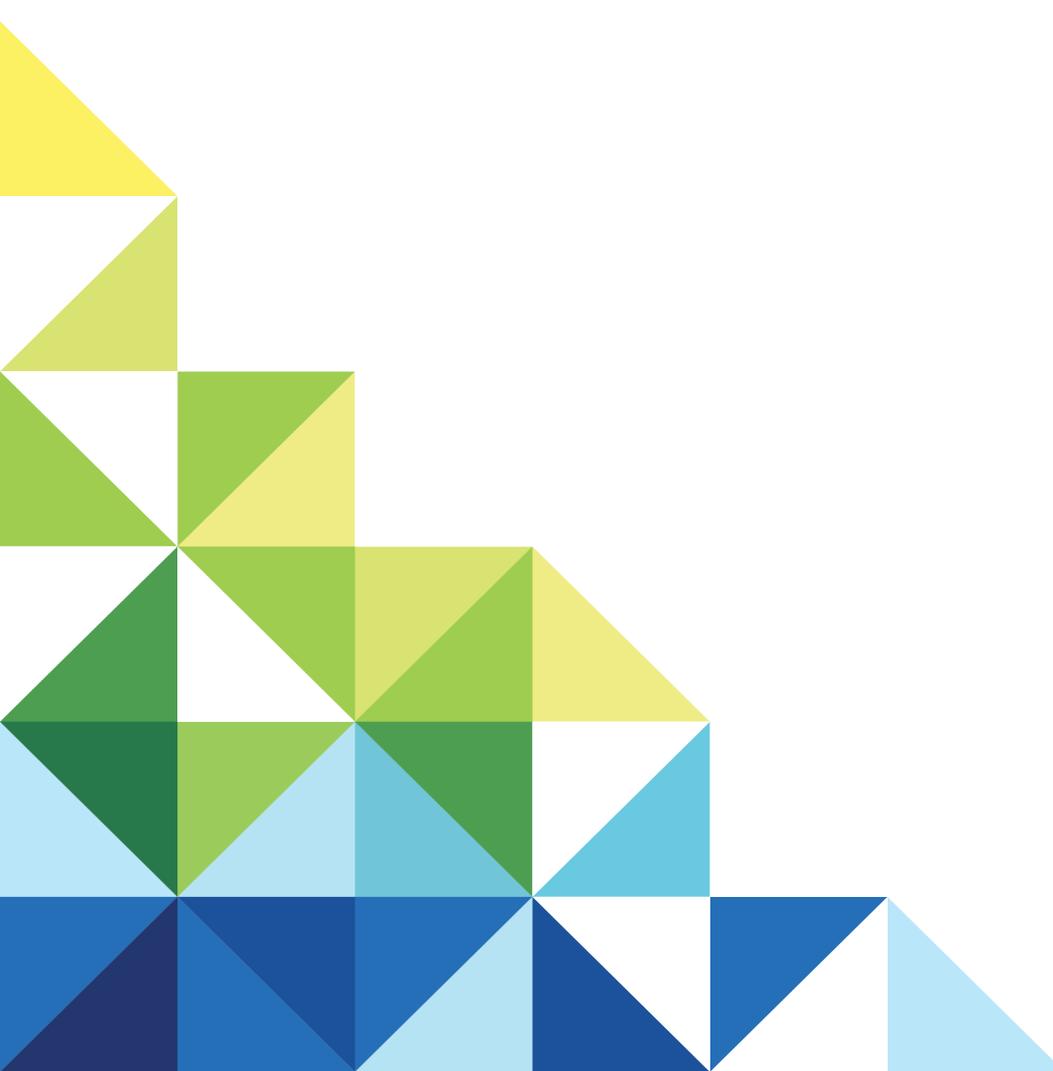


# Deployment for Region B

Modified on 26 SEP 2017

VMware Validated Design 4.0

VMware Validated Design for Software-Defined Data  
Center 4.0



vmware®

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

<https://docs.vmware.com/>

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

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2016, 2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

- 1 About VMware Validated Design Deployment for Region B 4**
  - Updated Information 5
  
- 2 Region B Virtual Infrastructure Implementation 8**
  - Install and Configure ESXi Hosts in Region B 9
  - Deploy and Configure the Platform Services Controller and Virtual Center Components in Region B 18
  - Deploy and Configure the Management Cluster NSX Instance in Region B 55
  - Deploy and Configure the Shared Edge and Compute Cluster Components Region B 107
  - Deploy and Configure the Shared Edge and Compute Cluster NSX Instance in Region B 130
  - Deploy and Configure VMware Site Recovery Manager 164
  - Deploy and Configure vSphere Replication 179
  - Deploy vSphere Data Protection in Region B 200
  - Replace Certificates in Region B 206
  
- 3 Region B Cloud Management Platform Implementation 219**
  - Prerequisites for Cloud Management Platform Implementation in Region B 219
  - Configure Service Account Privileges in Region B 220
  - vRealize Automation Installation in Region B 225
  - vRealize Orchestrator Configuration in Region B 248
  - vRealize Business Installation in Region B 250
  - Create Anti-Affinity Rules for vRealize Automation Proxy Agent Virtual Machines in Region B 260
  - Content Library Configuration in Region B 261
  - Tenant Content Creation in Region B 264
  
- 4 Region B Operations Implementation 305**
  - Region B vRealize Operations Manager Implementation 305
  - Region B vRealize Log Insight Implementation 335
  - Region B vSphere Update Manager Download Service Implementation 378

# About VMware Validated Design Deployment for Region B

1

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

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

## Intended Audience

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

## Required VMware Software

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

# 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.

Revision	Description
26 SEP 2017	<ul style="list-style-type: none"><li>Added missing number in filename for the command to configure symbolic link between the UMDS and the PostgreSQL. See <a href="#">Configure PostgreSQL Database on Your Linux-Based Host Operating System for UMDS in Region B</a>.</li></ul>
EN-002469-02	<ul style="list-style-type: none"><li>Added step 9, which instructs users to configure the MTU value on the vMotion VMkernel adapter to 9000. See <a href="#">Create a vSphere Distributed Switch for the Management Cluster in Region B</a>.</li><li>Added step 9, which instructs users to configure the MTU value on the vMotion VMkernel adapter to 9000. See <a href="#">Create a vSphere Distributed Switch for the Shared Edge and Compute Cluster in Region B</a>.</li></ul>

Revision	Description
EN-002469-01	<ul style="list-style-type: none"> <li>■ Step 4d incorrectly instructed you to use the fully qualified domain name (FQDN) lax01psc01.lax01.rainpole.local and a NSX Load Balancer name of LAX01PSC01. This error has been corrected such that the FQDN is lax01psc51.lax01.rainpole.local and the NSX Load Balancer name is LAX01PSC51. See <a href="#">Update the Platform Services Controller SSO Configuration and Endpoints in Region B</a>.</li> <li>■ Step 4d has been corrected to use the FQDN lax01psc51.lax01.rainpole.local. See <a href="#">Update the Platform Services Controller SSO Configuration and Endpoints in Region B</a></li> <li>■ Step 6 has been corrected to use the name LAX01PSC51. The hostname has also been updated to lax01psc51.lax01.rainpole.local. See <a href="#">Deploy the Platform Services Controller NSX Load Balancer in Region B</a>.</li> <li>■ Step 8 incorrectly listed the datastore name as SFO01A-VSAN01-MGMT01. This has been corrected to read LAX01A-VSAN01-MGMT01. See <a href="#">Deploy the Platform Services Controller NSX Load Balancer in Region B</a>.</li> <li>■ Step 13c and 14c have been updated to LAX01PSC51. See <a href="#">Deploy the Platform Services Controller NSX Load Balancer in Region B</a>.</li> <li>■ Step 4 now states that you should double-click the NSX Edge labeled LAX01PSC51 to manage its settings. See <a href="#">Create Platform Services Controller Application Profiles in Region B</a>.</li> <li>■ Step 4 now states that you should double-click the NSX Edge labeled LAX01PSC51 to manage its settings. See <a href="#">Create Virtual Servers in Region B</a>.</li> <li>■ Step 4 now states that you should double-click the NSX Edge labeled LAX01PSC51 to manage its settings. See <a href="#">Create Platform Services Controller Server Pools in Region B</a>.</li> <li>■ Step 4 incorrectly instructed you to use the FQDN of lax01psc01.lax01.rainpole.local and a DNS record name of LAX01PSC01. This error has been corrected such that the FQDN is lax01psc51.lax01.rainpole.local and the DNS record name of LAX01PSC51. See <a href="#">Update DNS Records for the Platform Services Controller Load Balancer in Region B</a>.</li> <li>■ Step 10 incorrectly instructed you to save the vRealize Automation server pool. This has been corrected to save the Platform Services Controller server pools. See <a href="#">Create Platform Services Controller Server Pools in Region B</a>.</li> <li>■ The topic <a href="#">Configure Service Account Privileges on the Compute vCenter Server in Region B</a> was incorrectly included twice in the previous version of this document. The extra occurrence has been removed.</li> <li>■ The topic <a href="#">Configure the Service Account Privilege on the Compute Cluster NSX Instance in Region B</a> was incorrectly included twice in the previous version of this document. The extra occurrence has been removed.</li> <li>■ Steps 3b and 3c have been updated to make Bash your default command shell. See <a href="#">Replace the Platform Services Controller Certificates in Region B</a>.</li> <li>■ This topic incorrectly instructed you to use a fully qualified domain name (FQDN) of lax01psc01.lax01.rainpole.local and a NSX Load Balancer name of LAX01PSC01. This error has been corrected such that the FQDN is lax01psc51.lax01.rainpole.local and the NSX Load Balancer name is LAX01PSC51. See <a href="#">Replace the NSX Manager Certificates in Region B</a> and <a href="#">Deploy the NSX Manager for the Shared Edge and Compute Cluster NSX Instance in Region B</a>.</li> <li>■ Step 4e incorrectly referred to lax01psc01.lax01.rainpole.local as the Platform Services Controller FQDN for the lookup service IP address. The correct FQDN is lax01psc51.lax01.rainpole.local. See <a href="#">Replace the NSX Manager Certificates in Region B</a>.</li> <li>■ Step 3h has been corrected to use the FQDN comp01nsxm51.lax01.rainpole.local. See <a href="#">Deploy the NSX Manager for the Shared Edge and Compute Cluster NSX Instance in Region B</a>.</li> <li>■ Step 4e has been corrected to use the Lookup Service FQDN lax01psc51.lax01.rainpole.local. See <a href="#">Deploy the NSX Manager for the Shared Edge and Compute Cluster NSX Instance in Region B</a>.</li> <li>■ Step 4h has been corrected to use the vCenter Server FQDN comp01vc51.lax01.rainpole.local. See <a href="#">Deploy the NSX Manager for the Shared Edge and Compute Cluster NSX Instance in Region B</a>.</li> <li>■ Step 2 has been corrected to use the vCenter FQDN mgmt01vc51.lax01.rainpole.local. See <a href="#">Configure a DRS Anti-Affinity Rule for vRealize Log Insight in Region B</a></li> <li>■ The Platform Services Controller instances URLs in the "Appliance Management Interface URL" table have been corrected. Also, the vRealize Log Insight URL in Step 2a has been corrected. See <a href="#">Configure vCenter Server to Forward Log Events to vRealize Log Insight in Region B</a>.</li> </ul>

Revision	Description
	<ul style="list-style-type: none"> <li data-bbox="331 222 1422 285">■ Step 4a has been updated to LAX01-Comp01 (comp01vc51.lax01.rainpole.local). See <a href="#">Create Reservations for the Compute Cluster in Region B</a>.</li> <li data-bbox="331 296 1422 359">■ Step 15 has been corrected to use mgmt01vc51.lax01.rainpole.local. See <a href="#">Deploy the vSphere Replication Appliance in Region B</a>.</li> <li data-bbox="331 369 1422 432">■ Steps 2 and 3 were duplicated, and this has been corrected. In addition, the vCenter FQDN in step 2 has been corrected, as has the host FQDN in step 4. See <a href="#">Configure Lockdown Mode on All ESXi Hosts in Region B</a></li> <li data-bbox="331 443 1422 506">■ Step 3i incorrectly listed the default gateway IP address as 172.17.11 .1. The correct IP address is 172.17.11.253. See <a href="#">Deploy the External Platform Services Controllers for the vCenter Servers in Region B</a>.</li> <li data-bbox="331 516 1422 600">■ The step about powering on vSphere Replication in Region B now contains the correct host name mgmt01vc51.lax01.rainpole.local for the Management vCenter Server in Region B. See <a href="#">Deploy the vSphere Replication Appliance in Region B</a>.</li> <li data-bbox="331 611 1422 674">■ A step was added instructing you to power on vSphere Data Protection after appliance deployment. See <a href="#">Deploy the Virtual Appliance of vSphere Data Protection in Region B</a>.</li> <li data-bbox="331 684 1422 768">■ <a href="#">Use the UMDS Shared Repository as the Download Source in Update Manager in Region B</a> now provides instructions about adding the repository of the Update Manager Download Service in Region B to the Update Manager on the Compute vCenter Server.</li> <li data-bbox="331 779 1422 898">■ The vRealize Log Insight deployment documentation now contains the correct host names of the vCenter Server instances in Region B. See <a href="#">Configure vCenter Server to Forward Log Events to vRealize Log Insight in Region B</a> and <a href="#">Configure the Log Insight Agent on vRealize Operations Manager to Forward Log Events to vRealize Log Insight in Region B</a>.</li> </ul>
EN-002469-00	Initial release.

# Region B Virtual Infrastructure Implementation

# 2

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

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

## Procedure

### 1 [Install and Configure ESXi Hosts in Region B](#)

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

### 2 [Deploy and Configure the Platform Services Controller and 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 VMware Site Recovery Manager](#)

You deploy VMware 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.

### 6 [Set Up vSAN Datastore for the Management Cluster in Region B](#)

Before you can use vSAN storage in your environment, you must set it up.

## 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 will be needed to join the common SSO domain.

You must also prepare the installation files.

- Download the ESXi ISO installer.
- Create a bootable USB drive that contains the ESXi Installation. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade" in *vSphere Installation and Setup*.

## IP Addresses, Hostnames, and Network Configuration

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

**Table 2-1. Management Cluster Hosts in Region B**

FQDN	IP	Management VLAN	Default Gateway	NTP Server
mgmt01esx51.lax01.rainpole.local	172.17.11.101	1711	172.17.11.253	<ul style="list-style-type: none"> <li>■ ntp.lax01.rainpole.local</li> <li>■ ntp.sfo01.rainpole.local</li> </ul>
mgmt01esx52.lax01.rainpole.local	172.17.11.102	1711	172.17.11.253	<ul style="list-style-type: none"> <li>■ ntp.lax01.rainpole.local</li> <li>■ ntp.sfo01.rainpole.local</li> </ul>
mgmt01esx53.lax01.rainpole.local	172.17.11.103	1711	172.17.11.253	<ul style="list-style-type: none"> <li>■ ntp.lax01.rainpole.local</li> <li>■ ntp.sfo01.rainpole.local</li> </ul>
mgmt01esx54.lax01.rainpole.local	172.17.11.104	1711	172.17.11.253	<ul style="list-style-type: none"> <li>■ ntp.lax01.rainpole.local</li> <li>■ ntp.sfo01.rainpole.local</li> </ul>

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

FQDN	IP	Management VLAN	Default Gateway	NTP Server
comp01esx51.lax01.rainpole.local	172.17.31.101	1731	172.17.31.253	<ul style="list-style-type: none"> <li>■ ntp.lax01.rainpole.local</li> <li>■ ntp.sfo01.rainpole.local</li> </ul>
comp01esx52.lax01.rainpole.local	172.17.31.102	1731	172.17.31.253	<ul style="list-style-type: none"> <li>■ ntp.lax01.rainpole.local</li> <li>■ ntp.sfo01.rainpole.local</li> </ul>
comp01esx53.lax01.rainpole.local	172.17.31.103	1731	172.17.31.253	<ul style="list-style-type: none"> <li>■ ntp.lax01.rainpole.local</li> <li>■ ntp.sfo01.rainpole.local</li> </ul>
comp01esx54.lax01.rainpole.local	172.17.31.104	1731	172.17.31.253	<ul style="list-style-type: none"> <li>■ ntp.lax01.rainpole.local</li> <li>■ ntp.sfo01.rainpole.local</li> </ul>

## Install ESXi Interactively on All Hosts in Region B

Install all ESXi hosts for all clusters interactively.

### Procedure

- 1 Power on the mgmt01esx51 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.



- 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.

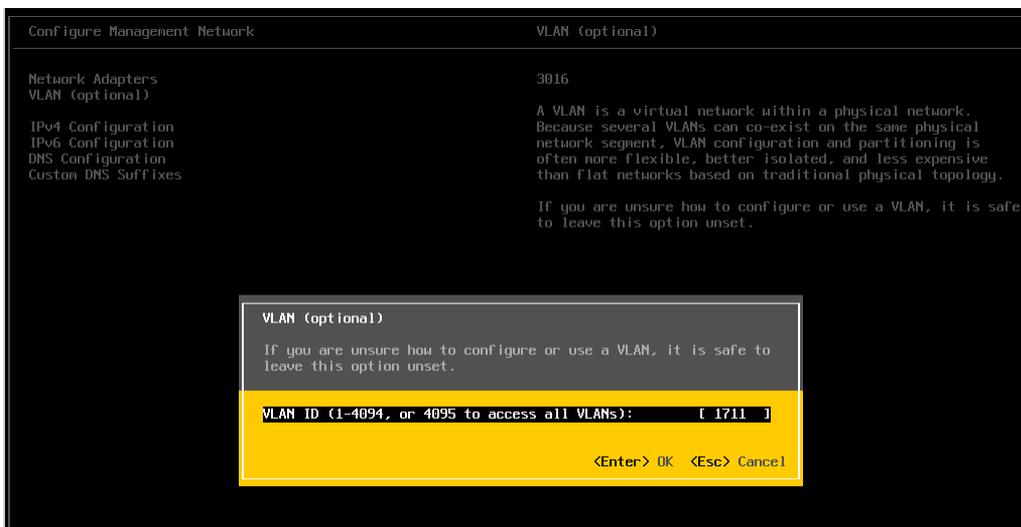
Perform the following tasks to configure the host network settings:

- 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

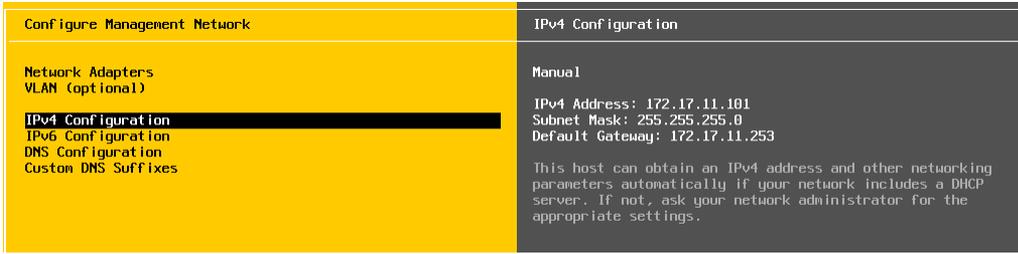
- 1 Open the DCUI on the physical ESXi host `mgmt01esx51`.
  - a Open a console window to the host.
  - b Press F2 to enter the DCUI.
  - c Enter `root` as login name, and `esxi_root_user_password`, and press Enter.
- 2 Configure the network.
  - a Select **Configure Management Network** and press Enter.
  - 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**.

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



- f Select **DNS Configuration** and press **Enter**.
- g Configure the DNS using the following settings, and press **Enter**.

Setting	Value
Use the following DNS Server address and hostname	Selected
Primary DNS Server	172.17.11.5
Alternate DNS Server	172.17.11.4
Hostname	mgmt01esx51.lax01.rainpole.local

- h Select **Custom DNS Suffixes** and press Enter.
  - i Ensure there are no suffixes listed, and press Enter.
- 3 After completing all host network settings press Escape to exit, and press Y to confirm the changes.
  - 4 Repeat this procedure for all hosts in 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://mgmt01esx51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Options	Description
User name	root
Password	esxi_root_user_password

- 2 Click **OK** to Join the Customer Experience Improvement Program.
- 3 Configure a VLAN for the VM Network Portgroup.
  - a In the Navigator, click **Networking**, click the **Port Groups** tab, 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 mgmt01esx51.lax01.rainpole.local host by using the VMware Host Client.
  - a Open a Web browser and go to **mgmt01esx51.lax01.rainpole.local**.

Setting	Value
User name	root
Password	esxi_root_user_password

- 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**.

## Set Up vSAN Datastore for the Management Cluster in Region B

Before you can use vSAN storage in your environment, you must set it up.

This process is divided into two main tasks.

- Bootstrap the first ESXi host from the command line and create the vSAN datastore.
- After vCenter Server installation, perform vSAN configuration for all other hosts from the vSphere Web Client.

### Procedure

- 1 Open an SSH client to connect to the ESXi Shell on mgmt01esx51.lax01.rainpole.local.

- a Open a console window to the host.
- b Log in using the following credentials.

Options	Description
login as:	root
Password	esxi_root_user_password

- 2 Run the following command to determine the current vSAN storage policy.

```
esxcli vsan policy getdefault
```

```
[root@mgmt01esx51:~] esxcli vsan policy getdefault
Policy Class  Policy Value
-----
cluster      (("hostFailuresToTolerate" i1))
vdisk        (("hostFailuresToTolerate" i1))
vmnamespace  (("hostFailuresToTolerate" i1))
vmswap       (("hostFailuresToTolerate" i1) ("forceProvisioning" i1))
vmem         (("hostFailuresToTolerate" i1) ("forceProvisioning" i1))
[root@mgmt01esx51:~] █
```

- 3 Modify the default vSAN storage policy to force provisioning of vSAN datastore without generating errors.

```
esxcli vsan policy setdefault -c vdisk -p "(\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1)"
esxcli vsan policy setdefault -c vmnamespace -p "(\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1)"
esxcli vsan policy getdefault
```

```
[root@mgmt01esx51:~] esxcli vsan policy setdefault -c vdisk -p "(\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1)
[root@mgmt01esx51:~] esxcli vsan policy setdefault -c vmnamespace -p "(\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1)
[root@mgmt01esx51:~] esxcli vsan policy getdefault
Policy Class Policy Value
-----
cluster      (\"hostFailuresToTolerate\" i1)
vdisk       (\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1)
vmnamespace  (\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1)
vmswap      (\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1)
vmem        (\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1)
```

- 4 Generate the vSAN cluster UUID and create the vSAN cluster.

```
python -c 'import uuid; print (uuid.uuid4());'
```

**Note** You need the \$UUID\_GENERATED from the generated output for the next command.

```
esxcli vsan cluster join -u <UUID_GENERATED>
esxcli vsan cluster get
```

```
[root@mgmt01esx51:~] python -c 'import uuid; print str(uuid.uuid4());'
914a3564-8aab-4c7c-b430-9381935980ef
[root@mgmt01esx51:~] esxcli vsan cluster join -u 914a3564-8aab-4c7c-b430-9381935980ef
[root@mgmt01esx51:~] esxcli vsan cluster get
Cluster Information
  Enabled: true
  Current Local Time: 2016-01-04T22:58:05Z
  Local Node UUID: 5628701b-f916-1140-77a4-ecf4bbd89a48
  Local Node Type: NORMAL
  Local Node State: MASTER
  Local Node Health State: HEALTHY
  Sub-Cluster Master UUID: 5628701b-f916-1140-77a4-ecf4bbd89a48
  Sub-Cluster Backup UUID:
  Sub-Cluster UUID: 914a3564-8aab-4c7c-b430-9381935980ef
  Sub-Cluster Membership Entry Revision: 0
  Sub-Cluster Member Count: 1
  Sub-Cluster Member UUIDs: 5628701b-f916-1140-77a4-ecf4bbd89a48
  Sub-Cluster Membership UUID: ecf88a56-d723-4593-59d7-ecf4bbd89a48
```

- 5 List the devices and determine the device name for the SSD and HDD.

These disks will be used to provision the vSAN datastore.

```
vdq -q
```

Identify all devices that can be used by vSAN.

Property	SDD Value	HDD Value
State	Eligible for use by VSAN	Eligible for use by VSAN
IsSSD	1	0

```

[root@mgmt01esx51:~] vdisk -q
[
  {
    "Name"      : "mpx.vmhba36:C0:T0:L1",
    "VSANUUID" : "",
    "State"     : "Ineligible for use by VSAN",
    "ChecksumSupport" : "0",
    "Reason"    : "Has partitions",
    "IsSSD"     : "0",
    "IsCapacityFlash" : "0",
    "IsPDL"    : "0",
  },
  {
    "Name"      : "naa.50000396a83a47f5",
    "VSANUUID" : "",
    "State"     : "Eligible for use by VSAN",
    "ChecksumSupport" : "0",
    "Reason"    : "Non-local disk",
    "IsSSD"     : "0",
    "IsCapacityFlash" : "0",
    "IsPDL"    : "0",
  },
  {
    "Name"      : "naa.50000396a83a7845",
    "VSANUUID" : "",
    "State"     : "Eligible for use by VSAN",
    "ChecksumSupport" : "0",
    "Reason"    : "Non-local disk",
    "IsSSD"     : "0",
    "IsCapacityFlash" : "0",
    "IsPDL"    : "0",
  },
  {
    "Name"      : "mpx.vmhba32:C0:T0:L0",
    "VSANUUID" : "",
    "State"     : "Ineligible for use by VSAN",
    "ChecksumSupport" : "0",
    "Reason"    : "Has partitions",
    "IsSSD"     : "0",
    "IsCapacityFlash" : "0",
    "IsPDL"    : "0",
  },
  {
    "Name"      : "naa.5000c5007f0befe7",
    "VSANUUID" : "",
    "State"     : "Eligible for use by VSAN",
    "ChecksumSupport" : "0",
    "Reason"    : "Non-local disk",
    "IsSSD"     : "0",
    "IsCapacityFlash" : "0",
    "IsPDL"    : "0",
  },
  {
    "Name"      : "naa.55cd2e404c0479f9",
    "VSANUUID" : "",
    "State"     : "Eligible for use by VSAN",
    "ChecksumSupport" : "0",
    "Reason"    : "None",
    "IsSSD"     : "1",
    "IsCapacityFlash" : "0",
    "IsPDL"    : "0",
  },
  {
    "Name"      : "naa.5000c5007f164c03",
    "VSANUUID" : "",
    "State"     : "Eligible for use by VSAN",
    "ChecksumSupport" : "0",
    "Reason"    : "Non-local disk",
    "IsSSD"     : "0",
    "IsCapacityFlash" : "0",
    "IsPDL"    : "0",
  },
  {
    "Name"      : "naa.55cd2e404b78c107",
    "VSANUUID" : "",
    "State"     : "Eligible for use by VSAN",
    "ChecksumSupport" : "0",
    "Reason"    : "None",
    "IsSSD"     : "1",
    "IsCapacityFlash" : "0",
    "IsPDL"    : "0",
  },
]
[root@mgmt01esx01:~] ]

```

- 6 Create vSAN datastore by using the available SSD and HDD disks determined in the previous step.

```
esxcli vsan storage add -s SSD_Device_name -d HDD_Device_Name
```

```
[root@ngnt01esx51:~] esxcli vsan storage add -s naa.55cd2e404c0479f9 -d naa.5000c5007f0befe7 -d naa.5000c5007f164c03
```

- 7 Verify that the vSAN datastore has been created successfully.

```
esxcli storage filesystem list
```

A vSAN datastore is now created and ready for the Management vCenter Server installation.

## 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 Servers 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 Controllers to Active Directory in Region B](#)

After you have successfully installed the Platform Services Controller instance, you must add the appliance to your Active Directory domain. After that add the Active Directory domain as an identity source to vCenter Single Sign-On. When you do, users in the Active Directory domain are visible to vCenter Single Sign-On and can be assigned permissions to view or manage SDDC components.

- 3 [Replace the Platform Services Controller Certificates in Region B](#)

The first step is replacing the machine SSL certificate on each Platform Services Controller instance 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 [Configure the Management Cluster in Region B](#)

You must now create and configure the management cluster.

- 7 [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.

## 8 [Set vSAN Storage Policy in Region B](#)

This step is to set the vSAN storage policy for the Platform Services Controller and vCenter Server appliances.

## 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.

## 10 [Enable vSphere HA on the Management Cluster in Region B](#)

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

## 11 [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.

## 12 [Mount NFS Storage for the Management Cluster in Region B](#)

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

## 13 [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.

## 14 [Set vSAN 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 vSAN Default Storage Policy.

## 15 [Create the VM and Template Folders in Region B](#)

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

## 16 [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.

## 17 [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 Servers 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.
  - a Browse the vCenter Server Appliance ISO file.
  - b Open the <dvd-drive>:\vcsa-ui-installer\win32\Installer.exe application file.
- 3 Complete Stage 1 of the **vCenter Server Appliance Installer** wizard.
  - a Click **Install** to start the installation.
  - b Click **Next** on the **Introduction** page.
  - c On the **End User License Agreement** page, select the **I accept the terms of the license agreement** check box, and click **Next**.
  - d On the **Select deployment type** page, click **Platform Services Controller** and click **Next**.
  - e On the **Appliance deployment target** page, enter the following settings and click **Next**.

