BGP_password</td>
</tr>
</tbody>
</table>

Click the **Add** icon to add another Neighbor.

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

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.100.4</td>
</tr>
<tr>
<td>Remote AS</td>
<td>65000</td>
</tr>
<tr>
<td>Weight</td>
<td>60</td>
</tr>
<tr>
<td>Keep Alive Time</td>
<td>1</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>3</td>
</tr>
<tr>
<td>Password</td>
<td>BGP_password</td>
</tr>
</tbody>
</table>

Click the **Add** icon to add another Neighbor.

The **New Neighbor** dialog box appears. Configure the distributed logical router (DLR) as a neighbor.
In the **New Neighbor** dialog box, enter the following values, and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.102.4</td>
</tr>
<tr>
<td>Remote AS</td>
<td>65000</td>
</tr>
<tr>
<td>Weight</td>
<td>60</td>
</tr>
<tr>
<td>Keep Alive Time</td>
<td>1</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>3</td>
</tr>
<tr>
<td>Password</td>
<td>BGP_password</td>
</tr>
</tbody>
</table>

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 Under **Route Redistribution** table, click the **Add** icon.
   d In the **New Redistribution Criteria** dialog box, enter the following settings and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>Any</td>
</tr>
<tr>
<td>Learner Protocol</td>
<td>BGP</td>
</tr>
<tr>
<td>OSPF</td>
<td>Deselected</td>
</tr>
<tr>
<td>Static routes</td>
<td>Selected</td>
</tr>
<tr>
<td>Connected</td>
<td>Selected</td>
</tr>
<tr>
<td>Action</td>
<td>Permit</td>
</tr>
</tbody>
</table>

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 need to 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: 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td><code>edge_admin_password</code></td>
</tr>
</tbody>
</table>

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

   The BGP State will display `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, as such they will not display the `Established, UP` status message.

   ![BGP Neighbor Output]

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 image below 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.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>


3. In the Navigator, click NSX Edges.

4. Select 172.16.11.66 from the NSX Manager drop-down menu.

5. Configure the routing for the Universal Distributed Logical Router.
   a. Double-click sfo01w01udlr01.
   b. Click the Manage tab and click Routing.
   c. On the Global Configuration page, perform the following configuration steps.
   d. Click the Edit button under Routing Configuration, select Enable ECMP, and click OK.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable BGP</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable Graceful Restart</td>
<td>Selected</td>
</tr>
<tr>
<td>Local AS</td>
<td>65000</td>
</tr>
</tbody>
</table>

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 UDLR for both NSX Edge devices: lax01w01esg01 and lax01w01esg02.

<table>
<thead>
<tr>
<th>Setting</th>
<th>lax01w01esg01 Value</th>
<th>lax01w01esg02 Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.100.50</td>
<td>192.168.100.51</td>
</tr>
<tr>
<td>Forwarding Address</td>
<td>192.168.100.3</td>
<td>192.168.100.3</td>
</tr>
<tr>
<td>Protocol Address</td>
<td>192.168.100.4</td>
<td>192.168.100.4</td>
</tr>
<tr>
<td>Remote AS</td>
<td>65000</td>
<td>65000</td>
</tr>
<tr>
<td>Weight</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>Keep Alive Time</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Password</td>
<td>bgp_password</td>
<td>bgp_password</td>
</tr>
</tbody>
</table>

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) needs to 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>udlr_admin_password</td>
</tr>
</tbody>
</table>

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

   The BGP State will display `Established, UP` if you have successfully peered with the Edge Service Gateway.

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 image below 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.
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**.
   
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical (Distributed) Router</td>
<td>Selected</td>
</tr>
<tr>
<td>Name</td>
<td>lax01w01dlr01</td>
</tr>
<tr>
<td>Deploy Edge Appliance</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable High Availability</td>
<td>Selected</td>
</tr>
</tbody>
</table>
7 On the **Settings** page, enter the following settings, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>dir_admin_password</td>
</tr>
<tr>
<td>Enable SSH access</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable FIPS mode</td>
<td>Deselected</td>
</tr>
<tr>
<td>Edge Control Level logging</td>
<td>INFO</td>
</tr>
</tbody>
</table>

8 On the **Configure deployment** page, click the **Add** icon.

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

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster/Resource Pool</td>
<td>lax01-w01rp-sddc-edge</td>
</tr>
<tr>
<td>Datastore</td>
<td>lax01_shared_edge_and_compute_datastore</td>
</tr>
</tbody>
</table>

10 On the **Configure deployment** page, click the **Add** icon a second time to add a second NSX Edge device.

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

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster/Resource Pool</td>
<td>lax01-w01rp-sddc-edge</td>
</tr>
<tr>
<td>Datastore</td>
<td>lax01_shared_edge_and_compute_datastore</td>
</tr>
</tbody>
</table>

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 Click the **Add** icon.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary IP Address</td>
<td>1.4.1.1</td>
</tr>
<tr>
<td>Subnet Prefix Length</td>
<td>24</td>
</tr>
</tbody>
</table>

   b Enter the following settings in the **Add Interface** dialog box, and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Uplink</td>
</tr>
<tr>
<td>Type</td>
<td>Uplink</td>
</tr>
<tr>
<td>Connected To</td>
<td>Global Transit Network</td>
</tr>
<tr>
<td>Connectivity Status</td>
<td>Connected</td>
</tr>
</tbody>
</table>
14 In the Default gateway settings page, deselect Configure Default Gateway and click Next.

15 In the Ready to complete page, click Finish.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 Edit button under Routing Configuration, select Enable ECMP, and click OK.
   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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable BGP</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable Graceful Restart</td>
<td>Selected</td>
</tr>
<tr>
<td>Local AS</td>
<td>65000</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>lax01w01esg01 Value</th>
<th>lax01w01esg02 Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.102.1</td>
<td>192.168.102.2</td>
</tr>
<tr>
<td>Forwarding Address</td>
<td>192.168.102.3</td>
<td>192.168.102.3</td>
</tr>
<tr>
<td>Protocol Address</td>
<td>192.168.102.4</td>
<td>192.168.102.4</td>
</tr>
<tr>
<td>Remote AS</td>
<td>65000</td>
<td>65000</td>
</tr>
<tr>
<td>Weight</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>Keep Alive Time</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Password</td>
<td>bgp_password</td>
<td>bgp_password</td>
</tr>
</tbody>
</table>

e Click **Publish Changes**.

7 On the left, select **Route Redistribution** to configure it.
   a Click the **Edit** button.
   b In the **Change redistribution settings** dialog box, enter the following settings, and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF</td>
<td>Deselected</td>
</tr>
<tr>
<td>BGP</td>
<td>Selected</td>
</tr>
</tbody>
</table>

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) needs to 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.
   - Open an SSH connection to lax01w01dlr01, the DLR whose peering and BGP configuration you want to verify.
   - Log in using the following credentials.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>dlr_admin_password</td>
</tr>
</tbody>
</table>

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

The BGP State will display Established, UP if you have successfully peered with the Edge Service Gateway.
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 image below 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.

---

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td><code>vsphere_admin_password</code></td>
</tr>
</tbody>
</table>
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.

3 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 BGP routing state.
   a Open an SSH connection to sfo01w01udlr01.
   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>udlr_admin_password</td>
</tr>
</tbody>
</table>
c Run `show ip route` 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 ESG's.

---

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.

---

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
   To be able to 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**

To be able to 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 2-10. Software and Configuration Requirements for Site Recovery Manager VMs**

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Join each VM to the domain in Region A or Region B (sfo01.rainpole.local or lax01.rainpole.local).</td>
</tr>
<tr>
<td>Network interface</td>
<td>Connect the VMs to the management port group on the distributed switch.</td>
</tr>
<tr>
<td>Time synchronization</td>
<td>Synchronize both VMs with the NTP servers ntp.sfo01.rainpole.local and ntp.lax01.rainpole.local.</td>
</tr>
<tr>
<td>vSphere cluster configuration</td>
<td>Provide a cluster for hosting management application with enabled vSphere DRS and vSphere HA.</td>
</tr>
<tr>
<td>Site Recovery Manager installation file</td>
<td>Download Site Recovery Manager installer to both VMs.</td>
</tr>
<tr>
<td>Email address of Site Recovery Manager administrators</td>
<td>Get the email addresses of the Site Recovery Manager site administrators.</td>
</tr>
</tbody>
</table>

**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 2-11. Network Configuration of Site Recovery Manager in Region A**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>sfo01m01srm01</td>
</tr>
<tr>
<td>Static IPv4 address</td>
<td>172.16.11.124</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default gateway</td>
<td>172.16.11.253</td>
</tr>
<tr>
<td>DNS server</td>
<td>172.16.11.5</td>
</tr>
<tr>
<td>FQDN</td>
<td>sfo01m01srm01.sfo01.rainpole.local</td>
</tr>
</tbody>
</table>
Table 2-11. Network Configuration of Site Recovery Manager in Region A (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used ports</td>
<td>■ 9086</td>
</tr>
<tr>
<td></td>
<td>■ 5678</td>
</tr>
</tbody>
</table>

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 2-12. Network Configuration of Site Recovery Manager in Region B

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>lax01m01srm01</td>
</tr>
<tr>
<td>Static IPv4 address</td>
<td>172.17.11.124</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default gateway</td>
<td>172.17.11.253</td>
</tr>
<tr>
<td>DNS server</td>
<td>172.17.11.5</td>
</tr>
<tr>
<td>FQDN</td>
<td>lax01m01srm01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Used ports</td>
<td>■ 9086</td>
</tr>
<tr>
<td></td>
<td>■ 5678</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.
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 dialog box](image)

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.

**Procedure**

1. Log in to `sfo01m01srm01.sfo01.rainpole.local` by using a Remote Desktop Protocol (RDP) client.
   
   a  Open an RDP connection to the virtual machine `sfo01m01srm01.sfo01.rainpole.local`.
   
   b  Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Windows administrator user</td>
</tr>
<tr>
<td>Password</td>
<td><code>windows_administrator_password</code></td>
</tr>
</tbody>
</table>

2. Navigate to the folder where you downloaded the VMware Site Recovery Manager installer, and open the file to start the installation wizard.

3. In the **Select Language** dialog box click **OK**.

4. On the **Welcome** page click **Next**.

5. On the **VMware Patents** page click **Next**.

6. On the **End User License Agreement** page, select the **I agree to the terms in the license agreement** radio button, and click **Next**.
7 On the **Installation Prerequisites** page click **Next**.

8 On the **Destination Folder** page click **Next**.

9 On the **vSphere Platform Services Controller** page, enter the following settings, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>sfo01psc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>443</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:svc-srm@rainpole.local">svc-srm@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-srm_password</td>
</tr>
</tbody>
</table>

10 If prompted, in the **Platform Services Controller Certificate** dialog box, click **Accept**.

11 On the **VMware vCenter Server** page, select `sfo01m01vc01.sfo01.rainpole.local` from the drop-down menu, and click **Next**.

12 If prompted, in the **vCenter Server Certificate** dialog box, click **Accept**.

13 On the **Site Recovery Manager Extension** page, enter the following settings, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Site Name</td>
<td>sfo01m01vc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>Administrator E-mail</td>
<td>srm_admin_sfo_email_address</td>
</tr>
<tr>
<td>Local Host</td>
<td>172.16.11.124</td>
</tr>
<tr>
<td>Listener Port</td>
<td>9086</td>
</tr>
</tbody>
</table>

14 On the **Site Recovery Manager Plug-in ID** page, select **Default Site Recovery Manager Plug-in Identifier**, and click **Next**.

15 On the **Certificate Type** page, select **Automatically generate a certificate**, and click **Next**.

16 On the **Generate Certificate** page, enter the following settings, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Rainpole</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Rainpole</td>
</tr>
</tbody>
</table>

17 On the **Database Server Selection** page, select **Use the embedded database server**, and click **Next**.

18 On the **Embedded Database Configuration** page, enter the following settings, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Source Name</td>
<td>SRM_SITE_SFO01</td>
</tr>
<tr>
<td>Database User Name</td>
<td>srm_admin</td>
</tr>
<tr>
<td>Database Password</td>
<td>srm_admin_sfo_password</td>
</tr>
<tr>
<td>Database Port</td>
<td>5678</td>
</tr>
<tr>
<td>Setting</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Connection Count</td>
<td>5</td>
</tr>
<tr>
<td>Max. Connections</td>
<td>20</td>
</tr>
</tbody>
</table>

19 On the **Site Recovery Manager Service Account** page, enter the following credentials, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Local System account</td>
<td>Deselected</td>
</tr>
<tr>
<td>Username</td>
<td>SFO01M01SRM01\Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>sfo01m01srm01_admin_password</td>
</tr>
</tbody>
</table>

20 On the **Ready to Install the Program** page click **Install**.

21 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.

**Procedure**

1 Log in to lax01m01srm01.lax01.rainpole.local, by using a Remote Desktop Protocol (RDP) client.
   a Open an RDP connection to the virtual machine lax01m01srm01.lax01.rainpole.local.
   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Windows administrator user</td>
</tr>
<tr>
<td>Password</td>
<td>windows_administrator_password</td>
</tr>
</tbody>
</table>

2 Navigate to the folder where you downloaded the VMware Site Recovery Manager installer, and open the file to start the installation wizard.

3 In the **Select Language** dialog box click **OK**.

4 On the **Welcome** page click **Next**.

5 On the **VMware Patents** page click **Next**.

6 On the **End User License Agreement** page, select the **I agree to the terms in the license agreement** radio button, and click **Next**.

7 On the **Installation Prerequisites** page click **Next**.

8 On the **Destination Folder** page click **Next**.
9 On the vSphere Platform Services Controller page, enter the following settings, and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>443</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:svc-srm@rainpole.local">svc-srm@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-srm_password</td>
</tr>
</tbody>
</table>

10 If prompted, in the Platform Services Controller Certificate dialog box, click Accept.

11 On the VMware vCenter Server page, select lax01m01vc01.lax01.rainpole.local from the drop-down menu, and click Next.

12 If prompted, in the vCenter Server Certificate dialog box, click Accept.

13 On the Site Recovery Manager Extension page, enter the following settings, and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Site Name</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Administrator E-mail</td>
<td>smr_admin_lax_email_address</td>
</tr>
<tr>
<td>Local Host</td>
<td>172.17.11.124</td>
</tr>
<tr>
<td>Listener Port</td>
<td>9086</td>
</tr>
</tbody>
</table>

14 On the Site Recovery Manager Plug-in ID page, select Default Site Recovery Manager Plug-in Identifier, and click Next.

15 On the Certificate Type page, select Automatically generate a certificate, and click Next.

16 On the Generate Certificate page, enter the following settings, and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Rainpole</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Rainpole</td>
</tr>
</tbody>
</table>

17 On the Database Server Selection page, select Use the embedded database server, and click Next.

18 On the Embedded Database Configuration page, enter the following settings, and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Source Name</td>
<td>SRM_SITE_LAX01</td>
</tr>
<tr>
<td>Database User Name</td>
<td>srm_admin</td>
</tr>
<tr>
<td>Database Password</td>
<td>srm_admin_lax_password</td>
</tr>
<tr>
<td>Database Port</td>
<td>5678</td>
</tr>
<tr>
<td>Connection Count</td>
<td>5</td>
</tr>
<tr>
<td>Max. Connections</td>
<td>20</td>
</tr>
</tbody>
</table>
19 On the **Site Recovery Manager Service Account** page, enter the following credentials, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Local System account</td>
<td>Deselected</td>
</tr>
<tr>
<td>Username</td>
<td>LAX01M01SRM01\Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>lax01m01srm01_admin_password</td>
</tr>
</tbody>
</table>

20 On the **Ready to Install the Program** page click **Install**.

21 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](https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client).
   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:svc-srm@rainpole.local">svc-srm@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-srm_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Protected Region</th>
<th>Recovery Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>sfo01m01vc01.sfo01.rainpole.local</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Data center</td>
<td>sfo01-m01dc</td>
<td>lax01-m01dc</td>
</tr>
<tr>
<td>Cluster</td>
<td>sfo01-m01-mgmt01</td>
<td>lax01-m01-mgmt01</td>
</tr>
<tr>
<td>Inventory path</td>
<td>sfo01m01vc01.sfo01.rainpole.local &gt; sfo01-m01dc &gt; sfo01-m01-mgmt01</td>
<td>lax01m01vc01.lax01.rainpole.local &gt; lax01-m01dc &gt; lax01-m01-mgmt01</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Recovery Region</th>
<th>Protected Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
<td>sfo01m01vc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>Data center</td>
<td>lax01-m01dc</td>
<td>sfo01-m01dc</td>
</tr>
<tr>
<td>Cluster</td>
<td>lax01-m01-mgmt01</td>
<td>sfo01-m01-mgmt01</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Protected Region</th>
<th>Recovery Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>sfo01m01vc01.sfo01.rainpole.local</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Data center</td>
<td>sfo01-m01dc</td>
<td>lax01-m01dc</td>
</tr>
<tr>
<td>Folder</td>
<td>sfo01-m01fd-vrops</td>
<td>lax01-m01fd-vrops</td>
</tr>
<tr>
<td>Inventory path</td>
<td>sfo01m01vc01.sfo01.rainpole.local &gt; sfo01-m01dc &gt; sfo01-m01fd-vrops</td>
<td>lax01m01vc01.lax01.rainpole.local &gt; lax01-m01dc &gt; lax01-m01fd-vrops</td>
</tr>
</tbody>
</table>
d On the **Prepare Mappings** page, select the folders of vRealize Automation core components, click **Add mappings**, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Protected Region</th>
<th>Recovery Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>sfo01m01vc01.sfo01.rainpole.local</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Data center</td>
<td>sfo01-m01dc</td>
<td>lax01-m01dc</td>
</tr>
<tr>
<td>Folder</td>
<td>sfo01-m01fd-vra</td>
<td>lax01-m01fd-vra</td>
</tr>
<tr>
<td>Inventory path</td>
<td>sfo01m01vc01.sfo01.rainpole.local &gt; sfo01-m01dc &gt; sfo01-m01fd-vra</td>
<td>lax01m01vc01.lax01.rainpole.local &gt; lax01-m01dc &gt; lax01-m01fd-vra</td>
</tr>
</tbody>
</table>


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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Recovery Region</th>
<th>Protected Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
<td>sfo01m01vc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>Data center</td>
<td>lax01-m01dc</td>
<td>sfo01-m01dc</td>
</tr>
<tr>
<td>Folder for vRealize Operations Manager</td>
<td>lax01-m01fd-vrops</td>
<td>sfo01-m01fd-vrops</td>
</tr>
<tr>
<td>Folder for vRealize Automation</td>
<td>lax01-m01fd-vra</td>
<td>sfo01-m01fd-vra</td>
</tr>
</tbody>
</table>