Setting	Value
FQDN or IP Address	mgmt01esx51.lax01.rainpole.local
HTTPS port	443
User name	root
Password	<i>esxi_root_user_password</i>

- f In the **Certificate Warning** dialog box, click **Yes** to accept the host certificate.
- g On the **Set up appliance VM** page, enter the following settings, and click **Next**.

Setting	Management Value	Edge/Compute Value
VM name	mgmt01psc51	comp01psc51
Root password	<i>mgmtpsc_root_password</i>	<i>comppsc_root_password</i>
Confirm root password	<i>mgmtpsc_root_password</i>	<i>comppsc_root_password</i>

- h On the **Select datastore** page, select the **vsanDatastore** datastore, select the **Enable Thin Disk Mode** check box, and click **Next**.
- i On the **Configure network settings** page, enter the following settings and click **Next**.

Setting	Management Value	Edge/Compute Value
Network	VM Network	VM Network
IP version	IPv4	IPv4
IP assignment	static	static
System name	mgmt01psc51.lax01.rainpole.local	comp01psc51.lax01.rainpole.local
IP address	172.17.11.61	172.17.11.63
Subnet mask or prefix length	255.255.255.0	255.255.255.0
Default gateway	172.17.11.253	172.17.11.253
DNS servers	172.17.11.5,172.17.11.4	172.17.11.5,172.17.11.4

- j On the **Ready to complete stage 1** page, review the configuration and click **Finish** to start the deployment.
- k When the deployment completes, click **Continue** to proceed to second stage of the installation, setting up the Platform Services Controller Appliance.

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

- a Click **Next** on the **Introduction** page.
- b On the **Appliance configuration** page, enter the following settings and click **Next**.

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

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

Setting	Management Value	Edge/Compute Value
SSO configuration	Join an existing SSO domain	Join an existing SSO domain
Platform Services Controller	mgmt01psc01.sfo01.rainpole.local	mgmt01psc51.lax01.rainpole.local
HTTPS port	N/A	443
SSO domain name	vsphere.local	vsphere.local
SSO password	<i>sso_password</i>	<i>sso_password</i>

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

Setting	mgmt01psc51	comp01psc51
SSO Site Creation	Create a new site	Join an existing site
Site name	LAX01	LAX01

- e On the **Configure CEIP** page, verify that the **Join the VMware's Customer Experience Improvement Program (CEIP)** check box is checked and click **Next**
- f On the **Ready to complete** page, review the configuration and click **Finish** to complete the setup.
- g Click **OK** on the Warning.

5 Repeat this procedure for each platform services controller, using the respective values for each.

- 6 Create replication agreement between the Platform Services Controllers for the compute clusters in the regions.
- a Open an SSH connection to the virtual appliance by using the following settings.

Setting	Value
SSH Server	comp01psc01.sfo01.rainpole.local
User name	root
Password	<i>comppsc_root_password</i>

- 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-vmtoolsd/bin/vdcrepadmin -f createagreement -2 -h
comp01psc01.sfo01.rainpole.local -u Administrator -w vcenter_admin_password -H
comp01psc51.lax01.rainpole.local
```

## Join the Platform Services Controllers to Active Directory in Region B

After you have successfully installed the Platform Services Controller instance, you must add the appliance to your Active Directory domain. After that add the Active Directory domain as an identity source to vCenter Single Sign-On. When you do, users in the Active Directory domain are visible to vCenter Single Sign-On and can be assigned permissions to view or manage SDDC components.

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

## Procedure

- 1 Log in to the Platform Services Controller administration interface.
  - a Open a Web browser and go to the URL for either the Management or Edge/Compute cluster.

Setting	Management Value	Edge/Compute Value
PSC Link	<a href="https://mgmt01psc51.lax01.rainpole.local">https://mgmt01psc51.lax01.rainpole.local</a>	<a href="https://comp01psc51.lax01.rainpole.local">https://comp01psc51.lax01.rainpole.local</a>

- b Click the link for **Platform Services Controller web interface**.
  - c Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Add the management Platform Services Controller instance to the Active Directory domain.
  - a In the **Navigator**, click **Appliance Settings**, click the **Manage** tab, and click **Join**.
  - b In the **Join Active Directory Domain** dialog box, enter the following settings and click **OK**.

Setting	Value
Domain	lax01.rainpole.local
User name	ad_admin_acct@lax01.rainpole.local
Password	ad_admin_password

- 3 Reboot the Platform Services Controller instance to apply the changes.
  - a Click the **Appliance settings** tab, and click the **VMware Platform Services Appliance** link.
  - b Log in to the VMware vCenter Server Appliance administration interface with the following credentials.

Setting	Value
User name	root
Password	psc_root_password

- c On the **Summary** page, click **Reboot**.
  - d In the **System Reboot** dialog box, click **Yes**.
  - e Wait for the reboot process to finish.
- 4 After the reboot process finishes, log in to <https://mgmt01psc51.lax01.rainpole.local/> using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 5 Verify that the Platform Services Controller has successfully joined the domain, click **Appliance Settings**, and click the **Manage** tab.
- 6 In the **Navigator**, click **Configuration**, and click the **Identity Sources** tab.  
Verify that the rainpole.local domain is available as an Identity Source.
- 7 Repeat this procedure for the Platform Services Controller of the shared edge and compute cluster.

## Replace the Platform Services Controller Certificates in Region B

The first step is replacing the machine SSL certificate on each Platform Services Controller instance with a custom certificate that is signed by the certificate authority (CA) available on the parent Active Directory (AD) server.

Since the Platform Services Controllers will be load balanced the machine certificate on both must be the same. The certificate will have a common name of the load balanced Fully Qualified Domain Name (FQDN) and each Platform Service Controllers FQDN and short name along with the load balanced FQDN and short name must be in the Subject Alternate Name (SAN) of the generated certificate.

You replace certificates twice: on the Platform Services Controller for the Management vCenter Server mgmt01psc51.lax01.rainpole.local and on the Platform Services Controller for the Compute vCenter Server comp01psc51.lax01.rainpole.local. You start replacing certificates on Platform Services Controller mgmt01psc51.lax01.rainpole.local first.

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

Platform Services Controller	Config File Name	Certificate File Name	Replacement Order
mgmt01psc51.lax01.rainpole.local	lax01psc51.lax01.txt	lax01psc51.lax01.1.cer	First
comp01psc51.lax01.rainpole.local	-	lax01psc51.lax01.1.cer	Second

### Procedure

- 1 Log in to a Windows host that has access to both the AD server and the Platform Services Controllers as an administrator.
- 2 Generate the certificate for the Platform Services Controllers if you have not done so already.
  - a Download the VMware Validated Design Certificate Generation Utility from [KB2146215](#).
  - b Extract the contents of the zip file to C:\CertGenVVD-2.1.
  - c Open a Windows PowerShell prompt as an administrator and navigate to the C:\CertGenVVD-2.1.
  - d Run Set-ExecutionPolicy RemoteSigned.
  - e Run the following command to generate the certificate for the Platform Services Controller.

```
.\CertGenVVD-2.1.ps1 -MSCASigned -attrib 'CertificateTemplate:VMware'
```

- f The certificate and supporting files will be saved in C:\CertGenVVD\SignedByMSCACerts folder.

### 3 Change the Platform Services Controller shell to bash to allow SCP connections.

- a SSH to `mgmt01psc51.lax01.rainpole.local` and logon with the following credentials.

Options	Description
Setting	Value
Username	Root
Password	<code>mgmtpsc_root_password</code>

- b Enter **shell** and press Enter.

- c Run the command `chsh -s "/bin/bash" root`.

### 4 Copy the generated certificates to the Platform Services Controllers.

- a SCP the contents of the `C:\CertGenVVD-2.1\SignedByMSCACerts\lax01psc51.lax01` folder to `/tmp/certs`.
- b SCP the `Root64.cer` file from `C:\CertGenVVD-2.1\SignedByMSCACerts\RootCA` to `/tmp/certs`.

### 5 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 `/tmp/certs/lax01psc51.lax01.1.cer`.
- f When prompted for the custom key enter `/tmp/certs/lax01psc51.lax01.key`.
- g When prompted for the signing certificate enter `/tmp/certs/Root64.cer`.

- h When prompted to Continue operation enter Y.

```
Note : Use Ctrl-D to exit.
Option[1 to 8]: 1
Please provide valid SSO and VC privileged user credential to perform certificate operations.
Enter username [Administrator@vmsphere.local]:
Enter password:
  1. Generate Certificate Signing Request(s) and Key(s) for Machine SSL certificate
  2. Import custom certificate(s) and key(s) to replace existing Machine SSL certificate
Option [1 or 2]: 2
Please provide valid custom certificate for Machine SSL.
File : /tmp/certs/lax01psc51.lax01.cer
Please provide valid custom key for Machine SSL.
File : /tmp/certs/lax01psc51.lax01.key
Please provide the signing certificate of the Machine SSL certificate
File : /tmp/certs/Root64.cer
You are going to replace Machine SSL cert using custom cert
Continue operation : Option[Y/N] ? : Y
Get site nameCompleted [Replacing Machine SSL Cert...]
lax01
Lookup all services
Get service lax01:0ac7cf31-d7d0-44a1-9866-f7e5728e9aad
Update service lax01:0ac7cf31-d7d0-44a1-9866-f7e5728e9aad: spec: /tmp/avcspec_Q21vwh
Get service lax01:ac12ca63-dac7-46fc-a27f-0ce2c3921ada
Update service lax01:ac12ca63-dac7-46fc-a27f-0ce2c3921ada: spec: /tmp/avcspec_C3PS1R
```

- i The Platform Services Controller services will restart automatically.

- 6 Replace the certificate on comp01psc51.lax01.rainpole.local by repeating steps 3-5.

## 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 mgmt01psc51.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:

FQDN	IP
lax01psc51.lax01.rainpole.local	172.17.11.61

**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 mgmt01psc51.lax01.rainpole.local

- 2 Update the Platform Services Controller SSO configuration on `mgmt01psc51.lax01.rainpole.local`.
  - a Open an SSH connection to `mgmt01psc51.lax01.rainpole.local`.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>mgmtpsc_root_password</i>

- c Enter `cd /usr/lib/vmware-ssso/bin/` and press Enter.
  - d Enter `python updateSSOConfig.py --lb-fqdn=lax01psc51.lax01.rainpole.local` and press Enter.

```

root@mgmt01psc51 [ ~ ]# cd /usr/lib/vmware-ssso/bin/
root@mgmt01psc51 [ /usr/lib/vmware-ssso/bin ]# python updateSSOConfig.py --lb-fqdn=lax01psc51.lax01.rainpole.local
script version:1.0.0
executing vmafd-cli command
Modifying hostname.txt
modifying server.xml
Executing StopService --all
Executing StartService --all

```

- 3 Update the Platform Services Controller SSO configuration on `comp01psc51.lax01.rainpole.local`.
  - a Open an SSH connection to `comp01psc51.lax01.rainpole.local`.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>compssc_root_password</i>

- c Enter `cd /usr/lib/vmware-ssso/bin/` and press Enter.
  - d Enter `python updateSSOConfig.py --lb-fqdn=lax01psc51.lax01.rainpole.local` and press Enter.

```

root@comp01psc51 [ ~ ]# cd /usr/lib/vmware-ssso/bin/
root@comp01psc51 [ /usr/lib/vmware-ssso/bin ]# python updateSSOConfig.py --lb-fqdn=lax01psc51.lax01.rainpole.local
script version:1.0.0
executing vmafd-cli command
Modifying hostname.txt
modifying server.xml
Executing StopService --all
Executing StartService --all
root@comp01psc51 [ /usr/lib/vmware-ssso/bin ]#

```

#### 4 Update the Platform Services Controller endpoints.

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

- a Open an SSH connection to `mgmt01psc51.lax01.rainpole.local`.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>mgmtpsc_root_password</i>

- c Enter `cd /usr/lib/vmware-ssso/bin/` and press **Enter**.
- d Enter `python UpdateLsEndpoint.py --lb-fqdn=lax01psc51.lax01.rainpole.local --user=Administrator@vsphere.local` and press **Enter**.
- e Enter the *vsphere\_admin\_password* when prompted.

```
root@mgmt01psc51 [ /usr/lib/vmware-ssso/bin ]# python UpdateLsEndpoint.py --lb-fqdn=lax01psc51.lax01.rainpole.local --user-administrator@vsphere.local
Password:
```

## 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**.

Setting	Value
ESXi host or vCenter Server name	mgmt01esx51.lax01.rainpole.local
HTTPS port	443
User name	root
Password	<i>esxi_root_user_password</i>

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

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

Setting	Value
Appliance name	mgmt01vc51
OS password	<i>mgmtvc_root_password</i>
Confirm OS password	<i>mgmtvc_root_password</i>

- 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, and click **Next**.

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

Setting	Value
Network	VM Network
IP version	IPv4
IP assignment	static
System name	mgmt01vc51.lax01.rainpole.local
IP address	172.17.11.62
Subnet mask or prefix length	255.255.255.0
Default gateway	172.17.11.253
DNS servers	172.17.11.5,172.17.11.4

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

- l 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**.

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

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

Setting	Value
Platform Services Controller	lax01psc51.lax01.rainpole.local
HTTPS port	443
SSO domain name	vsphere.local
SSO password	<i>sso_password</i>

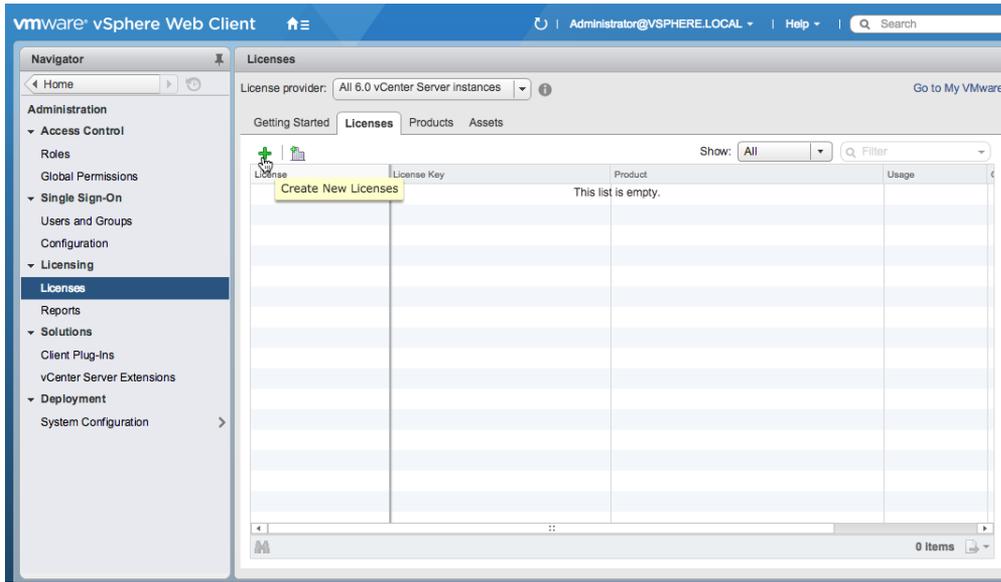
- d On the **Ready to complete** page, review the configuration and click **Finish**.
  - e Click **OK** on the **Warning** dialog box.
- 4 Add new licenses for this vCenter Server instance and the management cluster ESXi hosts if needed.

- a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
- b Log in using the following credentials.

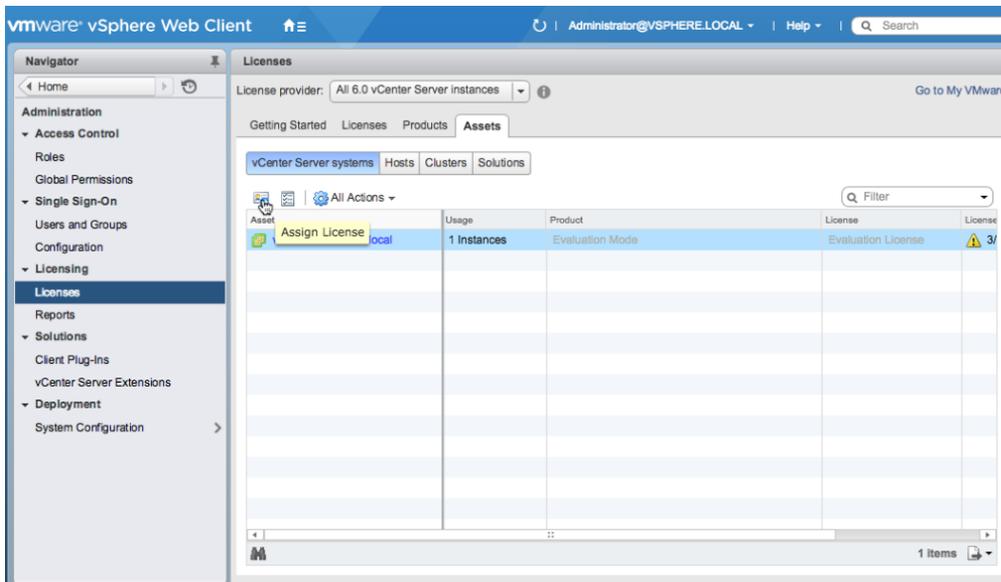
Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 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.

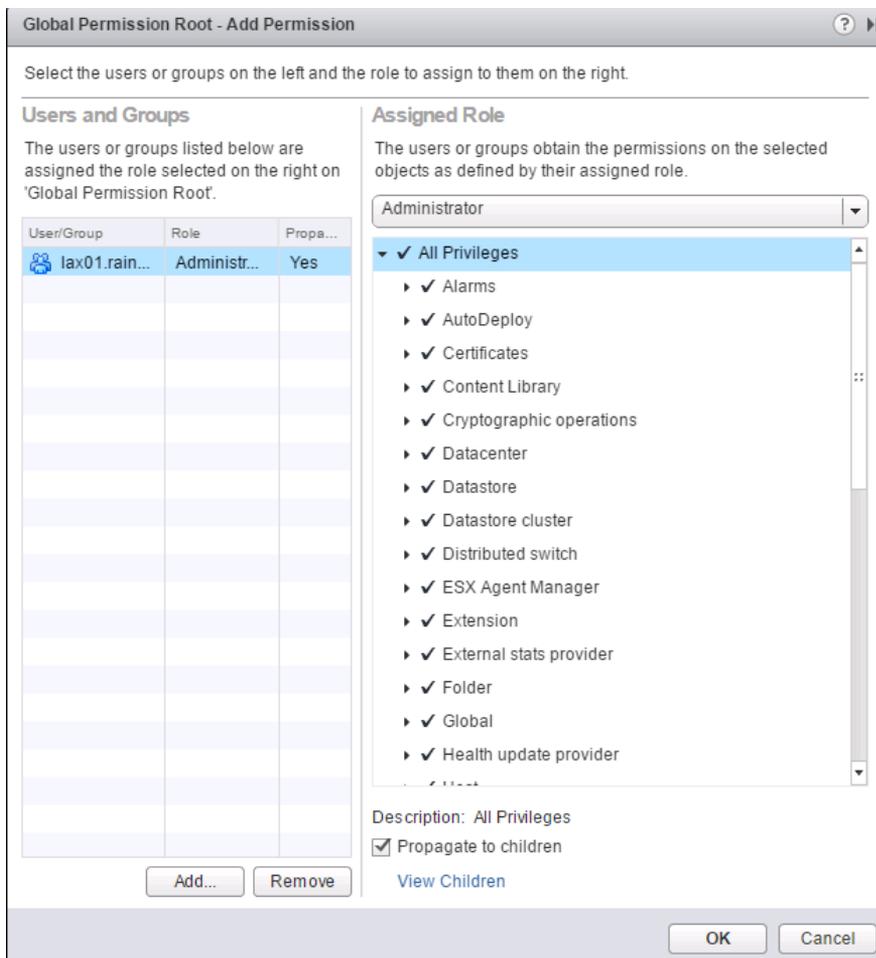


- f On the **Enter license keys** page, enter license keys for vCenter Server, ESXi and vSAN, one per line and click **Next**.
  - g On the **Edit license name** page, enter a descriptive name for each license key and click **Next**.
  - h On the **Ready to complete** page, review your entries and click **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**.



## Configure the Management Cluster in Region B

You must now create and configure the management cluster.

This process consists of the following actions:

- Create the cluster.
- Configure DRS.
- Enable vSAN for the cluster.
- Add the hosts to the cluster.
- Add a host to the active directory domain.
- Reset the vSAN Storage Policy to default for the ESXi host that is used for Bootstrap.
- 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

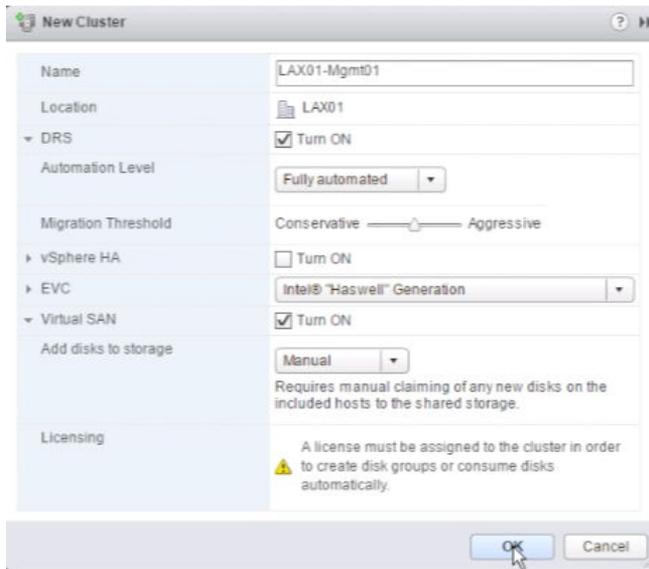
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a Datacenter object.
  - a In the **Navigator**, click **Hosts and Clusters**.
  - b Right-click **mgmt01vc51.lax01.rainpole.local** and click **New Datacenter**.
  - c In the **New Datacenter** dialog box, enter **LAX01** as Datacenter name, and click **OK**.

3 Create the management cluster.

- a Right-click the **LAX01** datacenter and click **New Cluster**.
- b In the **New Cluster** wizard, enter the following values and click **OK**.

Setting	Value				
<b>Name</b>	LAX01-Mgmt01				
<b>DRS</b>	<table border="0"> <tr> <td><b>Turn ON</b></td> <td>Selected</td> </tr> <tr> <td>Other DRS options</td> <td>Default values</td> </tr> </table>	<b>Turn ON</b>	Selected	Other DRS options	Default values
<b>Turn ON</b>	Selected				
Other DRS options	Default values				
<b>vSphere HA</b>	<table border="0"> <tr> <td><b>Turn ON</b></td> <td>Deselected</td> </tr> </table>	<b>Turn ON</b>	Deselected		
<b>Turn ON</b>	Deselected				
<b>EVC</b>	Set EVC mode to the lowest available setting supported for the hosts in the cluster				
<b>vSAN</b>	<table border="0"> <tr> <td><b>Turn ON</b></td> <td>Selected</td> </tr> <tr> <td><b>Add disks to storage</b></td> <td><b>Manual</b></td> </tr> </table>	<b>Turn ON</b>	Selected	<b>Add disks to storage</b>	<b>Manual</b>
<b>Turn ON</b>	Selected				
<b>Add disks to storage</b>	<b>Manual</b>				



4 Add a management host to the management cluster.

- a Right-click the **LAX01-Mgmt01** cluster, and click **Add Host**.
- b On the **Name and location** page, enter `mgmt01esx51.lax01.rainpole.local` in the **Host name or IP address** text box and click **Next**.
- c On the **Connection settings** page, enter the following credentials and click **Next**.

Setting	Value
<b>User name</b>	root
<b>Password</b>	<code>esxi_root_user_password</code>

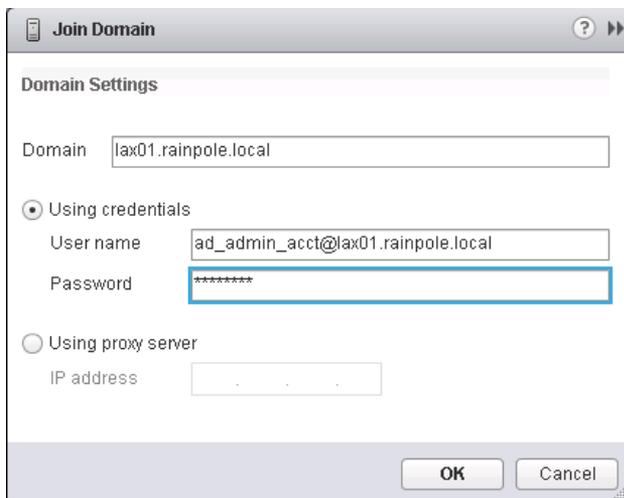
- d In the **Security Alert** dialog box, click **Yes**.
- e On the **Host summary** page, review the host information and click **Next**.

- f On the **Assign license** page, select the ESXi license key that you entered during the vCenter Server deployment and click **Next**.
  - g On the **Lockdown Mode** page, click **Next**.
  - h On the **Resource pool** page, click **Next**.
  - i On the **Ready to complete** page, review your entries and click **Finish**.
- 5 Repeat the previous step for the three remaining hosts to add them to the management cluster.

Setting	Value
Host 2	mgmt01esx52.lax01.rainpole.local
Host 3	mgmt01esx53.lax01.rainpole.local
Host 4	mgmt01esx54.lax01.rainpole.local

- 6 Add an ESXi host to the active directory domain.
- a In the **Navigator**, click **Hosts and Clusters** and expand the entire **mgmt01vc51.lax01.rainpole.local** tree.
  - b Select the **mgmt01esx51.lax01.rainpole.local** host.
  - c Click the **Configure** tab.
  - d Under **System**, select **Authentication Services**.
  - e In the **Authentication Services** panel, click the **Join Domain** button.
  - f In the **Join Domain** dialog box, enter the following settings and click **OK**.

Setting	Value
Domain	lax01.rainpole.local
Using credentials	Selected
User name	ad_admin_acct@lax01.rainpole.local
Password	ad_admin_lax_password



- 7 Set the Active Directory Service to Start and stop with host.
  - a In the **Navigator**, click **Hosts and Clusters** and expand the entire **mgmt01vc51.lax01.rainpole.local** tree.
  - b Select the **mgmt01esx51.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 Select the **LAX01-Mgmt01** cluster.
  - b Click the **Datastores** tab.
  - c Select **vsanDatastore**, and select **Actions > Rename..**
  - d In the **Datastore - Rename** dialog box, enter **LAX01A-VSAN01-MGMT01** 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create vSphere Distributed Virtual Switch.
  - a In the **Navigator**, click **Networking** and expand the **lax01m01vc01.lax01.rainpole.local** tree.
  - b Right-click the **lax01-m01dc** datacenter, and select **Distributed Switch > New Distributed Switch** to start the **New Distributed Switch** wizard.
  - c On the **Name and location** page, enter **lax01-m01-vds01** as the name and click **Next**.

- d On the **Select version** page, ensure the **Distributed switch: 6.5.0** radio button is selected and click **Next**.
- e On the **Edit settings** page, enter the following values and click **Next**.

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

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

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

- a Right-click the **lax01-m01-vds01** distributed switch, and select **Settings > Edit Settings**.
- b Click the **Advanced** tab.
- c Enter **9000** as MTU (Bytes) value, and click **OK**.

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

- a Right-click the **lax01-m01-vds01** distributed switch, and select **Distributed Port Group > New Distributed Port Group**.
- b Create port groups with the following settings and click **Next**.

Port Group Name	Port Binding	VLAN Type	VLAN ID
lax01-m01-vds01-management	Ephemeral - no binding	VLAN	1711
lax01-m01-vds01-vmotion	Static binding	VLAN	1712
lax01-m01-vds01-vsan	Static binding	VLAN	1713
lax01-m01-vds01-nfs	Static binding	VLAN	1715
lax01-m01-vds01-replication	Static binding	VLAN	1716
lax01-m01-vds01-ext-management	Static binding	VLAN	150
lax01-m01-vds01-uplink01	Static binding	VLAN	2714
lax01-m01-vds01-uplink02	Static binding	VLAN	2715

---

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

---

- c On the **Ready to complete** page, review your entries, and click **Finish**.
- d Repeat this step for each port group.

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

- a Right-click the **lax01-m01-vds01** distributed switch and select **Distributed Port Group > Manage Distributed Port Groups**.
- b On the **Select port group policies** page, select **Teaming and failover** and click **Next**.

- c Click the **Select distributed port groups** button, add all port groups 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 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**.
- 7 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 7c. - 7f. to create the remaining VMkernel network adapters.

Port Group	Port Properties	IPv4 Address	Netmask
lax01-m01-vds01-replication	<ul style="list-style-type: none"> <li>■ vSphere Replication traffic</li> <li>■ vSphere Replication NFC traffic</li> </ul>	172.17.16.101	255.255.255.0
lax01-m01-vds01-nfs	N/A	172.17.15.101	255.255.255.0

- i On the **Analyze impact** page, click **Next**.
- j On the **Ready to complete** page, review your entries and click **Finish**.

- 8 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**.
- 9 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**.
- 10 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**.
- 11 Migrate the Management Platform Services Controller and vCenter Server instances from the standard switch to the distributed switch.
  - a In the **Navigator**, click **Networking** and expand the **lax01m01vc01.lax01.rainpole.local** tree.
  - b Right-click the **lax01-m01-vds01** distributed switch and click **Migrate VM to Another Network**.
  - c On the **Select source and destination networks** page, browse the following networks and click **Next**.
 

Setting	Value
Source network	VM Network
Destination network	lax01-m01-vds01-management
  - d On the **Select VMs to migrate** page, select **lax01m01psc01.lax01.rainpole.local**, **lax01w01psc01.lax01.rainpole.local** and **lax01m01vc01.lax01.rainpole.local**, and click **Next**.
  - e On the **Ready to complete** page, review your entries and click **Finish**.

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

- a Click the **lax01-m01-vds01** distributed switch, click the **Configure** tab, and click **Resource Allocation > System traffic**.
- b Under **System Traffic**, configure each of the following traffic types with the following values.

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

13 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**.

14 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**.

**15** 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.

## Set vSAN Storage Policy in Region B

This step is to set the vSAN storage policy for the Platform Services Controller and vCenter Server appliances.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Reset the vSAN Storage Policy to default for the ESXi host that is used for bootstrap.
  - a Open an SSH connection to the ESXi host **mgmt01esx51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	esxi_root_user_password

- c Run the following command to determine the current vSAN storage policy.

```
esxcli vsan policy getdefault
```

```
[root@mgmt01esx51:~] esxcli vsan policy getdefault
Policy Class Policy Value
-----
cluster      ((("hostFailuresToTolerate" i1))
vdisk        ((("hostFailuresToTolerate" i1) ("forceProvisioning" i1))
vmnamespace  ((("hostFailuresToTolerate" i1) ("forceProvisioning" i1))
vmswap       ((("hostFailuresToTolerate" i1) ("forceProvisioning" i1))
vmem         ((("hostFailuresToTolerate" i1) ("forceProvisioning" i1))
[root@mgmt01esx51:~] █
```

- d Modify the default vSAN storage policy to force provisioning of vSAN datastore without generating errors.

```
esxcli vsan policy setdefault -c vdisk -p "((("hostFailuresToTolerate" i1))"
esxcli vsan policy setdefault -c vmnamespace -p "((("hostFailuresToTolerate" i1))"
esxcli vsan policy getdefault
```

```
[root@mgmt01esx51:~] esxcli vsan policy setdefault -c vdisk -p "((("hostFailuresToTolerate" i1))"
[root@mgmt01esx51:~] esxcli vsan policy setdefault -c vmnamespace -p "((("hostFailuresToTolerate" i1))"
[root@mgmt01esx51:~] esxcli vsan policy getdefault
Policy Class Policy Value
-----
cluster      ((("hostFailuresToTolerate" i1))
vdisk        ((("hostFailuresToTolerate" i1))
vmnamespace  ((("hostFailuresToTolerate" i1) ("forceProvisioning" i1))
vmswap       ((("hostFailuresToTolerate" i1) ("forceProvisioning" i1))
vmem         ((("hostFailuresToTolerate" i1) ("forceProvisioning" i1))
[root@mgmt01esx51:~] █
```

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

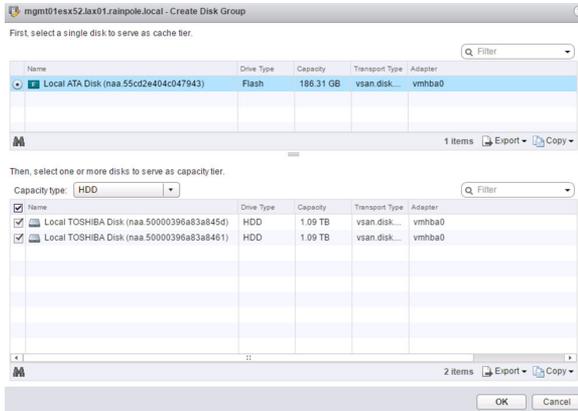
vSAN disk groups must be created on each host that is contributing storage to the vSAN datastore.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://mgmt01vc51.lax01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc51.lax01.rainpole.local** tree.
- 3 Click on the **LAX01-Mgmt01** cluster and click the **Configure** tab.
- 4 Under **Virtual SAN**, click **Disk Management**.
- 5 Click on **mgmt01esx52.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 **mgmt01esx53.lax01.rainpole.local** and **mgmt01esx54.lax01.rainpole.local**.
- 8 Assign a license to vSAN.
  - a Right click the **LAX01-Mgmt01** cluster and select **Assign License**.
  - b In the **LAX01-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

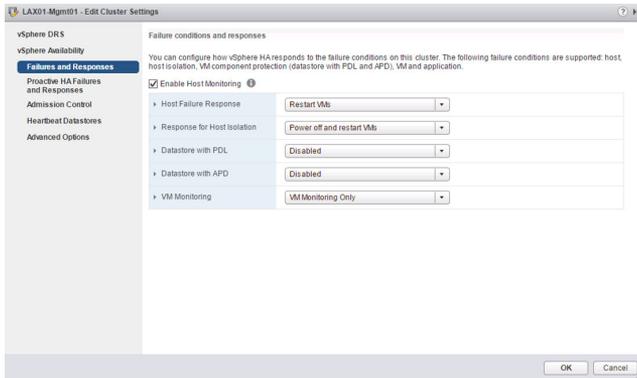
- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Hosts and Clusters**.
  - a Expand the **mgmt01vc51.lax01.rainpole.local** inventory.
  - b Select the **LAX01-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.

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



6 Click **Admission Control**.

7 In the **Admission Control** page enter following settings.

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

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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Change the default ESX Admins group.
  - a In the **Navigator**, click **Hosts and Clusters**.
  - b Expand the entire **mgmt01vc51.lax01.rainpole.local** vCenter inventory tree, and select the **mgmt01esx51.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 **mgmt01vc51.lax01.rainpole.local** vCenter inventory tree, and select the **mgmt01esx51.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 **mgmt01vc51.lax01.rainpole.local** vCenter inventory tree, and select the **mgmt01esx51.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-Mgmt01 cluster.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://mgmt01vc51.lax01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Host and Clusters** and expand the **mgm01vc51.lax01.rainpole.local** tree.
- 3 Click on **mgmt01esx51.lax01.rainpole.local**.
- 4 Click on **Datastores**.
- 5 Click the **Create a New Datastore** icon.  
The **New Datastore** wizard opens.
- 6 On the **Type** page, select **NFS** and click **Next**.
- 7 On the **Select NFS version** page, select **NFS 3** and click **Next**.
- 8 On the **Name and configuration** page, enter the following datastore information and click **Next**.

Setting	Value
Datastore Name	LAX01A-NFS01-VDP01
Folder	/V2D_vDP_MgmtB_4TB
Server	172.17.15.251

## 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a Host Profile from *mgmt01esx51.lax01.rainpole.local*
  - a In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc51.lax01.rainpole.local** tree.
  - b Right-click the ESXi host **mgmt01esx51.lax01.rainpole.local** and choose **Host Profiles > Extract Host Profile**.
  - c In the **Extract Host Profile** window, enter **LAX01-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 **mgm01vc51.lax01.rainpole.local** tree.
  - b Right-click on the **LAX01-Mgmt01** cluster and choose **Host Profiles > Attach Host Profile**.
  - c In the **Attach Host Profile** window, click the **LAX01-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-Mgmt01** and choose **Export Host Customizations**.
  - c Click **Save**.
  - d Choose a file location to save the *LAX01-Mgmt01\_host\_customizations.csv* file.
  - e Open the *LAX01-Mgmt01\_host\_customizations.csv* in Excel.

f Edit the Excel file to include the following values.

<b>ESXi Host</b>	<b>Active Directory Configuration Password</b>	<b>Active Directory Configuration Username</b>	<b>NetStack Instance defaultTcpipStack-&gt;DNS configuration Name for this host</b>
mgmt01esx51.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	mgmt01esx51
mgmt01esx52.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	mgmt01esx52
mgmt01esx53.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	mgmt01esx53
mgmt01esx54.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	mgmt01esx54

<b>ESXi Host</b>	<b>Host virtual NIC vDS-Mgmt:vDS-Mgmt-Management:management-&gt;IP address settings Host IPv4 address</b>	<b>Host virtual NIC vDS-Mgmt:vDS-Mgmt-Management:management-&gt;IP address settings SubnetMask</b>
mgmt01esx51.lax01.rainpole.local	172.17.11.101	255.255.255.0
mgmt01esx52.lax01.rainpole.local	172.17.11.102	255.255.255.0
mgmt01esx53.lax01.rainpole.local	172.17.11.103	255.255.255.0
mgmt01esx54.lax01.rainpole.local	172.17.11.104	255.255.255.0

<b>ESXi Host</b>	<b>Host virtual NIC vDS-Mgmt:vDS-Mgmt-NFS:&lt;UNRESOLVED&gt;-&gt;IP address settings Host IPv4 address</b>	<b>Host virtual NIC vDS-Mgmt:vDS-Mgmt-NFS:&lt;UNRESOLVED&gt;-&gt;IP address settings SubnetMask</b>
mgmt01esx51.lax01.rainpole.local	172.17.15.101	255.255.255.0
mgmt01esx52.lax01.rainpole.local	172.17.15.102	255.255.255.0
mgmt01esx53.lax01.rainpole.local	172.17.15.103	255.255.255.0
mgmt01esx54.lax01.rainpole.local	172.17.15.104	255.255.255.0

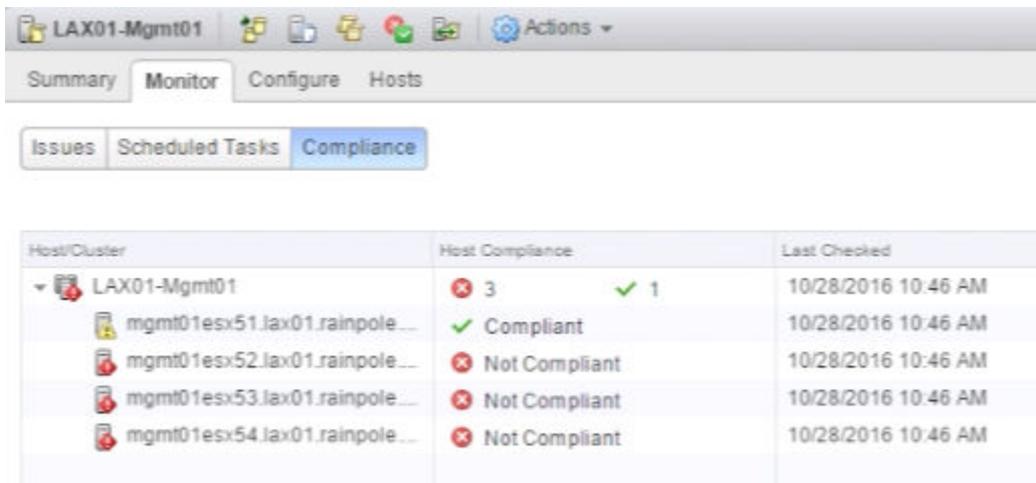
<b>ESXi Host</b>	<b>Host virtual NIC vDS-Mgmt:vDS-Mgmt-VR:vSphereReplication,vSphereReplicationNFC-&gt;IP address settings Host IPv4 address</b>	<b>Host virtual NIC vDS-Mgmt:vDS-Mgmt-VR:vSphereReplication,vSphereReplicationNFC-&gt;IP address settings SubnetMask</b>
mgmt01esx51.lax01.rainpole.local	172.17.16.101	255.255.255.0
mgmt01esx52.lax01.rainpole.local	172.17.16.102	255.255.255.0
mgmt01esx53.lax01.rainpole.local	172.17.16.103	255.255.255.0
mgmt01esx54.lax01.rainpole.local	172.17.16.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VSAN:vsan->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VSAN:vsan->IP address settings SubnetMask
mgmt01esx51.lax01.rainpole.local	172.17.13.101	255.255.255.0
mgmt01esx52.lax01.rainpole.local	172.17.13.102	255.255.255.0
mgmt01esx53.lax01.rainpole.local	172.17.13.103	255.255.255.0
mgmt01esx54.lax01.rainpole.local	172.17.13.104	255.255.255.0

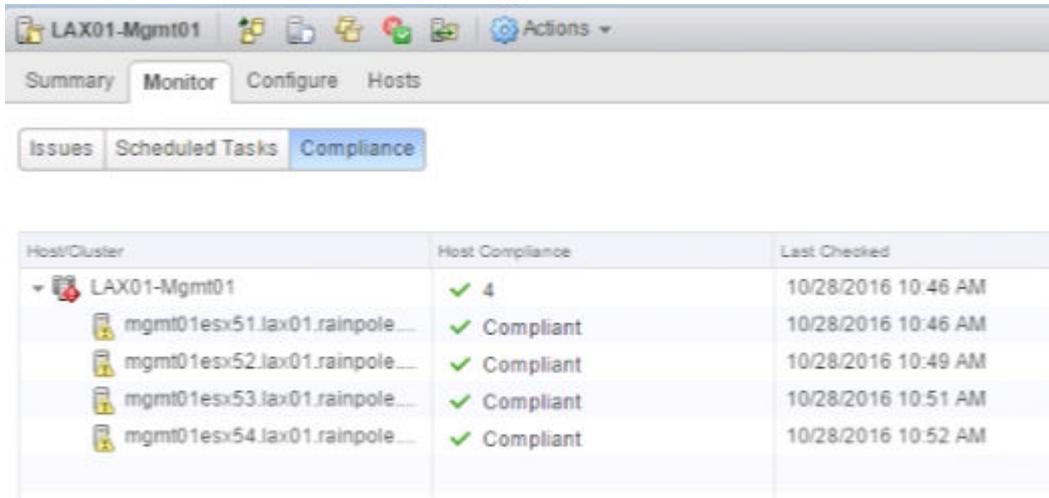
ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-vMotion:vmotion->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-vMotion:vmotion->IP address settings SubnetMask
mgmt01esx51.lax01.rainpole.local	172.17.12.101	255.255.255.0
mgmt01esx52.lax01.rainpole.local	172.17.12.102	255.255.255.0
mgmt01esx53.lax01.rainpole.local	172.17.12.103	255.255.255.0
mgmt01esx54.lax01.rainpole.local	172.17.12.104	255.255.255.0

- g When you have updated the Excel file, save it in the CSV file format and close Excel.
  - h Click the **Configure** tab.
  - i Click the **Edit Host Customizations** button.
  - j In the **Edit Host Customizaions** window select all hosts and click **Next**.
  - k Click the **Browse** button to use a customization file, locate the *LAX01-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-Mgmt01** and click the **Check Host Profile Compliance** button.



- c Select **mgmt01esx52.lax01.rainpole.local**, click the **Remediate host based on its host profile** button, and click **Finish** on the **Ready to complete** window.
- d Select **mgmt01esx53.lax01.rainpole.local**, click the **Remediate host based on its host profile** button, and click **Finish** on the **Ready to complete** window.
- e Select **mgmt01esx54.lax01.rainpole.local**, click the **Remediate host based on its host profile** button, and click **Finish** on 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-Mgmt01**, click the **Monitor** tab, and then click the **Scheduled Tasks** subtab.
  - 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-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 vSAN 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 vSAN Default Storage Policy.

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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Hosts and Clusters**.
- 3 Expand the **mgmt01vc51.lax01.rainpole.local** tree.
- 4 Select the **mgmt01psc51** virtual machine.
- 5 Click the **Configure** tab, click **Policies**, and click **Edit VM Storage Policies**.
- 6 In the **mgmt01psc01:Manage VM Storage Policies** dialog box, from the **VM storage policy** drop down menu, select **Virtual SAN 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 Virtual SAN Default Storage Policy on **comp01psc51** and **mgmt01vc51** 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 2-4. Folders for the Management Applications in Region B**

Management Applications	Folder
vCenter Server + Platform Services Controllers	MGMT51
vRealize Log Insight	vRLI51
vRealize Automation + vRealize Orchestrator + vRealize Business	vRA51
vRealize Automation (Proxy Agent) + vRealize Business (Data Collector)	vRA51IAS
vRealize Operations Manager	vROps51
vRealize Operations Manager (Remote Collectors)	vROps51RC
NSX Manager + Controllers + Edges	NSX51
VMware Site Recovery Manager + vSphere Data Protection	BCDR51

## Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a folder for the vRealize Log Insight management application.
  - a In the **Navigator**, click **VMs and Templates**.
  - b Expand the **mgmt01vc51.lax01.rainpole.local** tree.
  - c Right-click the **LAX01** data center, and select **New Folder > New VM and Template Folder**.
  - d In the **New Folder** dialog box enter **MGMT51** 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 MGMT51 folder.
  - a In the **Navigator**, click **VMs and Templates**.
  - b Expand the **mgmt01vc51.lax01.rainpole.local** tree.
  - c Expand the **Discovered Virtual Machines** folder.
  - d Drag **mgmt01vc51**, **mgmt01psc51** and **comp01psc51** to the **MGMT51** folder.
- 4 Delete the **Discovered Virtual Machines** folder.
  - a In the **Navigator**, click **VMs and Templates**.
  - b Expand the **mgmt01vc51.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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator** select **Hosts and Clusters** and expand the **mgm01vc51.lax01.rainpole.local** tree.
- 3 Select the **LAX01-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 **mgmt01psc51** and **comp01psc51** 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.

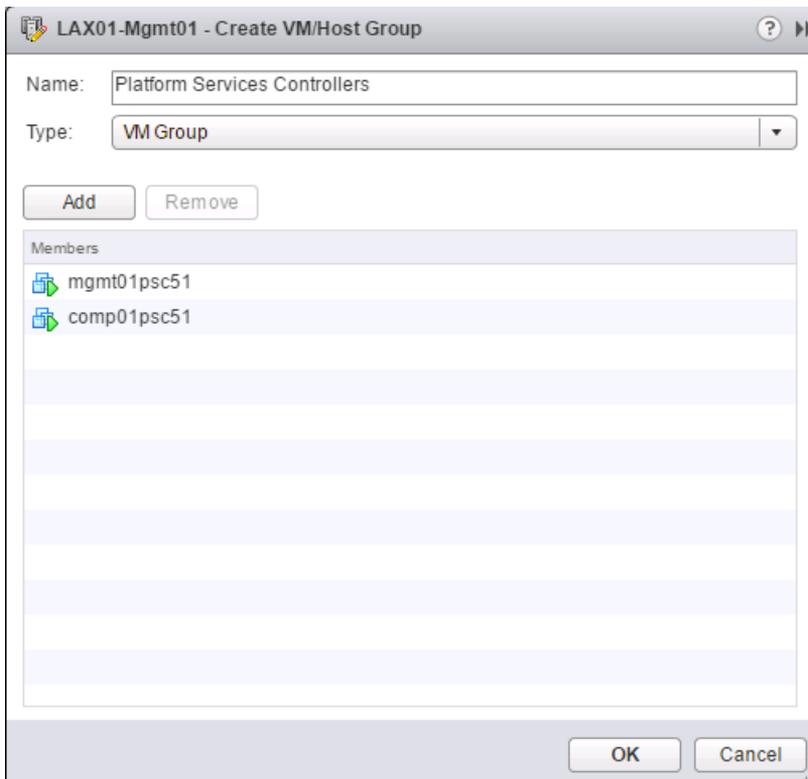
**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator** select **Hosts and Clusters** and expand the **mgm01vc51.lax01.rainpole.local** tree.

- 3 Create a VM Group for the Platform Services Controllers.
  - a Select the **LAX01-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 **mgmt01psc51** and **comp01psc51** and click **OK**.



- 4 Create a VM Group for the vCenter Server virtual machine.
  - a Select the **LAX01-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 **mgmt01vc51** and click **OK**.
- 5 Create a Rule to power on the Platform Services Controllers followed by vCenter Servers.
  - a Select the **LAX01-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**.

**LAX01-Mgmt01 - Create VM/Host Rule**

Name:

Enable rule.

Type:

Description:

Virtual machines in the VM group Platform Services Controllers will be restarted first.  
Virtual machines in the VM group vCenter Servers will be restarted afterwards, when the cluster dependency restart condition has been met.

First restart VMs in VM group:

Then restart VMs in VM group:

## 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](#)

When an authorized change is made to a host, the Host Profile must be updated to reflect the changes.

### 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

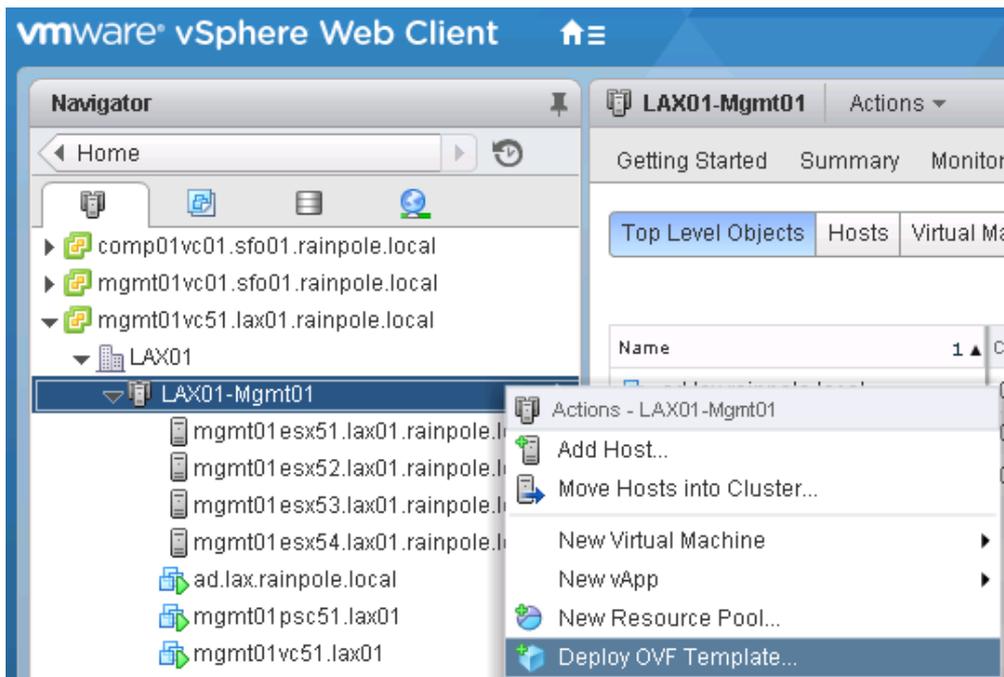
You deploy the NSX Manager appliance from the OVA file to the LAX01-Mgmt cluster.

### Procedure

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, expand the entire **mgmt01vc51.lax01.rainpole.local** tree.
- 3 Right-click the **LAX01-Mgmt01** cluster and click **Deploy OVF Template**.



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

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

Setting	Value
Name	mgmt01nsxm51
Datacenter or folder	NSX51

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

Setting	Value
Cluster	LAX01-Mgmt01

- 7 On the **Review details** page, click **Next**.
- 8 On the **Accept license agreements** page, click **Accept** and click **Next**.
- 9 On the **Select storage** page, enter the following settings, and click **Next**.

Setting	Value
VM storage policy	vSAN Default Storage Policy
Datastore	LAX01A-VSAN01-MGMT01

- 10 On the **Setup networks** page, under **Destination Network**, select **vDS-Mgmt-Management** and click **Next**.
- 11 On the **Customize template** page, expand all options, enter the following settings, and click **Next**.

Setting	Value
DNS Server List	172.17.11.5,172.17.11.4
Domain Search List	lax01.rainpole.local
Default IPv4 Gateway	172.17.11.253
Hostname	mgmt01nsxm51.lax01.rainpole.local
Network 1 IPv4 Address	172.17.11.65
Network 1 Netmask	255.255.255.0
Enable SSH	Selected
NTP Server List	<ul style="list-style-type: none"> <li>■ ntp.lax01.rainpole.local</li> <li>■ ntp.sfo01.rainpole.local</li> </ul>
CLI "admin" User Password / enter	<i>mgmtnsx_admin_password</i>
CLI "admin" User Password / confirm	<i>mgmtnsx_admin_password</i>
CLI Privilege Mode Password / enter	<i>mgmtnsx_priviledge_password</i>
CLI Privilege Mode Password / confirm	<i>mgmtnsx_priviledge_password</i>

- 12 On the **Ready to Complete** page, click **Finish**.
- 13 In the **Navigator**, expand the entire **mgmt01vc51.lax01.rainpole.local** tree, select the virtual machine **mgmt01nsxm51**, 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://mgmt01nsxm51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>nsx_manager_admin_password</i>

- 2 Click **Manage vCenter Registration**.
- 3 Under **Lookup Service**, click the **Edit** button.
- 4 In the **Lookup Service** dialog box, enter the following settings, and click **OK**.

Setting	Value
Lookup Service IP	ax01psc51.lax01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 5 In the **Trust Certificate?** dialog box, click **Yes**.
- 6 Under **vCenter Server**, click the **Edit** button.
- 7 In the **vCenter Server** dialog box, enter the following settings, and click **OK**.

Setting	Value
vCenter Server	mgmt01vc51.lax01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	<i>svc-nsxmanager_password</i>

- 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	svc-nsxmanager@rainpole.local
Password	svc-nsxmanager_password

- 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Assign the secondary role to the management NSX Manager in Region B.
  - a Under **Inventories**, click **Networking & Security**.
  - b In the **Navigator**, click **Installation**.
  - c On the **Management** tab, select the primary **172.16.11.65** instance.
  - d Select **Actions > Add Secondary NSX Manager**.

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

Setting	Value
NSX Manager	172.17.11.65
User name	admin
Password	<i>mgmtnsx_admin_password</i>
Confirm Password	<i>mgmtnsx_admin_password</i>

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

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