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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Protected Region</th>
<th>Recovery Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>sfo01m01vc01.sfo01.rainpole.local</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Data center</td>
<td>sfo01-m01dc</td>
<td>lax01-m01dc</td>
</tr>
<tr>
<td>Distributed switch</td>
<td>sfo01-m01-vds01</td>
<td>lax01-m01-vds01</td>
</tr>
<tr>
<td>Port group</td>
<td>port_group_prefix-xRegion01-VXLAN</td>
<td>port_group_prefix-xRegion01-VXLAN</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Recovery Region</th>
<th>Protected Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
<td>sfo01m01vc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>Data center</td>
<td>lax01-m01dc</td>
<td>sfo01-m01dc</td>
</tr>
<tr>
<td>Folder</td>
<td>lax01-m01fd-vra</td>
<td>sfo01-m01fd-vra</td>
</tr>
<tr>
<td>Distributed switch</td>
<td>lax01-m01-vds01</td>
<td>sfo01-m01-vds01</td>
</tr>
<tr>
<td>Port group</td>
<td>port_group_prefix-xRegion01-VXLAN</td>
<td>port_group_prefix-xRegion01-VXLAN</td>
</tr>
</tbody>
</table>

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-vs01** 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-vs01** 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.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation package</td>
<td>Download the vSphere Replication .iso image and mount it on the machine that you use to access the vSphere Web Client.</td>
</tr>
<tr>
<td>Email address of the vSphere Replication site administrators</td>
<td>Get the email addresses of the vSphere Replication site administrators.</td>
</tr>
</tbody>
</table>

**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 2-13. Network Configuration of vSphere Replication in Region A**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>sfo01m01vrms01</td>
</tr>
<tr>
<td>Static IPv4 address</td>
<td>172.16.11.123</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default gateway</td>
<td>172.16.11.253</td>
</tr>
<tr>
<td>DNS servers</td>
<td>172.16.11.5</td>
</tr>
<tr>
<td>FQDN</td>
<td>sfo01m01vrms01.sfo01.rainpole.local</td>
</tr>
</tbody>
</table>
Table 2-13. Network Configuration of vSphere Replication in Region A (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used ports</td>
<td>5480</td>
</tr>
</tbody>
</table>
| NTP servers   | ntp.sfo01.rainpole.local
                | ntp.lax01.rainpole.local |

Table 2-14. Network Configuration of vSphere Replication in Region B

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>lax01m01vrms01</td>
</tr>
<tr>
<td>Static IPv4 address</td>
<td>172.17.11.123</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default gateway</td>
<td>172.17.11.253</td>
</tr>
<tr>
<td>DNS servers</td>
<td>172.17.11.5</td>
</tr>
<tr>
<td>FQDN</td>
<td>lax01m01vrms01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Used ports</td>
<td>5480</td>
</tr>
</tbody>
</table>
| NTP servers   | ntp.lax01.rainpole.local
                | ntp.sfo01.rainpole.local |

Table 2-15. VLAN and IP Requirements for vSphere Replication Traffic

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Region A</th>
<th>Region B</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>1616</td>
<td>1716</td>
</tr>
<tr>
<td>Static IPv4 address</td>
<td>172.16.16.71</td>
<td>172.17.16.71</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>172.16.16.253</td>
<td>172.17.16.253</td>
</tr>
</tbody>
</table>

**Deployment Prerequisites**

Verify that your environment satisfies the following prerequisites for the deployment of vSphere Replication.

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Verify that you have a parent active directory with the SDDC user roles configured for the rainpole.local domain and that the users and groups are available in Region A and Region B.</td>
</tr>
<tr>
<td>Software Features</td>
<td>Verify that the Platform Services Controller instances for Region A and Region B are connected to the Active Directory domain.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>sfo01m01vrms01</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>sfo01m01vc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>Data center</td>
<td>sfo01-m01dc</td>
</tr>
<tr>
<td>Folder</td>
<td>sfo01-m01fd-bcdr</td>
</tr>
</tbody>
</table>

6. On the Select a resource page, select the sfo01-m01-mgmt01 cluster and 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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Network Destination</td>
<td>sfo01-m01-vds01-management</td>
</tr>
<tr>
<td>IP protocol</td>
<td>IPv4</td>
</tr>
<tr>
<td>IP allocation</td>
<td>Static - Manual</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS servers</td>
<td>172.16.11.5,172.16.11.4</td>
</tr>
<tr>
<td>Domain name</td>
<td>sfo01.rainpole.local</td>
</tr>
<tr>
<td>Gateway</td>
<td>172.16.11.253</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>DNS search path</td>
<td>sfo01.rainpole.local</td>
</tr>
<tr>
<td>Management Network IP Address</td>
<td>172.16.11.123</td>
</tr>
<tr>
<td>NTP Servers</td>
<td>ntp.sfo01.rainpole.local, ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td>Enter password</td>
<td>vr_sfo_root_password</td>
</tr>
<tr>
<td>Confirm password</td>
<td>vr_sfo_root_password</td>
</tr>
</tbody>
</table>

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.

**Configure vSphere Replication 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 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vr_sfo_root_password</td>
</tr>
</tbody>
</table>
2 On the VR tab, click Configuration, enter the following settings, and click Save and Restart Service.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Configure using the embedded database</td>
</tr>
<tr>
<td>LookupService Address</td>
<td>sfo01psc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>SSO Administrative Account</td>
<td><a href="mailto:svc-vr@rainpole.local">svc-vr@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-vr_password</td>
</tr>
<tr>
<td>VRM Host</td>
<td>172.16.11.123</td>
</tr>
<tr>
<td>VRM Site Name</td>
<td>sfo01m01vc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>vCenter Server Address</td>
<td>sfo01m01vc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>vCenter Server Port</td>
<td>80</td>
</tr>
<tr>
<td>vCenter Server Admin Mail</td>
<td>vcenter_server_admin_email</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>lax01m01vrms01</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Data center</td>
<td>lax01-w01dc</td>
</tr>
<tr>
<td>Folder</td>
<td>lax01-m01fd-bcdr</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select virtual disk format</td>
<td>Thin provision</td>
</tr>
<tr>
<td>VM Storage Policy</td>
<td>vSAN Default Storage Policy</td>
</tr>
<tr>
<td>Datastore</td>
<td>lax01-m01-vsan01</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Network Destination</td>
<td>lax01-m01-vds01-management</td>
</tr>
<tr>
<td>IP protocol</td>
<td>IPv4</td>
</tr>
<tr>
<td>IP allocation</td>
<td>Static - Manual</td>
</tr>
</tbody>
</table>

12 On the Customize template page, enter the following settings and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS servers</td>
<td>172.17.11.5,172.17.11.4</td>
</tr>
<tr>
<td>Domain name</td>
<td>lax01.rainpole.local</td>
</tr>
<tr>
<td>Gateway</td>
<td>172.17.11.253</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>DNS search path</td>
<td>lax01.rainpole.local</td>
</tr>
</tbody>
</table>
Setting | Value
--- | ---
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.

**Configure vSphere Replication in Region B**

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 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vr_lax_root_password</td>
</tr>
</tbody>
</table>

2 On the **VR** tab, click **Configuration**, enter the following settings, and click **Save and Restart Service**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Configure using the embedded database</td>
</tr>
<tr>
<td>LookupService Address</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>SSO Administrative Account</td>
<td><a href="mailto:svc-vr@rainpole.local">svc-vr@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-vr_password</td>
</tr>
<tr>
<td>VRM Host</td>
<td>172.17.11.123</td>
</tr>
<tr>
<td>VRM Site Name</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>vCenter Server Address</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>vCenter Server Port</td>
<td>80</td>
</tr>
<tr>
<td>vCenter Server Admin Mail</td>
<td>vcenter_server_admin_email</td>
</tr>
</tbody>
</table>

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](https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client).
   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSC address of the remote site</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>User name</td>
<td><a href="mailto:svc-vr@rainpole.local">svc-vr@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-vr_password</td>
</tr>
</tbody>
</table>

   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Values for the Management Cluster in Region A</th>
<th>Values for the Management Cluster in Region B</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server URL</td>
<td><a href="https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client/">https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client/</a></td>
<td><a href="https://lax01m01vc01.lax01.rainpole.local/vsphere-client/">https://lax01m01vc01.lax01.rainpole.local/vsphere-client/</a></td>
</tr>
<tr>
<td>Host profile</td>
<td>sfo01-m01hp-mgmt01</td>
<td>lax01-m01hp-mgmt01</td>
</tr>
<tr>
<td>Template ESXi host</td>
<td>sfo01m01esx01.sfo01.rainpole.local</td>
<td>lax01m01esx01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Filter value</td>
<td>172.16.16.253</td>
<td>172.17.16.253</td>
</tr>
<tr>
<td>IP Next Hop</td>
<td>172.16.16.253</td>
<td>172.17.16.253</td>
</tr>
<tr>
<td>Destination network address</td>
<td>172.17.16.0</td>
<td>172.16.16.0</td>
</tr>
<tr>
<td>Device name</td>
<td>vmk2</td>
<td>vmk2</td>
</tr>
<tr>
<td>Host/Cluster</td>
<td>sfo01-m01-mgmt01</td>
<td>lax01-m01-mgmt01</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.
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 vSphere Replication appliance management interface.
   a Open a Web browser and go to https://sfo01m01vrms01.sfo01.rainpole.local:5480.
   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vr_sfo_root_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Address Type</td>
<td>Static</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>172.16.16.71</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>IPv6 Address Type</td>
<td>Auto</td>
</tr>
</tbody>
</table>

   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.
Repeat the steps to reconfigure the lax01m01vrms01 vSphere Replication appliance in Region B, using the values from the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object to configure</td>
<td>lax01m01vrms01</td>
</tr>
<tr>
<td>Connect New Network Adapter To</td>
<td>lax01-m01-vds01-replication</td>
</tr>
<tr>
<td>URL of vSphere Replication Appliance</td>
<td><a href="https://lax01m01vrms01.lax01.rainpole.local:5480">https://lax01m01vrms01.lax01.rainpole.local:5480</a></td>
</tr>
<tr>
<td>IPv4 Address Type</td>
<td>Static</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>172.17.16.71</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>IP Address For Incoming Storage Traffic</td>
<td>172.17.16.71</td>
</tr>
</tbody>
</table>

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

- Open a Web browser and go to https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client.
- Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Appliance Host Name</th>
<th>Source Gateway</th>
<th>Target Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>sfo01m01vrms01.sfo01.rainpole.local</td>
<td>172.16.16.253</td>
<td>172.16.16.0/24</td>
</tr>
<tr>
<td>lax01m01vrms01.lax01.rainpole.local</td>
<td>172.17.16.253</td>
<td>172.16.16.0/24</td>
</tr>
</tbody>
</table>

- In the Navigator, click Hosts and Clusters.
- Expand the entire sfo01m01vc01.sfo01.rainpole.local tree.
- Right-click the sfo01m01vrms01 virtual appliance and select Open Console to open the console to the appliance.
- Press ALT+F2 to switch to the command prompt.
- Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vr_root_password</td>
</tr>
</tbody>
</table>

- Open the /etc/sysconfig/network/routes file using vi editor.
g To create a route to the recovery region for the hosts in Region A or to the protected region for the hosts in Region B, add the following line after the default gateway 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.

<table>
<thead>
<tr>
<th>Region of the vSphere Replication Appliance</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region A</td>
<td>172.16.0.0/24 172.16.16.253 dev eth1</td>
</tr>
<tr>
<td>Region B</td>
<td>172.16.0.0/24 172.17.16.253 dev eth1</td>
</tr>
</tbody>
</table>

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 ESXi hosts in the management clusters in all regions.

<table>
<thead>
<tr>
<th>Region</th>
<th>Host Name</th>
<th>Source Gateway</th>
<th>Target Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region A</td>
<td>sfo01m01esx01.sfo01.rainpole.local</td>
<td>172.16.16.253</td>
<td>172.17.16.0/24</td>
</tr>
<tr>
<td>Region B</td>
<td>lax01m01esx01.lax01.rainpole.local</td>
<td>172.17.16.253</td>
<td>172.16.16.0/24</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td><code>esxi_root_user_password</code></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Region of the ESXi Host</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region A</td>
<td><code>esxcli network ip route ipv4 add --gateway 172.16.16.253 --network 172.17.16.0/24</code></td>
</tr>
<tr>
<td>Region B</td>
<td><code>esxcli network ip route ipv4 add --gateway 172.17.16.253 --network 172.16.16.0/24</code></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 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.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Next Hop</td>
<td>172.16.16.253</td>
</tr>
<tr>
<td>Destination Network address</td>
<td>172.17.16.0</td>
</tr>
<tr>
<td>Device Name</td>
<td>vmk2</td>
</tr>
</tbody>
</table>

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.

## Deploy vSphere Data Protection in Region B

Deploy vSphere Data Protection for backup and restore of SDDC management components in Region B. vSphere Data Protection enables the backup and restore of virtual machines associated with the following components:

- **vCenter Server**
  - Management vCenter Server and connected external Platform Services Controller
  - Compute vCenter Server and connected external Platform Services Controller
- **vRealize Automation**
- **vRealize Operations Manager**
- **vRealize Log Insight**
- **vRealize Business for Cloud**
- **vSphere Update Manager Download Service (UMDS)**

### Procedure

1. **Prerequisites for Deploying vSphere Data Protection in Region B**
   Before you deploy vSphere Data Protection in Region B, verify that your environment satisfies the requirements for this deployment.

2. **Deploy the Virtual Appliance of vSphere Data Protection in Region B**
   Deploy vSphere Data Protection as a virtual appliance on the management cluster in Region B.

3. **Enable SSH Root User Access on vSphere Data Protection Appliance in Region B**
   Enable the login to the vSphere Data Protection appliance in Region B over Secure Shell (SSH) as the root user. You connect to the appliance over SSH to install custom certificates and to perform troubleshooting operations.

4. **Replace vSphere Data Protection Certificates in Region B**
   After you use the VMware Validated Design Certificate Generation Utility (**CertGenVVD**) to generate certificates for the SDDC management components, replace the default VMware-signed certificate on vSphere Data Protection in Region B with the certificate that is generated by **CertGenVVD**.

5. **Register vSphere Data Protection with Management vCenter Server in Region B**
   After you deploy the virtual appliance for vSphere Data Protection on the management cluster in Region B, complete the initial configuration of vSphere Data Protection.
Prerequisites for Deploying vSphere Data Protection in Region B

Before you deploy vSphere Data Protection in Region B, verify that your environment satisfies the requirements for this deployment.

IP Addresses and Host Names

Verify that static IP address and FQDN for vSphere Data Protection are available for the Region B of the SDDC deployment.

Table 2-16. IP Addresses and Host Names for vSphere Data Protection in Region B

<table>
<thead>
<tr>
<th>Network Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>172.17.11.81</td>
</tr>
<tr>
<td>FQDN</td>
<td>lax01m01vdp01.lax01.rainpole.local</td>
</tr>
<tr>
<td>DNS servers</td>
<td>172.17.11.5, 172.16.11.4</td>
</tr>
<tr>
<td>Default gateway</td>
<td>172.17.11.253</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

Deployment Prerequisites

Verify that you have fulfilled the following prerequisites in addition to the networking settings.

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Storage</td>
<td>▪ Virtual disk provisioning.</td>
</tr>
<tr>
<td></td>
<td>▪ Thin</td>
</tr>
<tr>
<td></td>
<td>▪ Required storage</td>
</tr>
<tr>
<td></td>
<td>▪ 6 TB NFS</td>
</tr>
<tr>
<td>Software Features</td>
<td>▪ vSphere</td>
</tr>
<tr>
<td></td>
<td>▪ Management vCenter Server</td>
</tr>
<tr>
<td></td>
<td>▪ Management cluster with enabled DRS and HA.</td>
</tr>
<tr>
<td></td>
<td>▪ vSphere Distributed Switch configured for the vSphere management network</td>
</tr>
<tr>
<td>Installation Package</td>
<td>Download the vSphere Data Protection virtual appliance .ova file to the machine where you use the vSphere Web Client.</td>
</tr>
</tbody>
</table>

Deploy the Virtual Appliance of vSphere Data Protection in Region B

Deploy vSphere Data Protection 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 vSphere Data Protection 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>lax01m01vdp01</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Data center</td>
<td>lax01-m01dc</td>
</tr>
<tr>
<td>Folder</td>
<td>lax01-m01fd-bcdr</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datacenter</td>
<td>lax01-m01dc</td>
</tr>
<tr>
<td>Cluster</td>
<td>lax01-m01-mgmt01</td>
</tr>
</tbody>
</table>

7 On the Review details page, examine the virtual appliance details, such as product, version, download size, and size on disk, and click Next.

8 On the Accept license agreements page, accept the end user license agreement and click Next.

9 On the Select storage page, select the NFS datastore that is provisioned for vSphere Data Protection, configure storage settings, and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore</td>
<td>lax01-m01-vdp01</td>
</tr>
<tr>
<td>Select virtual disk format</td>
<td>Thin provision</td>
</tr>
<tr>
<td>VM storage policy</td>
<td>None</td>
</tr>
</tbody>
</table>
10 On the **Select networks** page, select the **lax01-m01-vds01-management** distributed port group from the **Isolated Network** drop-down menu, select **IPv4** from the **IP protocol** drop-down menu and click **Next**.

11 On the **Customize template** page, enter the networking settings for the virtual appliance, and click **Next**.

<table>
<thead>
<tr>
<th>IPv4 Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>172.17.11.5,172.16.11.4</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>172.17.11.253</td>
</tr>
<tr>
<td>Network 1 IP Address</td>
<td>172.17.11.81</td>
</tr>
<tr>
<td>Network 1 Netmask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

12 On the **Ready to complete** page, verify that the settings are correct and click **Finish**.

13 After the virtual appliance is deployed, right-click the virtual appliance object in the vSphere Web Client and select **Power > Power On**.

**Enable SSH Root User Access on vSphere Data Protection Appliance in Region B**

Enable the login to the vSphere Data Protection appliance in Region B over Secure Shell (SSH) as the root user. You connect to the appliance over SSH to install custom certificates and to perform troubleshooting 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2 Navigate to the vSphere Data Protection virtual appliance **lax01m01vdp01**.

3 Right-click **lax01m01vdp01** and select **Open Console** to open the remote console to the appliance.

4 Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vdp_default_root_password</td>
</tr>
</tbody>
</table>
Run the following console command to open the sshd_config file for editing.

```
vi /etc/ssh/sshd_config
```

Remove the # comment from the beginning of the line `PermitRootLogin yes`.