NSX kernel modules packaged in VIB files run within the hypervisor kernel and provide services such as distributed routing, distributed firewall, and VXLAN bridging capabilities. 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://mgmt01vc51.lax01.rainpole.local/vsphere-client>**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 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-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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

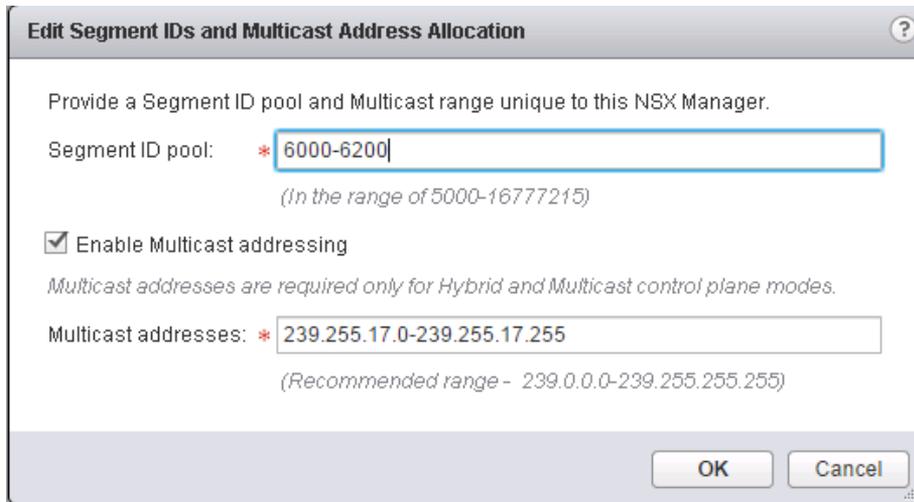
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Configure the Segment ID allocation.
  - a In the **Navigator**, click **Networking & Security**.
  - b Click **Installation**, click 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.

Setting	Value
Segment ID pool	6000-6200
Enable Multicast addressing	Selected
Multicast addresses	239.5.0.0-239.5.255.255



**3** Configure the VXLAN networking.

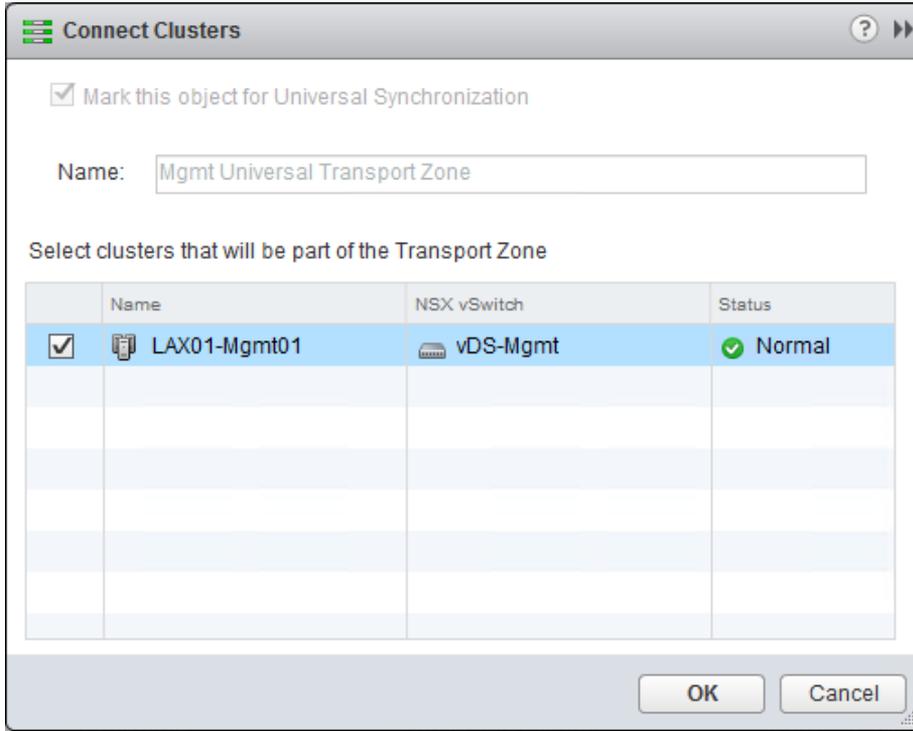
- a Click the **Host Preparation** tab.
- b Under **VXLAN**, click **Not Configured**, enter the following values, and click **OK**.

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

**4** Configure the transport zone.

- a On the **Installation** 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-Mgmt01** and click **OK**.



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

When an authorized change is made to a host, the Host Profile must be updated to reflect the changes.

### Procedure

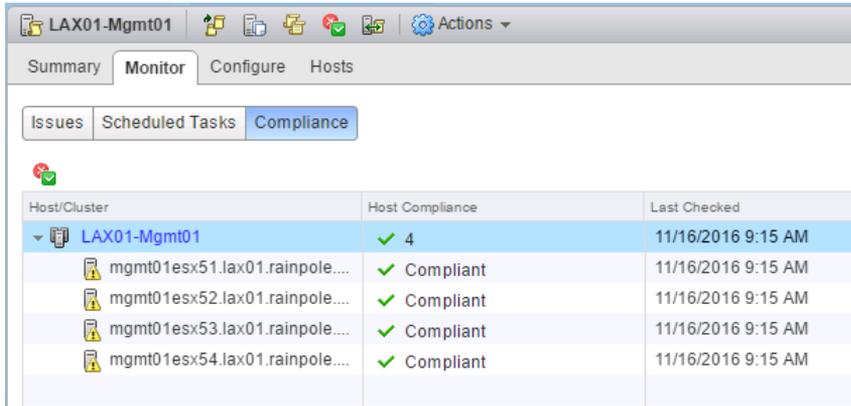
- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Update the Host Profile for the management cluster.
  - a In the **Navigator** select **Policies and Profiles**.
  - b Click **Host Profiles**, right click **LAX01-Mgmt01**, and select **Copy settings from Host**.
  - c Select **mgmt01esx51.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-Mgmt0** and click the **Check Host Profile Compliance** button.

All hosts should display a **Host Compliance** status of **Compliant**.



## 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

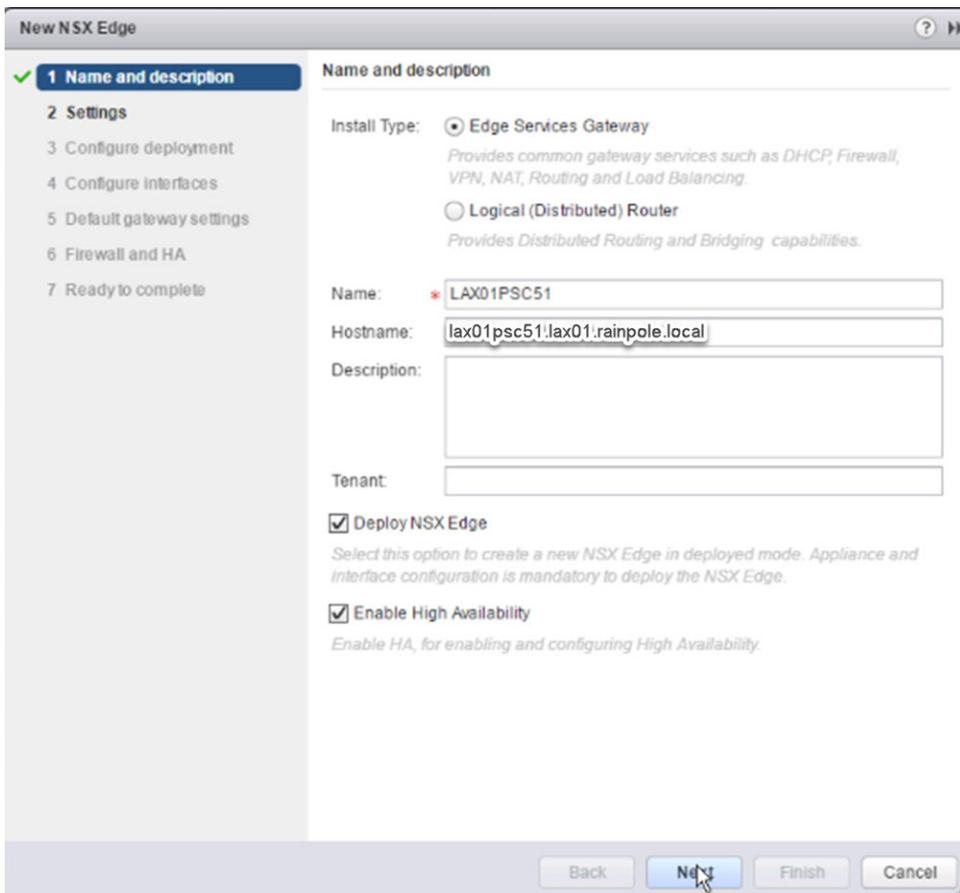
- 2 Click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.65** from the NSX Manager drop-down menu.

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

The **New NSX Edge** wizard appears.

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

Setting	Value
Install Type	Edge Services Gateway
Name	LAX01PSC51
Hostname	lax01psc51.lax01.rainpole.local
Deploy NSX EDGE	Selected
Enable High Availability	Selected



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

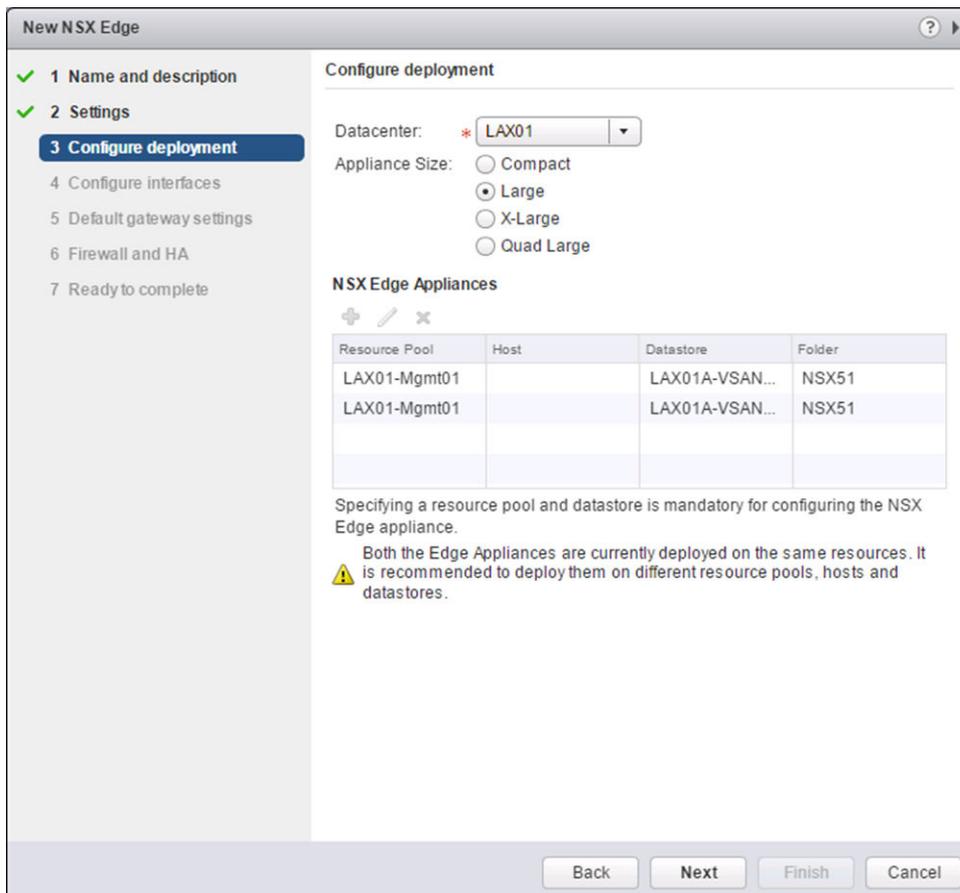
Setting	Value
User Name	admin
Password	edge_admin_password
Enable SSH access	Selected

Enable auto rule generation	Selected
Edge Control Level logging	INFO

- 8 On the **Configure deployment** page, perform the following configuration steps and click **Next**.
  - a Select **LAX01**, from the **Datacenter** drop-down menu.
  - b Click **Large** to specify the **Appliance Size**.
  - c Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Resource pool	LAX01-Mgmt01
Datastore	LAX01A-VSAN01-MGMT01
Folder	NSX51

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



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

Setting	Value
Name	PSCLB
Type	Internal
Connected To	vDS-Mgmt-Management
Connectivity Status	Connected
Primary IP Address	172.17.11.71
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

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

Setting	Value
Gateway IP	172.17.11.253
MTU	9000

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

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

New NSX Edge

- ✓ 1 Name and description
- ✓ 2 Settings
- ✓ 3 Configure deployment
- ✓ 4 Configure interfaces
- ✓ 5 Default gateway settings
- 6 Firewall and HA**
- 7 Ready to complete

### Firewall and HA

Configure Firewall default policy

Default Traffic Policy:  Accept  Deny

Logging:  Enable  Disable

**Configure HA parameters**  
Configuring HA parameters is mandatory for HA to work.

vNIC: \* any

Declare Dead Time: 15 (seconds)

Management IPs:

*Management IPs must be in CIDR format with /30 subnet and must not overlap with any vnic subnets.*

Back Next Finish Cancel

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

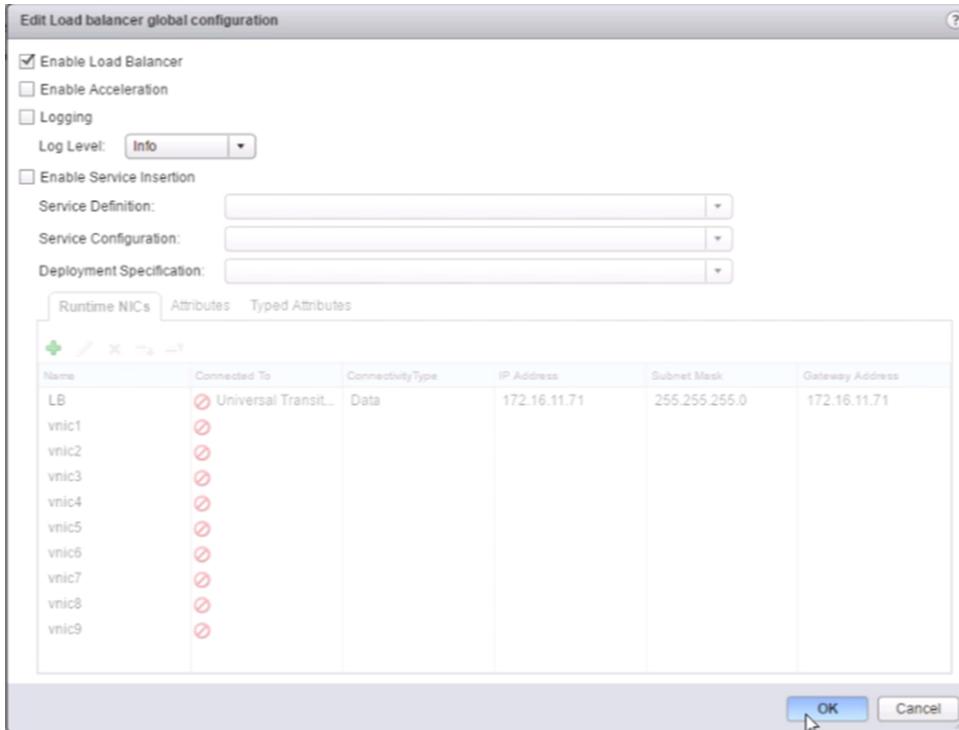
13 Enable HA logging.

- 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 **LAX01PSC51**.
- 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 **LAX01PSC51**.
- 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.

- 4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **LAX01PSC51** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Application Profiles**.
- 6 Click the **Add** icon and in the **New Profile** dialog box, enter the following values.

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

**New Profile**
?

Name:

Type: TCP ▼

Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP ▼

Cookie Name:

Mode:  ▼

Expires in (Seconds):

Insert X-Forwarded-For HTTP header

Enable Pool Side SSL

Virtual Server Certifica...
Pool Certificates

Service Certificates
CA Certificates
CRL

Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	lax01psc51.lax01.rainp	rainpole-DC01RPL-CA	Mon Mar 20 2017 - Wed M
<input type="radio"/>	VSM_SOLUTION_ca88:	VSM_SOLUTION_ca88:	Mon Mar 20 2017 - Wed Fi
<input type="radio"/>	VSM_SOLUTION_ca88:	VSM_SOLUTION_ca88:	Mon Mar 20 2017 - Wed Fi
<input type="radio"/>	VSM_SOLUTION_19e1:	VSM_SOLUTION_19e1:	Sun Feb 26 2017 - Tue Fe
<input type="radio"/>	VSM_SOLUTION_19e1:	VSM_SOLUTION_19e1:	Sun Feb 26 2017 - Tue Fe

Cipher: Default ▼

ECDHE-RSA-AES128-GCM-SHA256

ECDHE-RSA-AES256-GCM-SHA384

Client Authentication: Ignore ▼

OK
Cancel

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.

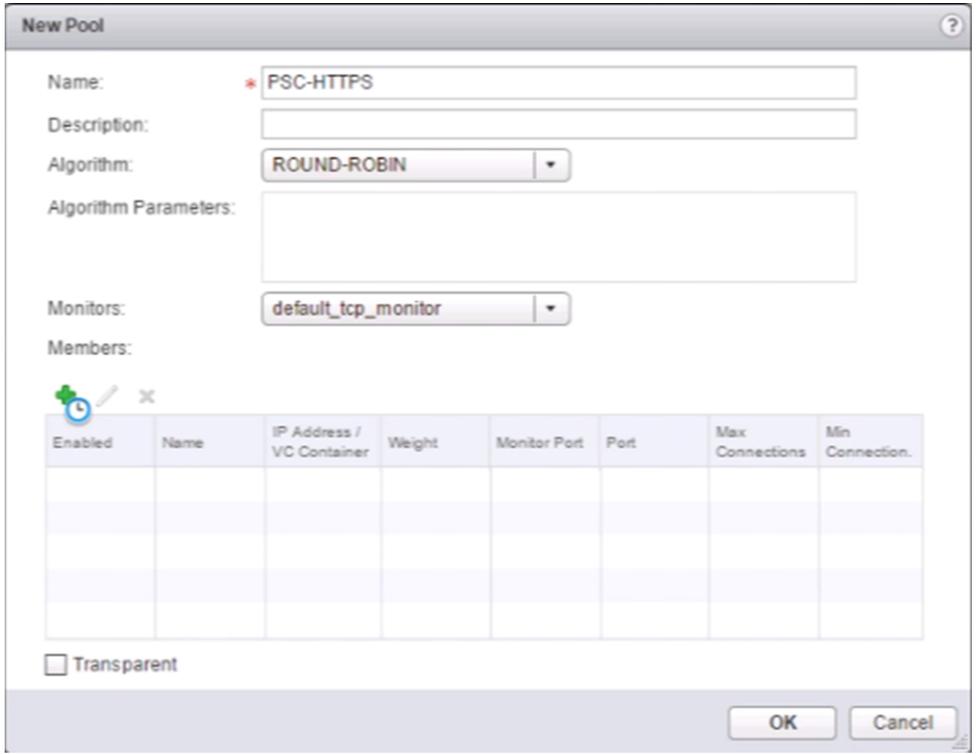
### Procedure

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

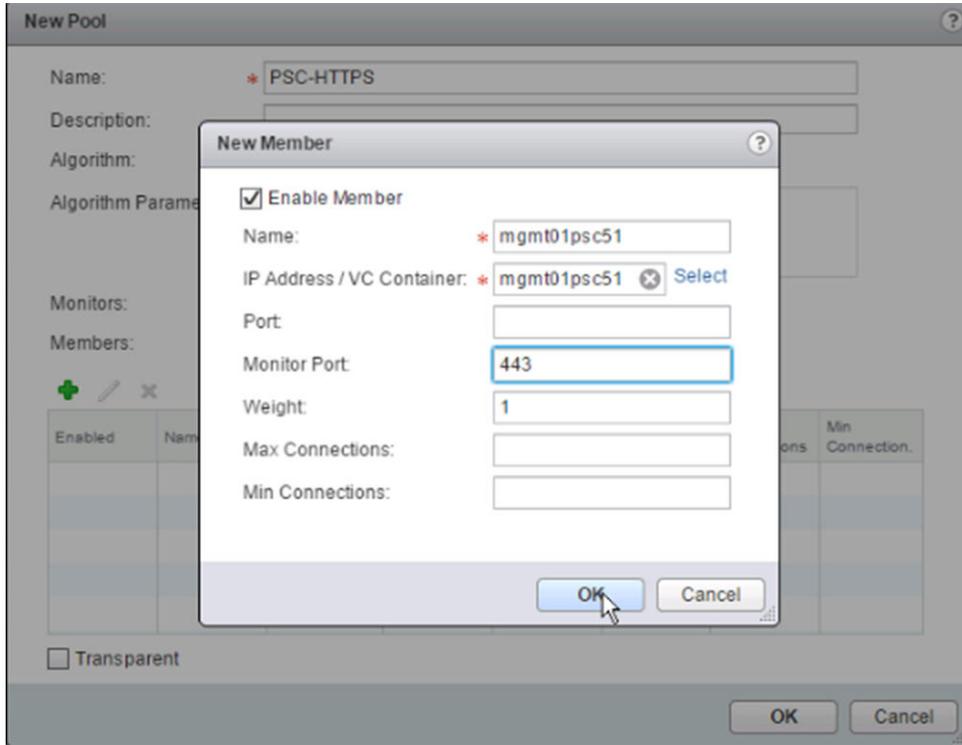
- 2 Click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **LAX01PSC51** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.
- 6 Click the **Add** icon and in the **New Pool** dialog box, enter the following values.

Setting	Value
Name	PSC-HTTPS
Algorithm	ROUND-ROBIN
Monitors	default-tcp-monitor



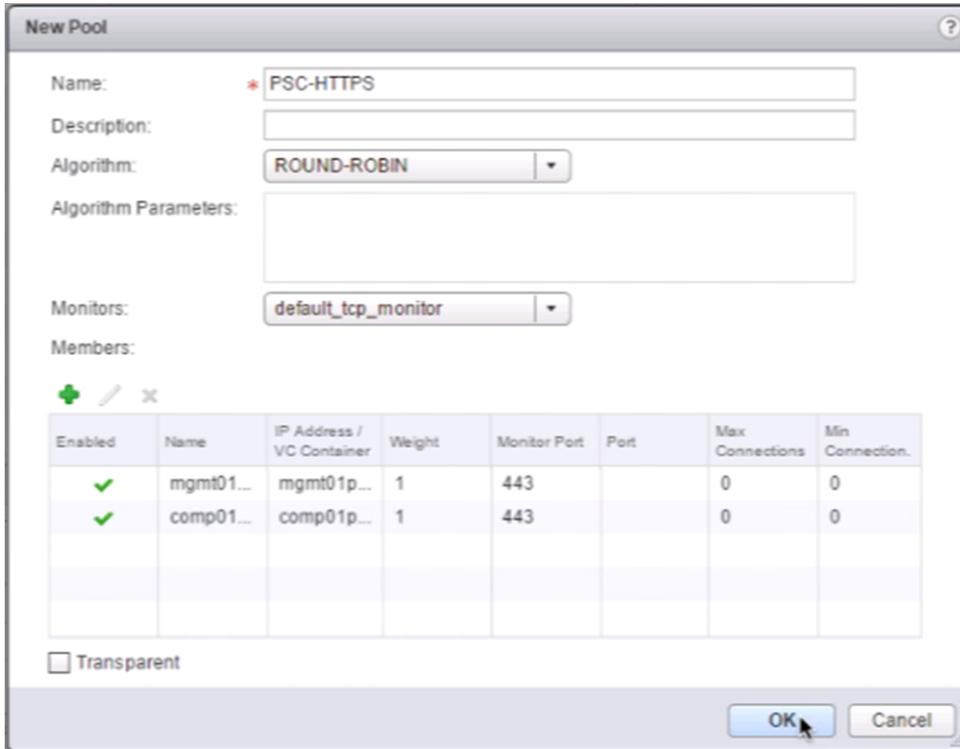
- 7 **New Members** dialog box, click the **Add** icon to add the first pool member.
- 8 In the **New Member** dialog box, enter the following values, and click **OK**.

Setting	Values for First Server Pool	Values for Second Server Pool
Name	mgmt01psc51	mgmt01psc51
IP Address/VC Container	mgmt01psc51	mgmt01psc51
Monitor Port	443	389
Weight	1	1



- 9 Under **Members**, click the **Add** icon to add the second pool member.
- 10 In the **New Member** dialog box, enter the following values, click **OK** and click **OK** to save the PSC server pools.

Setting	Values for First Server Pool	Values for Second Server Pool
Enable Member	Selected	Selected
Name	comp01psc51	comp01psc51
IP Address/VC Container	comp01psc51	comp01psc51
Port		
Monitor Port	443	389
Weight	1	1



11 Repeat the procedure to create the remaining server pool.

## 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

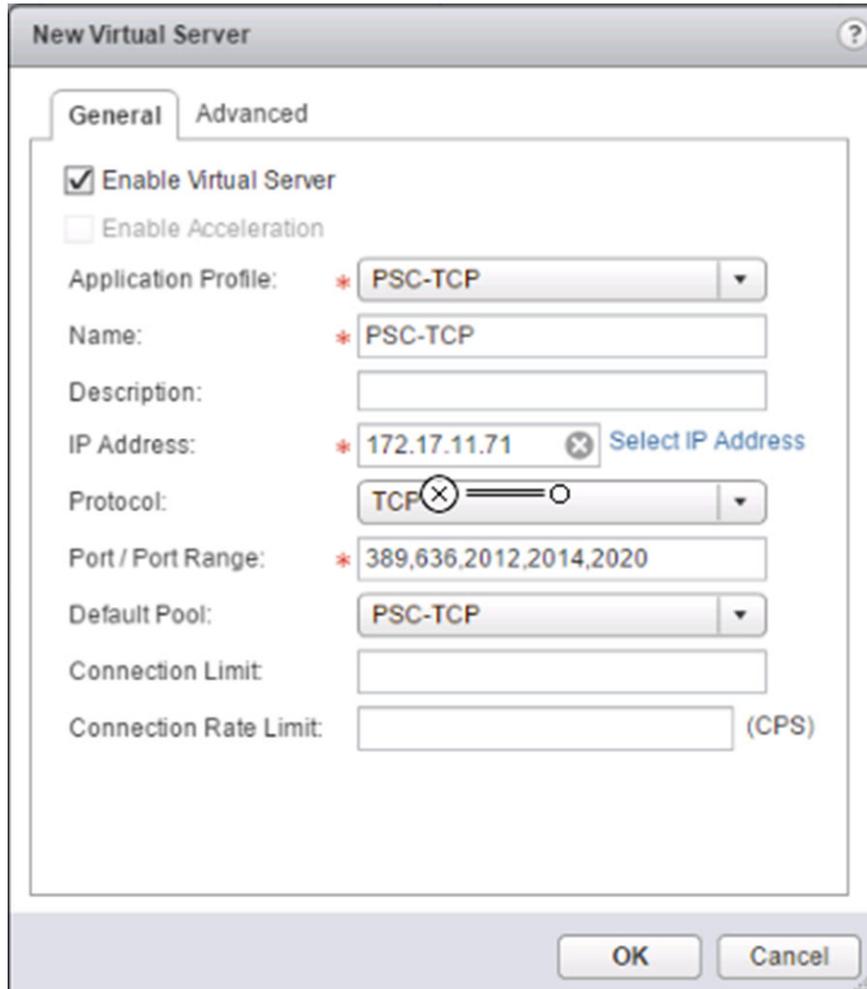
- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **LAX01PSC51** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Virtual Servers**.

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

Setting	Value	Value
Enable Virtual server	Selected	Selected
Application Profile	PSC-TCP	PSC-HTTPS
Name	PSC-TCP	PSC-HTTPS
Description	389-LDAP,2012-Control Interface,2014-RPC Port,2020-Authentication,636-SSL LDAP	Data from the vSphere Web Client
IP Address	172.17.11.71	172.17.11.71
Protocol	TCP	HTTPS
Port	389,636,2012,2014,2020	443
Default Pool	PSC-TCP	PSC-HTTPS



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

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

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

For the Platform Services Controller Load Balancer, you edit the DNS entry of `lax01psc51.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 `mgmt01psc51`.

### 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 `lax01psc51` record on the right.
- 4 Double-click the **lax01psc51** record, change the IP address of the record from `172.17.11.61` to **172.17.11.71**, and click **OK**.

Setting	Value
Fully Qualified domain name (FQDN)	<code>lax01psc51.lax01.rainpole.local</code>
IP Address	<code>172.17.11.71</code>
Update Associated Pointer (PTR) record	Selected

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

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

### Procedure

- 1 [Deploy NSX Edge Devices for North-South Routing in Region B](#)  
Deploy two NSX Edge devices for North-South Routing.
- 2 [Disable the Firewall Service in Region B](#)  
Disable the firewall of the NSX Edge devices, this is required for equal-cost multi-path (ECMP) to operate correctly.
- 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**

NSX Edge Device	Device Name
NSX Edge Device 1	LAXMGMT-ESG01
NSX Edge Device 2	LAXMGMT-ESG02

**Table 2-6. NSX Edge Interfaces Settings**

Interface	Primary IP Address	Primary IP Address
	LAXMGMT-ESG01	LAXMGMT-ESG02
Uplink01	172.27.14.2	172.27.14.3
Uplink02	172.27.15.3	172.27.15.2
SFOMGMT-UDLR01	192.168.10.50	192.168.10.51

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **<https://mgmt01vc51.lax01.rainpole.local/vsphere-client>**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.
- 5 Click the **Add** icon to deploy a new NSX Edge.

The **New NSX Edge** wizard appears.

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

Settings	Value
Install Type	Edge Service Gateway
Name	LAXMGMT-ESG01
Deploy NSX Edge	Selected
Enable High Availability	Deselected

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

Settings	Value
User Name	admin
Password	<i>edge_admin_password</i>
Enable SSH access	Selected
Enable FIPS mode	Deselected
Enable auto rule generation	Selected
Edge Control Level logging	INFO

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

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

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

Setting	Value
Cluster/Resource Pool	LAX01-Mgmt01
Datastore	LAX01A-VSAN01-MGMT01
Folder	NSX51

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

Setting	Value
Name	Uplink01
Type	Uplink
Connected To	vDS-Mgmt-Uplink01
Connectivity Status	Connected
Primary IP Address	172.27.14.2
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

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

Setting	Value
Name	Uplink02
Type	Uplink
Connected To	vDS-Mgmt-Uplink02
Connectivity Status	Connected
Primary IP Address	172.27.15.3
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

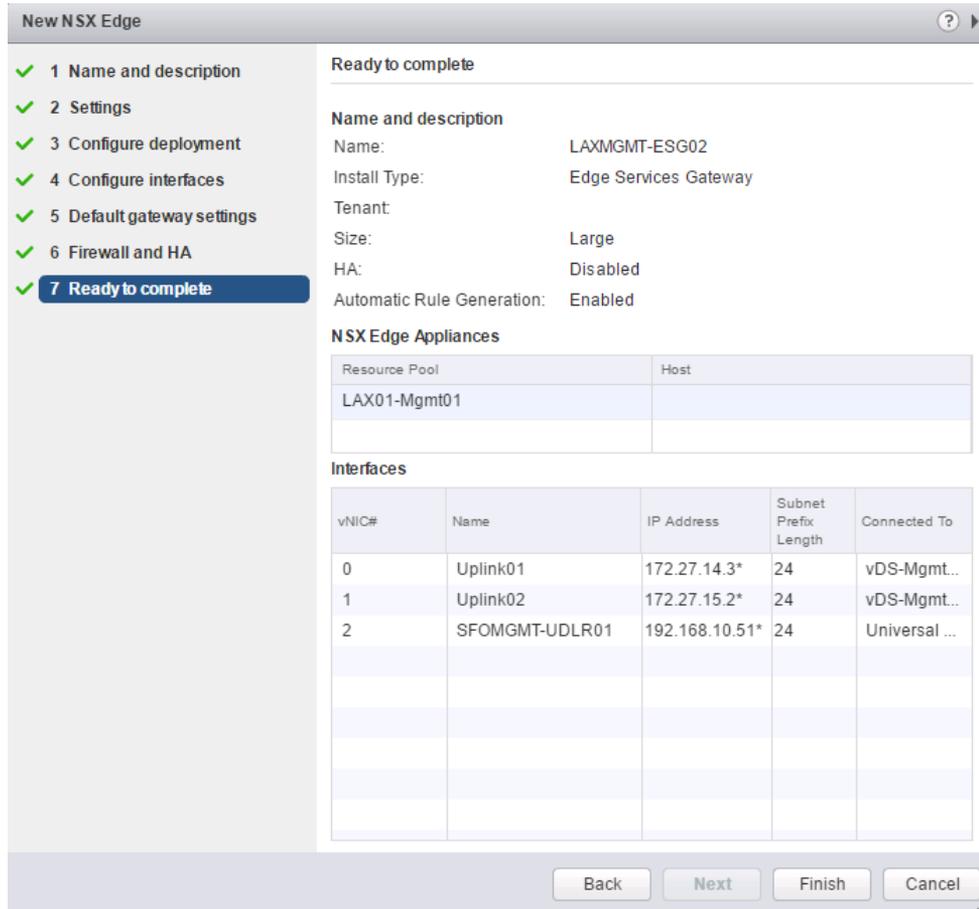
- g Click the **Add** icon a third time to configure the UDLR interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	SFOMGMT-UDLR01
Type	Internal
Connected To	Universal Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.10.50
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

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

- i On the **Firewall and HA** page, click **Next**.
  - j On the **Ready to Complete** page, review the configuration settings you entered and click **Finish**.
- 6 Repeat this procedure to configure another NSX edge using the settings for the second NSX Edge device.

Upon repeating the procedure to configure LAXMGMT-ESG02, 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 **mgmt01vc51.lax01.rainpole.local** tree control.
  - c Select the **LAX01-Mgmt01** cluster, and click the **Configure** tab.
  - d Under **Configuration**, click **VM/Host Rules**.
  - e Click **Add**.

- f In the **LAX01-Mgmt01 - Create VM/Host Rule** dialog box, enter the following settings and click **Add**.

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

- g In the **Add Rule Member** dialog box, select the check box next to each of the two, newly deployed NSX ESGs, and click OK.
- h In the **LAX01-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 LAXMGMT-ESG01 and LAXMGMT-ESG02.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.
- 5 Double-click the **LAXMGMT-ESG01** 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 LAXMGMT-ESG02.

## 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: LAXMGMT-ESG01 and LAXMGMT-ESG02.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.
- 5 Double-click the **LAXMGMT-ESG01** 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**.
  - d Click **Publish Changes**.

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

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

Setting	Value
Network	192.168.11.0/24
Next Hop	192.168.10.3
Interface	SFOMGMT-UDLR01
MTU	9000
Admin Distance	210

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

Setting	Value
Network	192.168.31.0/24
Next Hop	192.168.10.3
Interface	SFOMGMT-UDLR01
MTU	9000
Admin Distance	210

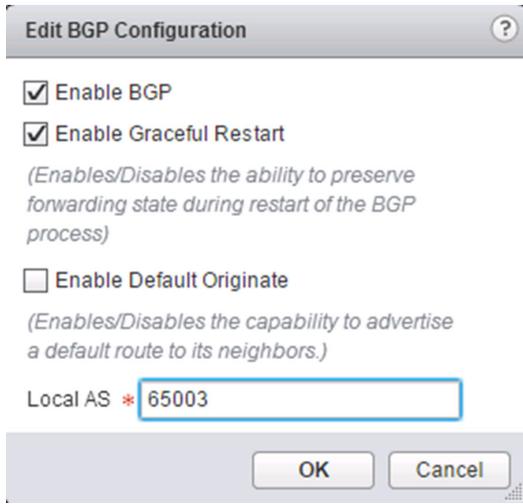
c Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Network	192.168.32.0/24
Next Hop	192.168.10.3
Interface	SFOMGMT-UDLR01
MTU	9000
Admin Distance	210

d Click **Publish Changes**.

- 9 On the **Routing** tab, select **BGP** to configure it.
  - a Click the **Edit** button, enter the following settings, and click **OK**.

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



- b Click the **Add** icon to add a neighbor.

The **New Neighbor** dialog box appears. You add two neighbors: the first Top of Rack Switch and the second Top of Rack Switch.

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

Setting	Value
IP Address	172.27.14.1
Remote AS	65002
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	<i>BGP_password</i>

**New Neighbour** ?

IP Address : \* 172.27.14.1

Remote AS : \* 65002

Weight : 60

Keep Alive Time : 4 (Seconds)

Hold Down Time : 12 (Seconds)

*(BGP Keep alive timer value needs to be one third of hold down timer)*

Password : \*\*\*\*\*

BGP Filters :

+ ✎ ✕ ≡↑ ≡↓ Filter

Direction	Action	Network	IP Prefix GE	IP Prefix LE

0 items

OK Cancel

- 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.

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

Setting	Value
IP Address	172.27.15.1
Remote AS	65002
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	<i>BGP_password</i>

**New Neighbour** ?

IP Address : \* 172.27.15.1

Remote AS : \* 65002

Weight : 60

Keep Alive Time : 4 (Seconds)

Hold Down Time : 12 (Seconds)

*(BGP Keep alive timer value needs to be one third of hold down timer)*

Password : \*\*\*\*\*

**BGP Filters :**

+ ✎ ✕ ≡ ≡

Q Filter

Direction	Action	Network	IP Prefix GE	IP Prefix LE

0 items

OK Cancel

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

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

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

Setting	Value
IP Address	192.168.10.4
Remote AS	65003
Weight	10
Keep Alive Time	1
Hold Down Time	3
Password	<i>BGP_password</i>

**New Neighbour**

IP Address : \* 192.168.10.4

Remote AS : \* 65003

Weight : 60

Keep Alive Time : 1 (Seconds)

Hold Down Time : 3 (Seconds)

*(BGP Keep alive timer value needs to be one third of hold down timer)*

Password : \*\*\*\*\*

BGP Filters :

Direction	Action	Network	IP Prefix GE	IP Prefix LE

0 items

OK Cancel

h Click **Publish Changes**.

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

- 10 On the **Routing** tab, select **Route Redistribution** to configure it.
  - a On the **Route Redistribution** page, click the **Edit** button.
  - b In the **Change Redistribution Settings** dialog box, select the **BGP** check box and click **OK**.



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

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

- e Click **Publish Changes**.

The route redistribution configuration is now visible in the **Route Redistribution** table.

- 11 Repeat this procedure for the LAXMGMT-ESG02 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 it's 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: LAXMGMT-ESG01 and LAXMGMT-ESG02.

## Procedure

- 1 Log in to the NSX Edge device using a Secure Shell (SSH) client.
  - a Open an SSH connection to the **LAXMGMT-ESG01** NSX Edge device.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	edge_admin_password

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

The BGP State 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.