Run the following command in the vi editor to save the file and exit the editor.

```
:wq!
```

In the console, restart the SSH service to update the running configuration.

```
/etc/init.d/sshd restart
```

Log out and close the console of the appliance.

**Replace vSphere Data Protection Certificates in Region B**

After you use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate certificates for the SDDC management components, replace the default VMware-signed certificate on vSphere Data Protection in Region B with the certificate that is generated by CertGenVVD.

**Procedure**

1. Log in to the vSphere Data Protection appliance.
   a. Open an SSH connection to the virtual machine lax01m01vdp01.lax01.rainpole.local.
   b. Log in using the following credentials.

     | Setting     | Value          |
     |-------------|----------------|
     | User name   | root           |
     | Password    | vdp_root_password |
2 Stop the vSphere Data Protection Web services by running the following command.

```
emwebapp.sh --stop
```

**Note** If you see errors related to the database server, ignore them.

3 Delete the **tomcat** alias from the Java keystore by running the following command.

```
/usr/java/latest/bin/keytool -delete -alias tomcat -storepass changeit
```

4 Copy the `.keystore` file generated by the CertGenVVD tool to the `/tmp` folder on the vSphere Data Protection virtual appliance.

You can use FileZilla or WinSCP.

5 Run the following command to insert the new certification chain into the keystore

```
keytool -importkeystore --srckeystore /tmp/.keystore --destkeystore /root/.keystore -srcstorepass changeit -deststorepass changeit
```

6 Run the following command and in the command output verify whether the certificate entry with the **tomcat** alias exists in the keystore.

```
/usr/java/latest/bin/keytool -list -v -keystore /root/.keystore -storepass changeit -keypass changeit
```

7 If the certificate entry exists in the keystore, run the `addFingerprint.sh` script to update the vSphere Data Protection server thumbprint.

```
/usr/local/avamar/bin/addFingerprint.sh
```

8 Start the services by running the following command.

```
emwebapp.sh --start
```

9 Execute the following command to remove the `/tmp/.keystore` file

```
rm /tmp/.keystore
```

**Register vSphere Data Protection with Management vCenter Server in Region B**

After you deploy the virtual appliance for vSphere Data Protection on the management cluster in Region B, complete the initial configuration of vSphere Data Protection.
Procedure

1. Log in to the vSphere Data Protection Configuration Utility.
   a. Open a Web browser and go to https://lax01m01vdp01.lax01.rainpole.local:8543/vdp-configure.
   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vdp_default_root_password</td>
</tr>
</tbody>
</table>

   The configuration wizard of vSphere Data Protection appears.

2. On the **Welcome** page, click **Next**.

3. On the **Network Settings** page, verify that the network settings are populated correctly and click **Next**.

4. On the **Time Zone** page, select the **UTC** time zone and click **Next**.

5. On the **VDP Credentials** page, enter and confirm a new password for the root Linux appliance user, and click **Next**.

   The password must satisfy the following requirements:
   - If all four character classes are used, the password must be at least 6 characters.
   - If three character classes are used, the password must be at least 7 characters.
   - If one or two character classes are used, the password must be at least 8 characters.
   - The four-character classes are as follows:
     - Upper case letters A-Z
     - Lower case letters a-z
     - Numbers 0-9
     - Special characters (for example: ~!@#..)
On the vCenter Registration page, configure the settings for registration with the Management vCenter Server.

a. Enter the settings for connection to the Management vCenter Server.

<table>
<thead>
<tr>
<th>vCenter Server Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter username</td>
<td>rainpole.local\svc-vdp</td>
</tr>
<tr>
<td>vCenter password</td>
<td>svc-vdp_password</td>
</tr>
<tr>
<td>vCenter FQDN or IP</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>vCenter HTTP port</td>
<td>80</td>
</tr>
<tr>
<td>vCenter HTTPS port</td>
<td>443</td>
</tr>
<tr>
<td>Verify vCenter certificate</td>
<td>Deselected</td>
</tr>
<tr>
<td>Use vCenter for SSO authentication</td>
<td>Deselected</td>
</tr>
<tr>
<td>SSO FQDN or IP</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>SSO port</td>
<td>443</td>
</tr>
</tbody>
</table>

b. Click Test Connection and in the Connection success message box, click OK.

c. On the vCenter Registration page, click Next.

On the Create Storage page, select Create new storage, in the Capacity text box enter 4 TiB, and click Next.

On the Device Allocation page, from the Provision drop-down menu select Thin and click Next.

On the CPU and Memory page, leave the default settings and click Next.

On the Product Improvement page, select Enable Customer Experience Improvement Program and click Next.

On the Ready to Complete page, select Run performance analysis on storage configuration and Restart the appliance if successful, and click Next.

In the warning message box about storage configuration, click Yes.

vSphere Data Protection setup starts configuring data disks.

After disk configuration is complete, click OK in the Note dialog box. The appliance will automatically restart.
14 Verify that the vSphere Data Protection is accessible in the vSphere Web Client after you complete the initial configuration of vSphere Data Protection.

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

b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

c. On the vSphere Web Client Home page, verify that the VDP icon is available and is able to connect to the appliance.

Replace Certificates in Region B

By default, virtual infrastructure management components use TLS/SSL certificates that are signed by the VMware Certificate Authority (VMCA). These certificates are not trusted by end-user devices. For example, a certificate warning might appear when a user connects to a vCenter Server system by using the vSphere Web Client.

Infrastructure administrators connect to SDDC components, such as vCenter Server, from a Web browser. The authenticity of the network node to which the administrator connects must be confirmed with a valid TLS/SSL certificate.

In this design, you replace user-facing certificates with certificates that are signed by a Microsoft Certificate Authority (CA). You can use other certificate authorities according to the requirements of your organization. You do not replace certificates for machine-to-machine communication. If necessary, you can manually mark these certificates as trusted.

In a dual-region SDDC deployment, you must replace certificates in both regions for the following VMware products:

- vCenter Server system in both management pod and shared edge and compute pod
- VMware NSX Manager in both management pod and shared edge and compute pod
- VMware Site Recovery Manager
- VMware vSphere Replication
- vSphere Data Protection

Method of Certificate Generation

You use the VMware Validated Design Certificate Generation (CertGenVVD) utility for automatic generation of Certificate Signing Requests (CSRs) and CA-signed certificate files for all VMware management products that are deployed in this validated design. For more information about using the CertGenVVD utility, see the VMware Validated Design Planning and Preparation documentation and VMware Knowledge Base article 2146215.
Product Order for Certificate Replacement

After you generate the certificates by using the CertGenVVD utility, replace them on the virtual infrastructure products as follows:

<table>
<thead>
<tr>
<th>Location</th>
<th>Replacement Order</th>
</tr>
</thead>
</table>
| Replace only in Region B | 1 Management Platform Services Controller  
| | 2 Management vCenter Server  
| | 3 Management NSX Manager  
| | 4 Compute Platform Services Controller  
| | 5 Compute vCenter Server  
| | 6 Compute NSX Manager  
| | 7 vSphere Data Protection  
| Replace in both Region A and Region B | 1 Site Recovery Manager  
| | 2 vSphere Data Protection  

Replace the vCenter Server Certificates in Region B

After you replace the Platform Services Controller certificate, you replace the vCenter Server machine SSL certificate.

You replace the certificates of the Platform Services Controller nodes during their deployment. You replace vCenter Server certificates after you deploy all virtual infrastructure components.

You replace certificates twice, once for each vCenter Server instance. You can start replacing certificates on the Management vCenter Server lax01m01vc01.lax01.rainpole.local first.

Table 2-17. Certificate-Related Files on the vCenter Server Instances

<table>
<thead>
<tr>
<th>vCenter Server FQDN</th>
<th>Files for Certificate Replacement</th>
<th>Replacement Order</th>
</tr>
</thead>
</table>
| lax01m01vc01.lax01.rainpole.local | lax01m01vc01.key  
| | lax01m01vc01.1.cer  
| | Root64.cer  
| lax01w01vc01.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 Change the vCenter Server appliance command shell to the Bash shell to allow secure copy (scp) connections.
   a Open an SSH connection to lax01w01vc01.lax01.rainpole.local.
   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vcenter_server_root_password</td>
</tr>
</tbody>
</table>
   c Run the following commands to enable Bash shell access for the root user.

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

2 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 lax01m01vc01.1.cer, lax01m01vc01.key, and Root64.cer to the /root/certs folder.
      You can use an scp software such as WinSCP.

3 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 default vCenter Single Sign-On user name administrator@vsphere.local and the vsphere_admin-password password.
   c When prompted for the Infrastructure Server IP, provide the IP address of the Platform Services Controller that manages this vCenter Server instance.

<table>
<thead>
<tr>
<th>vCenter Server</th>
<th>IP Address of Connected Platform Services Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01m01vc01.lax01.rainpole.local</td>
<td>172.17.11.61</td>
</tr>
<tr>
<td>lax01w01vc01.lax01.rainpole.local</td>
<td>172.17.11.63</td>
</tr>
</tbody>
</table>
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 have been generated by vSphere Certificate Manager earlier, and confirm the import with Yes (Y).

<table>
<thead>
<tr>
<th>vCenter Server</th>
<th>Path to Certificate-Related Files</th>
</tr>
</thead>
</table>
| 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 |
| lax01w01vc01.lax01.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 |

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

5 Perform the following command to restart the vami-lighttp service and to remove certificate files.

```
service vami-lighttp restart
cd /root/certs
rm lax01m01vc01.1.cer lax01m01vc01.key Root64.cer
```

6 After you replace the certificate on the lax01m01vc01.lax01.rainpole.local, repeat the procedure to replace the certificate on the compute vCenter Server lax01w01vc01.lax01.rainpole.local.

**Replace the NSX Manager Certificates in Region B**

After you replace the certificates of all Platform Services Controller instances and all vCenter Server instances, replace the certificates for the NSX Manager instances.

You replace certificates twice, once for each NSX Manager. You start by replacing certificates on the NSX Manager lax01m01nsx51.lax01.rainpole.local for the management cluster.

**Table 2-18. Certificate-Related Files on the NSX Manager Instances in Region B**

<table>
<thead>
<tr>
<th>NSX Manager FQDN</th>
<th>Certificate File Name</th>
<th>Replacement Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01m01nsx51.lax01.rainpole.local</td>
<td>lax01m01nsx51.4.p12</td>
<td>After you replace the certificate on the Management vCenter Server</td>
</tr>
<tr>
<td>lax01w01nsx51.lax01.rainpole.local</td>
<td>lax01w01nsx51.4.p12</td>
<td>After you replace the certificate on the Compute vCenter Server</td>
</tr>
</tbody>
</table>
**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. 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 the following URL.

<table>
<thead>
<tr>
<th>NSX Manager</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager for the management cluster</td>
<td><a href="https://lax01m01nsx01.lax01.rainpole.local">https://lax01m01nsx01.lax01.rainpole.local</a></td>
</tr>
<tr>
<td>NSX Manager for the shared compute and edge cluster</td>
<td><a href="https://lax01w01nsx01.lax01.rainpole.local">https://lax01w01nsx01.lax01.rainpole.local</a></td>
</tr>
</tbody>
</table>

   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>nsx_manager_admin_password</td>
</tr>
</tbody>
</table>

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

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

4. Browse to the certificate chain file `lax01m01nsx01.4.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**.

6. Re-register the NSX Manager to the Management vCenter Server.
   
   a. Open a Web browser and go to the NSX Manager Web interface.

<table>
<thead>
<tr>
<th>NSX Manager</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager for the management cluster</td>
<td><a href="https://lax01m01nsx01.lax01.rainpole.local">https://lax01m01nsx01.lax01.rainpole.local</a></td>
</tr>
<tr>
<td>NSX Manager for the shared compute and edge cluster</td>
<td><a href="https://lax01w01nsx01.lax01.rainpole.local">https://lax01w01nsx01.lax01.rainpole.local</a></td>
</tr>
</tbody>
</table>

   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>nsx_manager_admin_password</td>
</tr>
</tbody>
</table>

   c. Click **Manage vCenter Registration**.

   d. Under **Lookup Service**, click the **Edit** button.
e  In the **Lookup Service** dialog box, enter the following settings, and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup Service IP</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Lookup Service Port</td>
<td>443</td>
</tr>
<tr>
<td>SSO Administrator User Name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value for the NSX Manager for the Management Cluster</th>
<th>Value for the NSX Manager for the Shared Edge and Compute Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>vCenter User Name</td>
<td><a href="mailto:svc-nsxmanager@rainpole.local">svc-nsxmanager@rainpole.local</a></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>svc-nsxmanager_password</td>
<td></td>
</tr>
</tbody>
</table>

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

j  Wait until the Status indicators for the Lookup Service and vCenter Server change to **Connected**.

k  Repeat this step for the NSX Manager instance for the shared compute and edge cluster.

7 Reconnect to the NSX Manager instances in Region A.

a  Open a Web browser and go to **https://lax01m01vc51.lax01.rainpole.local**

b  Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

c  From the vSphere Web Client **Home** menu, select **Networking & Security**.

d  Click **Installation** in the **Navigator**.

e  On the **Management** tab, select the **172.17.11.65** instance from the **NSX Manager** menu.

f  Select **Actions > Disconnect from Primary NSX Manager**.

g  On the **Management** tab, select the **172.16.11.65** instance from the **NSX Manager** drop-down menu.

h  Select **Actions > Add Secondary NSX Manager**.
In the **Add Secondary NSX Manager** dialog box, enter the following settings and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager</td>
<td>172.17.11.65</td>
</tr>
<tr>
<td>Username</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>mgmtnsx_admin_password</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>mgmtnsx_admin_password</td>
</tr>
</tbody>
</table>

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

Repeat this step for the NSX Manager instance for the shared edge and compute cluster.

Reconnect the 172.17.11.66 secondary NSX Manager for the shared edge and compute cluster in Region B to the primary NSX Manager 172.16.11.66 for the shared edge and compute cluster in Region A.

### Replace the VMware Site Recovery Manager Certificates

After you replace the certificates of all Platform Services Controller, vCenter Server and NSX Manager instances, replace the certificates on the Site Recovery Manager instances.

You replace certificates twice, once for each Site Recovery Manager. You start by replacing certificates on sfo01m01srm01.sfo01.rainpole.local, the Site Recovery Manager in Region A.

**Table 2-19. Certificate-Related Files for Site Recovery Manager in Region A and Region B**

<table>
<thead>
<tr>
<th>File Name</th>
<th>Site Recovery Manager in Region A</th>
<th>Site Recovery Manager in Region B</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA Certificate Name</td>
<td>Root64.cer</td>
<td>Root64.cer</td>
</tr>
<tr>
<td>PKCS#12 File Name</td>
<td>sfo01m01srm01.5.p12</td>
<td>lax01m01srm01.5.p12</td>
</tr>
</tbody>
</table>

**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 following virtual machine.

   **Region**
   
   **Site Recovery Manager**
   
   **Region A**
   
   sfo01m01srm01.sfo01.rainpole.local
   
   **Region B**
   
   lax01m01srm01.lax01.rainpole.local

   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>rainpole\svc-srm</td>
</tr>
<tr>
<td>Password</td>
<td>svc-srm_user_password</td>
</tr>
</tbody>
</table>
2 Install the CA certificates in the Windows trusted root certificate store of the Site Recovery Manager virtual machine.
   a Copy the CA Certificate and PKCS#12 File to the C:\certs folder
   b Double-click the CA Certificate 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, browse to select Trusted Root Certificate Authorities store, and click OK.
   f On the Completing the Certificate Import Wizard page, click Finish.

3 Replace the certificate on Site Recovery Manager with CA-signed Certificates.
   a Open Programs and Features from the Windows Control Panel.
   b From the list of programs, select VMware vCenter Site Recovery Manager and click Change.
   c Select the Modify option on the Maintenance Options screen and follow the wizard until you reach the Certificate Type screen.
   d Select the Use a PKCS#12 certificate file option and click Next.
   e Browse to the C:\certs folder, select the sfo01m01srm01.5.p12 or lax01m01srm01.5.p12 file, and enter the certificate password VMware1! that you specified when generating the PKCS#12 file.
   f Click Yes in the certificate warning dialog box and complete the modify installation wizard.

4 If you were previously using credential-based authentication, you might need to restore the connection between the two Site Recovery Manager sites after replacing the default certificates with CA-signed certificates.
   a Open a Web Browser and go to the following URL.

<table>
<thead>
<tr>
<th>Region</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region A</td>
<td><a href="https://sfo01m01vc01.sfo01.rainpole.local">https://sfo01m01vc01.sfo01.rainpole.local</a></td>
</tr>
</tbody>
</table>

   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

   c In the vSphere Web Client, click Site Recovery > Sites.
   d Right-click the site sfo01m01vc01.sfo01.rainpole.local and select Reconfigure Pairing.
e Enter the address of the Platform Services Controller lax01psc01.lax01.rainpole.local on the remote site and click Next.

f Select the vCenter Server instance lax01m01vc01.lax01.rainpole.local with which Site Recovery Manager is registered on the remote site, enter the vCenter Single Sign-On administrator user name svc-srm@rainpole.local and svc-srm_password password, and click Finish.

5 Repeat the steps to replace the default VMware-signed certificate on lax01m01srms01.lax01.rainpole.local.

Replace the CA-Signed Certificate on vSphere Replication

After you replace the certificates on Site Recovery Manager, replace the certificates on vSphere Replication in Region A and Region B.

You can start replacing certificates on vSphere Replication in Region A sfo01m01vrms01.sfo01.rainpole.local first.

Table 2-20. PKCS#12 Files for vSphere Replication in Region A and Region B

<table>
<thead>
<tr>
<th>vSphere Replication FQDN</th>
<th>PKCS#12 File Name from the CertGenVVD Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>sfo01m01vrms01.sfo01.rainpole.local</td>
<td>sfo01m01vrms01.5.p12</td>
</tr>
<tr>
<td>lax01m01vrms01.lax01.rainpole.local</td>
<td>lax01m01vrms01.5.p12</td>
</tr>
</tbody>
</table>

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 the following URL.

<table>
<thead>
<tr>
<th>vSphere Replication</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere Replication in Region A</td>
<td><a href="https://sfo01m01vrms01.sfo01.rainpole.local:5480">https://sfo01m01vrms01.sfo01.rainpole.local:5480</a></td>
</tr>
<tr>
<td>vSphere Replication in Region B</td>
<td><a href="https://lax01m01vrms01.lax01.rainpole.local:5480">https://lax01m01vrms01.lax01.rainpole.local:5480</a></td>
</tr>
</tbody>
</table>

b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vr_root_password</td>
</tr>
</tbody>
</table>

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 lax01m01v rms01.5.p12 file on your local file system.

f Click the Upload and Install button and enter the certificate password when prompted.

After you change the SSL certificate, the vSphere Replication status changes to disconnected because the new certificate is not validated by the vSphere Replication instance in the other site.

2 Reconnect the sites to resolve the connection issue.

    a Open a Web browser and go to
            https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client.
    b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

    c On the vSphere Web Client Home page, click vSphere Replication.
    d Select sfo01m01vc01.sfo01.rainpole.local, click Manage, and select Target Sites.
    e Right-click lax01m01vc01.lax01.rainpole.local and click Reconnect site.
    f In the Reconnect Sites dialog box, click Yes to proceed.
Region B Cloud Management Platform Implementation

The Cloud Management Platform (CMP) consists of integrated products that provide for the management of public, private and hybrid cloud environments. VMware’s 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.

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 address 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 3-1. 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 | ntp.sfo01.rainpole.local |
| | 172.16.11.252 | ntp.lax01.rainpole.local |
| | 172.17.11.251 | ntp.lax01.rainpole.local |
| | 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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**.
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.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

   ![Assign Role wizard](image)

   - 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.

   - 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.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary IP Address</td>
<td>192.168.11.53, 192.168.11.56, 192.168.11.59, 192.168.11.65</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vRealize-https-persist</td>
</tr>
<tr>
<td>Type</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Enable SSL Passthrough</td>
<td>Selected</td>
</tr>
<tr>
<td>Persistence</td>
<td>Source IP</td>
</tr>
<tr>
<td>Expires in (Seconds)</td>
<td>1800</td>
</tr>
</tbody>
</table>
7 Click OK to save the configuration.

8 Repeat this procedure to create the following application profile.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vRealize-https</td>
</tr>
<tr>
<td>Type</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

Deployment for Region B
## 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>vra-svr-443-monitor</th>
<th>vra-iaas-web-443-monitor</th>
<th>vra-iaas-mgr-443-monitor</th>
<th>vra-vro-8283-monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vra-svr-443-monitor</td>
<td>vra-iaas-web-443-monitor</td>
<td>vra-iaas-mgr-443-monitor</td>
<td>vra-vro-8283-monitor</td>
</tr>
<tr>
<td>Interval</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Timeout</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Max Retries</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Type</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Expected</td>
<td>204</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Method</td>
<td>GET</td>
<td>GET</td>
<td>GET</td>
<td>GET</td>
</tr>
<tr>
<td>URL</td>
<td>/vcac/services/api/health</td>
<td>/wapi/api/status/web</td>
<td>/VMPSPrevision</td>
<td>/vco-controlcenter/docs</td>
</tr>
<tr>
<td>Receive</td>
<td>REGISTERED</td>
<td>ProvisionService</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 3-2. Server Pools for the Cloud Management Platform in Region B

<table>
<thead>
<tr>
<th>Pool Name</th>
<th>Algorithm</th>
<th>Monitors</th>
<th>Members</th>
<th>Member Name</th>
<th>IP address</th>
<th>Port</th>
<th>Monitor Port</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>vra-svr-443</td>
<td>ROUND-ROBIN</td>
<td>vra-svr-443-monitor</td>
<td>Yes</td>
<td>vra01svr01a</td>
<td>192.168.11.51</td>
<td>443</td>
<td>443</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>vra01svr01b</td>
<td>192.168.11.52</td>
<td>443</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>vra-iaas-web-443</td>
<td>ROUND-ROBIN</td>
<td>vra-iaas-web-443-monitor</td>
<td>Yes</td>
<td>vra01iws01a</td>
<td>192.168.11.54</td>
<td>443</td>
<td>443</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>vra01iws01b</td>
<td>192.168.11.55</td>
<td>443</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>
Table 3-2. Server Pools for the Cloud Management Platform in Region B (Continued)

<table>
<thead>
<tr>
<th>Pool Name</th>
<th>Algorithm</th>
<th>Monitors</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enable</td>
</tr>
<tr>
<td>vra-iaas-mgr-443</td>
<td>ROUND-ROBIN</td>
<td>vra-iaas-mgr-443-monitor</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>vra-svr-8444</td>
<td>ROUND-ROBIN</td>
<td>vra-svr-443-monitor</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>vra-vro-8283</td>
<td>ROUND-ROBIN</td>
<td>vra-vro-8283-monitor</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vra-svr-443</td>
</tr>
<tr>
<td>Algorithm</td>
<td>ROUND-ROBIN</td>
</tr>
<tr>
<td>Monitors</td>
<td>vra-svr-443-monitor</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vra01svr01a</td>
</tr>
<tr>
<td>IP Address/VC Container</td>
<td>192.168.11.51</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vra01svr01b</td>
</tr>
<tr>
<td>IP Address/VC Container</td>
<td>192.168.11.52</td>
</tr>
<tr>
<td>State</td>
<td>Enabled</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
</tr>
<tr>
<td>Monitor Port</td>
<td>443</td>
</tr>
<tr>
<td>Weight</td>
<td>1</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>vra-svr-443</th>
<th>vra-iaas-web-443</th>
<th>vra-iaas-mgr-443</th>
<th>vra-svr-8444</th>
<th>vra-vro-8283</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Virtual server</td>
<td>Selected</td>
<td>Selected</td>
<td>Selected</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>Name</td>
<td>vra-svr-443</td>
<td>vra-iaas-web-443</td>
<td>vra-iaas-mgr-443</td>
<td>vra-svr-8444</td>
<td>vra-vro-8283</td>
</tr>
<tr>
<td>Description</td>
<td>vRealize Automation Appliance UI</td>
<td>vRealize Automation IaaS Web UI</td>
<td>vRealize Automation IaaS Manager</td>
<td>vRealize Automation Remote Console Proxy</td>
<td>vRealize Orchestrator Control Center</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.11.53</td>
<td>192.168.11.56</td>
<td>192.168.11.59</td>
<td>192.168.11.53</td>
<td>192.168.11.53</td>
</tr>
<tr>
<td>Protocol</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>
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.

7. Repeat the previous step to create a virtual server for each component.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target VM Operating System</td>
<td>Windows</td>
</tr>
<tr>
<td>Use custom Sysprep answer file</td>
<td>Deselected</td>
</tr>
<tr>
<td>Customization Spec Name</td>
<td>vra7-proxy-agent-template</td>
</tr>
</tbody>
</table>

6 On the Set Registration Information page, configure the following settings, and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Rainpole</td>
</tr>
<tr>
<td>Organization</td>
<td>Rainpole IT</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Key</td>
<td><code>volume_license_key</code></td>
</tr>
<tr>
<td>Include Server License Information</td>
<td>Selected</td>
</tr>
<tr>
<td>Server License Mode</td>
<td>Per seat</td>
</tr>
</tbody>
</table>

9 On the **Set Administrator Password** page, configure the following settings, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td><code>local_administrator_pwd</code></td>
</tr>
<tr>
<td>Confirm password</td>
<td><code>local_administrator_pwd</code></td>
</tr>
<tr>
<td>Automatically logon as Administrator</td>
<td>Selected</td>
</tr>
<tr>
<td>Number of times to logon automatically</td>
<td>1</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prompt the user for an address when the specification is used</td>
<td>Selected</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>192.168.32.1</td>
</tr>
</tbody>
</table>
14 On the DNS page, provide DNS servers and search suffixes.
   
   a Configure the following DNS server settings.
      
      | Setting                      | Value       |
      |------------------------------|-------------|
      | 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server Domain</td>
<td>lax01.rainpole.local</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:ad_admin_acct@lax01.rainpole.local">ad_admin_acct@lax01.rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>ad_admin_password</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Name for Virtual Machines</th>
<th>NetBIOS name</th>
<th>vCenter Folder</th>
<th>IP</th>
<th>vCPU number</th>
<th>Memory Size</th>
<th>Image Customization Specifications Template</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01ias01a.lax01.rainpole.local</td>
<td>lax01ias01a</td>
<td>lax01-m01fd-vraias</td>
<td>192.168.32.5</td>
<td>2</td>
<td>4 GB</td>
<td>vra7-proxy-agent-template</td>
<td>vxw-dvs-xxxx-Mgmt-RegionB01-VXLAN</td>
</tr>
<tr>
<td>lax01ias01b.lax01.rainpole.local</td>
<td>lax01ias01b</td>
<td>lax01-m01fd-vraias</td>
<td>192.168.32.5</td>
<td>3</td>
<td>4 GB</td>
<td>vra7-proxy-agent-template</td>
<td>vxw-dvs-xxxx-Mgmt-RegionB01-VXLAN</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 windows2012r2-template 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.lax01.rainpole.local 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBIOS name</td>
<td>lax01ias01a</td>
</tr>
<tr>
<td>IPv4 address</td>
<td>192.168.32.52</td>
</tr>
<tr>
<td>IPv4 subnet mask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

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.lax01.rainpole.local 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.lax01.rainpole.local, and select Power > Power on.

15 From the Virtual Machine Console, verify that lax01ias01a.lax01.rainpole.local 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRA Appliance Address</td>
<td><a href="https://vra01svr01a.rainpole.local:5480">https://vra01svr01a.rainpole.local:5480</a></td>
</tr>
<tr>
<td>Root username</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vra_appA_root_password</td>
</tr>
</tbody>
</table>
   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>rainpole/svc-vra</td>
</tr>
<tr>
<td>Password</td>
<td>svc-vra_password</td>
</tr>
</tbody>
</table>

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 console using the vRealize Automation service account.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Rainpole\svc-vra</td>
</tr>
<tr>
<td>Password</td>
<td>svc-vra_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance host name</td>
<td>vra01svr01a.rainpole.local:5480</td>
</tr>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>root_password</td>
</tr>
<tr>
<td>Accept Certificate</td>
<td>Selected</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local server</td>
<td>Use the default host name</td>
</tr>
<tr>
<td>User name</td>
<td>RAINPOLE\svc-vra</td>
</tr>
<tr>
<td>Password</td>
<td>svc-vra_password</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent type</td>
<td>vSphere</td>
</tr>
<tr>
<td>Agent name</td>
<td>VSPHERE-AGENT-51</td>
</tr>
<tr>
<td>Manager Service Host</td>
<td>vra01ims01.rainpole.local</td>
</tr>
<tr>
<td>Model Manager Web Service Host</td>
<td>vra01iws01.rainpole.local</td>
</tr>
<tr>
<td>vSphere Endpoint</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

Click **Next**.

Verify the configuration, and click **Install** to install the proxy agent.

Click **Next** when the installation is completed, and click **Finish** to exit the wizard.

Repeat the procedure for virtual machine **lax01ias01b.lax01.rainpole.local** to install another proxy agent for redundancy, using the following values.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Type</td>
<td>vSphere</td>
</tr>
<tr>
<td>Agent Name</td>
<td>VSPHERE-AGENT-51</td>
</tr>
<tr>
<td>Manager Service Host</td>
<td>vra01ims01.rainpole.local</td>
</tr>
<tr>
<td>Model Manager Web Service Host</td>
<td>vra01iws01.rainpole.local</td>
</tr>
<tr>
<td>vSphere Endpoint</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>vra01svr01.rainpole.local:443</td>
</tr>
<tr>
<td>User name</td>
<td>svc-vra</td>
</tr>
<tr>
<td>Password</td>
<td>svc-vra_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP or hostname of the vCenter Server instance to add</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>HTTPS port of the vCenter Server instance</td>
<td>443</td>
</tr>
<tr>
<td>Location of SDK that you use to connect</td>
<td>/sdk</td>
</tr>
<tr>
<td>Will you orchestrate this instance</td>
<td>Yes</td>
</tr>
<tr>
<td>Do you want to ignore certificate warnings</td>
<td>Yes</td>
</tr>
</tbody>
</table>

   b. On the Set the connection properties page, configure the following settings, and click Submit.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a session per user</td>
<td>No</td>
</tr>
<tr>
<td>vCenter Server user name</td>
<td>rainpole.local\svc-vro</td>
</tr>
<tr>
<td>vCenter Server user password</td>
<td>svc-vro_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>lax01vrbc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Select a folder or datacenter</td>
<td>lax01-m01fd-vraias</td>
</tr>
</tbody>
</table>

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.
11 On the **Customize template** page, configure the following values and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currency</td>
<td>USD</td>
</tr>
<tr>
<td>Enable SSH service</td>
<td>Deselected</td>
</tr>
<tr>
<td>Enable Server</td>
<td>Deselected</td>
</tr>
<tr>
<td>Join the VMware Customer Experience Improvement Program</td>
<td>Selected</td>
</tr>
<tr>
<td>Root user password</td>
<td><code>vrb_collector_root_password</code></td>
</tr>
<tr>
<td>Default gateway</td>
<td>192.168.32.1</td>
</tr>
<tr>
<td>Domain Name</td>
<td><code>lax01vrbc01.lax01.rainpole.local</code></td>
</tr>
<tr>
<td>Domain Name Servers</td>
<td>172.17.11.5,172.17.11.4</td>
</tr>
<tr>
<td>Domain Search Path</td>
<td><code>lax01.rainpole.local</code></td>
</tr>
<tr>
<td>Network 1 IP Address</td>
<td>192.168.32.54</td>
</tr>
<tr>
<td>Network 1 Netmask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td><code>vrb_collector_root_password</code></td>
</tr>
</tbody>
</table>
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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Sync. Mode</td>
<td>Use Time Server</td>
</tr>
<tr>
<td>Time Server #1</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td>Time Server #2</td>
<td>ntp.sfo01.rainpole.local</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>Rainpole.local</td>
</tr>
</tbody>
</table>

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.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vrb_collector_root_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the vRB Server Url:</td>
<td><a href="https://vrb01svr01.rainpole.local">https://vrb01svr01.rainpole.local</a></td>
</tr>
<tr>
<td>Enter the One Time Key:</td>
<td>one_time_use_key</td>
</tr>
</tbody>
</table>
   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vrb_collector_root_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td><a href="mailto:svc-vra@rainpole.local">svc-vra@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc_vra_password</td>
</tr>
</tbody>
</table>

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.lax01.rainpole.local` and `lax01ias01b.lax01.rainpole.local` 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. From the Home page, click Content Libraries and click content library SFO01-ContentLib01 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LAX01-ContentLib01</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

8 On the Configure content library page, select Subscribed content library specify the following settings, and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribed content library</td>
<td>Selected</td>
</tr>
<tr>
<td>Subscription URL</td>
<td>SFO01-ContentLib01_subscription_URL</td>
</tr>
<tr>
<td>Enable authentication</td>
<td>Selected</td>
</tr>
<tr>
<td>Password</td>
<td>SFO01-ContentLib01_password</td>
</tr>
<tr>
<td>Download all library content immediately</td>
<td>Selected</td>
</tr>
</tbody>
</table>

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 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.
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.

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.

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.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

2. Select Infrastructure > Endpoints > Fabric Groups.
3 Click **New Fabric Group**, enter the following settings and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LAX Fabric Group</td>
</tr>
<tr>
<td>Fabric administrators</td>
<td><a href="mailto:ug-ITAC-TenantAdmins@rainpole.local">ug-ITAC-TenantAdmins@rainpole.local</a></td>
</tr>
</tbody>
</table>

**Note** You have not yet configured a vCenter Endpoint, so no compute resource is currently available for you to select. You will 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](https://vra01svr01.rainpole.local/vcac/org/rainpole).
   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>Rainpole.local</td>
</tr>
</tbody>
</table>

2 Navigate to **Infrastructure > Reservation > Reservation Policies**.

3 Click the **New** icon, configure the following settings, and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LAX-Production-Policy</td>
</tr>
<tr>
<td>Description</td>
<td>Reservation policy for Production Business Group in LAX</td>
</tr>
</tbody>
</table>
4 Click the **New** icon, configure the following settings, and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LAX-Development-Policy</td>
</tr>
<tr>
<td>Description</td>
<td>Reservation policy for Development Business Group in LAX</td>
</tr>
</tbody>
</table>

5 Click the **New** icon, configure the following settings, and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LAX-Edge-Policy</td>
</tr>
<tr>
<td>Description</td>
<td>Reservation policy for Tenant Edge resources in LAX</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Address</td>
<td><a href="https://lax01w01vc01.lax01.rainpole.local/sdk">https://lax01w01vc01.lax01.rainpole.local/sdk</a></td>
</tr>
<tr>
<td>User Name</td>
<td>rainpole\svc-vra</td>
</tr>
<tr>
<td>Password</td>
<td>svc-vra_password</td>
</tr>
</tbody>
</table>

   **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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LAX-NSXEndpoint</td>
</tr>
<tr>
<td>Address</td>
<td><a href="https://lax01w01nsx01.lax01.rainpole.local">https://lax01w01nsx01.lax01.rainpole.local</a></td>
</tr>
<tr>
<td>User Name</td>
<td>rainpole\svc-vra</td>
</tr>
<tr>
<td>Password</td>
<td>svc-vra_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

2 Navigate to Infrastructure > End Points > Fabric Groups.

3 In the Name column, hover the mouse pointer over the fabric group name LAX Fabric Group, and click Edit.
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 are still not able to see the compute cluster after sufficient time has passed, 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, hover the mouse pointer over the 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 3-3. Business Group Names

<table>
<thead>
<tr>
<th>Group</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production</td>
<td>LAX01-Comp01-Prod-Res01</td>
</tr>
<tr>
<td>Development</td>
<td>LAX01-Comp01-Dev-Res01</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Production Group Value</th>
<th>Development Group Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LAX01-Comp01-Prod-Res01</td>
<td>LAX01-Comp01-Dev-Res01</td>
</tr>
<tr>
<td>Tenant</td>
<td>rainpole</td>
<td>rainpole</td>
</tr>
<tr>
<td>Business Group</td>
<td>Production</td>
<td>Development</td>
</tr>
<tr>
<td>Reservation Policy</td>
<td>LAX-Production-Policy</td>
<td>LAX-Development-Policy</td>
</tr>
<tr>
<td>Priority</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Enable This Reservation</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>

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.
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.

a Configure the Production Business Group with the following values.

<table>
<thead>
<tr>
<th>Production Network Path</th>
<th>Production Group Network Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>vxw-dvs-xxxxx-Production-Web-VXLAN</td>
<td>Ext-Net-Profile-Production-Web</td>
</tr>
<tr>
<td>vxw-dvs-xxxxx-Production-DB-VXLAN</td>
<td>Ext-Net-Profile-Production-DB</td>
</tr>
<tr>
<td>vxw-dvs-xxxxx-Production-App-VXLAN</td>
<td>Ext-Net-Profile-Production-App</td>
</tr>
</tbody>
</table>

b Configure the Development Business Group with the following values.