```

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

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

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

You verify multiple routes to BGP learned networks by locating the same route using a different IP address. The IP addresses are listed after the word `via` in the right-side column of the routing table output. In the 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.

```

NSX-edge-5-0> show ip route

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

Total number of routes: 15

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

```

- 4 Repeat this procedure for the NSX Edge device LAXMGMT-ESG02.

## 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://mgmt01vc51.lax01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under Inventories, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.16.11.65** from the **NSX Manager** drop-down menu.

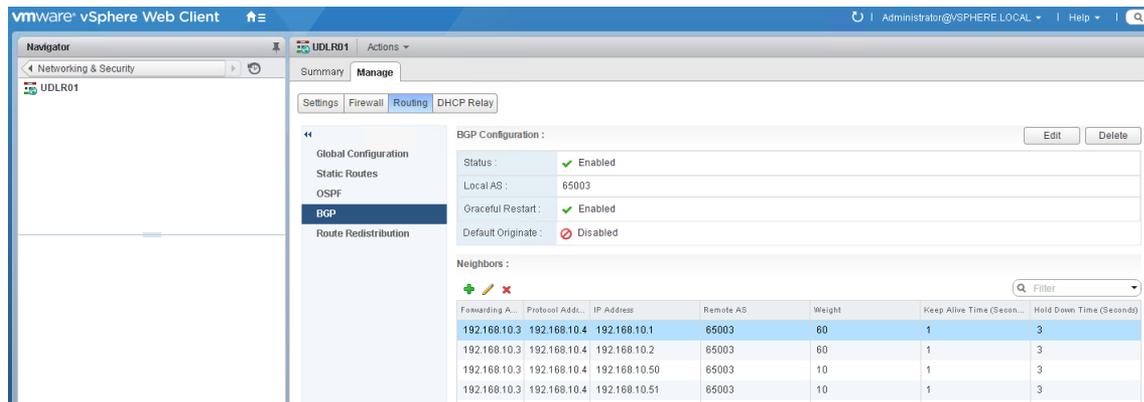
5 Configure the Universal Distributed Logical Router.

- a Double-click **SFOMGMT-UDLR01**.
- 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: LAXMGMT-ESG01 and LAXMGMT-ESG02.

Setting	LAXMGMT-ESG01 Value	LAXMGMT-ESG02 Value
IP Address	192.168.10.50	192.168.10.51
Forwarding Address	192.168.10.3	192.168.10.3
Protocol Address	192.168.10.4	192.168.10.4
Remote AS	65003	65003
Weight	10	10
Keep Alive Time	1	1
Hold Down Time	3	3
Password	<i>BGP_password</i>	<i>BGP_password</i>

- 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 UDLR01, the UDLR whose peering and BGP configuration you want to verify.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>udlr_admin_password</i>

- 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.

```

192.168.10.4 - PuTTY
BGP neighbor is 192.168.10.1, remote AS 65003,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 351566 messages, Sent 351576 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 1 Identifier 0x3b7a3cc
  Route refresh request:received 0 sent 0
  Prefixes received 3 sent 3 advertised 3
Connections established 2, dropped 1
Local host: 192.168.10.4, Local port: 179
Remote host: 192.168.10.1, Remote port: 21217

BGP neighbor is 192.168.10.2, remote AS 65003,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 351547 messages, Sent 351560 messages
byte 1108
  
```

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

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

```

UDLR01-0> show ip route

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

Total number of routes: 16

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

UDLR01-0>

```

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

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

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://mgmt01vc51.lax01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Configure the Universal Distributed Logical Router static routes.
  - a Under **Inventories**, click **Networking and Security**.
  - b In the **Navigator**, click **NSX Edges**.
  - c Select **172.16.11.65** from the **NSX Manager** drop-down menu.

- d Double-click **UDLR01**.
- 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**.

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

**Add Static Route** ?

Network: \* 172.17.11.0/24  
*Network should be entered in CIDR format  
 e.g. 192.169.1.0/24*

Next Hop: \* 192.168.10.50,192.168.10.51  
*Comma-separated list of IP addresses  
 (ex.1.1.1.1,1.2.3.4,10.10.10.10)*

MTU: 9000

Admin Distance: 1

LocaleId:

Description:

OK Cancel

- 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Exclude vCenter Server in Region B from firewall protection.
  - a 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 **mgmt01vc51** 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**

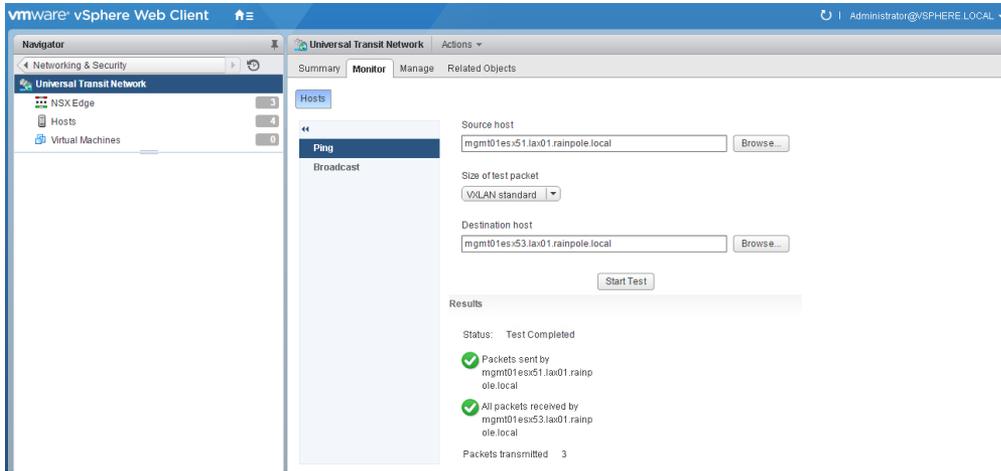
Test the configuration of the NSX logical network using a ping test. A ping test checks if two hosts in a network can reach each other.

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Use the Ping Monitor to test connectivity.
  - a Under **Logical Switches**, double-click **Universal Transit Network**.
  - b Click the **Monitor** tab.
  - c From the **Source host** drop-down menu select **mgmt01esx51.lax01.rainpole.local**.
  - d From the **Destination host** drop-down menu select **mgmt01esx53.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://mgmt01vc51.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 **mgmt01vc01.sfo01.rainpole.local** tree.

- c Right-click **SFOMGMT-ESG01-0** and select **Power > Shut Down Guest OS**.
  - d Right-click **SFOMGMT-ESG02-0** 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 **UDLR01**.
  - 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-43c8-9402-4965b0651f98-0> show ip route
Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
Total number of routes: 8
B 0.0.0.0/0 [20/0] via 192.168.100.50
B 0.0.0.0/0 [20/0] via 192.168.100.51
C 169.254.1.0/30 [0/0] via 169.254.1.1
B 172.16.35.0/24 [20/0] via 192.168.100.50
B 172.16.35.0/24 [20/0] via 192.168.100.51
B 172.17.35.0/24 [200/0] via 192.168.100.50
B 172.17.35.0/24 [200/0] via 192.168.100.51
B 172.27.13.0/24 [20/0] via 192.168.100.50
B 172.27.13.0/24 [20/0] via 192.168.100.51
B 172.27.21.0/24 [200/0] via 192.168.100.50
B 172.27.21.0/24 [200/0] via 192.168.100.51
B 172.27.22.0/24 [20/0] via 192.168.100.50
B 172.27.22.0/24 [20/0] via 192.168.100.51
C 192.168.100.0/24 [0/0] via 192.168.100.4
NSX-edge-7b98db5b-b32b-43c8-9402-4965b0651f98-0>
    
```

- 4 Power on the NSX Edge services gateways in Region A.
- a In the **Navigator**, click **Hosts and Clusters**.
  - b Expand the entire **mgmt01vc01.sfo01.rainpole.local** tree.
  - c Right-click **SFOMGMT-ESG01-0** and select **Power > Power On**.
  - d Right-click **SFOMGMT-ESG02-0** and select **Power > Power On**.

5 Verify the new state of the BGP routing.

a Go back to the SSH connection to UDLR01 and run the show ip route command.

b Verify that you receive routes via BGP.

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

c Verify that you have multiple routes to BGP learned networks and that routes also come from the NSX Edge services gateways in Region A.

```

NSX-edge-7b90d5b-b32b-43c0-9402-4965b0651f98-0) show ip route
Codes: 0 - OSPF derived, 1 - IS-IS derived, B - BGP derived,
        C - connected, S - static, I1 - IS-IS level-1, I2 - IS-IS level-2,
        O - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
        N1 - OSPF NSSR external type 1, N2 - OSPF NSSR external type 2
Total number of routes: 8
0.0.0.0/0 (2B/0) via 192.168.188.1
0.0.0.0/0 (2B/0) via 192.168.188.2
169.254.1.0/30 (0/0) via 169.254.1.1
172.16.35.0/24 (2B0/0) via 192.168.188.1
172.16.35.0/24 (2B0/0) via 192.168.188.2
172.17.35.0/24 (2B/0) via 192.168.188.1
172.17.35.0/24 (2B0/0) via 192.168.188.2
172.27.13.0/24 (2B0/0) via 192.168.188.1
172.27.13.0/24 (2B0/0) via 192.168.188.2
172.27.21.0/24 (2B/0) via 192.168.188.1
172.27.21.0/24 (2B/0) via 192.168.188.2
172.27.22.0/24 (2B/0) via 192.168.188.1
172.27.22.0/24 (2B/0) via 192.168.188.2
192.168.188.0/24 (0/0) via 192.168.188.4
NSX-edge-7b90d5b-b32b-43c0-9402-4965b0651f98-0)
    