<table>
<thead>
<tr>
<th>Development Network Path</th>
<th>Development Group Network Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>vxw-dvs-xxxxx-Development-Web-VXLAN</td>
<td>Ext-Net-Profile-Development-Web</td>
</tr>
<tr>
<td>vxw-dvs-xxxxx-Development-DB-VXLAN</td>
<td>Ext-Net-Profile-Development-DB</td>
</tr>
<tr>
<td>vxw-dvs-xxxxx-Development-App-VXLAN</td>
<td>Ext-Net-Profile-Development-App</td>
</tr>
</tbody>
</table>

Click **OK** to save the reservation.

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 3-4. Business Group Names

<table>
<thead>
<tr>
<th>Group</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production</td>
<td>LAX01-Edge01-Prod-Res01</td>
</tr>
<tr>
<td>Development</td>
<td>LAX01-Edge01-Dev-Res01</td>
</tr>
</tbody>
</table>

#### 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](https://vra01svr01.rainpole.local/vcac/org/rainpole).
   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>
Navigate to Infrastructure > Reservations > Reservations, and click New vSphere (vCenter).

On the New Reservation - vSphere (vCenter) page, click the General tab, and configure the following values for your business group.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Production Group Value</th>
<th>Development Group Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LAX01-Edge01-Prod-Res01</td>
<td>LAX01-Edge01-Dev-Res01</td>
</tr>
<tr>
<td>Tenant</td>
<td>rainpole</td>
<td>rainpole</td>
</tr>
<tr>
<td>Business Group</td>
<td>Production</td>
<td>Development</td>
</tr>
<tr>
<td>Reservation Policy</td>
<td>LAX-Edge-Policy</td>
<td>LAX-Edge-Policy</td>
</tr>
<tr>
<td>Priority</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Enable This Reservation</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>

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.

On the New Reservation - vSphere (vCenter) page, click the Network tab.

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

<table>
<thead>
<tr>
<th>Production Port Group</th>
<th>Production Network Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>vxw-dvs-xxxxx-Production-Web-VXLAN</td>
<td>Ext-Net-Profile-Production-Web</td>
</tr>
<tr>
<td>vxw-dvs-xxxxx-Production-DB-VXLAN</td>
<td>Ext-Net-Profile-Production-DB</td>
</tr>
<tr>
<td>vxw-dvs-xxxxx-Production-App-VXLAN</td>
<td>Ext-Net-Profile-Production-App</td>
</tr>
</tbody>
</table>

### Development Business Group

<table>
<thead>
<tr>
<th>Development Port Group</th>
<th>Development Network Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>vxw-dvs-xxxxx-Development -Web-VXLAN</td>
<td>Ext-Net-Profile-Development -Web</td>
</tr>
<tr>
<td>vxw-dvs-xxxxx-Development -DB-VXLAN</td>
<td>Ext-Net-Profile-Development -DB</td>
</tr>
<tr>
<td>vxw-dvs-xxxxx-Development -App-VXLAN</td>
<td>Ext-Net-Profile-Development -App</td>
</tr>
</tbody>
</table>

Click OK to save the reservation.

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       |

3. Select the vCenter Server lax01w01vc01.lax01.rainpole.local from the drop-down menu.
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 `itac-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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>America</td>
</tr>
<tr>
<td>Location</td>
<td>Los Angeles</td>
</tr>
<tr>
<td>Hardware Clock Set To</td>
<td>Local Time</td>
</tr>
</tbody>
</table>

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.
   - Open a Web browser and go to `https://lax01w01vc01.lax01.rainpole.local/vsphere-client`.
   - Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. Navigate to **Home > Operations and Policies > 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 dropdown menu, enter itac-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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>lax01.rainpole.local</td>
</tr>
<tr>
<td>User name</td>
<td><a href="mailto:ad_admin_acct@lax01.rainpole.local">ad_admin_acct@lax01.rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>ad_admin_pwd</td>
</tr>
</tbody>
</table>

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 3-5. VM Templates and their Guest Operating Systems

<table>
<thead>
<tr>
<th>VM Template Name</th>
<th>Guest OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>redhat6-enterprise-64</td>
<td>Red Hat Enterprise Server 6 (64-bit)</td>
</tr>
<tr>
<td>windows-2012r2-64</td>
<td>Windows Server 2012 R2 (64-bit)</td>
</tr>
<tr>
<td>windows-2012r2-64-sql2012</td>
<td>Windows Server 2012 R2 (64-bit)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.


7. Click LAX01-ContentLib01 > Templates.

8. Right-click the VM Template redhat6-enterprise-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 3-6. VM Templates and their Guest Operating Systems**

<table>
<thead>
<tr>
<th>VM Template Name</th>
<th>Guest OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>redhat6-enterprise-64</td>
<td>Red Hat Enterprise Server 6 (64-bit)</td>
</tr>
<tr>
<td>windows-2012r2-64</td>
<td>Windows Server 2012 R2 (64-bit)</td>
</tr>
<tr>
<td>windows-2012r2-64-sql2012</td>
<td>Windows Server 2012 R2 (64-bit)</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LAX Service Catalog</td>
</tr>
<tr>
<td>Description</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>Icon</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>Status</td>
<td>Active</td>
</tr>
<tr>
<td>Hours</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>Owner</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>Support Team</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>Change Window</td>
<td>Default setting (blank)</td>
</tr>
</tbody>
</table>

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 Table

<table>
<thead>
<tr>
<th>Blueprint Name</th>
<th>VM Template</th>
<th>Customization Specification</th>
<th>Reservation Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2012 R2 - LAX Prod</td>
<td>windows-2012r2-64 (lax01w01vc01.lax01.rainpole.local)</td>
<td>itac-windows-joindomain-custom-spec</td>
<td>LAX-Production-Policy</td>
</tr>
<tr>
<td>Windows Server 2012 R2 - LAX Dev</td>
<td>windows-2012r2-64 (lax01w01vc01.lax01.rainpole.local)</td>
<td>itac-windows-joindomain-custom-spec</td>
<td>LAX-Development-Policy</td>
</tr>
<tr>
<td>Windows Server 2012 R2 With SQL2012 - LAX Prod</td>
<td>windows-2012r2-64-sql2012(lax01w01vc01.lax01.rainpole.local)</td>
<td>itac-windows-joindomain-custom-spec</td>
<td>LAX-Production-Policy</td>
</tr>
<tr>
<td>Windows Server 2012 R2 With SQL2012 - LAX Dev</td>
<td>windows-2012r2-64-sql2012(lax01w01vc01.lax01.rainpole.local)</td>
<td>itac-windows-joindomain-custom-spec</td>
<td>LAX-Development-Policy</td>
</tr>
<tr>
<td>Redhat Enterprise Linux 6 - LAX Prod</td>
<td>redhat6-enterprise-64(lax01w01vc01.lax01.rainpole.local)</td>
<td>itac-linux-custom-spec</td>
<td>LAX-Production-Policy</td>
</tr>
<tr>
<td>Redhat Enterprise Linux 6 - LAX Dev</td>
<td>redhat6-enterprise-64(lax01w01vc01.lax01.rainpole.local)</td>
<td>itac-linux-custom-spec</td>
<td>LAX-Development-Policy</td>
</tr>
</tbody>
</table>

### 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](https://vra01svr01.rainpole.local/vcac/org/rainpole).
   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Windows Server 2012 R2 - LAX Prod</td>
</tr>
<tr>
<td>Deployment limit</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>Minimum</td>
<td>30</td>
</tr>
<tr>
<td>Maximum</td>
<td>270</td>
</tr>
<tr>
<td>Archive (days)</td>
<td>15</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Default setting (vSphere_vCenter_Machine_1)</td>
</tr>
<tr>
<td>Description</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>Display location on request</td>
<td>Deselected</td>
</tr>
<tr>
<td>Reservation policy</td>
<td>LAX-Production-Policy</td>
</tr>
<tr>
<td>Machine prefix</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>Minimum</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>Maximum</td>
<td>Default setting (blank)</td>
</tr>
</tbody>
</table>

![Infrastructure Service Portal](image)

7 Click the **Build Information** tab, configure the following settings, and click **Save**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blueprint type</td>
<td>Server</td>
</tr>
<tr>
<td>Action</td>
<td>Clone</td>
</tr>
<tr>
<td>Provisioning workflow</td>
<td>CloneWorkflow</td>
</tr>
<tr>
<td>Clone from</td>
<td>windows-2012r2-64</td>
</tr>
<tr>
<td>Customization spec</td>
<td>itac-windows-joindomain-custom-spec</td>
</tr>
</tbody>
</table>

**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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Memory (MB)</td>
<td>4096</td>
<td>16384</td>
</tr>
<tr>
<td>Storage</td>
<td>Default setting (blank)</td>
<td>Default setting (50)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Blueprint Name</th>
<th>Existing network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2012 R2 - LAX Prod</td>
<td>Ext-Net-Profile-Production-Web</td>
</tr>
<tr>
<td>Windows Server 2012 R2 - LAX Dev</td>
<td>Ext-Net-Profile-Development-Web</td>
</tr>
<tr>
<td>Windows Server 2012 R2 With SQL2012 - LAX Prod</td>
<td>Ext-Net-Profile-Production-DB</td>
</tr>
<tr>
<td>Windows Server 2012 R2 With SQL2012 - LAX Dev</td>
<td>Ext-Net-Profile-Development-DB</td>
</tr>
<tr>
<td>Redhat Enterprise Linux 6 - LAX Prod</td>
<td>Ext-Net-Profile-Production-App</td>
</tr>
<tr>
<td>Redhat Enterprise Linux 6 - LAX Dev</td>
<td>Ext-Net-Profile-Development-App</td>
</tr>
</tbody>
</table>

   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**.

<table>
<thead>
<tr>
<th>Network</th>
<th>Assignment Type</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExtNetProfileProductionWeb</td>
<td>Static IP</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>ExtNetProfileDevelopmentWeb</td>
<td>Static IP</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>ExtNetProfileProductionDB</td>
<td>Static IP</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>ExtNetProfileDevelopmentDB</td>
<td>Static IP</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>ExtNetProfileProductionApp</td>
<td>Static IP</td>
<td>Default setting (blank)</td>
</tr>
<tr>
<td>ExtNetProfileDevelopmentApp</td>
<td>Static IP</td>
<td>Default setting (blank)</td>
</tr>
</tbody>
</table>

   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.

<table>
<thead>
<tr>
<th>Blueprint Name</th>
<th>VM Template</th>
<th>Reservation Policy</th>
<th>Service Catalog</th>
<th>Add to Entitlement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2012 R2 - LAX Prod</td>
<td>windows-2012r2-64 (lax01w01vc01.lax01.rainpole.local)</td>
<td>LAX-Production-Policy</td>
<td>LAX Service Catalog</td>
<td>Prod-SingleVM-Entitlement</td>
</tr>
<tr>
<td>Windows Server 2012 R2 - LAX Dev</td>
<td>windows-2012r2-64 (lax01w01vc01.lax01.rainpole.local)</td>
<td>LAX-Development-Policy</td>
<td>LAX Service Catalog</td>
<td>Dev-SingleVM-Entitlement</td>
</tr>
<tr>
<td>Windows Server 2012 R2 With SQL2012 - LAX Prod</td>
<td>windows-2012r2-64-sql2012(lax01w01vc01.lax01.rainpole.local)</td>
<td>LAX-Production-Policy</td>
<td>LAX Service Catalog</td>
<td>Prod-SingleVM-Entitlement</td>
</tr>
<tr>
<td>Windows Server 2012 R2 With SQL2012 - LAX Dev</td>
<td>windows-2012r2-64-sql2012(lax01w01vc01.lax01.rainpole.local)</td>
<td>LAX-Development-Policy</td>
<td>LAX Service Catalog</td>
<td>Dev-SingleVM-Entitlement</td>
</tr>
<tr>
<td>Redhat Enterprise Linux 6 - LAX Prod</td>
<td>redhat6-enterprise-64(lax01w01vc01.lax01.rainpole.local)</td>
<td>LAX-Production-Policy</td>
<td>LAX Service Catalog</td>
<td>Prod-SingleVM-Entitlement</td>
</tr>
<tr>
<td>Redhat Enterprise Linux 6 - LAX Dev</td>
<td>redhat6-enterprise-64(lax01w01vc01.lax01.rainpole.local)</td>
<td>LAX-Development-Policy</td>
<td>LAX Service Catalog</td>
<td>Dev-SingleVM-Entitlement</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

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.
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**.

---

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.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>Rainpole.local</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vcenter_admin_password</td>
</tr>
</tbody>
</table>

   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 new 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vcenter_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Data Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFO</td>
<td>San Francisco DataCenter</td>
</tr>
<tr>
<td>LAX</td>
<td>Los Angeles DataCenter</td>
</tr>
</tbody>
</table>

![DataCenterLocations - Notepad.png](attachment:image)
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.

<table>
<thead>
<tr>
<th>Location</th>
<th>vCenter Server Compute Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFO</td>
<td>sfo01-w01-comp01</td>
</tr>
<tr>
<td>LAX</td>
<td>lax01-w01-comp01</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>


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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Francisco</td>
<td>SFO</td>
</tr>
<tr>
<td>Los Angeles</td>
<td>LAX</td>
</tr>
</tbody>
</table>
   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 new 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

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 list.
   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.

<table>
<thead>
<tr>
<th>Region</th>
<th>Business Group</th>
<th>Reservation Name</th>
<th>Reservation Policy</th>
<th>Compute Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region A</td>
<td>Production</td>
<td>SFO01-Comp01-Prod-UnifiedBlueprint</td>
<td>UnifiedBlueprint-Policy</td>
<td>sfo01-w01-comp01(sfo01w01vc01.sfo01.rainpole.local)</td>
</tr>
<tr>
<td>Region B</td>
<td>Production</td>
<td>LAX01-Comp01-Prod-UnifiedBlueprint</td>
<td>UnifiedBlueprint-Policy</td>
<td>lax01-w01-comp01(lax01w01vc01.lax01.rainpole.local)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Production Business Group Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>SFO01-Comp01-Prod-UnifiedBlueprint</td>
</tr>
<tr>
<td>Tenant</td>
<td>rainpole</td>
</tr>
<tr>
<td>Business Group</td>
<td>Production</td>
</tr>
<tr>
<td>Reservation Policy</td>
<td>UnifiedBlueprint-Policy</td>
</tr>
<tr>
<td>Priority</td>
<td>100</td>
</tr>
<tr>
<td>Enable This Reservation</td>
<td>Selected</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Production Network Path</th>
<th>Production Group Network Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>vxw-dvs-xxxxx-Production-Web-VXLAN</td>
<td>Ext-Net-Profile-Production-Web</td>
</tr>
<tr>
<td>vxw-dvs-xxxxx-Production-DB-VXLAN</td>
<td>Ext-Net-Profile-Production-DB</td>
</tr>
<tr>
<td>vxw-dvs-xxxxx-Production-App-VXLAN</td>
<td>Ext-Net-Profile-Production-App</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Blueprint Name</th>
<th>VM Template</th>
<th>Reservation Policy</th>
<th>Customization Specification</th>
<th>Service Catalog</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2012 R2 - Unified Prod</td>
<td>windows-2012r2-64 (sfo01w01vc01.sfo01.rainpole.local)</td>
<td>UnifiedBlueprint-Policy</td>
<td>itac-windows-joindomain-custom-spec</td>
<td>Unified Single Machine Catalog</td>
</tr>
<tr>
<td>Windows Server 2012 R2 With SQL2012 -</td>
<td>windows-2012r2-64-sql2012(sfo01w01vc01.sfo01.rainpole.local)</td>
<td>UnifiedBlueprint-Policy</td>
<td>itac-windows-joindomain-custom-spec</td>
<td>Unified Single Machine Catalog</td>
</tr>
<tr>
<td>Redhat Enterprise Linux 6 - Unified Prod</td>
<td>redhat6-enterprise-64(sfo01w01vc01.sfo01.rainpole.local)</td>
<td>UnifiedBlueprint-Policy</td>
<td>itac-linux-custom-spec</td>
<td>Unified Single Machine Catalog</td>
</tr>
</tbody>
</table>

**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](https://vra01svr01.rainpole.local/vcac/org/rainpole).
   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>rainpole.local</td>
</tr>
</tbody>
</table>

2. Navigate to **Design > Blueprints**.
3. Click **New**.
4. In the **New Blueprint** dialog box, configure the following settings on the **General** tab.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Windows Server 2012 R2 - Unified Prod</td>
</tr>
<tr>
<td>Archive (days)</td>
<td>15</td>
</tr>
<tr>
<td>Deployment limit</td>
<td>Default setting (blank)</td>
</tr>
</tbody>
</table>
5 Click the **Properties** tab.
   a Click **Add** on the **Property Groups** tab.
   b Select the property group **Select Location** and click **OK**.

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Default setting (vSphere_vCenter_Machine_1)</td>
</tr>
<tr>
<td>Reservation Policy</td>
<td>UnifiedBlueprint-Policy</td>
</tr>
<tr>
<td>Machine Prefix</td>
<td>Use group default</td>
</tr>
<tr>
<td>Minimum</td>
<td>Default setting</td>
</tr>
<tr>
<td>Maximum</td>
<td>Default setting</td>
</tr>
</tbody>
</table>

9 Click the **Build Information** tab, configure the following settings, and click **Save**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blueprint Type</td>
<td>Server</td>
</tr>
<tr>
<td>Action</td>
<td>Clone</td>
</tr>
<tr>
<td>Provisioning Workflow</td>
<td>CloneWorkflow</td>
</tr>
<tr>
<td>Clone from</td>
<td>windows-2012r2-64</td>
</tr>
<tr>
<td>Customization spec</td>
<td>itac-windows-joindomain-custom-spec</td>
</tr>
</tbody>
</table>
10 Click the **Machine Resources** tab, configure the following settings, and click **Save**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Memory (MB)</td>
<td>4096</td>
<td>16384</td>
</tr>
<tr>
<td>Storage</td>
<td>50</td>
<td>60</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Blueprint Name</th>
<th>Existing Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2012 R2 - Unified</td>
<td>Ext-Net-Profile-Production-Web</td>
</tr>
<tr>
<td>Windows Server 2012 R2 with SQL2012 - Unified</td>
<td>Ext-Net-Profile-Production-DB</td>
</tr>
<tr>
<td>Redhat Enterprise Linux 6 - Unified</td>
<td>Ext-Net-Profile-Production-App</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>ExtNetProfileProductionWeb</td>
</tr>
<tr>
<td>Assignment Type</td>
<td>Static IP</td>
</tr>
<tr>
<td>Address</td>
<td>Default setting (blank)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Region</th>
<th>Compute vCenter Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Francisco</td>
<td>sfo01w01vc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>Los Angeles</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

**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](https://vra01svr01.rainpole.local/vcac/org/rainpole).
   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>Rainpole.local</td>
</tr>
</tbody>
</table>

2. Select the **Catalog** tab, and click **Unified Single Machine Catalog** from the catalog of available services.

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**.
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](https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client).
   b Log in as the vCenter Server administrator using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vcenter_admin_password</td>
</tr>
</tbody>
</table>

   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.
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 Region B vRealize Operations Manager Implementation
   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 Region B vRealize Log Insight Implementation
   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 Region B vSphere Update Manager Download Service Implementation
   Install the vSphere Update Manager Download Service (UMDS) on a Linux virtual machine to download and store binaries and metadata in a shared repository in Region B.

Region B vRealize Operations Manager Implementation

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 2 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 service 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, add vCenter Adapter instances for the Management and Compute vCenter Server instances in Region B.

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 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.

7 Verify Connectivity of vRealize Operations Manager to vRealize Business in Region B
   To verify integration of VMware vRealize Business for Cloud with vRealize Operations Manager, run a Private Cloud Reclamation report from the vRealize Operations Manager operations interface. If the integration is interrupted, re-register the Compute vCenter Server in Region B with vRealize Business.

8 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.

9 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.

10 Configure NTP Server on vRealize Operations Manager Cluster in Region B
    To avoid misconfiguration of vRealize Operations Manager analytics cluster in case of fail over to Region B during disaster recovery, add Region B NTP Server in vRealize Operations Manager.

**Deploy vRealize Operations Manager in Region B**

In Region B, deploy 2 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. The remote collectors are used 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 4-1. Application Virtual Network Names for vRealize Operations Manager**

<table>
<thead>
<tr>
<th>vRealize Operations Manager Component</th>
<th>Application Virtual Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics Cluster</td>
<td>Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>Remote Collector Group</td>
<td>Mgmt-RegionB01-VXLAN</td>
</tr>
</tbody>
</table>
Table 4-2. IP Addresses and Host Names for the Remote Collector Nodes in Region B

<table>
<thead>
<tr>
<th>Role</th>
<th>IP Address</th>
<th>FQDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote collector node 1</td>
<td>192.168.32.31</td>
<td>lax01vropsc01a.lax01.rainpole.local</td>
</tr>
<tr>
<td>Remote collector node 2</td>
<td>192.168.32.32</td>
<td>lax01vropsc01b.lax01.rainpole.local</td>
</tr>
<tr>
<td>Default gateway</td>
<td>192.168.32.1</td>
<td>-</td>
</tr>
<tr>
<td>DNS server</td>
<td>172.17.11.5</td>
<td>-</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
<td>-</td>
</tr>
</tbody>
</table>

Deployment Prerequisites

Verify that your environment satisfies the following prerequisites for deployment of vRealize Operations Manager remote collector nodes.

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>Virtual disk provisioning.</td>
</tr>
<tr>
<td></td>
<td>- Thíñ</td>
</tr>
<tr>
<td></td>
<td>- Required storage per analytics cluster node to support replication and failover: 1TB</td>
</tr>
<tr>
<td></td>
<td>- Required storage per remote collector group nodes.</td>
</tr>
<tr>
<td></td>
<td>- Initial storage per node: 274GB</td>
</tr>
<tr>
<td>Software Features</td>
<td>Verify that vCenter Server is operational.</td>
</tr>
<tr>
<td></td>
<td>- Verify that the vSphere cluster has DRS and HA enabled.</td>
</tr>
<tr>
<td></td>
<td>- Verify that the NSX Manager is operational.</td>
</tr>
<tr>
<td></td>
<td>- Verify that the application virtual networks are available.</td>
</tr>
<tr>
<td></td>
<td>- Verify that the Load Balancer service is disabled on the NSX Edge service gateway.</td>
</tr>
<tr>
<td></td>
<td>- Verify vRealize Operations Manager Analytics Cluster is operational.</td>
</tr>
<tr>
<td></td>
<td>- Verify vRealize Log Insight is operational.</td>
</tr>
<tr>
<td></td>
<td>- Verify that vRealize Automation is operational.</td>
</tr>
<tr>
<td></td>
<td>- Verify that vRealize Business for Cloud is operational.</td>
</tr>
<tr>
<td></td>
<td>- Verify that Postman REST API App is installed in your browser.</td>
</tr>
</tbody>
</table>

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. The remote collectors are used 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of remote collector 1</td>
<td>lax01vropsc01a</td>
</tr>
<tr>
<td>Name of remote collector 2</td>
<td>lax01vropsc01b</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Data center</td>
<td>lax01-m01dc</td>
</tr>
<tr>
<td>Folder</td>
<td>lax01-m01fd-vropsrc</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data center</td>
<td>lax01-m01dc</td>
</tr>
<tr>
<td>Cluster</td>
<td>lax01-m01-mgmt01</td>
</tr>
</tbody>
</table>

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 datastore indicated in the table below, and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select virtual disk format</td>
<td>Thin provision</td>
</tr>
<tr>
<td>VM Storage Policy</td>
<td>vSAN Default Storage Policy</td>
</tr>
<tr>
<td>Datastore</td>
<td>lax01-m01-vsxn01</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS server</td>
<td>172.17.11.5</td>
</tr>
<tr>
<td>Default gateway</td>
<td>192.168.32.1</td>
</tr>
<tr>
<td>Static IPv4 address</td>
<td>192.168.32.31 for remote collector 1</td>
</tr>
<tr>
<td></td>
<td>192.168.32.32 for remote collector 2</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Timezone setting</td>
<td>Etc/UTC</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01vropsc01a</td>
<td>Remote collector 1</td>
</tr>
<tr>
<td>lax01vropsc01b</td>
<td>Remote collector 2</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Remote Collector Node</th>
<th>URL for Setup Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote collector 1</td>
<td><a href="https://lax01vropsc01a.lax01.rainpole.local">https://lax01vropsc01a.lax01.rainpole.local</a></td>
</tr>
<tr>
<td>Remote collector 2</td>
<td><a href="https://lax01vropsc01b.lax01.rainpole.local">https://lax01vropsc01b.lax01.rainpole.local</a></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node name</td>
<td>vrops01svr01a.rainpole.local</td>
</tr>
<tr>
<td>Node type</td>
<td>Remote Collector</td>
</tr>
<tr>
<td>Master node IP address or FQDN</td>
<td>vrops01svr01a.rainpole.local</td>
</tr>
</tbody>
</table>

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.


   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 UI of vRealize Operations Manager, click Finish Adding New Node(s) next to Cluster Status.
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 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 Configure tab.
4. Under the **Configuration** group of settings, select **VM/Host Rules**.
   
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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>anti-affinity-rule-vropsr</td>
</tr>
<tr>
<td>Enable rule</td>
<td>Selected</td>
</tr>
<tr>
<td>Type</td>
<td>Separate Virtual Machines</td>
</tr>
<tr>
<td>Members</td>
<td>lax01vropsc01a</td>
</tr>
<tr>
<td></td>
<td>lax01vropsc01b</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrops_admin_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>lax01-remote-collectors</td>
</tr>
<tr>
<td>Description</td>
<td>Remote collector group for lax01</td>
</tr>
<tr>
<td>lax01vropsc01a</td>
<td>Selected</td>
</tr>
<tr>
<td>lax01vropsc01b</td>
<td>Selected</td>
</tr>
</tbody>
</table>

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 service 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vrops-https</td>
</tr>
<tr>
<td>Type</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Enable SSL Passthrough</td>
<td>Selected</td>
</tr>
<tr>
<td>Persistence</td>
<td>Source IP</td>
</tr>
<tr>
<td>Expires in (Seconds)</td>
<td>1800</td>
</tr>
<tr>
<td>Client Authentication</td>
<td>Ignore</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vrops-443-monitor</td>
</tr>
<tr>
<td>Interval</td>
<td>3</td>
</tr>
<tr>
<td>Timeout</td>
<td>5</td>
</tr>
<tr>
<td>Max Retries</td>
<td>2</td>
</tr>
<tr>
<td>Type</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Method</td>
<td>GET</td>
</tr>
<tr>
<td>URL</td>
<td>/suite-api/api/deployment/node/status</td>
</tr>
<tr>
<td>Receive</td>
<td>ONLINE (must be upper case)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vrops-svr-443</td>
</tr>
<tr>
<td>Algorithm</td>
<td>LEASTCONN</td>
</tr>
<tr>
<td>Monitors</td>
<td>vrops-443-monitor</td>
</tr>
</tbody>
</table>

   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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Member</td>
<td>Selected</td>
</tr>
<tr>
<td>Name</td>
<td>vrops01svr01a</td>
</tr>
<tr>
<td></td>
<td>vrops01svr01b</td>
</tr>
<tr>
<td></td>
<td>vrops01svr01c</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.11.31</td>
</tr>
<tr>
<td></td>
<td>192.168.11.32</td>
</tr>
<tr>
<td></td>
<td>192.168.11.33</td>
</tr>
<tr>
<td>State</td>
<td>Enable</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
</tr>
<tr>
<td>Monitor Port</td>
<td>443</td>
</tr>
<tr>
<td>Weight</td>
<td>1</td>
</tr>
<tr>
<td>Max Connections</td>
<td>8</td>
</tr>
<tr>
<td>Min Connections</td>
<td>8</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Virtual Server</td>
<td>Selected</td>
</tr>
<tr>
<td>Application Profile</td>
<td>vrops-https</td>
</tr>
<tr>
<td>Name</td>
<td>vrops-svr-443</td>
</tr>
<tr>
<td>Description</td>
<td>vRealize Operations Manager Cluster</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.11.35</td>
</tr>
<tr>
<td>Protocol</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
</tr>
<tr>
<td>Default Pool</td>
<td>vrops-svr-443</td>
</tr>
<tr>
<td>Connection Limit</td>
<td>0</td>
</tr>
<tr>
<td>Connection Rate Limit</td>
<td>0</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vrops-http-redirect</td>
</tr>
<tr>
<td>Type</td>
<td>HTTP</td>
</tr>
<tr>
<td>HTTP Redirect URL</td>
<td><a href="https://vrops01svr01.rainpole.local/vcops-web-ent/login.action">https://vrops01svr01.rainpole.local/vcops-web-ent/login.action</a></td>
</tr>
<tr>
<td>Persistence</td>
<td>Source IP</td>
</tr>
<tr>
<td>Expires in (Seconds)</td>
<td>1800</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Virtual Server</td>
<td>Selected</td>
</tr>
<tr>
<td>Application Profile</td>
<td>vrops-http-redirect</td>
</tr>
<tr>
<td>Name</td>
<td>vrops-svr-80-redirect</td>
</tr>
<tr>
<td>Description</td>
<td>HTTP Redirect for vRealize Operations Manager</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.11.35</td>
</tr>
<tr>
<td>Protocol</td>
<td>HTTP</td>
</tr>
<tr>
<td>Port</td>
<td>80</td>
</tr>
<tr>
<td>Default Pool</td>
<td>NONE</td>
</tr>
<tr>
<td>Connection Limit</td>
<td>0</td>
</tr>
<tr>
<td>Connection Rate Limit</td>
<td>0</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrops_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Active Directory Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Display Name</td>
<td>LAX01.RAINPOLE.LOCAL</td>
</tr>
<tr>
<td>Source Type</td>
<td>Active Directory</td>
</tr>
<tr>
<td>Integration Mode</td>
<td>Basic</td>
</tr>
<tr>
<td>Domain/Subdomain</td>
<td>LAX01.RAINPOLE.LOCAL</td>
</tr>
<tr>
<td>Use SSL/TLS</td>
<td>Deselected</td>
</tr>
<tr>
<td>User Name</td>
<td><a href="mailto:svc-vrops@rainpole.local">svc-vrops@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-vrops_password</td>
</tr>
<tr>
<td>Settings under the Details section</td>
<td></td>
</tr>
<tr>
<td>Automatically synchronize user membership for configured groups</td>
<td>Selected</td>
</tr>
<tr>
<td>Host</td>
<td>dc51lax.lax01.rainpole.local</td>
</tr>
<tr>
<td>Port</td>
<td>389</td>
</tr>
<tr>
<td>Base DN</td>
<td>dc=LAX01,dc=RAINPOLE,dc=LOCAL</td>
</tr>
<tr>
<td>Common Name</td>
<td>userPrincipalName</td>
</tr>
</tbody>
</table>

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.

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, add vCenter Adapter instances for the Management and Compute vCenter Server instances 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrops_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value for Management vCenter Server</th>
<th>Value for Compute vCenter Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>vCenter Adapter - lax01m01vc01</td>
<td>vCenter Adapter - lax01w01vc01</td>
</tr>
<tr>
<td>Description</td>
<td>Management vCenter Server for lax01</td>
<td>Compute vCenter Server for lax01</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>
   c. Click the Add icon on the right side, configure the collection credentials for connection to the vCenter Server instances, and click OK.

<table>
<thead>
<tr>
<th>Management vCenter Server Credentials Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential name</td>
<td>vCenter Adapter Credentials - lax01m01vc01</td>
</tr>
<tr>
<td></td>
<td>vCenter Adapter Credentials - lax01w01vc01</td>
</tr>
<tr>
<td>User Name</td>
<td><a href="mailto:svc-vrops-vsphere@rainpole.local">svc-vrops-vsphere@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-vrops-vsphere-password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration user</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Registration password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

6. Click Define Monitoring Goals.

7. In the Define Monitoring Goals page, 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

   #unique_177/unique_177_Connect_42_step_CA2344B969D040E4B9562E2F72AA7CDD 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 that are required to access monitoring data from the Management NSX Manager and Compute Manager in Region B in vRealize Operations Manager to the operations local service account svc-vrops-nsx.

2 Add NSX-vSphere Adapter Instances to vRealize Operations Manager for Region B

Configure the connection between vRealize Operations Manager and the NSX instances for the management cluster and for the shared edge and compute cluster in Region B.

Configure User Privileges in NSX Manager for Integration with vRealize Operations Manager for Region B

Assign the permissions that are required to access monitoring data from the Management NSX Manager and Compute Manager in Region B in vRealize Operations Manager to the operations local service account svc-vrops-nsx.

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.

<table>
<thead>
<tr>
<th>NSX Manager</th>
<th>Host name</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager for the management cluster</td>
<td>lax01m01nsx01.lax01.rainpole.local</td>
</tr>
<tr>
<td>NSX Manager for the shared compute and edge cluster</td>
<td>lax01w01nsx01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>mgmtnsx_admin_password</td>
</tr>
<tr>
<td></td>
<td>compnsx_admin_password</td>
</tr>
</tbody>
</table>

2 Create the local service account svc-vrops-nsx on the NSX Manager instances.

   a Run the following command to switch to Privileged mode of the NSX Manager.

   ```
   enable
   ```

   b Enter the `mgmtnsx_admin_password` or `compnsx_admin_password` 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 Leave the Configuration mode.

```
exit
```

g Commit these updates to the NSX Managers:

```
copy running-config startup-config
``` 

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 In a Chrome Web browser, 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.

<table>
<thead>
<tr>
<th>NSX Manager</th>
<th>POST URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager for the management cluster</td>
<td><a href="https://lax01m01nsx01.lax01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true">https://lax01m01nsx01.lax01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true</a></td>
</tr>
<tr>
<td>NSX Manager for the shared edge and compute cluster</td>
<td><a href="https://lax01w01nsx01.lax01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true">https://lax01w01nsx01.lax01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true</a></td>
</tr>
</tbody>
</table>

e On the **Authorization** tab, configure the following authorization settings and click **Update Request**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Basic Auth</td>
</tr>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>mgmtnsx_admin_password</td>
</tr>
<tr>
<td></td>
<td>compnsx_admin_password</td>
</tr>
</tbody>
</table>

f On the **Headers** tab, enter the following header details.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Content-Type</td>
</tr>
<tr>
<td>Value</td>
<td>Application/xml</td>
</tr>
</tbody>
</table>
In the **Body** tab, select **raw** and paste the following request body in the **Body** text box and click **Send**.

```xml
<accessControlEntry>
  <role>security_admin</role>
  <resource>
    <resourceId>globalroot-0</resourceId>
  </resource>
</accessControlEntry>
```

The Status changes to **204 No Content**.

Repeat the step for the other NSX Manager.

**Add NSX-vSphere Adapter Instances to vRealize Operations Manager for Region B**

Configure the connection between vRealize Operations Manager and the NSX instances for the management cluster and for the shared edge and compute cluster 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrops_admin_password</td>
</tr>
</tbody>
</table>

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 for the management cluster or to the NSX Manager for the shared edge and compute cluster.

   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 and the FQDN of the vCenter Server instance that is connected to the NSX Manager.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value for the NSX Manager for the Management Cluster</th>
<th>Value for the NSX Manager for the Shared Edge and Compute Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>NSX Adapter - lax01m01nsx01</td>
<td>NSX Adapter - lax01w01nsx01</td>
</tr>
<tr>
<td>Description</td>
<td>Management NSX Manager for lax01</td>
<td>Compute NSX Manager for lax01</td>
</tr>
<tr>
<td>NSX Manager Host</td>
<td>lax01m01nsx01.lax01.rainpole.local</td>
<td>lax01w01nsx01.lax01.rainpole.local</td>
</tr>
<tr>
<td>VC Host</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Enable Log Insight integration if configured</td>
<td>false</td>
<td>false</td>
</tr>
</tbody>
</table>

   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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value for the NSX Manager for the Management Cluster</th>
<th>Value for the NSX Manager for the Shared Edge and Compute Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential name</td>
<td>NSX Adapter Credentials - lax01m01nsx01</td>
<td>NSX Adapter Credentials - lax01w01nsx01</td>
</tr>
<tr>
<td>NSX Manager User Name</td>
<td>svc-vrops-nsx</td>
<td>svc-vrops-nsx</td>
</tr>
<tr>
<td>NSX Manager Password</td>
<td>svc-vrops-nsx_password</td>
<td>svc-vrops-nsx_password</td>
</tr>
<tr>
<td>vCenter User Name</td>
<td><a href="mailto:svc-vrops-nsx@rainpole.local">svc-vrops-nsx@rainpole.local</a></td>
<td><a href="mailto:svc-vrops-nsx@rainpole.local">svc-vrops-nsx@rainpole.local</a></td>
</tr>
<tr>
<td>vCenter Password</td>
<td>svc-vrops-nsx-password</td>
<td>svc-vrops-nsx-password</td>
</tr>
</tbody>
</table>

   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.

   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.

k  Repeat this procedure to create an NSX-vSphere Adapter for the NSX Manager for the shared edge and compute cluster.

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.