```

## Deploy Application Virtual Networks in Region B

Deploy the application virtual networks for the region.

### Procedure

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

a Open a Web browser and go to <https://mgmt01vc51.lax01.rainpole.local/vsphere-client>.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 Create a Universal Logical Switch for workloads specific to Region B.

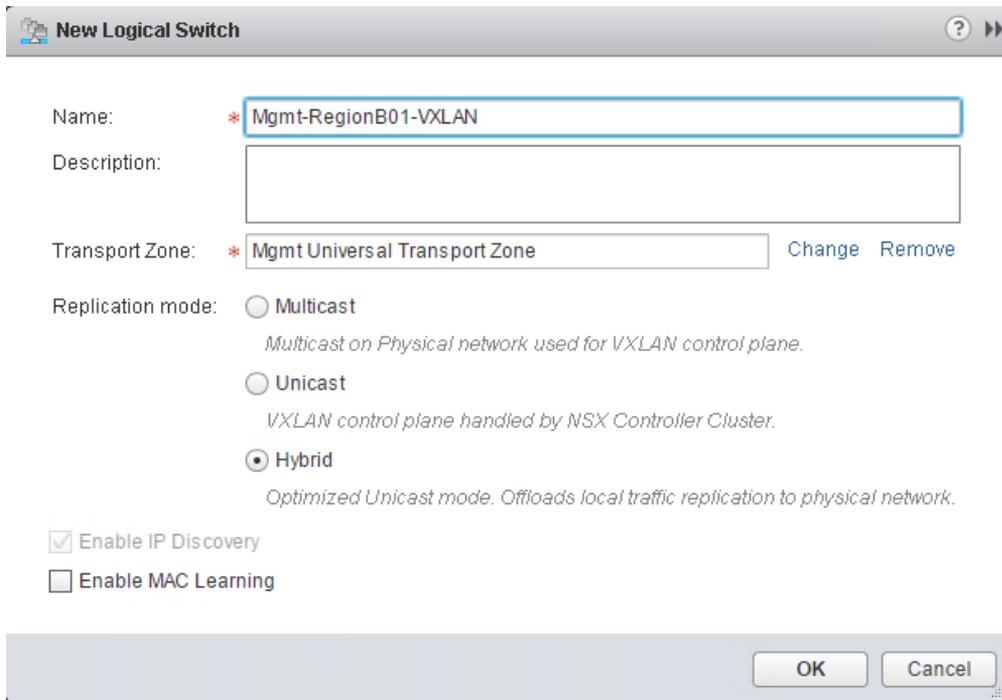
a Under **Inventories**, click **Networking & Security**.

b In the **Navigator**, click **Logical Switches**.

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

- d Click the **Add** icon to create a new Logical Switch.
- e In the **New Logical Switch** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	Mgmt-RegionB01-VXLAN
Transport Zone	Mgmt Universal Transport Zone
Replication Mode	Hybrid



- 3 Connect the Mgmt-RegionB01-VXLAN to the UDLR01 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 **SFOMGMT-UDLR01** and click **Next**.
  - d On the **Edit NSX Edge Interface** page, enter the following settings and click **Next**.

Setting	Value
Name	Mgmt-RegionB01-VXLAN
Type	Internal
Connectivity Status	Connected
Primary IP Address	192.168.32.1
Subnet Prefix Length	24

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

## 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.
- 5 Click the **Add** icon to create a new NSX Edge.
- 6 On the **Name and Description** page, enter the following settings, and click **Next**.

Setting	Value
Install Type	Edge Services Gateway
Name	LAXMGMT-LB01
Deploy NSX Edge	Selected
Enable High Availability	Selected

**New NSX Edge**

1 Name and description  
 2 Settings  
 3 Configure deployment  
 4 Configure interfaces  
 5 Default gateway settings  
 6 Firewall and HA  
 7 Ready to complete

**Name and description**

Install Type:  Edge Services Gateway  
*Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.*

Logical (Distributed) Router  
*Provides Distributed Routing and Bridging capabilities.*

Name: \* LAXMGMT-LB01  
 Hostname:  
 Description:  
 Tenant:

Deploy NSX Edge  
*Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.*

Enable High Availability  
*Enable HA, for enabling and configuring High Availability.*

Back Next Finish Cancel

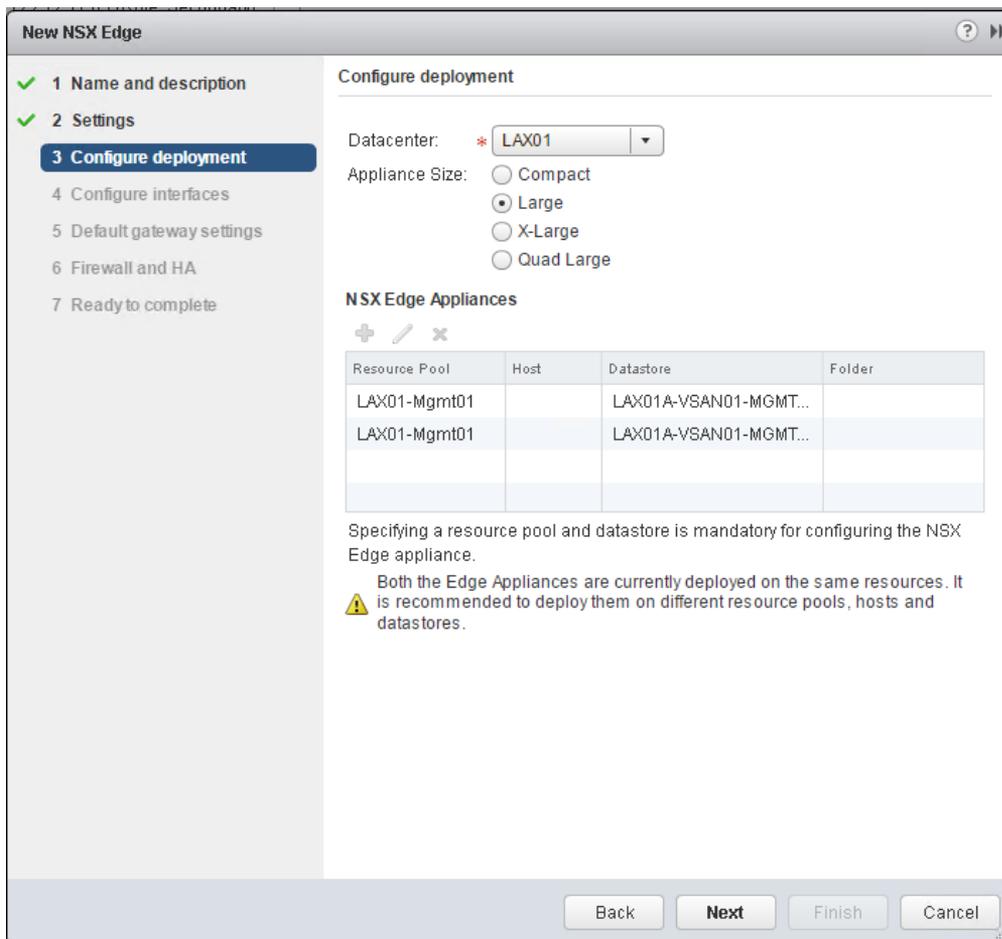
7 On the **Settings** page, enter the following settings, and click **Next**.

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

- 8 On the **Configure Deployment** page, perform the following configuration steps, and click **Next**.
  - a Select **LAX01** from the **Datacenter** drop-down menu.
  - b Select the **Large** radio button to specify the **Appliance Size**.
  - c Click the **Add** icon, enter the following settings, and click **OK**.

Perform twice to add two NSX Edge appliances with the same settings.

Setting	Value
Resource pool	LAX01-Mgmt01
Datastore	LAX01A-VSAN01-MGMT01
Folder	NSX51



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

Setting	Value
Name	OneArmLB
Type	Internal
Connected To	Mgmt-xRegion01-VXLAN

Setting	Value
Connectivity Status	Connected
Primary IP Address	192.168.11.2
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

**Add NSX Edge Interface**
?

vNIC#: 0

Name: \* OneArmLB

Type:  Internal  Uplink

Connected To: Mgmt-xRegion01-VXLAN Change Remove

Connectivity Status:  Connected  Disconnected

+ ✎ ✖

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
192.168.11.2 ✖		24 ✖

*Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.1.2,1.1.1.3*

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU:

Options:  Enable Proxy ARP  Send ICMP Redirect

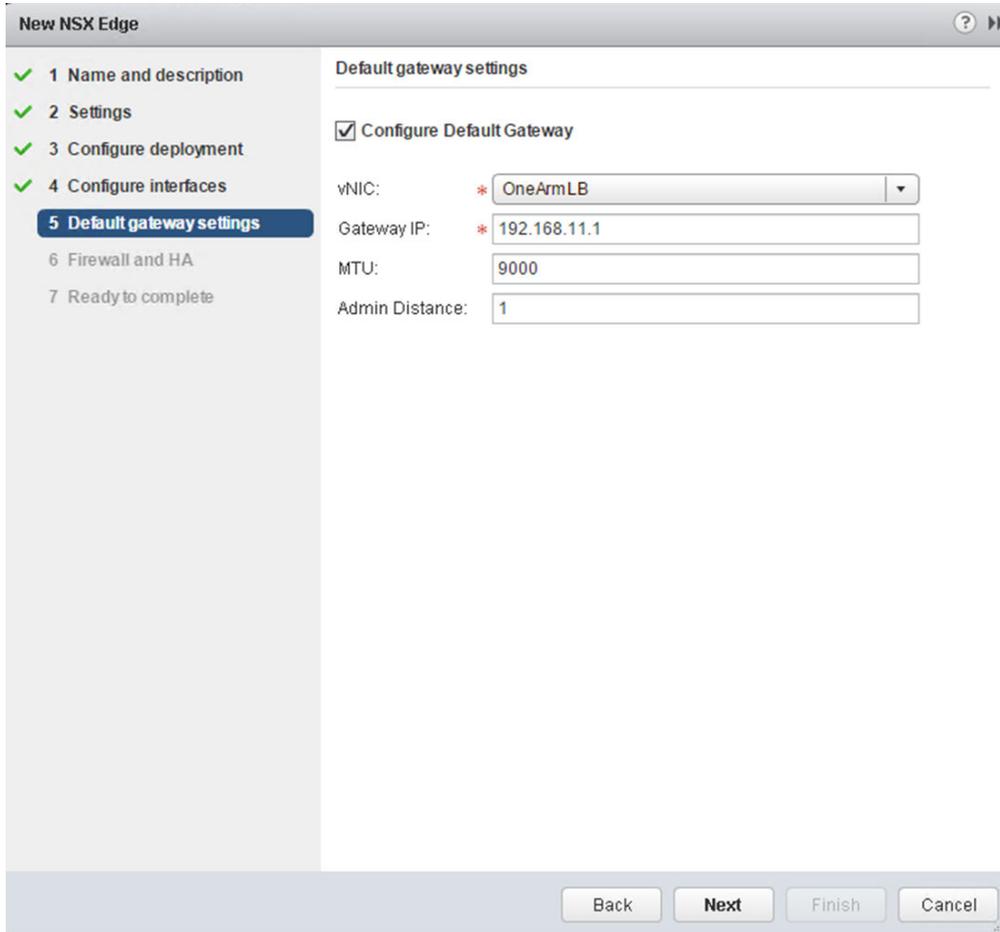
Reverse Path Filter  ▼

Fence Parameters:

Example: ethernet0.filter1.param1=1

10 On the **Default Gateway Settings** page, enter the following settings and click **Next**.

Setting	Value
Gateway IP	192.168.11.1
MTU	9000



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

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

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

13 Enable HA logging.

- a In the **Navigator**, click **NSX Edges**.
- b Select **172.17.11.65** from the **NSX Manager** drop-down menu.
- c Double-click the device labeled **LAXMGMT-LB01**.
- 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 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 **LAXMGMT-LB01** 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 **LAXMGMT-LB01** 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 [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.
- 3 [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.
- 4 [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.

## 5 [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.

## 6 [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.

## 7 [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.

## 8 [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.

## 9 [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.

## 10 [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.

## 11 [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**.

Setting	Value
ESXi host or vCenter Server name	mgmt01vc51.lax01.rainpole.local
HTTPS port	443
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

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

- g On the **Select folder** page choose **MGMT51**.

- h On the **Select compute resource** page choose the **LAX01-Mgmt01** cluster.

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

Setting	Value
Appliance name	comp01vc51
OS password	<i>compvc_root_password</i>
Confirm OS password	<i>compvc_root_password</i>

- j On the **Select deployment size** page, select **Large vCenter Server** and click **Next**.

- k On the **Select datastore** page, select the **LAX01A-VSAN01-MGMT01** datastore, select the **Enable Thin Disk Mode** check box, and click **Next**.

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

Setting	Value
Network	vDS-Mgmt-Management
IP version	IPv4
IP assignment	Static
System name	comp01vc51.lax01.rainpole.local
IP address	172.17.11.64
Subnet mask or prefix length	255.255.255.0
Default gateway	172.17.11.253
DNS servers	172.17.11.5,172.17.11.4

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

- n 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**.

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

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

Setting	Value
Platform Services Controller	lax01psc51.lax01.rainpole.local
HTTPS port	443
SSO domain name	vsphere.local
SSO password	sso_password

- d On the **Ready to complete** page, review the configuration and click **Finish**.
- e Click **OK** on the Warning.

## 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 Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click the **Home** icon above the **Navigator** and 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 comp01vc51 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc01.lax01.rainpole.local tree**.
- 3 Select the **LAX01-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 **comp01vc51** and click **OK**.
- 8 In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc51.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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator, click **Networking & Security**.
- 3 Click **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 **comp01vc51** 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.

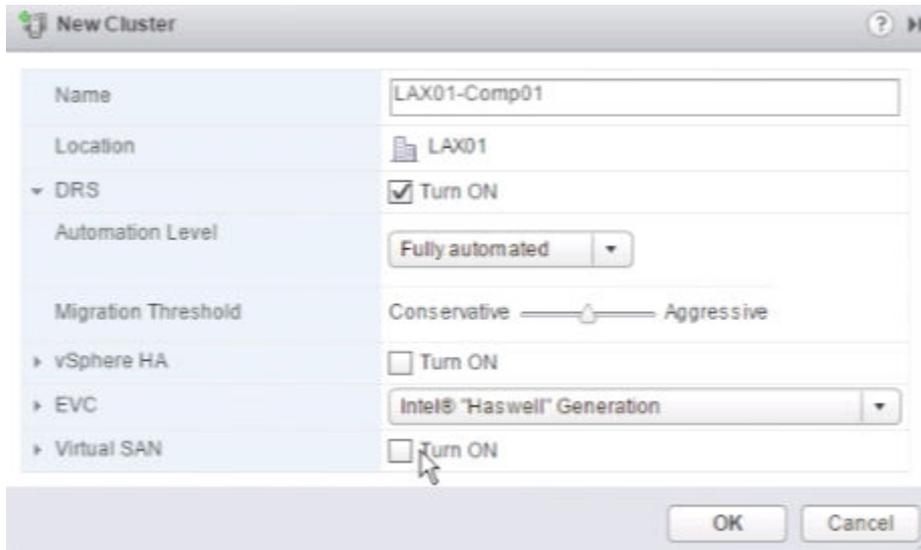
**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a Datacenter object.
  - a In the **Navigator**, click **Hosts and Clusters**.
  - b Right-click the **comp01vc51.lax01.rainpole.local** instance, and select **New Datacenter**.
  - c In the **New Datacenter** dialog box, enter **LAX01** as name, and click **OK**.
- 3 Create the shared edge and compute cluster.
  - a Right-click the **LAX01** datacenter and click **New Cluster**.
  - b In the **New Cluster** wizard, enter the following values, and click **OK**.

Setting	Value				
<b>Name</b>	LAX01-Comp01				
<b>DRS</b>	<table border="0"> <tr> <td><b>Turn ON</b></td> <td>Selected</td> </tr> <tr> <td>Other DRS options</td> <td>Default values</td> </tr> </table>	<b>Turn ON</b>	Selected	Other DRS options	Default values
<b>Turn ON</b>	Selected				
Other DRS options	Default values				
<b>vSphere HA</b>	<table border="0"> <tr> <td><b>Turn ON</b></td> <td>Deselected</td> </tr> </table>	<b>Turn ON</b>	Deselected		
<b>Turn ON</b>	Deselected				
<b>EVC</b>	Set EVC mode to the lowest available setting supported for the hosts in the cluster				
<b>vSAN</b>	<table border="0"> <tr> <td><b>Turn ON</b></td> <td>Deselected</td> </tr> </table>	<b>Turn ON</b>	Deselected		
<b>Turn ON</b>	Deselected				



- 4 Add a host to the shared edge and compute cluster.
  - a Right-click the **LAX01-Comp01** cluster, and click **Add Host**.
  - b On the **Name and location** page, enter **comp01esx51.lax01.rainpole.local** in the **Host name or IP address** text box, and click **Next**.
  - c On the **Connection settings** page, enter the following credentials, and click **Next**.

Setting	Value
<b>User name</b>	root
<b>Password</b>	esxi_root_user_password

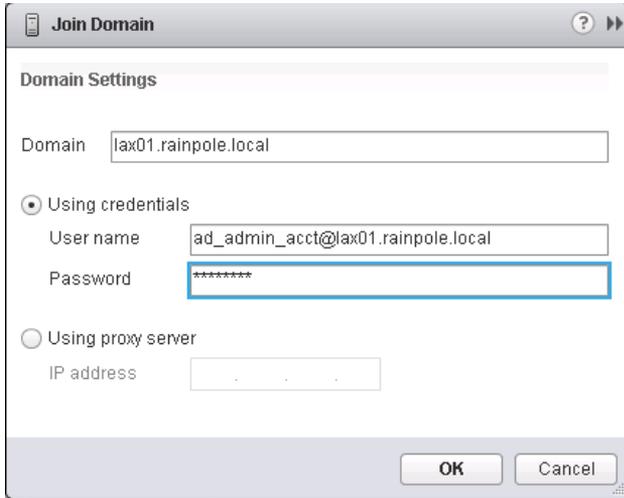
- d In the **Security Alert** dialog box, click **Yes**.
  - e On the **Host summary** page, review the host information and click **Next**.
  - f On the **Assign license** page, select the ESXi license key, that you entered during the vCenter Server deployment, and click **Next**.
  - g On the **Lockdown mode** page, click **Next**.
  - h On the **Resource pool** page, click **Next**.
  - i On the **Ready to complete** page, review your entries and click **Finish**.
- 5 Repeat the previous step to add the remaining hosts to the cluster.

Setting	Value
Host 2	comp01esx52.lax01.rainpole.local
Host 3	comp01esx53.lax01.rainpole.local
Host 4	comp01esx54.lax01.rainpole.local

- 6 Add an ESXi host to the active directory domain.
- a In the **Navigator**, click **Hosts and Clusters** and expand the entire **comp01vc51.lax01.rainpole.local** tree.
  - b Select the **comp01esx51.lax01.rainpole.local** host.
  - c Click the **Configure** tab.
  - d Under **System**, select **Authentication Services**.

- e In the **Authentication Services** panel, click the **Join Domain** button.
- f In the **Join Domain** dialog box, enter the following settings and click **OK**.

Setting	Value
Domain	lax01.rainpole.local
User name	ad_admin_acct@lax01.rainpole.local
Password	ad_admin_lax_password



- 7 Set the Active Directory Service to Start and stop with host.
  - a In the **Navigator**, click **Hosts and Clusters** and expand the entire **comp01vc51.lax01.rainpole.local** tree.
  - b Select the **comp01esx51.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-Comp01** cluster and select **New Resource Pool**.
  - b In the **New Resource Pool** dialog box, enter the following values and click **OK**.

Setting	Value
Name	SDDC-EdgeRP51
CPU-Shares	High
CPU-Reservation	0
CPU-Reservation Type	Expandable selected
CPU-Limit	Unlimited
Memory-Shares	Normal
Memory-Reservation	16 GB
Memory-Reservation type	Expandable selected
Memory-Limit	Unlimited

- 9 Repeat step [Step 8](#) to add two more additional resource pools.

Setting	Resource Pool 2	Resource Pool 3
Name	User-EdgeRP51	User-VMRP51
CPU-Shares	Normal	Normal
CPU-Reservation	0	0
CPU-Reservation Type	Expandable selected	Expandable selected
CPU-Limit	Unlimited	Unlimited
Memory-Shares	Normal	Normal
Memory-Reservation	0	0
Memory-Reservation type	Expandable selected	Expandable selected
Memory-Limit	Unlimited	Unlimited

## Create a vSphere Distributed Switch for the Shared Edge and Compute Cluster in Region B

After all ESXi hosts have been added to the cluster, create a vSphere Distributed Switch.

## Procedure

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

- a Open a Web browser and go to **https://comp01vc51.lax01.rainpole.local/vsphere-client**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a vSphere Distributed Switch for the shared edge and compute cluster.

- a In the **Navigator**, click **Networking** and expand the **lax01w01vc01.lax01.rainpole.local** control tree.
- b Right-click the **lax01-w01dc** datacenter and select **Distributed Switch > New Distributed Switch** to start the **New Distributed Switch** wizard.
- c On the **Name and location** page, enter **lax01-w01-vds01** as the name, and click **Next**.
- d On the **Select version** page, ensure the **Distributed switch version - 6.5.0** radio button is selected, and click **Next**.
- e On the **Edit settings** page, enter the following values and click **Next**.

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

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

- 3 Edit the settings of the lax01-w01-vds01 distributed switch.

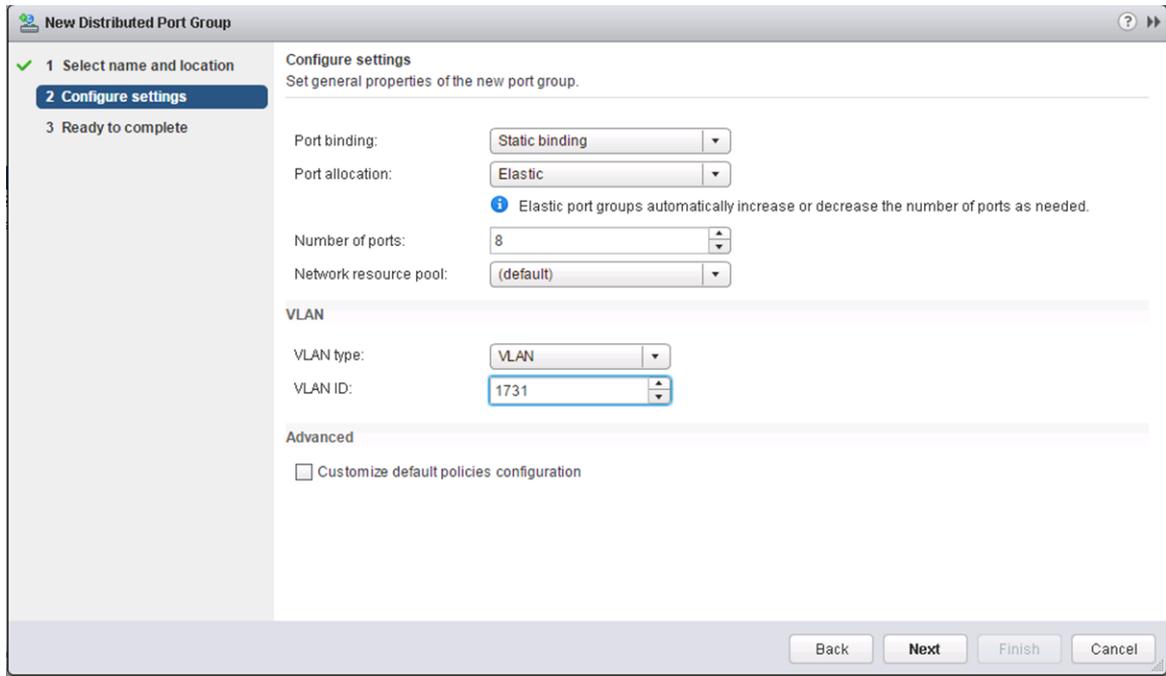
- a Right-click the **lax01-w01-vds01** distributed switch and select **Settings > Edit Settings**.
- b Click the **Advanced** tab.
- c Enter **9000** as MTU (Bytes) value and click **OK**.

4 Create new port groups in the lax01-w01-vds01 distributed switch.

- a Right-click the **lax01-w01-vds01** distributed switch, and select **Distributed Port Group > New Distributed Port Group**.
- b Create port groups with the following settings, and click **Next**.

Port Group Name	Port Binding	VLAN Type	VLAN ID
lax01-w01-vds01-management	Static binding	VLAN	1731
lax01-w01-vds01-vmotion	Static binding	VLAN	1732
lax01-w01-vds01-vsan	Static binding	VLAN	1733
lax01-w01-vds01-nfs	Static binding	VLAN	1725
lax01-w01-vds01-uplink01	Static binding	VLAN	1735
lax01-w01-vds01-uplink02	Static binding	VLAN	2721

**Note** You create the VXLAN port group 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 and click **Next**.

- d Select **Route based on physical NIC load** under **Load Balancing** and click **Next**.
- e Click **Finish**.
- 6 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**.
- 7 Configure the VMkernel network adapters by editing the existing adapter and adding new adapters as needed.
  - a On the **Manage VMkernel network adapters** page, click **vmk0**, and click **Assign port group**.
  - b Select **lax01-w01-vds01-management** and click **OK**.
  - c On the **Manage VMkernel network adapters** page, click **On this switch** and click **New adapter**.
  - d On the **Add Networking** page, select **Select an existing network**, browse to select the **lax01-w01-vds01-nfs** port group, click **OK**, and click **Next**.
  - e On the **Port properties** page click **Next**.
  - f Under **IPv4 settings**, select **Use static IPv4 settings**, enter the IP address `172.17.25.101`, enter the subnet `255.255.255.0`, and click **Next**.
  - g Click **Finish**.
  - h On the **Analyze impact** page, click **Next**.
  - i On the **Ready to complete** page, review your entries and click **Finish**.
- 8 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**.
- 9** 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**.
- 10** 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**.
- 11** Define Network I/O Control shares for the different traffic types on the **lax01-w01-vds01** distributed switch.
- a In the **Navigator**, click **Networking**, and click the **lax01-w01dc** datacenter.
  - b Click the **lax01-w01-vds01** distributed switch.
  - c Click the **Configure** tab and click **Resource Allocation > System traffic**.
  - d Under **System Traffic**, edit each of the following traffic types with the values from the table.

Traffic Types	Shares
vSAN Traffic	Low
NFS Traffic	Low
vMotion Traffic	Low
vSphere Replication Traffic	Low
Management Traffic	Normal
vSphere Data Protection Backup Traffic	Low
Virtual Machine Traffic	High
Fault Tolerance Traffic	Low
iSCSI Traffic	Low

- 12** 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**.
- 13** 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**.
- 14** 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.

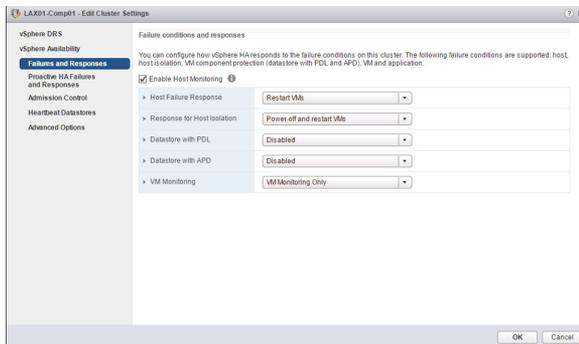
**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator, click Hosts and Clusters.
  - a Expand the **comp01vc51.lax01.rainpole.local** inventory.
  - b Select the **LAX01-Comp01** cluster.
- 3 Click the **Configure** tab and click **vSphere Availability**.
- 4 Click **Edit**.
- 5 In the **Edit Cluster Settings** dialog box, select the **Turn on vSphere HA** check box.
- 6 In the **Edit Cluster Settings** dialog box, under **Failures and Responses**, select the following values.

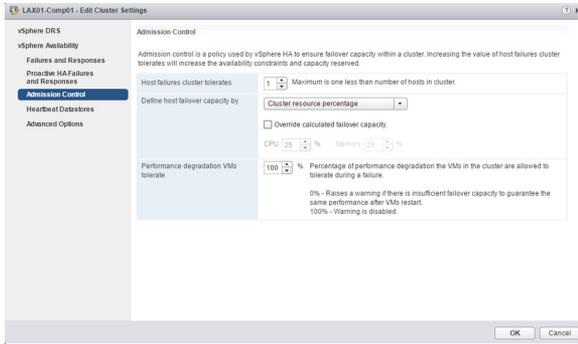
Setting	Value
Enable Host Monitoring	Selected
Host Failure Response	Restart VM's
Response for Host Isolation	Power off and restart VM's
Datastore with PDL	Disabled
Datastore with APD	Disabled
VM Monitoring	VM Monitoring Only



- 7 Click **Admission Control**.

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

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



9 Click **OK**.

## 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 vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://mgmt01vc51.lax01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Change the default ESX Admins group.
  - a In the **Navigator**, click **Hosts and Clusters**.
  - b Expand the **comp01vc51.lax01.rainpole.local** vCenter inventory tree, and select the **comp01esx51.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 **comp01vc51.lax01.rainpole.local** vCenter inventory tree, and select the **comp01esx51.lax01.rainpole.local** host.
  - c Click the **Configure** tab and under **System**, click **Advanced System Settings**.
  - d Click the **Edit** button.
  - e In the filter box, enter **ssh** and wait for the search results.
  - f Change the value of **UserVars.SuppressShellWarning** to **1** and click **OK**.

## Mount NFS Storage for the Shared Edge and Compute Cluster in Region B

You must mount an NFS datastore for the content library consumed by vRealize Automation for virtual machine provisioning.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Hosts and Clusters** and expand the **comp01vc51.lax01.rainpole.local**.
- 3 Click on **comp01esx51.lax01.rainpole.local**.
- 4 Click on the **Datastores** tab.
- 5 Click the **Create a New Datastore** icon.  
The **New Datastore** wizard opens.
- 6 On the **Type** page, select **NFS** and click **Next**.
- 7 On the **NFS version** page, select **NFS 3** and click **Next**.

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

Setting	Value
Datastore Name	LAX01A-NFS01-VRALIB01
Folder	/V2D_vRA_ComputeB_1TB
server	172.17.25.251

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

## Create and Apply the Host Profile for the Shared Edge and Compute Cluster in Region B

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

### Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://comp01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a Host Profile from **comp01esx51.lax01.rainpole.local**
  - a In the **Navigator** select **Hosts and Clusters** and expand the **comp01vc51.lax01.rainpole.local** tree.
  - b Right Click the ESXi host **comp01esx51.lax01.rainpole.local** and choose **Host Profiles > Extract Host Profile**.
  - c In the **Extract Host Profile** window enter **LAX01-Comp01** for the **Name** and click **Next**.
  - d In the **Ready to complete** window click **Finish**.
- 3 Attach the Host Profile to the shared edge and compute cluster.
  - a In the **Navigator** select **Hosts and Clusters** and expand the **comp01vc51.lax01.rainpole.local** tree.
  - b Right Click on the **LAX01-Comp01** cluster and choose **Host Profiles > Attach Host Profile**.
  - c In the **Attach Host Profile** window select the **LAX01-Comp01** Host Profile, select the **Skip Host Customization** checkbox and click **Finish**.

- 4 Create Host Customizations for the hosts in the shared edge and compute cluster.
  - a In the **Navigator** select **Policies and Profiles**.
  - b Click on **Host Profiles** then right click on **LAX01-Comp01** and choose **Export Host Customizations**.
  - c In the dialog box click **Save**.
  - d Choose a file location to save the *LAX01-Comp01\_host\_customizations.csv* file.
  - e Open the *LAX01-Comp01\_host\_customizations.csv* in Excel.

f Edit the file using the following configuration value.

<b>ESXi Host</b>	<b>Active Directory Configuration Password</b>	<b>Active Directory Configuration Username</b>	<b>NetStack Instance defaultTcpipStack-&gt;DNS configuration Name for this host</b>
comp01esx51.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	comp01esx51
comp01esx52.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	comp01esx52
comp01esx53.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	comp01esx53
comp01esx54.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	comp01esx54

<b>ESXi Host</b>	<b>Host virtual NIC vDS-Comp01:vDS-Comp01-Management:management-&gt;IP address settings IPv4 address</b>	<b>Host virtual NIC vDS-Comp01:vDS-Comp01-Management:management-&gt;IP address settings SubnetMask</b>
comp01esx51.lax01.rainpole.local	172.17.31.101	255.255.255.0
comp01esx52.lax01.rainpole.local	172.17.31.102	255.255.255.0
comp01esx53.lax01.rainpole.local	172.17.31.103	255.255.255.0
comp01esx54.lax01.rainpole.local	172.17.31.104	255.255.255.0

<b>ESXi Host</b>	<b>Host virtual NIC vDS-Comp01:vDS-Comp01-NFS:&lt;UNRESOLVED&gt;-&gt;IP address settings IPv4 address</b>	<b>Host virtual NIC vDS-Comp01:vDS-Comp01-Management:management-&gt;IP address settings SubnetMask</b>
comp01esx51.lax01.rainpole.local	172.17.25.101	255.255.255.0
comp01esx52.lax01.rainpole.local	172.17.25.102	255.255.255.0
comp01esx53.lax01.rainpole.local	172.17.25.103	255.255.255.0
comp01esx54.lax01.rainpole.local	172.17.25.104	255.255.255.0

<b>ESXi Host</b>	<b>Host virtual NIC vDS-Comp01:vDS-Comp01-vMotion:vmotion-&gt;IP address settings IPv4 address</b>	<b>Host virtual NIC vDS-Comp01:vDS-Comp01-vMotion:vmotion-&gt;IP address settings SubnetMask</b>
comp01esx51.lax01.rainpole.local	172.17.32.101	255.255.255.0
comp01esx52.lax01.rainpole.local	172.17.32.102	255.255.255.0
comp01esx53.lax01.rainpole.local	172.17.32.103	255.255.255.0
comp01esx54.lax01.rainpole.local	172.17.32.104	255.255.255.0

- g 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 Customizaions** window select all hosts and click **Next**.
  - k Click the **Browse** button to use a customization file, locate the *LAX01-Comp01\_host\_customizations.csv* file saved earlier and select it and click **Open** then click **Finish**.
- 5 Remediate the hosts in the shared edge and compute cluster
- a Click the **Monitor** tab and click **Compliance**.
  - b Select **LAX01-Comp01** and click the **Check Host Profile Compliance** button.

Host/Cluster	Host Compliance	Last Checked
LAX01-Comp01	3 Not Compliant, 1 Compliant	10/31/2016 10:06 AM
comp01esx51.lax01.rainpole.local	Compliant	10/31/2016 10:06 AM
comp01esx52.lax01.rainpole.local	Not Compliant	10/31/2016 10:06 AM
comp01esx53.lax01.rainpole.local	Not Compliant	10/31/2016 10:06 AM
comp01esx54.lax01.rainpole.local	Not Compliant	10/31/2016 10:06 AM

- c Select **comp01esx52.lax01.rainpole.local** and click the **Remediate host based on its host profile** button.
- d Select **comp01esx53.lax01.rainpole.local** and click the **Remediate host based on its host profile** button.
- e Select **comp01esx54.lax01.rainpole.local** and click the **Remediate host based on its host profile** button.

**Note** All hosts should now show a status of **Compliant**.

Host/Cluster	Host Compliance	Last Checked
LAX01-Comp01	4 Compliant	11/8/2016 10:00 PM
comp01esx51.lax01.rainpole.local	Compliant	11/8/2016 10:00 PM
comp01esx52.lax01.rainpole.local	Compliant	11/8/2016 10:00 PM
comp01esx53.lax01.rainpole.local	Compliant	11/8/2016 10:00 PM
comp01esx54.lax01.rainpole.local	Compliant	11/8/2016 10:00 PM

- 6 Schedule nightly compliance checks.
  - a On the **Policies and Profiles** page, click **LAX01-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-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**

Host	FQDN
Management host 1	mgmt01esx51.lax01.rainpole.local
Management host 2	mgmt01esx52.lax01.rainpole.local
Management host 3	mgmt01esx53.lax01.rainpole.local
Management host 4	mgmt01esx54.lax01.rainpole.local
Shared Edge and Compute host 1	comp01esx51.lax01.rainpole.local
Shared Edge and Compute host 2	comp01esx52.lax01.rainpole.local
Shared Edge and Compute host 3	comp01esx53.lax01.rainpole.local
Shared Edge and Compute host 4	comp01esx54.lax01.rainpole.local

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://mgmt01vc51.lax01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Hosts and Clusters** and expand the entire **comp01vc51.lax01.rainpole.local** tree control.
- 3 Select the **comp01esx51.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 vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Open the **Deploy OVF Template** wizard.
  - a In the **Navigator**, expand the entire **mgmt01vc51.lax01.rainpole.local** tree.
  - b Right-click the **LAX01-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**.

Setting	Value
Name	comp01nsxm51
Folder or Datacenter	NSX51

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

Setting	Value
Datacenter	LAX01
Cluster	LAX01-Mgmt01

- 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**.

Setting	Value
VM Storage Policy	vSAN Default Storage Policy
Datastore	LAX01A-VSAN01-MGMT01

- g On the **Setup Networks** page, under **Destination**, select **vDS-Mgmt-Management**, and click **Next**.
- h On the **Customize Template** page, expand the different options, enter the following settings, and click **Next**.

Setting	Value
DNS Server List	172.17.11.5,172.17.11.4
Domain Search List	lax01.rainpole.local
Default IPv4 Gateway	172.17.11.253
Hostname	comp01nsxm51.lax01.rainpole.local
Network 1 IPv4 Address	172.17.11.66
Network 1 Netmask	255.255.255.0
Enable SSH	Selected
NTP Server List	<ul style="list-style-type: none"> <li>■ ntp.lax01.rainpole.local</li> <li>■ ntp.sfo01.rainpole.local</li> </ul>
CLI "admin" User Password / enter	<i>compnsx_admin_password</i>
CLI "admin" User Password / confirm	<i>compnsx_admin_password</i>
CLI Privilege Mode Password / enter	<i>compnsx_privilege_password</i>
CLI Privilege Mode Password / confirm	<i>compnsx_privilege_password</i>

- i On the **Ready to Complete** page click **Finish**.
- j In the **Navigator**, expand the **mgmt01vc51.lax01.rainpole.local** control tree, select the comp01nsxm51 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://comp01nsxm51.lax01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>compnsx_admin_password</i>

- 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**.

Setting	Value
Lookup Service IP	lax01psc51.lax01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 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**.

Setting	Value
vCenter Server	comp01vc51.lax01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	<i>svc-nsxmanager_password</i>

- 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
- b Log in using the following credentials.

Setting	Value
User name	svc-nsxmanager@rainpole.local
Password	<i>svc-nsxmanager_password</i>



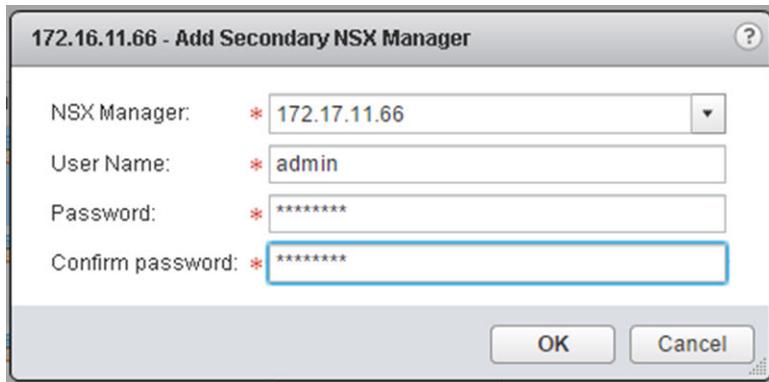
**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Assign the secondary role to the shared edge and compute NSX Manager in Region B.
  - a Under **Inventories**, click **Networking & Security**.
  - b In the **Navigator**, click **Installation**.
  - c On the **Management** tab, select the **172.16.11.66** instance.
  - d Select **Actions > Add Secondary NSX Manager**.
  - e In the **Add Secondary NSX Manager** dialog box, enter the following settings and click **OK**.

Setting	Value
NSX Manager	172.17.11.66
User name	admin
Password	mgmtnsx_admin_password
Confirm Password	mgmtnsx_admin_password



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

## Prepare the ESXi Hosts in the Shared Edge and Compute Cluster for NSX in Region B

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 vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 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-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 vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

## 2 Configure the Segment ID allocation.

- a In the **Navigator**, click **Networking & Security**.
- b Click **Installation**, click **Logical Network Preparation**, and click **Segment ID**.
- c Select **172.17.11.66** from the **NSX Manager** drop-down menu.
- d Click **Edit**, enter the following settings, and click **OK**.

Setting	Value
Segment ID pool	10000-14000
Enable Multicast addressing	Selected
Multicast addresses	239.6.0.0-239.6.255.255

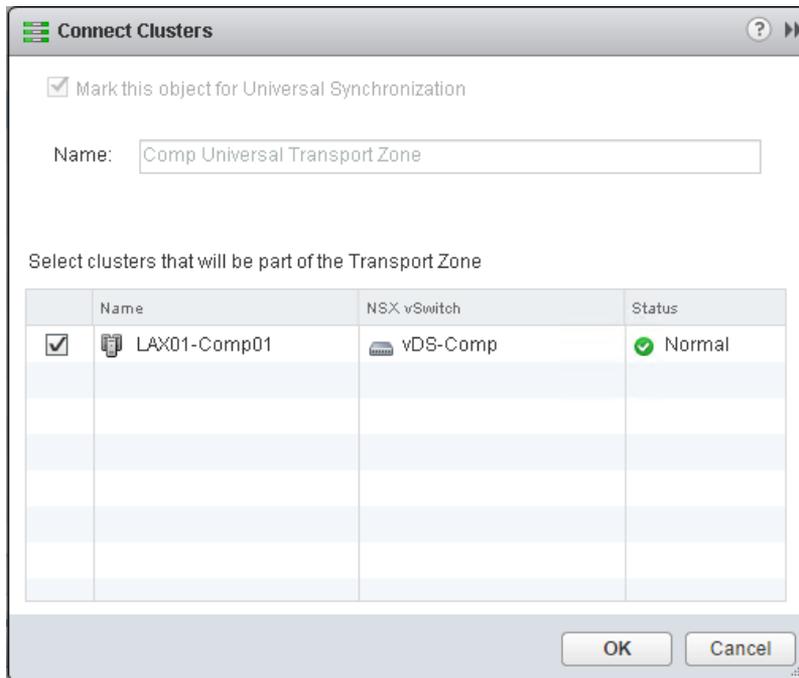
## 3 Configure the VXLAN networking.

- a Click the **Host Preparation** tab.
- b Under **VXLAN**, click **Not Configured** on the **LAX01-Comp01** row, enter the following settings, and click **OK**.

Setting	Value
Switch	vDS-Comp01
VLAN	1734
MTU	9000
VMKNic IP Addressing	Use DHCP
VMKNic Teaming Policy	Load Balance - SRCID
VTEP	2

4 Configure the Universal transport zone.

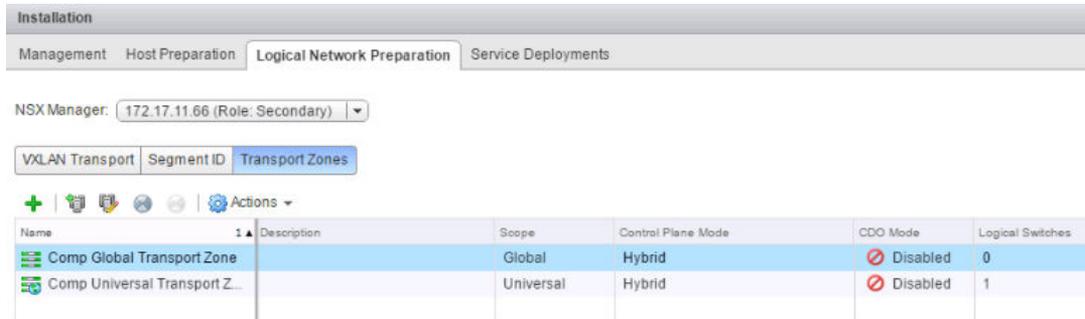
- a In the **Navigator**, click the **Logical Network Preparation** tab and click **Transport Zones**.
- b Select the **Comp Universal Transport Zone** and select **Connect Clusters** from the **Actions** menu.
- c In the **Connect Clusters** dialog box, select the **LAX01-Comp01** cluster and click **OK**.



5 Configure the Global transport zone.

- a In the Navigator, click the **Logical Network Preparation** tab and click **Transport Zones**.
- b Click the **Add New Transport zone** icon, enter the following settings, and click OK.

Setting	Value
Name	Comp Global Transport Zone
Replication mode	Hybrid
Select clusters part of the Transport Zone	LAX01-Comp01



## Update the Host Profile for the Compute Cluster in Region B

After an authorized change is made to a host the Host Profile must be updated to reflect the changes.

### Procedure

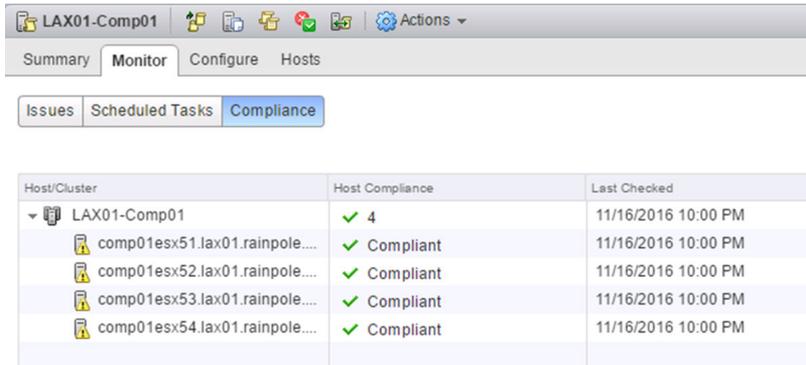
- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Update the Host Profile for the management cluster.
  - a In the **Navigator** select **Policies and Profiles**.
  - b Click on **Host Profiles** then right click on **LAX01-Comp01** and select **Copy settings from Host**.
  - c Select **comp01esx51.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-Comp01** and click the **Check Host Profile Compliance** button.

All hosts should show the status **Compliant**



Host/Cluster	Host Compliance	Last Checked
▼ LAX01-Comp01	✓ 4	11/16/2016 10:00 PM
⚠ comp01esx51.lax01.rainpole....	✓ Compliant	11/16/2016 10:00 PM
⚠ comp01esx52.lax01.rainpole....	✓ Compliant	11/16/2016 10:00 PM
⚠ comp01esx53.lax01.rainpole....	✓ Compliant	11/16/2016 10:00 PM
⚠ comp01esx54.lax01.rainpole....	✓ Compliant	11/16/2016 10:00 PM

## Configure NSX Dynamic Routing in the Shared Edge and Compute Cluster in Region B

NSX for vSphere creates a network virtualization layer on top of which all virtual networks are created. This layer is an abstraction between the physical and virtual networks.

You configure NSX dynamic routing within the management cluster, deploying two NSX Edge devices and configure a Universal Distributed Logical Router (UDLR).

### Procedure

- 1 [Create Logical Switches in the Shared Edge and Compute Cluster in Region B](#)  
Create a global transit logical switch for use as the transit network in the cluster.
- 2 [Deploy NSX Edge Devices for North-South Routing in the Shared Edge and Compute Cluster in Region B](#)  
Deploy NSX Edge Devices for North-South routing in the shared edge and compute cluster.
- 3 [Disable the Firewall Service in the Shared Edge and Compute Cluster in Region B](#)  
Disable the firewall of the two NSX Edge services gateways.
- 4 [Enable and Configure Routing in the Shared Edge and Compute Cluster in Region B](#)  
Enable the Border Gateway Protocol (BGP) to exchange routing information between the NSX Edge services gateways.
- 5 [Verify Peering of Upstream Switches and Establishment of BGP in Shared Edge and Compute Cluster in Region B](#)  
The NSX Edge devices 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://mgmt01vc51.lax01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under Inventories, click **Networking & Security**.
- 3 In the **Navigator**, click **Logical Switches**.
- 4 Select **172.17.11.66** from the **NSX Manager** drop-down menu and click the **Add** icon.

5 In the **New Logical Switch** dialog box, enter the following settings, and click OK.

Setting	Value
Name	Global Transit Network
Transport Zone	Comp Global Transport Zone
Replication Mode	Hybrid

## 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: LAXCOMP-ESG01 and LAXCOMP-ESG02.

**Table 2-8. NSX Edge Devices**

NSX Edge Device	Device Name
NSX Edge Device 1	LAXCOMP-ESG01
NSX Edge Device 2	LAXCOMP-ESG02

**Table 2-9. NSX Edge Interface Settings**

Interface	Primary IP Address LAXCOMP-ESG01	Primary IP Address LAXCOMP-ESG02
Uplink01	172.17.35.2	172.17.35.3
Uplink02	172.27.21.3	172.27.21.2
LAXCOMP-UDLR01	192.168.100.50	192.168.100.51
LAXCOMP-DLR01	192.168.102.1	192.168.102.2

### Prerequisites

To complete this procedure you must configure datastore for the shared edge and compute 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.
- 5 Click the **Add** icon to deploy a new NSX Edge.

The **New NSX Edge** wizard appears.

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

Setting	NSX Edge Device 1
Install Type	Edge Service Gateway
Name	LAXCOMP-ESG01
Deploy NSX Edge	Selected
Enable High Availability	Deselected

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

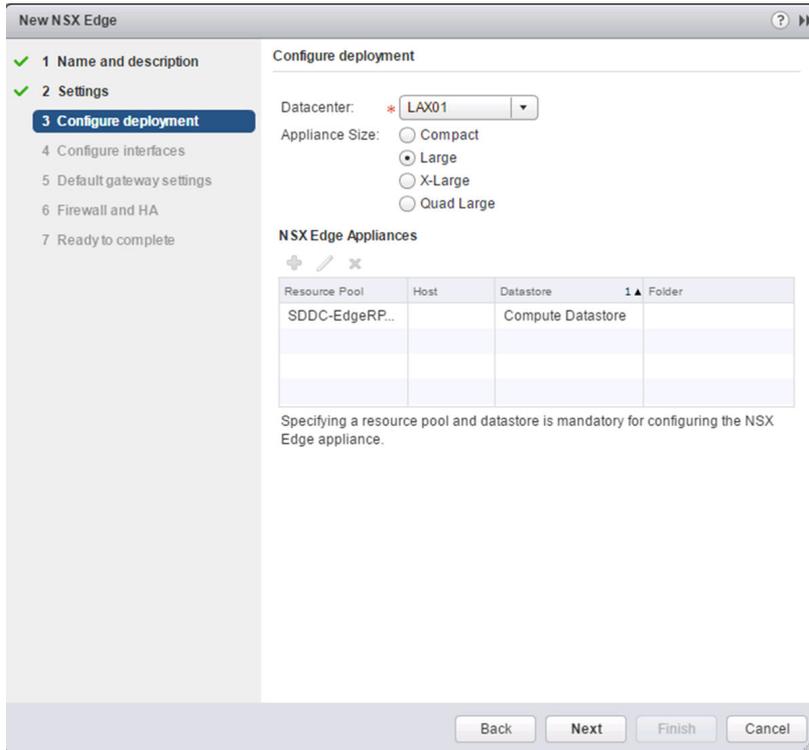
Setting	Value
User Name	admin
Password	<i>edge_admin_password</i>
Enable SSH access	Selected
Enable FIPS mode	Deselected
Enable auto rule generation	Selected
Edge Control Level logging	INFO

- c On the **Configure Deployment** page, select the **Large** radio button to specify the Appliance Size and click the **Add** icon.

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

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

Setting	Value
Cluster/Resource Pool	SDDC-EdgeRP01
Datastore	<i>lax01_shared_edge_and_compute_datastore</i>



- e Click the **Add** icon to configure the Uplink01 interface, enter the following settings and click **OK**.

Setting	Value
Name	Uplink01
Type	Uplink
Connected To	vDS-Comp01-Uplink01
Connectivity Status	Connected
Primary IP Address	172.17.35.2
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

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

Setting	Value
Name	Uplink02
Type	Uplink
Distributed Portgroup	vDS-Comp01-Uplink02
Connectivity Status	Connected
Primary IP Address	172.27.21.3
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- g Click the **Add** icon to configure the LAXCOMP-UDLR01 interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	LAXCOMP-UDLR01
Type	Internal
Connected To	Universal Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.100.1
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- h Click the **Add** icon to configure the LAXCOMP-DLR01 interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	LAXCOMP-DLR01
Type	Internal
Connected To	Global Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.102.1
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

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

- j On the **Firewall and HA** page click **Next**.
  - k On the **Ready to Complete** page, review the configuration settings you entered and click **Finish**.
- 6 Repeat this procedure to configure another NSX edge by using the settings for the second NSX Edge device.
- 7 Configure DRS affinity rules for the Edge Services Gateways.
- a Go back to the **Home** page.
  - b In the **Navigator**, click **Hosts and Clusters**, and expand the **comp01vc51.lax01.rainpole.local** tree.
  - c Select the **LAX01-Comp01** cluster, and click the **Configure** tab.
  - d Under **Configuration**, click **VM/Host Rules**.
  - e Click **Add**.
  - f In the **LAX01-Comp01 - Create VM/Host Rule** dialog box, enter the following settings and click **Add**.
- | Setting     | Value                        |
|-------------|------------------------------|
| Name        | anti-affinity-rule-ecmpedges |
| Enable rule | Selected                     |
| Type        | Separate Virtual Machine     |
- g In the **Add Rule Member** dialog box, select the check box next to each of the two, newly deployed NSX ESGs and click **OK**.
  - h In the **LAX01-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: LAXCOMP-ESG01 and LAXCOMP-ESG02.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.
- 5 Double-click the **LAXCOMP-ESG01** 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 LAXCOMP-ESG02.

## 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: LAXCOMP-ESG01 and LAXCOMP-ESG02.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.
- 5 Double-click the **LAXCOMP-ESG01** 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**.

Setting	Value
Network	<i>UDLR_Compute_Workload_Subnet</i>
Next Hop	192.168.100.3
Interface	LAXCOMP-UDLR01
MTU	9000
Admin Distance	210

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

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

Setting	Value
Network	<i>DLR_Compute_Workload_Subnet</i>
Next Hop	192.168.102.3
Interface	LAXCOMP-DLR01
MTU	9000
Admin Distance	210

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

c Click **Publish Changes**.

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

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

Setting	Value
<b>Enable BGP</b>	Selected
<b>Enable Graceful Restart</b>	Selected
<b>Enable Default Originate</b>	Deselected
<b>Local AS</b>	65000

b Click the **Add** icon to add a Neighbor.

The **New Neighbor** dialog box appears. You add two neighbors: the first Top of Rack Switch and the second Top of Rack Switch.

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

Setting	Value
IP Address	172.17.35.1
Remote AS	65002
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	<i>BGP_password</i>

- 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 172.27.21.1.

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

Setting	Value
IP Address	172.27.21.1
Remote AS	65002
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	<i>BGP_password</i>

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

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

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

Setting	Value
IP Address	192.168.100.4
Remote AS	65000
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	<i>BGP_password</i>

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

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

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

Setting	Value
IP Address	192.168.102.4
Remote AS	65000
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	<i>BGP_password</i>

- j 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**.

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

- e Click **Publish Changes**.

The route redistribution configuration is now visible in the **Route Redistribution** table.

- 11 Repeat this procedure for the NSX Edge device LAXCOMP-ESG02.

## 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: LAXCOMP-ESG01 and LAXCOMP-ESG02.

### Procedure

- 1 Log in to the NSX Edge device using a Secure Shell (SSH) client.
  - a Open an SSH connection to the `LAXCOMP-ESG01NSX` NSX Edge device.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<code>edge_admin_password</code>

- 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 is 172.17.35.1, remote AS 65002,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 328 messages, Sent 321 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 1 Identifier 0x3200a5bc
  Route refresh request:received 0 sent 0
  Prefixes received 5 sent 3 advertised 3
Connections established 1, dropped 1
Local host: 172.17.35.2, Local port: 37616
Remote host: 172.17.35.1, Remote port: 179

BGP neighbor is 172.27.21.1, remote AS 65002,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
```