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
<tr>
<td>Domain</td>
<td>Rainpole.local</td>
</tr>
</tbody>
</table>
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 **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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrops_admin_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Role</td>
<td>ReadOnly</td>
</tr>
<tr>
<td>Assign this role to the user</td>
<td>Selected</td>
</tr>
<tr>
<td>Select Object</td>
<td>vCenter Adapter &gt; vCenter Adapter - lax01w01vc01</td>
</tr>
</tbody>
</table>
Verify Connectivity of vRealize Operations Manager to vRealize Business in Region B

To verify integration of VMware vRealize Business for Cloud with vRealize Operations Manager, run a Private Cloud Reclamation report from the vRealize Operations Manager operations interface. If the integration is interrupted, re-register the Compute vCenter Server in Region B with vRealize Business.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrops_admin_password</td>
</tr>
</tbody>
</table>

2. On the main navigation bar, click Home.

3. In the left pane of vRealize Operations Manager, click Business Management.

4. Log in to vRealize Business using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>itac-tenantadmin</td>
</tr>
<tr>
<td>Tenant</td>
<td>rainpole</td>
</tr>
<tr>
<td>Password</td>
<td>itac-tenantadmin_password</td>
</tr>
</tbody>
</table>

   The dashboard of vRealize Business opens on the Business Management page of the vRealize Operations Manager operations interface.

5. On the Business Management page, click Overview and locate the Private Cloud Reclamation widget on the right.

6. If on running the report, the integration message Cost Savings from Private Cloud reclamation requires integration with vRealize Operations Manager appears, re-register vRealize Business with the Compute vCenter Server in Region B.
   a. Open a Web browser and go to https://lax01vrbc01.lax01.rainpole.local:5480.
   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vrb_collector_root_password</td>
</tr>
</tbody>
</table>
   c. Click Manage Private Cloud Connections and select vCenter Server.
d. Select the Compute vCenter Server lax01w01vc01.lax01.rainpole.local and click the Delete icon.

The connection to the Compute vCenter Server is removed.

e. Click Add.

f. In the Add vCenter Server Connections dialog box, enter the following settings and click Save.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:svc-vra@rainpole.local">svc-vra@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc_vra_password</td>
</tr>
</tbody>
</table>

g. In the SSL Certificate dialog box, click Install.

h. In the Success dialog box, click OK.

7. Wait a few minutes for vRealize Business for Cloud to initiate a synchronization, run the report again and verify that it is generated successfully.

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.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrops_admin_password</td>
</tr>
</tbody>
</table>

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.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value for the Management Cluster</th>
<th>Value for the Shared Edge and Compute Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Storage Devices Adapter - lax01m01vc01</td>
<td>Storage Devices Adapter - lax01w01vc01</td>
</tr>
<tr>
<td>Description</td>
<td>Storage Devices in Management vCenter for lax01</td>
<td>Storage Devices in Compute vCenter for lax01</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>SNMP Community</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Strings</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

   c Click the **Add** icon on the right side, configure the collection credentials for connection to the vCenter Server instances, and click **OK**.

<table>
<thead>
<tr>
<th>vCenter Server Credentials Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential name</td>
<td>Storage Devices Adapter Credentials - lax01m01vc01</td>
</tr>
<tr>
<td></td>
<td>Storage Devices Adapter Credentials - lax01w01vc01</td>
</tr>
<tr>
<td>User Name</td>
<td><a href="mailto:svc-vrops-mpsd@rainpole.local">svc-vrops-mpsd@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-vrops-mpsd-password</td>
</tr>
</tbody>
</table>

   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 VMware VSAN cluster, the performance service is disabled. Turn on 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 cluster's 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vSphere_admin_password</td>
</tr>
</tbody>
</table>

2. Enable the vSAN Performance Service.
   a. In the navigator, expand the `lax01-m01dc` Datacenter object.
   b. Click the `lax01-m01-mgmt01` cluster object then click the Configure tab.
   c. Under vSAN, select Health and Performance.
   d. Under Performance Service settings click Edit.
   e. Click the Turn ON vSAN performance service check box.
   f. Select the vSAN Default Storage Policy and click OK.

3. Repeat the procedure above if you have vSAN configured in the shared edge and compute `lax01-w01-comp01` cluster in Region B.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrops_admin_password</td>
</tr>
</tbody>
</table>

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 vCenter Server instances.

   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value for the Management vCenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>vSAN Adapter - lax01m01vc01</td>
</tr>
<tr>
<td>Description</td>
<td>Management vCenter Server VSAN Adapter for lax01</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

   c. Click the Add icon, and configure the credentials for connection to the vCenter Server, and click OK.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value for the Management vCenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential name</td>
<td>vSAN Adapter Credentials - lax01m01vc01</td>
</tr>
<tr>
<td>vCenter User Name</td>
<td><a href="mailto:svc-vrops-vsan@rainpole.local">svc-vrops-vsan@rainpole.local</a></td>
</tr>
<tr>
<td>vCenter Password</td>
<td>svc-vrops-vsan-password</td>
</tr>
</tbody>
</table>

   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 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  Repeat the steps above if you have vSAN configured in the shared edge and compute cluster.

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 Operations Manager analytics cluster in case of fail over to Region B during disaster recovery, add Region B NTP Server in vRealize Operations Manager.

Prerequisites

Make sure NTP Server for Region A is configured

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrops_admin_password</td>
</tr>
</tbody>
</table>

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.

Region B vRealize Log Insight Implementation

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**
   You can obtain the CA-signed vRealize Log Insight PEM certificate chain file that contains the own certificate, the signer certificate and the private key file by using the `CertGenVVD` tool.

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 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. **Connect vRealize Log Insight to vRealize Automation in Region B**
   Connect the vRealize Log to vRealize Automation to receive log information from the components of vRealize Automation in Region B in the vRealize Log Insight UI.

7. **Install the Linux Content Pack 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 about the management virtual appliances in vRealize Log Insight.

8. **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 vRealize Log Insight Design document.

9. **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 4-3. IP Addresses and Host Name for the vRealize Log Insight Cluster in Region B

<table>
<thead>
<tr>
<th>Role</th>
<th>IP Address</th>
<th>FQDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated load balancer VIP</td>
<td>192.168.32.10</td>
<td>lax01vrl01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Master node</td>
<td>192.168.32.11</td>
<td>lax01vrl01a.lax01.rainpole.local</td>
</tr>
<tr>
<td>Worker node 1</td>
<td>192.168.32.12</td>
<td>lax01vrl01b.lax01.rainpole.local</td>
</tr>
<tr>
<td>Worker node 2</td>
<td>192.168.32.13</td>
<td>lax01vrl01c.lax01.rainpole.local</td>
</tr>
<tr>
<td>Default gateway</td>
<td>192.168.32.1</td>
<td>-</td>
</tr>
<tr>
<td>DNS servers</td>
<td>172.17.11.5</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>172.17.11.4</td>
<td>-</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
<td>-</td>
</tr>
<tr>
<td>NTP servers</td>
<td>172.16.11.251</td>
<td>ntp.sfo01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td>172.16.11.252</td>
<td>ntp.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td>172.17.11.251</td>
<td></td>
</tr>
<tr>
<td></td>
<td>172.17.11.252</td>
<td></td>
</tr>
</tbody>
</table>

### Deployment Prerequisites

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>- Virtual disk provisioning</td>
</tr>
<tr>
<td></td>
<td>■ Thin</td>
</tr>
<tr>
<td></td>
<td>■ Required storage per node</td>
</tr>
<tr>
<td></td>
<td>■ Initial storage for node deployment: 510 GB</td>
</tr>
<tr>
<td></td>
<td>■ Required storage for cluster archiving</td>
</tr>
<tr>
<td></td>
<td>■ Initial storage for archiving: 400 GB</td>
</tr>
<tr>
<td>Software Features</td>
<td>- vSphere</td>
</tr>
<tr>
<td></td>
<td>■ Management vCenter Server</td>
</tr>
<tr>
<td></td>
<td>■ Management cluster with DRS and HA enabled.</td>
</tr>
<tr>
<td></td>
<td>■ NSX for vSphere</td>
</tr>
<tr>
<td></td>
<td>■ Application virtual network for the 3-node vRealize Log Insight cluster</td>
</tr>
<tr>
<td>Installation Package</td>
<td>Download the .ova file of the vRealize Log Insight virtual appliance on the machine where you use the vSphere Web Client.</td>
</tr>
<tr>
<td>License</td>
<td>Obtain a license that covers the use of vRealize Log Insight.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>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.</td>
</tr>
<tr>
<td>Certification Authority</td>
<td>Configure the Active Directory domain controller as a certificate authority for the environment.</td>
</tr>
<tr>
<td>E-mail account</td>
<td>Provide an email account to send vRealize Log Insight notifications from.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data center</td>
<td>lax01-m01dc</td>
</tr>
<tr>
<td>Cluster</td>
<td>lax01-m01fd-mgmt01</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select virtual disk format</td>
<td>Thin provision</td>
</tr>
<tr>
<td>VM Storage Policy</td>
<td>vSAN Default Storage Policy</td>
</tr>
<tr>
<td>Datastore</td>
<td>lax01-m01-vsan01</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS server</td>
<td>172.17.11.5,172.17.11.4</td>
</tr>
<tr>
<td>DNS domain</td>
<td>lax01.rainpole.local</td>
</tr>
<tr>
<td>DNS searchpath</td>
<td>lax01.rainpole.local,rainpole.local</td>
</tr>
<tr>
<td>Default gateway</td>
<td>192.168.32.1</td>
</tr>
</tbody>
</table>
   | 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.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Rule Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>anti-affinity-rule-vrli</td>
</tr>
<tr>
<td>Enable rule</td>
<td>Yes</td>
</tr>
<tr>
<td>Type</td>
<td>Separate Virtual Machines</td>
</tr>
<tr>
<td>Members</td>
<td>lax01vrli01a</td>
</tr>
<tr>
<td></td>
<td>lax01vrli01b</td>
</tr>
<tr>
<td></td>
<td>lax01vrli01c</td>
</tr>
</tbody>
</table>

**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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email System Notifications to</td>
<td>email address to receive system notifications</td>
</tr>
<tr>
<td>Send HTTP Post System Notifications To</td>
<td><a href="https://lax01vrl01.lax01.rainpole.local">https://lax01vrl01.lax01.rainpole.local</a></td>
</tr>
</tbody>
</table>

7 On the **Time Configuration** page, enter the following settings, click **Test** and click **Save and Continue**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync Server Time With</td>
<td>NTP Server (recommended)</td>
</tr>
<tr>
<td>NTP Servers</td>
<td>ntp.lax01.rainpole.local, ntp.sfo01.rainpole.local</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>SMTP Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server</td>
<td>FQDN of the SMTP server</td>
</tr>
<tr>
<td>Port</td>
<td>Server port for SMTP requests</td>
</tr>
<tr>
<td>SSL (SMTPS)</td>
<td>Sets whether encryption should be enabled for the SMTP transport option connection.</td>
</tr>
<tr>
<td>STARTTLS Encryption</td>
<td>Enable or disable the STARTTLS encryption.</td>
</tr>
<tr>
<td>Sender</td>
<td>Address that appears as the sender of the email.</td>
</tr>
<tr>
<td>Username</td>
<td>User name on the SMTP server</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the SMTP server you specified in Username.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Worker Node</th>
<th>HTTP URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worker node 1</td>
<td><a href="https://lax01vrli01b.lax01.rainpole.local">https://lax01vrli01b.lax01.rainpole.local</a></td>
</tr>
<tr>
<td>Worker node 2</td>
<td><a href="https://lax01vrli01c.lax01.rainpole.local">https://lax01vrli01c.lax01.rainpole.local</a></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>

2. Click the configuration drop-down menu icon and select Administration.


5. In the New Virtual IP dialog box, enter the following settings and click Save.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>192.168.32.10</td>
</tr>
<tr>
<td>FQDN</td>
<td>lax01vrli01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

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 4-1. 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>
2 On the **Authentication** page, select the checkbox 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Active Directory support</td>
<td>Selected</td>
</tr>
<tr>
<td>Default Domain</td>
<td>RAINPOLE.LOCAL</td>
</tr>
<tr>
<td>Domain Controller(s)</td>
<td>dc51rpl.rainpole.local</td>
</tr>
<tr>
<td>User Name</td>
<td>svc-vrli</td>
</tr>
<tr>
<td>Password</td>
<td>svc_vrli_password</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Standard</td>
</tr>
<tr>
<td>Require SSL</td>
<td>Yes or No according to the instructions from the IT administrator</td>
</tr>
</tbody>
</table>

   b  Click **Test Connection** to verify the connection, and click **Save**.

---

**Replace the Certificate to vRealize Log Insight in Region B**

You can obtain the CA-signed vRealize Log Insight PEM certificate chain file that contains the own certificate, the signer certificate and the private key file by using the CertGenVVD tool.

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Certificate Generation Option</th>
<th>Certificate File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the CertGenVVD tool</td>
<td>vrli.lax01.2.chain.pem</td>
</tr>
</tbody>
</table>

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-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 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 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.
   - Open a Web browser and go to https://lax01vrli01.lax01.rainpole.local.
   - Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>

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.
   - Enter the host name, user credentials, and collection options for the vCenter Server instances, and click Test Connection.

<table>
<thead>
<tr>
<th>vCenter Server Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>lax01m01vc01.lax01.rainpole.local for Management vCenter Server</td>
</tr>
<tr>
<td></td>
<td>lax01w01vc01.lax01.rainpole.local for Compute vCenter Server</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:svc-vrli@rainpole.local">svc-vrli@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-vrli_user_password</td>
</tr>
<tr>
<td>Collect vCenter Server events, tasks and alarms</td>
<td>Selected</td>
</tr>
<tr>
<td>Configure ESXi hosts to send logs to Log Insight</td>
<td>Selected</td>
</tr>
</tbody>
</table>

   - 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.

   - 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:

<table>
<thead>
<tr>
<th>Appliance Type</th>
<th>Appliance Management Interface URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server instances</td>
<td>- <a href="https://lax01vc01.lax01.rainpole.local:5480">https://lax01vc01.lax01.rainpole.local:5480</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://lax01w01vc01.lax01.rainpole.local:5480">https://lax01w01vc01.lax01.rainpole.local:5480</a></td>
</tr>
<tr>
<td>Platform Services Controller instances</td>
<td>- <a href="https://lax01psc01.lax01.rainpole.local:5480">https://lax01psc01.lax01.rainpole.local:5480</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://lax01w01psc01.lax01.rainpole.local:5480">https://lax01w01psc01.lax01.rainpole.local:5480</a></td>
</tr>
</tbody>
</table>

**Procedure**

1. Redirect the log events from the appliance to vRealize Log Insight.
   a. Open a Web browser and go to `https://lax01vc01.lax01.rainpole.local:5480`.
   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>mgmtvc_root_password</td>
</tr>
</tbody>
</table>

   c. In the **Navigator**, click **Syslog Configuration**.
   d. On the **Syslog Configuration** page, click **Edit**, configure the following settings, and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Log Level</td>
<td>*</td>
</tr>
<tr>
<td>Remote Syslog Host</td>
<td>lax01vrli01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Remote Syslog Port</td>
<td>514</td>
</tr>
<tr>
<td>Remote Syslog Protocol</td>
<td>UDP</td>
</tr>
</tbody>
</table>

   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>
In the vRealize Log Insight user interface, click **Dashboards** and select **VMware - vSphere** under **Content Pack Dashboards**.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value for the Management Cluster</th>
<th>Value for the Shared Edge and Computer Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server URL</td>
<td><a href="https://lax01m01vc01.lax01.rainpole.local/vsphere-client/">https://lax01m01vc01.lax01.rainpole.local/vsphere-client/</a></td>
<td><a href="https://lax01w01vc01.lax01.rainpole.local/vsphere-client/">https://lax01w01vc01.lax01.rainpole.local/vsphere-client/</a></td>
</tr>
<tr>
<td>Host Profiles</td>
<td>lax01-m01hp-mgmt01</td>
<td>lax01-w01hp-mgmt01</td>
</tr>
<tr>
<td>First ESXi host</td>
<td>lax01m01esx01.lax01.rainpole.local</td>
<td>lax01w01esx01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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 above procedure with Hosts in the Shared Edge and Compute cluster with the following setting

**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 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.

**Prerequisites**

- Verify that the vRealize Log Insight management pack is installed in vRealize Operations Manager
- Verify that you have connected vRealize Operations Manager to the lax01m01vc01.lax01.rainpole.local or lax01w01vc01.sfo01.rainpole.local vCenter Server instances.
- Verify that you have connected vRealize Log Insight to the lax01m01vc01.lax01.rainpole.local or lax01w01vc01.lax01.rainpole.local vCenter Server instances.
- Verify that you have configured the svc-vrli-vrops@rainpole.local service account within 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>vrops01svr01.rainpole.local</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:svc-vrli-vrops@rainpole.local">svc-vrli-vrops@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-vrli-vrops_password</td>
</tr>
<tr>
<td>Enable alerts integration</td>
<td>Selected</td>
</tr>
<tr>
<td>Enable launch in context</td>
<td>Deselected</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrops_admin_password</td>
</tr>
</tbody>
</table>

Deployment for Region B
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 vRealize Log Insight** dialog box appears.

5 Click on Add icon above **Instance Name**

6 Under **Instance Settings**, enter the settings for connection to vRealize Log Insight.

   a Enter the display name, description and the FQDN of the vRealize Log Insight instance.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value for vRealize Log Insight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Log Insight Adapter - lax01vrl01</td>
</tr>
<tr>
<td>Description</td>
<td>vRealize Log Insight for lax01</td>
</tr>
<tr>
<td>Log Insight server</td>
<td>lax01vrl01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

   b Click **Test Connection** to validate the connection to vRealize Log Insight.

   c Click **OK** in the **Info** box.

   d Expand the **Advanced Settings** pane and select **lax01-remote_collectors** from the **Collectors/Groups** drop-down menu.

   e Click **Save Settings**.

   f Click **OK** in the **Info** box.

7 In the **Manage Solution - VMware vRealize Log Insight** dialog box, click **Close**.

8 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>
   c. Under the lax01m01vc01.lax01.rainpole.local vCenter Server, navigate to the virtual appliance for the node.

<table>
<thead>
<tr>
<th>Virtual Appliance Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01vrops01a</td>
<td>Remote collector 1</td>
</tr>
<tr>
<td>lax01vrops01b</td>
<td>Remote collector 2</td>
</tr>
</tbody>
</table>
   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vrops_root_password</td>
</tr>
</tbody>
</table>
   g. Start the SSH service by running the command.

   ```bash
   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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>lax01vropsc01a.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td>lax01vropsc01b.lax01.rainpole.local</td>
</tr>
<tr>
<td>Username</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vrops_root_password</td>
</tr>
</tbody>
</table>

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=lax01vrl01.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:

```plaintext
[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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Location in liagent.ini</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmw_vr_ops_nodename</td>
<td>IP address or FQDN of the vRealize Operations Manager node</td>
<td>Replace each <code>&lt;Your VROPS Node Name Here&gt;</code> with the following names:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>lax01vropsc01a</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>lax01vropsc01b</code></td>
</tr>
<tr>
<td>vmw_vr_ops_hostname</td>
<td>Name of the vRealize Operations Manager node that is set during node initial configuration</td>
<td>Replace each <code>&lt;Your VROPS Hostname Here&gt;</code> with the following names:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>lax01vropsc01a.lax01.rainpole.local</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>lax01vropsc01b.lax01.rainpole.local</code></td>
</tr>
</tbody>
</table>

Use the following as an 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:

```plaintext
[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"}
```

e Press Esc and enter :wq! to save the file.

f Restart the Log Insight agent on node by running the following console command.

```
/etc/init.d/liagentd restart
```

g Verify that the Log Insight agent is running.

```
/etc/init.d/liagentd status
```

h Stop the SSH service on the virtual appliance by running the following command.

```
service sshd stop
```

i Repeat the steps for the second remote collector node.
3 Configure the Linux 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrii_admin_password</td>
</tr>
</tbody>
</table>

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 vRops6 – 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.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>matches</td>
<td>lax01vropsc01a.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>lax01vropsc01b.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

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 Managers 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 for Google Chrome.

4 Configure the NSX Edge Instances to Forward Log Events to vRealize Log Insight in Region B
Configure the NSX Edge service 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrl_admin_password</td>
</tr>
</tbody>
</table>

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 Managers 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.

<table>
<thead>
<tr>
<th>NSX Manager</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager for the management cluster</td>
<td><a href="https://lax01m01nsx01.lax01.rainpole.local">https://lax01m01nsx01.lax01.rainpole.local</a></td>
</tr>
<tr>
<td>NSX Manager for the shared compute and edge cluster</td>
<td><a href="https://lax01w01nsx01.lax01.rainpole.local">https://lax01w01nsx01.lax01.rainpole.local</a></td>
</tr>
</tbody>
</table>

   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>nsx_manager_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Syslog Server Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog Server</td>
<td>lax01vrli01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Port</td>
<td>514</td>
</tr>
<tr>
<td>Protocol</td>
<td>UDP</td>
</tr>
</tbody>
</table>

5. Repeat the steps for the other NSX Manager.

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 for Google Chrome.

Prerequisites

On a Windows host that has access to your data center, install a REST client, such as the Postman for Google Chrome.

Procedure

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

2. In a Chrome browser, start the Postman application.
3 Specify the request headers for requests to the NSX Manager.
   a On the **Authentication** tab, configure the following authorization settings and click **Update Request**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Basic Auth</td>
</tr>
<tr>
<td>Username</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>lax01m01nsx01_admin_password</td>
</tr>
<tr>
<td></td>
<td>lax01w01nsx01_admin_password</td>
</tr>
</tbody>
</table>

   The **Authorization:Basic XXX** header appears in the **Headers** pane.

   b On the **Headers** tab, enter the following header details.

<table>
<thead>
<tr>
<th>Request Header Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>application/xml</td>
</tr>
</tbody>
</table>

   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**.

<table>
<thead>
<tr>
<th>NSX Manager</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager for the management cluster</td>
<td><a href="https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller">https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller</a></td>
</tr>
<tr>
<td>NSX Manager for the shared compute and edge cluster</td>
<td><a href="https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller">https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller</a></td>
</tr>
</tbody>
</table>

   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.

<table>
<thead>
<tr>
<th>NSX Manager</th>
<th>NSX Controller in the Controller Cluster</th>
<th>POST URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager for the management</td>
<td>NSX Controller 4</td>
<td><a href="https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/control/cluster/4/syslog">https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/control/cluster/4/syslog</a></td>
</tr>
<tr>
<td>cluster</td>
<td>NSX Controller 5</td>
<td><a href="https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/control/cluster/5/syslog">https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/control/cluster/5/syslog</a></td>
</tr>
<tr>
<td></td>
<td>NSX Controller 6</td>
<td><a href="https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/control/cluster/6/syslog">https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/control/cluster/6/syslog</a></td>
</tr>
<tr>
<td>NSX Manager for the shared edge</td>
<td>NSX Controller 4</td>
<td><a href="https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/control/cluster/4/syslog">https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/control/cluster/4/syslog</a></td>
</tr>
<tr>
<td>and compute cluster</td>
<td>NSX Controller 5</td>
<td><a href="https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/control/cluster/5/syslog">https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/control/cluster/5/syslog</a></td>
</tr>
<tr>
<td></td>
<td>NSX Controller 6</td>
<td><a href="https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/control/cluster/6/syslog">https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/control/cluster/6/syslog</a></td>
</tr>
</tbody>
</table>

   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.

   ```xml
   <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, enter the controller-specific syslog URL from POST URL from the table above 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 service 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>NSX Manager Instance</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager for the management cluster</td>
<td>172.17.11.65</td>
</tr>
<tr>
<td>NSX Manager for the shared edge and compute cluster</td>
<td>172.17.11.66</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Traffic</th>
<th>Management NSX Edge Service Gateway</th>
<th>Compute NSX Edge Service Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>North-South Routing</td>
<td>lax01m01esg01</td>
<td>lax01w01esg01</td>
</tr>
<tr>
<td>North-South Routing</td>
<td>lax01m01esg02</td>
<td>lax01w01esg02</td>
</tr>
<tr>
<td>East-West Routing</td>
<td>-</td>
<td>lax01w01dir01</td>
</tr>
<tr>
<td>Load Balancer</td>
<td>lax01m01lb01</td>
<td>-</td>
</tr>
<tr>
<td>PSC Load Balancer</td>
<td>lax01psc01</td>
<td>-</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog server 1</td>
<td>192.168.32.10</td>
</tr>
<tr>
<td>Protocol</td>
<td>udp</td>
</tr>
</tbody>
</table>

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.

**Connect vRealize Log Insight to vRealize Automation in Region B**

Connect the 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 following content packs for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server to add the dashboards for viewing log information in vRealize Log Insight.

2 **Configure the vRealize Automation Proxy Agents to Forward Log Events to vRealize Log Insight 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 **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.
Install the vRealize Log Insight Content Pack for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server in Region B

Install the following content packs for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server to add the dashboards for viewing log information in vRealize Log Insight.

The content packs are available under the following names in the vRealize Log Insight user interface:

- 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrl1_admin_password</td>
</tr>
</tbody>
</table>

2. In the vRealize Log Insight user interface, click the configuration drop-down menu icon and select Content Packs.


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.

Configure the vRealize Automation Proxy Agents to Forward Log Events to vRealize Log Insight 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. Install Log Insight Windows Agents in all the vRealize Automation Windows VMs.
   a. Open a Remote Desktop Protocol (RDP) connection to each of the following vRealize Automation virtual machines.

<table>
<thead>
<tr>
<th>vRealize Automation Component</th>
<th>Host Name/VM Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere Proxy Agent</td>
<td>lax01ias01a.lax01.rainpole.local</td>
</tr>
<tr>
<td>vSphere Proxy Agent</td>
<td>lax01ias01b.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Rainpole\svc-vra</td>
</tr>
<tr>
<td>Password</td>
<td>svc-vra_user_password</td>
</tr>
</tbody>
</table>

   c. On the Windows host, open a Web browser and go to https://lax01vrli01.lax01.rainpole.local.

   d. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>

   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 lax01vrli01.lax01.rainpole.local selected in the Host text box, click Install.

   m. After the installation is complete, click Finish.

   n. Repeat the steps for the other vRealize Automation virtual machines.
2 Configure the Log Insight Windows Agents Group from 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>

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 vRealize Automation 7 - Windows from the Available Templates section.
f Click Copy Template.
g In the Copy Agent Group dialog box, enter vRA7 - Windows Agent Group in the name text box and click Copy.
h Configure the following agent filter.
   Press Enter to separate the host names.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Operator</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>matches</td>
<td>lax01ias01a.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>lax01ias01b.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

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.

All VMware vRA 7 dashboards become available on the vRealize Log Insight Home 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 SSH on both 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 |
      |------------------------|--------------------------------------------|
      | vRealize Business Data Collector | https://lax01vrbc01.lax01.rainpole.local:5480 |
      
   b  Log in using the following credentials.  
      
      | Setting     | Value                      |
      |-------------|-----------------------------|
      | User name   | root                        |
      | Password    | vrb_server_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      | lax01vrb01.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=lax01vrl01.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.

```
[lax01vrbc01.lax01.rainpole.local]
```

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 Confirm that the Log Insight agents are working in the vRealize Log Insight Web interface.

a Open a Web browser and go to https://lax01vrli01.lax01.rainpole.local.

b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>

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.
Install the Linux Content Pack 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 about the management virtual appliances in vRealize Log Insight.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrii_admin_password</td>
</tr>
</tbody>
</table>

2 Install the content pack for VMware Linux.
   a In the vRealize Log Insight user interface, click the configuration drop-down menu icon and select Content Packs.
   b Under Content Pack Marketplace, select Marketplace.
   c In the list of content packs, locate the Linux content pack and click its icon.
   d In the Install Content Pack dialog box, accept the License Agreement and click Install.
   e After the installation is complete, the Linux content pack appears in the Installed Content Packs list on the left.

3 Configure the Log Insight Linux agent group for the virtual appliances from the vRealize Log Insight user interface.
   a Click the configuration drop-down menu icon and select Administration.
   b Under Management, click Agents.
   c From the drop-down at the top, select Linux from the Available Templates section.
   d Click Copy Template.
   e In the Copy Agent Group dialog box, enter vAppliances - Agent Group in the Name text box and click Copy.
f  In the agent filter fields, use the following selections.

Press ENTER to separate the host name values.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Operator</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>matches</td>
<td>lax01vropsc01a.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>lax01vropsc01b.lax01.rainpole.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>lax01vrbc01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

g  Click Refresh and verify that all the agents listed in the filter appear in the Agents list.

h  Click Save New Group at the bottom of the page.

4 Verify logs data is showing up on the Linux dashboards.
   a  On the main navigation bar, click Dashboards.
   b  Expand Linux and click Security - Overview, you should see events showing up 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 vRealize Log Insight Design document.

Prerequisites

- Create an NFS share of 1 TB in Region B and export it as /V2D_vRLI_MgmtB_400GB.
- The NFS server must support NFS v3.
- The NFS partition must allow reading and writing 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).

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrii_admin_password</td>
</tr>
</tbody>
</table>

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_vRLT_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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>sfo01vrli01a.sfo01.rainpole.local</td>
<td>Master node</td>
</tr>
<tr>
<td>sfo01vrli01b.sfo01.rainpole.local</td>
<td>Worker node 1</td>
</tr>
<tr>
<td>sfo01vrli01c.sfo01.rainpole.local</td>
<td>Worker node 2</td>
</tr>
</tbody>
</table>

   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vrii_regionA_root_password</td>
</tr>
</tbody>
</table>

   c. Create a working directory on the vRealize Log Insight node.

   ```bash
   mkdir /tmp/ssl
   cd /tmp/ssl
   ```
d Extract the root certificate from the destination vRealize Log Insight in the Region B.

```bash
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` in the Java keystore of the vRealize Log Insight node.

```bash
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`

When prompted to accept the certificate, type `yes`

h Reboot the vRealize Log Insight node by executing the following command

```bash
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Forwarding Destination Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>SFO01 to LAX01</td>
</tr>
<tr>
<td>Host</td>
<td>lax01vrli01a.lax01.rainpole.local</td>
</tr>
<tr>
<td>Forwarding Destination Setting</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Protocol</td>
<td>Ingestion API</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Selected</td>
</tr>
<tr>
<td>Tags</td>
<td>site='SFO01'</td>
</tr>
<tr>
<td>Advanced Settings</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>9543</td>
</tr>
<tr>
<td>Disk Cache</td>
<td>2000 MB</td>
</tr>
<tr>
<td>Worker Count</td>
<td>8</td>
</tr>
</tbody>
</table>

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.
Deployment for Region B

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>lax01vrl01a.lax01.rainpole.local</td>
<td>Master node</td>
</tr>
<tr>
<td>lax01vrl01b.lax01.rainpole.local</td>
<td>Worker node 1</td>
</tr>
<tr>
<td>lax01vrl01c.lax01.rainpole.local</td>
<td>Worker node 2</td>
</tr>
</tbody>
</table>

   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_regionB_root_password</td>
</tr>
</tbody>
</table>

   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 sfo01vrl01a.sfo01.rainpole.local -connect sfo01vrl01a.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`. 
Reboot the vRealize Log Insight node by executing the following command

```
reboot
```

Wait until the vRealize Log Insight node finished rebooting.

Repeat this operation on all vRealize Log Insight nodes in Region B.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>

In the vRealize Log Insight user interface, click the configuration drop-down menu icon and select **Administration**.

Under **Management**, click **Event Forwarding**.

On the **Event Forwarding** page, click **New Destination** and enter the following forwarding settings in the **New Destination** dialog box.

<table>
<thead>
<tr>
<th>Forwarding Destination Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LAX01 to SFO01</td>
</tr>
<tr>
<td>Host</td>
<td>sfo01vrli01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>Protocol</td>
<td>Ingestion API</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Selected</td>
</tr>
<tr>
<td>Tags</td>
<td>site=&quot;LAX01&quot;</td>
</tr>
<tr>
<td>Filter</td>
<td></td>
</tr>
<tr>
<td>Filter Type</td>
<td>site</td>
</tr>
<tr>
<td>Operator</td>
<td>does not match</td>
</tr>
<tr>
<td>Value</td>
<td>'SFO01'</td>
</tr>
<tr>
<td>Advanced Settings</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>9543</td>
</tr>
<tr>
<td>Disk Cache</td>
<td>2000 MB</td>
</tr>
<tr>
<td>Worker Count</td>
<td>8</td>
</tr>
</tbody>
</table>

In the **New Destination** dialog box, click **Test** to verify that the connection settings are correct.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>vrli_admin_password</td>
</tr>
</tbody>
</table>

2. In the vRealize Log Insight user interface, click the configuration drop-down menu icon and select Administration.


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.

<table>
<thead>
<tr>
<th>Filter Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Type</td>
<td>site</td>
</tr>
<tr>
<td>Operator</td>
<td>does not match</td>
</tr>
<tr>
<td>Value</td>
<td>'LAX01'</td>
</tr>
</tbody>
</table>

5. Click Save.

The Event Forwarding page in the vRealize Log Insight user interface shows a summary of the forwarded events.

Region B vSphere Update Manager Download Service Implementation

Install the vSphere Update Manager Download Service (UMDS) on a Linux virtual machine to download and store binaries and metadata in a shared repository in Region B.
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 in Region B, install the UMDS software.

3  Set Up the Data to Download with UMDS in Region B
   By default UMDS downloads patch binaries, patch metadata, and notifications for hosts. Specify which patch binaries and patch metadata to download with UMDS in Region B.

4  Install and Configure the UMDS Web Server in Region B
   The UMDS server in Region B 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 Update Manager to use the UMDS shared repository in Region B 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 on the management cluster of Region B. 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

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.

   ```bash
   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:

   ```bash
   sudo apt-get -y install vim perl tar sed psmisc unixodbc postgresql postgresql-contrib odbc-postgresql
   sudo service postgresql start
   ```

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.

   ```bash
   sudo su - postgres
   createdb umds_db
   createuser -d -e -r umds_db_user -P
   ```

8 Enable password authentication for the database user.

   a Navigate to the folder that contains the PostgreSQL configuration file `pg_hba.conf`.

   ```bash
   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.

   ```plaintext
   #TYPE DATABASE USER ADDRESS METHOD
   local umds_db umds_db_user md5
   ```

   c Log out as a PostgreSQL user by running the following command.

   ```bash
   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
   ```

   ```
   [PostgreSQL]
   Description=PostgreSQL ODBC driver (Unicode version)
   Driver=/usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so
   Debug=0
   CommLog=1
   UsageCount=1
   ```

   b  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_user
   User = umds_db_user
   Database = umds_db
   ```

   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_user
   User = umds_db_user
   Database = umds_db
   ```

10  Create a symbolic link between the UMDS and the 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 in Region B, 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>svc-umds</td>
</tr>
<tr>
<td>Password</td>
<td>svc-umds_password</td>
</tr>
</tbody>
</table>

2. Mount the vCenter Server Appliance ISO to the UMDS virtual machine.

   ```
   sudo mkdir -p /mnt/cdrom
   sudo mount /dev/cdrom /mnt/cdrom
   ```

3. Unarchive the `VMware-UMDS-6.5.0--build_number.tar.gz` file:

   ```
   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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide the database DSN</td>
<td>UMDS_DSN</td>
</tr>
<tr>
<td>Provide the database username</td>
<td>umds_db_user</td>
</tr>
<tr>
<td>Provide the database password</td>
<td>umds_db_user_password</td>
</tr>
</tbody>
</table>

10. Type `yes` and press Enter to install UMDS.
Set Up the Data to Download with UMDS in Region B

By default UMDS downloads patch binaries, patch metadata, and notifications for hosts. Specify which patch binaries and patch metadata to download with UMDS in Region B.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>svc-umds</td>
</tr>
<tr>
<td>Password</td>
<td>svc-umds_password</td>
</tr>
</tbody>
</table>

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

   cd /etc/cron.daily/
   sudo touch umds-download
   sudo chmod 755 umds-download

5. Edit the download command to 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 in Region B 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 VUM instances within 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>svc-umds</td>
</tr>
<tr>
<td>Password</td>
<td>svc-umds_password</td>
</tr>
</tbody>
</table>

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 text.

   ```
   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;
   }
   ```
Deployment for Region B

```bash
# Uncomment to enable naxsi on this location
# include /etc/nginx/naxsi.rules
autoindex on;
```

6 Disable the existing default site.

```bash
sudo rm /etc/nginx/sites-enabled/default
```

7 Enable the new UMDS site.

```bash
sudo ln -s /etc/nginx/sites-available/umds /etc/nginx/sites-enabled/
```

8 Restart the Nginx Web service to apply the new configuration.

```bash
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 Update Manager to use the UMDS shared repository in Region B 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2 On the Home page of the vSphere Web Client, click the Update Manager icon.

3 From the Objects tab, click the `lax01m01vc01.lax01.rainpole.local` vCenter Server for Region B.
   
   The Objects tab also displays all the vCenter Server system 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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a shared repository</td>
<td>Selected</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://lax01umds01.lax01.rainpole.local">http://lax01umds01.lax01.rainpole.local</a></td>
</tr>
</tbody>
</table>

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.