- 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.

```

NSX-edge-3-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 7

B      0.0.0.0/0          [20/0]      via 172.17.35.1
B      0.0.0.0/0          [20/0]      via 172.27.21.1
B      172.16.35.0/24     [20/0]      via 172.17.35.1
B      172.16.35.0/24     [20/0]      via 172.27.21.1
C      172.17.35.0/24     [0/0]       via 172.17.35.2
B      172.27.13.0/24     [20/0]      via 172.17.35.1
B      172.27.13.0/24     [20/0]      via 172.27.21.1
C      172.27.21.0/24     [0/0]       via 172.27.21.3
B      172.27.22.0/24     [20/0]      via 172.17.35.1
B      172.27.22.0/24     [20/0]      via 172.27.21.1
C      192.168.100.0/24   [0/0]       via 192.168.100.50

```

- Repeat this procedure for the NSX Edge device LAXCOMP-ESG02.

## 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

- Log in to vCenter Server by using the vSphere Web Client.
  - Open a Web browser and go to <https://mgmt01vc51.lax01.rainpole.local/vsphere-client>.
  - Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- Under **Inventories**, click **Networking & Security**.
- In the **Navigator**, click **NSX Edges**.
- 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 **SFOCOMP-UDLR01**.
  - 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**.

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Local AS	65000

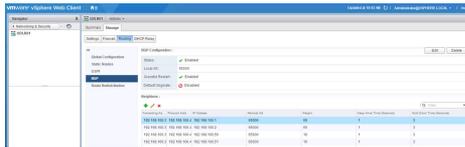
- c Click the **Add** icon to add a Neighbor.

The **New Neighbor** dialog box appears.

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

You repeat this step two times to configure the UDLR for both NSX Edge devices: LAXCOMP-ESG01 and LAXCOMP-ESG02.

Setting	LAXCOMP-ESG01 Value	LAXCOMP-ESG02 Value
IP Address	192.168.100.50	192.168.100.51
Forwarding Address	192.168.100.3	192.168.100.3
Protocol Address	192.168.100.4	192.168.100.4
Remote AS	65000	65000
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	<i>bgp_password</i>	<i>bgp_password</i>



- 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 UDLR01, the UDLR whose peering and BGP configuration you want to verify.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>udlr_admin_password</i>

- 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.

```

    Prefixes received 7 sent 1 advertised 1
Connections established 1, dropped 1
Local host: 192.168.100.4, Local port: 28997
Remote host: 192.168.100.50, Remote port: 179

BGP neighbor is 192.168.100.51, remote AS 65000,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 633 messages, Sent 631 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 4 Identifier 0xa5049fbc
  Route refresh request:received 0 sent 0
  Prefixes received 7 sent 1 advertised 1
Connections established 1, dropped 1
Local host: 192.168.100.4, Local port: 56862
Remote host: 192.168.100.51, Remote port: 179

```

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

You verify multiple routes to BGP learned networks by locating the same route using a different IP address. The IP addresses are listed after the word `via` in the right-side column of the routing table output. In the 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.

```

NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 8

B      0.0.0.0/0          [20/0]      via 192.168.100.1
B      0.0.0.0/0          [20/0]      via 192.168.100.2
C      169.254.1.0/30     [0/0]
B      172.16.35.0/24    [200/0]     via 192.168.100.1
B      172.16.35.0/24    [200/0]     via 192.168.100.2
B      172.17.35.0/24    [20/0]      via 192.168.100.1
B      172.17.35.0/24    [20/0]      via 192.168.100.2
B      172.27.13.0/24    [200/0]     via 192.168.100.1
B      172.27.13.0/24    [200/0]     via 192.168.100.2
B      172.27.21.0/24    [20/0]      via 192.168.100.1
B      172.27.21.0/24    [20/0]      via 192.168.100.2
B      172.27.22.0/24    [20/0]      via 192.168.100.1
B      172.27.22.0/24    [20/0]      via 192.168.100.2
C      192.168.100.0/24   [0/0]      via 192.168.100.4

```

## Deploy the Distributed Logical Router in the Shared Edge and Compute Cluster in Region B

Deploy the distributed logical routers (DLR).

### Procedure

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://mgmt01vc51.lax01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under Inventories, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.
- 5 Click the **Add** icon to create a new DLR.
- 6 On the **Name and description** page, enter the following settings, and click **Next**.

Setting	Value
Logical (Distributed) Router	Selected
Name	LAXCOMP-DLR01
Deploy Edge Appliance	Selected
Enable High Availability	Selected

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

Setting	Value
User Name	admin
Password	dlr_admin_password
Enable SSH access	Selected
Enable FIPS mode	Deselected
Edge Control Level logging	INFO

- 8 On the **Configure deployment** page, and 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**.

Setting	Value
Cluster/Resource Pool	SDDC-EdgeRP01
Datastore	<i>lax01_shared_edge_and_compute_datastore</i>
Folder	NSX51

- 10 On the **Configure deployment** page, and 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.

Setting	Value
Cluster/Resource Pool	SDDC-EdgeRP51
Datastore	<i>lax01_shared_edge_and_compute_datastore</i>
Folder	NSX51

- 12 On the **Configure interfaces** page, under HA Interface Configuration, click **Select** and connect to **vDS-Comp01-Management**.

- 13 On the **Configure interfaces** page enter the following configuration settings and click **Next**.

- a Click the **Add** icon.

Setting	Value
Primary IP Address	1.4.1.1
Subnet Prefix Length	24

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

Setting	Value
Name	Uplink
Type	Uplink
Connected To	Global Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.102.3
Subnet Prefix Length	24
MTU	9000

- 14 In the **Default gateway settings** page, deselect **Configure Default Gateway** and click **Next**.

- 15 In the **Ready to complete** page, click **Finish**.

## 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 Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.
- 5 Configure the routing for the Distributed Logical Router.
  - a Double-click **LAXCOMP-DLR01**.
  - 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**.

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Local AS	65000

- c Click the **Add** icon to add a Neighbor.

The **New Neighbor** dialog box appears.

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

You repeat this step two times to configure the DLR for both NSX Edge devices: LAXCOMP-ESG01 and LAXCOMP-ESG02.

Setting	LAXCOMP-ESG01 Value	LAXCOMP-ESG02 Value
IP Address	192.168.102.1	192.168.102.2
Forwarding Address	192.168.102.3	192.168.102.3
Protocol Address	192.168.102.4	192.168.102.4
Remote AS	65000	65000
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	<i>bgp_password</i>	<i>bgp_password</i>

- 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**.

Setting	Value
OSPF	Deselected
BGP	Selected

- c On the **Route Redistribution** page, select the default **OSPF** entry and click the **Edit** button.
- d Select **BGP** from the **Learner Protocol** drop-down menu, and click **OK**.
- e Click **Publish Changes**.

## Verify Establishment of BGP for the Distributed Logical Router in the Shared Edge and Compute Cluster in Region B

The distributed logical router (DLR) 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 LAXCOMP-DLR01 by using a Secure Shell (SSH) client.
  - a Open an SSH connection to LAXCOMP-DLR01, the DLR whose peering and BGP configuration you want to verify.
  - b Log in using the following credentials.

Options	Description
User name	admin
Password	dlr_admin_password

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

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

```
BGP neighbor is 192.168.102.1, remote AS 65000,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 1395218 messages, Sent 1395210 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 1 Identifier 0x718a966c
  Route refresh request:received 0 sent 0
  Prefixes received 19 sent 1 advertised 1
Connections established 3, dropped 5
Local host: 192.168.102.4, Local port: 179
Remote host: 192.168.102.1, Remote port: 63947

BGP neighbor is 192.168.102.2, remote AS 65000,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
byte 891_
```

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

You verify multiple routes to BGP learned networks by locating the same route using a different IP address. The IP addresses are listed after the word `via` in the right-side column of the routing table output. In the 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.

```

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 21

B      0.0.0.0/0          [200/0]      via 192.168.102.1
B      0.0.0.0/0          [200/0]      via 192.168.102.2
C      1.2.1.0/24         [0/0]        via 1.2.1.1
B      10.159.4.0/23      [200/0]      via 192.168.102.1
B      10.159.4.0/23      [200/0]      via 192.168.102.2
C      169.254.1.0/30     [0/0]        via 169.254.1.2
B      172.16.11.0/24     [200/0]      via 192.168.102.1
B      172.16.11.0/24     [200/0]      via 192.168.102.2
B      172.16.21.0/24     [200/0]      via 192.168.102.1
B      172.16.21.0/24     [200/0]      via 192.168.102.2
B      172.16.31.0/24     [200/0]      via 192.168.102.1
B      172.16.31.0/24     [200/0]      via 192.168.102.2
B      172.16.35.0/24     [200/0]      via 192.168.102.1
B      172.16.35.0/24     [200/0]      via 192.168.102.2
B      172.17.11.0/24    [200/0]      via 192.168.102.1
B      172.17.11.0/24    [200/0]      via 192.168.102.2
byte 1321

```

## Test the Shared Edge and Compute Cluster NSX Configuration in Region B

Test the configuration of the NSX logical network.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://mgmt01vc51.lax01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Use the Ping Monitor to test connectivity.
  - a In the **Navigator**, click **Networking & Security**.
  - b Under **Logical Switches**, double-click **Universal Transit Network**.
  - c Click the **Monitor** tab.
  - d Under **Test Parameters**, select **comp01esx51.lax01.rainpole.local** as the **Source** host.
  - e Under **Test Parameters**, select **comp01esx52.lax01.rainpole.local** as the **Destination** host, and click **Start Test**.
  - f There must be no error messages listed under **Results**.

## Test the Shared Edge and Compute Clusters Routing Failover

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

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.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 **comp01vc01.sfo01.rainpole.local** tree.
  - c Right-click **SFOCOMP-ESG01-0** and select **Power > Shut Down Guest OS**.
  - d Right-click **SFOCOMP-ESG02-0** 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 **SFOCOMP-UDLR01**.
  - 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-7b90db5b-b32b-43c8-9482-4965b0651f98-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 8

B      0.0.0.0/0          [20/0]      via 192.168.100.50
B      0.0.0.0/0          [20/0]      via 192.168.100.51
C      169.254.1.0/30      [0/0]       via 169.254.1.1
B      172.16.35.0/24      [20/0]      via 192.168.100.50
B      172.16.35.0/24      [20/0]      via 192.168.100.51
B      172.17.35.0/24      [200/0]     via 192.168.100.50
B      172.17.35.0/24      [200/0]     via 192.168.100.51
B      172.27.13.0/24      [20/0]      via 192.168.100.50
B      172.27.13.0/24      [20/0]      via 192.168.100.51
B      172.27.21.0/24      [200/0]     via 192.168.100.50
B      172.27.21.0/24      [200/0]     via 192.168.100.51
B      172.27.22.0/24      [20/0]      via 192.168.100.50
B      172.27.22.0/24      [20/0]      via 192.168.100.51
C      192.168.100.0/24     [0/0]       via 192.168.100.4
NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0>

```

- 4 Power on the NSX Edge services gateways in Region A.
  - a In the **Navigator**, click **Hosts and Clusters**.
  - b Expand the entire **comp01vc01.sfo01.rainpole.local** tree.
  - c Right-click **SFOCOMP-ESG01-0** and select **Power > Power On**.
  - d Right-click **SFOCOMP-ESG02-0** and select **Power > Power On**.

- 5 Verify the new state of the BGP routing.
  - a Go back to the SSH connection to UDLR01 and run the `show ip route` command.
  - b Verify that you receive routes via BGP.  
The letter B before the route indicates that BGP is used.
  - c Verify that you have multiple routes to BGP learned networks and that routes also come from the NSX Edge services gateways in Region A.

```

NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 8

B       0.0.0.0/0           [20/0]           via 192.168.100.1
B       0.0.0.0/0           [20/0]           via 192.168.100.2
C       169.254.1.0/30      [0/0]           via 169.254.1.1
B       172.16.35.0/24      [200/0]         via 192.168.100.1
B       172.16.35.0/24      [200/0]         via 192.168.100.2
B       172.17.35.0/24     [20/0]          via 192.168.100.1
B       172.17.35.0/24     [20/0]          via 192.168.100.2
B       172.27.13.0/24    [200/0]         via 192.168.100.1
B       172.27.13.0/24    [200/0]         via 192.168.100.2
B       172.27.21.0/24   [20/0]          via 192.168.100.1
B       172.27.21.0/24   [20/0]          via 192.168.100.2
B       172.27.22.0/24   [20/0]          via 192.168.100.1
B       172.27.22.0/24   [20/0]          via 192.168.100.2
C       192.168.100.0/24   [0/0]           via 192.168.100.4
NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0>

```

## Deploy and Configure VMware Site Recovery Manager

You deploy VMware 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 the VMware Site Recovery Manager Deployment

To be able to install two VMware 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 Deploy the VMware Site Recovery Manager Server in Region A

Deploy the first VMware Site Recovery Manager instance.

#### 4 Deploy the VMware Site Recovery Manager Server in Region B

In Region B, deploy the second VMware Site Recovery Manager instance.

## 5 Configure the VMware Site Recovery Manager Instances

After both VMware Site Recovery Manager Instances are deployed, assign the appropriate licensing and, 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 the VMware Site Recovery Manager Deployment

To be able to install two VMware 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.

### Hardware and 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. Hardware Requirements for Site Recovery Manager VMs**

Component	Requirement
vCPU	2 x 2.0 GHz or higher Intel or AMD x86 processors
Memory	2 GB minimum
Disk	5 GB minimum
Datastore	vSAN
Networking	1 Gbps for communication between regions

**Table 2-11. Software and Configuration Requirements for Site Recovery Manager VMs**

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

### 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 2-12. Network Configuration of Site Recovery Manager in Region A**

Setting	Value
Host name	mgmt01srm01
Static IPv4 address	172.16.11.124
Subnet mask	255.255.255.0
Default gateway	172.16.11.253
DNS server	172.16.11.5
FQDN	mgmt01srm01.sfo01.rainpole.local
Used ports	<ul style="list-style-type: none"> <li>■ 9086</li> <li>■ 5678</li> </ul>
Time synchronization	<ul style="list-style-type: none"> <li>■ Configure the VM with the following NTP servers:               <ul style="list-style-type: none"> <li>■ ntp.sfo01.rainpole.local</li> <li>■ ntp.lax01.rainpole.local</li> </ul> </li> <li>■ Verify that time synchronization is successful</li> </ul>

**Table 2-13. Network Configuration of Site Recovery Manager in Region B**

Setting	Value
Host name	mgmt01srm51
Static IPv4 address	172.17.11.124
Subnet mask	255.255.255.0
Default gateway	172.17.11.253
DNS server	172.17.11.5
FQDN	mgmt01srm51.lax01.rainpole.local
Used ports	<ul style="list-style-type: none"> <li>■ 9086</li> <li>■ 5678</li> </ul>
NTP servers	<ul style="list-style-type: none"> <li>■ Configure the VM with the following NTP servers:               <ul style="list-style-type: none"> <li>■ ntp.sfo01.rainpole.local</li> <li>■ ntp.lax01.rainpole.local</li> </ul> </li> <li>■ Verify that time synchronization is successful</li> </ul>

## 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.

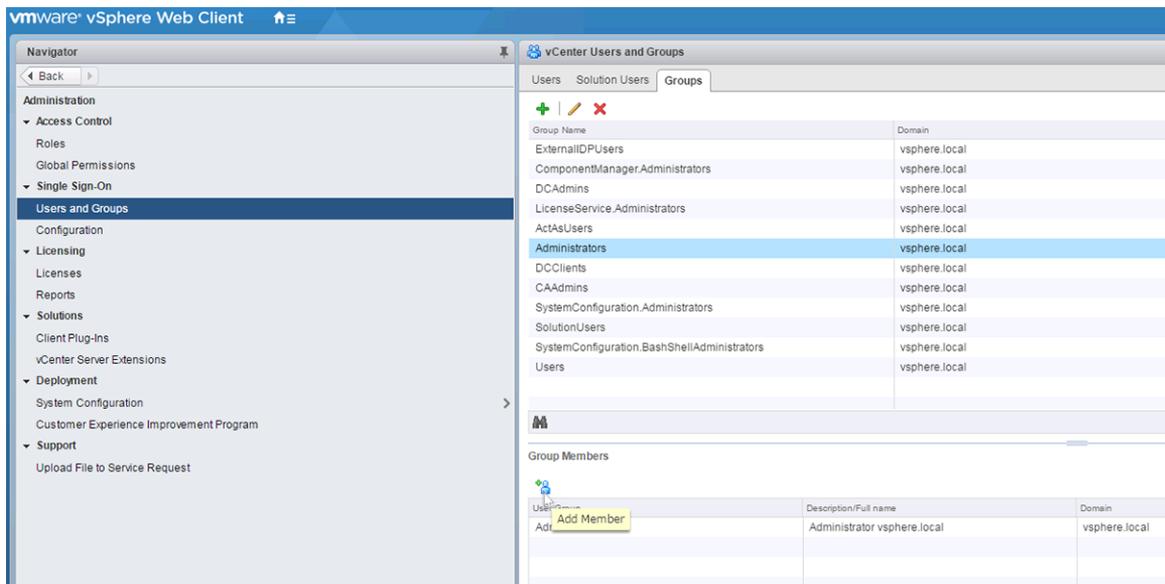
- Verify that the users and groups from the rainpole.local domain are available in Region A and Region B.

**Procedure**

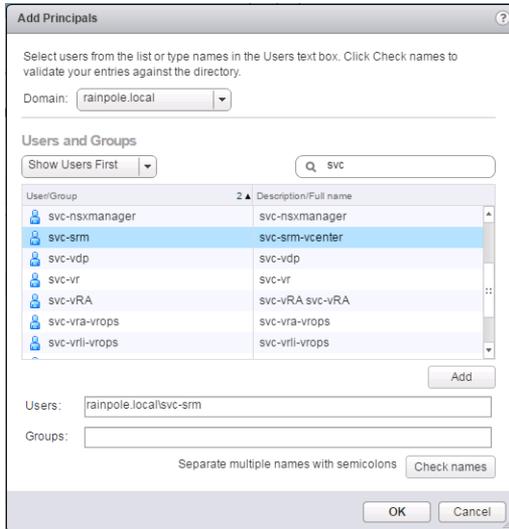
- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Administration**.
- 3 Add the service account svc-srm@rainpole.local to the Single Sign-On administrators group
  - a In the vSphere Web Client, select **Administration** from the **Home** menu and click **Users and Groups** under **Users and Groups**.
  - b On the **Groups** tab, 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-srm** user, click **Add**, and click **OK**.



The global vCenter Single Sign-On administrative permissions of the svc-srm account propagate to all other linked vCenter Server instances.

## Deploy the VMware Site Recovery Manager Server in Region A

Deploy the first VMware Site Recovery Manager instance.

### Procedure

- 1 Log in to the mgmt01srm01.sfo01.rainpole.local by using a Remote Desktop Protocol (RDP) client.
  - a Open an RDP connection to the virtual machine mgmt01srm01.sfo01.rainpole.local.
  - b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	windows_administrator_password

- 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**.

Setting	Value
Address	sfo01psc01.sfo01.rainpole.local
HTTPS Port	443
Username	svc-srm@rainpole.local
Password	svc-srm_password

- 10 If prompted, in the **Platform Services Controller Certificate** dialog box, click **Accept**.
- 11 On the **VMware vCenter Server** page, select **mgmt01vc01.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**.

Setting	Value
Local Site Name	mgmt01vc01.sfo01.rainpole.local
Administrator E-mail	srm_admin_sfo_email_address
Local Host	172.16.11.124
Listener Port	9086

- 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**.

Setting	Value
Organization	Rainpole
Organization Unit	Rainpole

- 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**.

Setting	Value
Data Source Name	SRM_SITE_SFO
Database User Name	srm_admin
Database Password	srm_admin_sfo_password
Database Port	5678

Setting	Value
Connection Count	5
Max. Connections	20

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

Setting	Value
Use Local System account	Deselected
Username	MGMT01SRM01\Administrator
Password	<i>mgmt01srm01_admin_password</i>

- 20 On the **Ready to Install the Program** page, click **Install**.
- 21 Click **Finish** to complete the installation.

## Deploy the VMware Site Recovery Manager Server in Region B

In Region B, deploy the second VMware Site Recovery Manager instance.

### Procedure

- 1 Log in to the mgmt01srm51.lax01.rainpole.local, by using a Remote Desktop Protocol (RDP) client.
  - a Open an RDP connection to the virtual machine mgmt01srm51.lax01.rainpole.local.
  - b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	<i>windows_administrator_password</i>

- 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**.

Setting	Value
Address	lax01psc51.lax01.rainpole.local
HTTPS Port	443
Username	svc-srm@rainpole.local
Password	<i>svc-srm_password</i>

- 10 If prompted, in the **Platform Services Controller Certificate** dialog box, click **Accept**.
- 11 On the **VMware vCenter Server** page, select **mgmt01vc51.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**.

Setting	Value
Local Site Name	mgmt01vc51.lax01.rainpole.local
Administrator E-mail	<i>srm_admin_lax_email_address</i>
Local Host	172.17.11.124
Listener Port	9086

- 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**.

Setting	Value
Organization	Rainpole
Organization Unit	Rainpole

- 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**.

Setting	Value
Data Source Name	SRM_SITE_LAX
Database User Name	srm_admin
Database Password	<i>srm_admin_lax_password</i>
Database Port	5678
Connection Count	5
Max. Connections	20

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

Setting	Value
Use Local System account	Deselected
Username	MGMT01SRM51\Administrator
Password	<i>mgmt01srm51_admin_password</i>

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

- 21 Click **Finish** to complete the installation.

## Configure the VMware Site Recovery Manager Instances

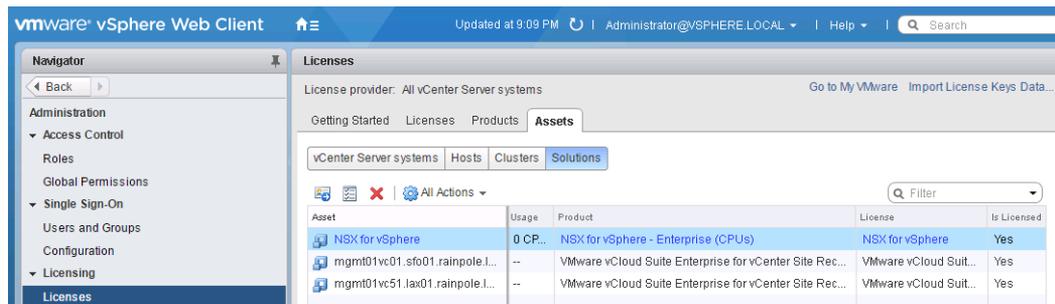
After both VMware Site Recovery Manager Instances are deployed, assign the appropriate licensing and, using the svc-srm service account, pair the Region A and Region B instances and configure the mappings between them to support disaster recovery.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 License the Site Recovery Manager instances.
  - a Under **Administration**, click **Licenses**.
  - b Click the **Assets** tab and click **Solutions**.
  - c Select the **mgmt01vc01.sfo01.rainpole.local** instance and click the **Assign License** icon.

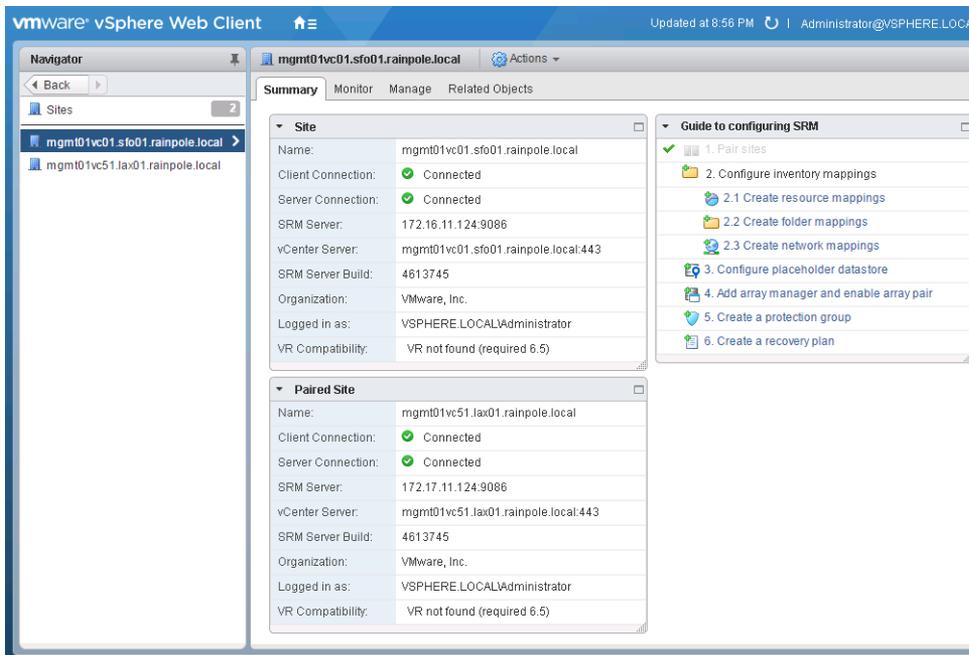


- d Select the available license from the list and click **OK**.

- e Select the **mgmt01vc51.lax01.rainpole.local** instance and click the **Assign License** icon.
  - f Select the available license from the list and click **OK**.
- 3 Pair the two Site Recovery Manager sites.
- a From the **Home** menu, select **Site Recovery**.
  - b In the **Navigator**, click **Sites**.
  - c Under **Sites**, click the **mgmt01vc01.sfo01.rainpole.local** site.
  - d Under **Guide to configuring SRM** on the right, click **Pair sites**.
  - e On the **Select Site** page, enter **lax01psc51.lax01.rainpole.local** in the **PSC address** text box, leave the port value and click **Next**.
  - f On the **Select vCenter Server** page, select **mgmt01vc51.lax01.rainpole.local**, enter the following credentials, and click **Finish**.

Setting	Value
User name	svc-srm@rainpole.local
Password	svc-srm_password

- g In the **Security Alert** dialog box that appears twice, click **Yes** and wait until a new pane, **Paired Site**, appears on the **Summary** tab.



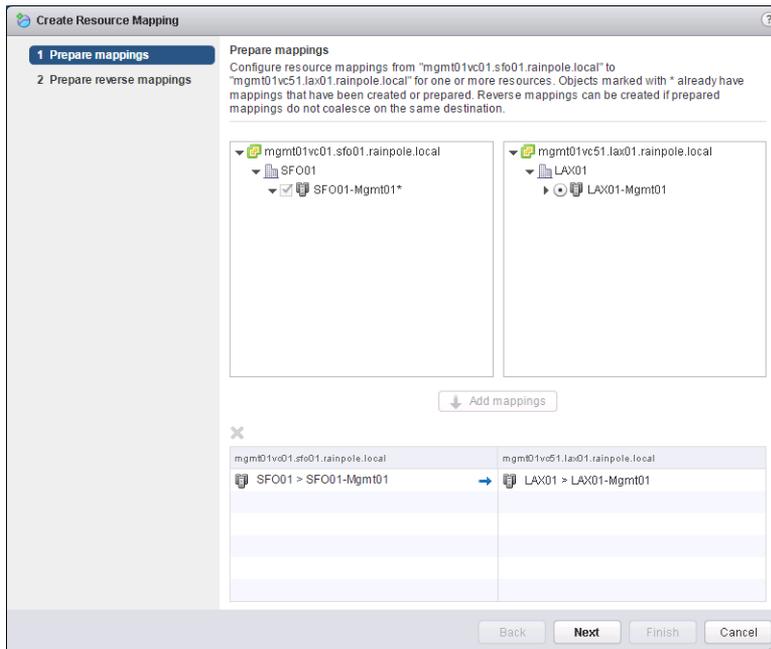
4 Configure resource mappings.

- a Under **Guide to configuring SRM**, click **2.1 Create resource mappings**.

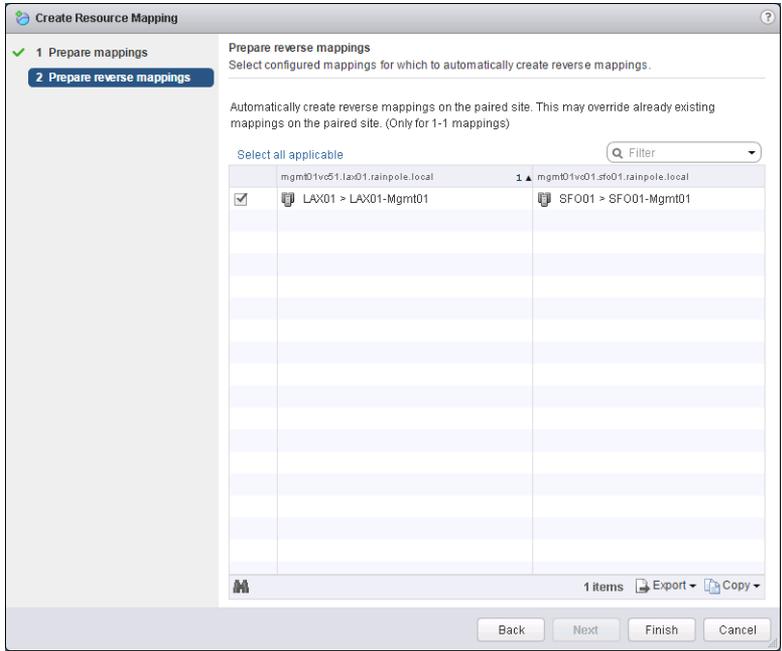


- b On the **Prepare Mappings** page, select the clusters underneath the vCenter Server instances for Region A and Region B to create a mapping between the resource in the clusters, click **Add mappings**, and click **Next**.

vCenter Server	Cluster
mgmt01vc01.sfo01.rainpole.local	SFO01-Mgmt01
mgmt01vc51.lax01.rainpole.local	LAX01-Mgmt01



- c On the **Prepare Reverse Mappings** page, click **Select all applicable** and click **Finish**.



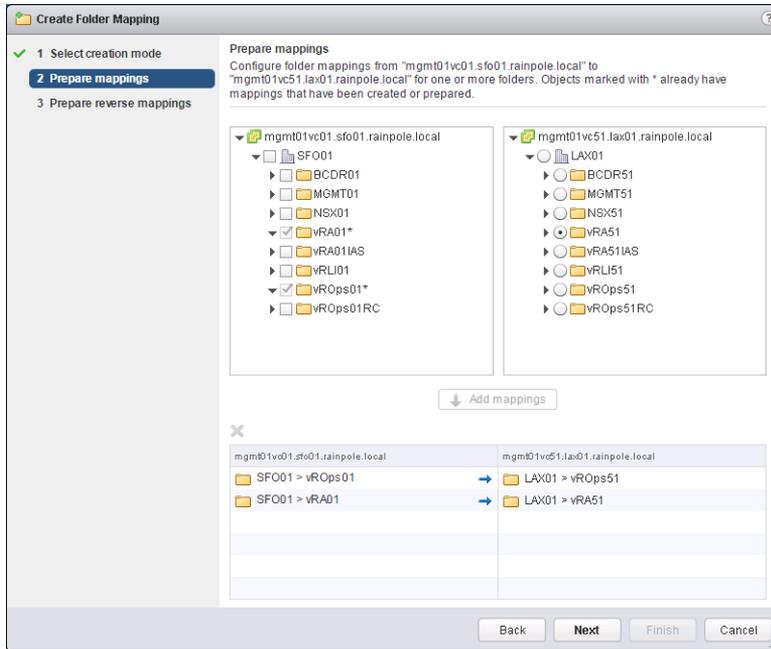
5 Configure folder mappings.

- a Under **Guide to configuring SRM**, click **2.2 Create folder mappings**.
- b On the **Select Creation Mode** page, select **Prepare mappings manually** and click **Next**.
- c On the **Prepare Mappings** page, select the folders of the vRealize Operations Manager components and click **Add mappings**.

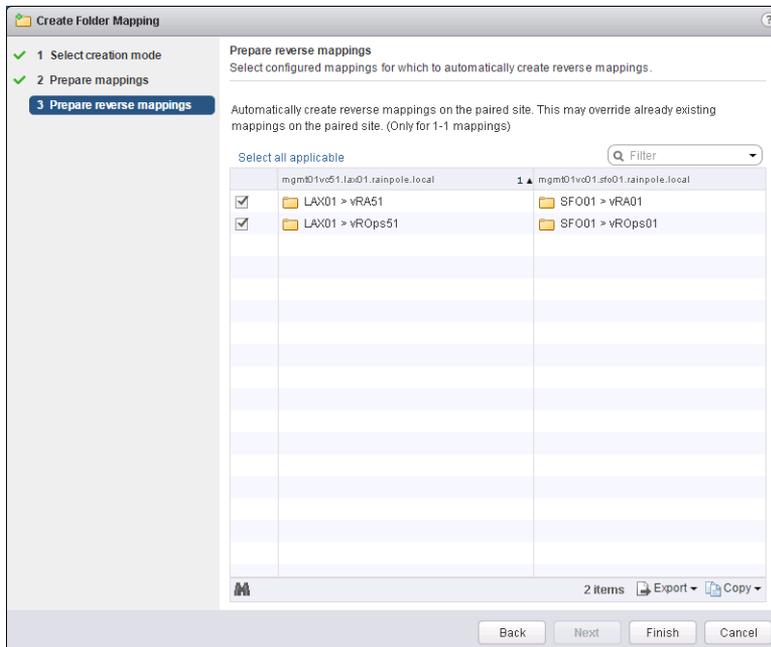
Setting	Protected Region	Recovery Region
vCenter Server	mgmt01vc01.sfo01.rainpole.local	mgmt01vc51.lax01.rainpole.local
Data center	SFO01	LAX01
Folder	vROps01	vROps51

- d On the **Prepare Mappings** page, select the folders of vRealize Automation core components, click **Add mappings**, and click **Next**.

Setting	Protected Region	Recovery Region
vCenter Server	mgmt01vc01.sfo01.rainpole.local	mgmt01vc51.lax01.rainpole.local
Data center	SFO01	LAX01
Folder	vRA01	vRA51

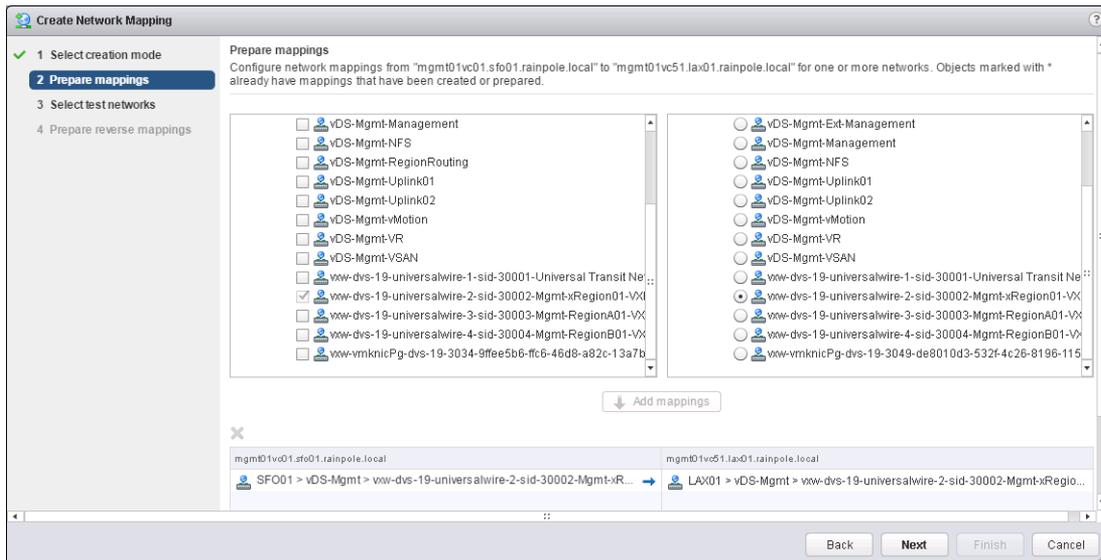


- e On the **Prepare Reverse Mappings** page, click **Select all applicable**, and click **Finish**.

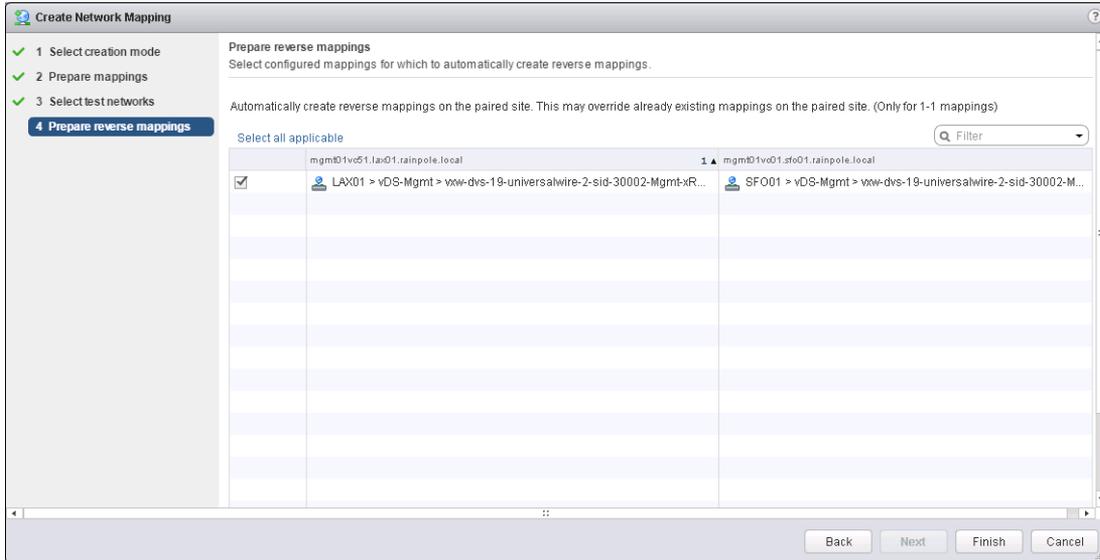


- 6 Configure network mappings to enable failover of vRealize Operations Manager and vRealize Automation.
  - a Under **Guide to configuring SRM**, click **2.3 Create network mappings**.
  - b On the **Select Creation Mode** page, select **Prepare mappings manually** and click **Next**.
  - c On the **Prepare Mappings** page, expand the object trees, select the distributed port groups to map, click **Add mappings**, and click **Next**.

Setting	Protected Region	Recovery Region
vCenter Server	mgmt01vc01.sfo01.rainpole.local	mgmt01vc51.lax01.rainpole.local
Data center	SFO01	LAX01
Distributed switch	vDS-Mgmt	vDS-Mgmt
Port group	<i>group_prefix-xRegion01-VXLAN</i>	<i>group_prefix-xRegion01-VXLAN</i>

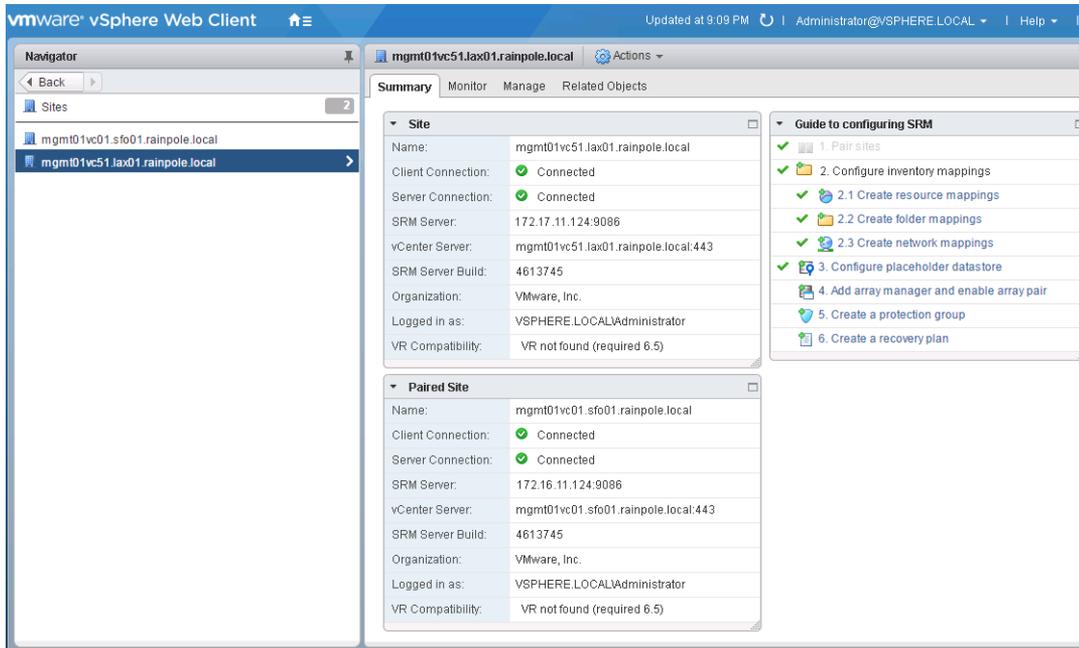


- d On the **Select Test Networks** page, keep the default values and click **Next**.
- e On the **Prepare Reverse Mappings** page, click **Select all applicable** and click **Finish**.



- 7 Configure placeholder datastore.
  - a Under **Guide to configuring SRM**, click **3. Configure placeholder datastore**.
  - b In the **Configure Placeholder Datastore** dialog box, select the **SFO01A-VSAN01-MGMT01** datastore, and click **OK**.
  - c Under **Sites**, click the **mgmt01vc51.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 **LAX01A-VSAN01-MGMT01** 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 be able 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-vm 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 be able to deploy the two vSphere Replication virtual appliances, one in the protected region, and one in the recovery region, your environment must satisfy certain hardware and software requirements.

## Software Requirements

Before you install vSphere Replication, make sure that you have the following configuration available in your environment.

Component	Requirement
Installation package	Download the vSphere Replication .iso image and mount it on the machine that you use to access the vSphere Web Client.
Email address of the vSphere Replication site administrators	Get the email addresses of the vSphere Replication site administrators.

## 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 2-14. Network Configuration of vSphere Replication in Region A**

Setting	Value
Host name	mgmt01vrms01
Static IPv4 address	172.16.11.123
Subnet mask	255.255.255.0
Default gateway	172.16.11.253
DNS servers	172.16.11.5
FQDN	mgmt01vrms01.sfo01.rainpole.local
Used ports	5480
NTP servers	<ul style="list-style-type: none"> <li>■ ntp.sfo01.rainpole.local</li> <li>■ ntp.lax01.rainpole.local</li> </ul>

**Table 2-15. Network Configuration of vSphere Replication in Region B**

Setting	Value
Host name	mgmt01vrms51
Static IPv4 address	172.17.11.123
Subnet mask	255.255.255.0
Default gateway	172.17.11.253
DNS servers	172.17.11.5
FQDN	mgmt01vrms51.lax01.rainpole.local
Used ports	5480
NTP servers	<ul style="list-style-type: none"> <li>■ ntp.lax01.rainpole.local</li> <li>■ ntp.sfo01.rainpole.local</li> </ul>

**Table 2-16. VLAN and IP Requirements for vSphere Replication Traffic**

Requirement	Region A	Region B
VLAN ID	1616	1716
Static IPv4 address	172.16.16.71	172.17.16.71
Subnet mask	255.255.255.0	255.255.255.0
Gateway	172.16.16.253	172.17.16.253

## 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.

### 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.

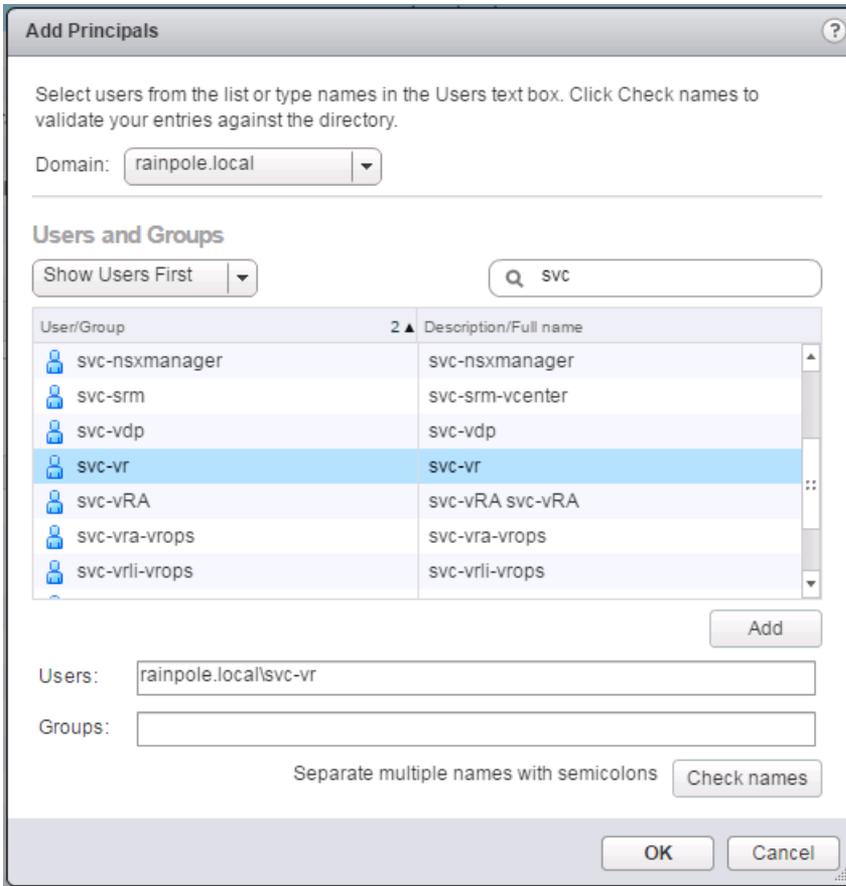
## Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Administration**.
- 3 Assign the service account **svc-vr@rainpole.local** to the Single Sign-On Administrators group
  - a In the vSphere Web Client, navigate to **Administration** and click **Users and Groups**.
  - b On the **Groups** tab, 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 propagates 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.

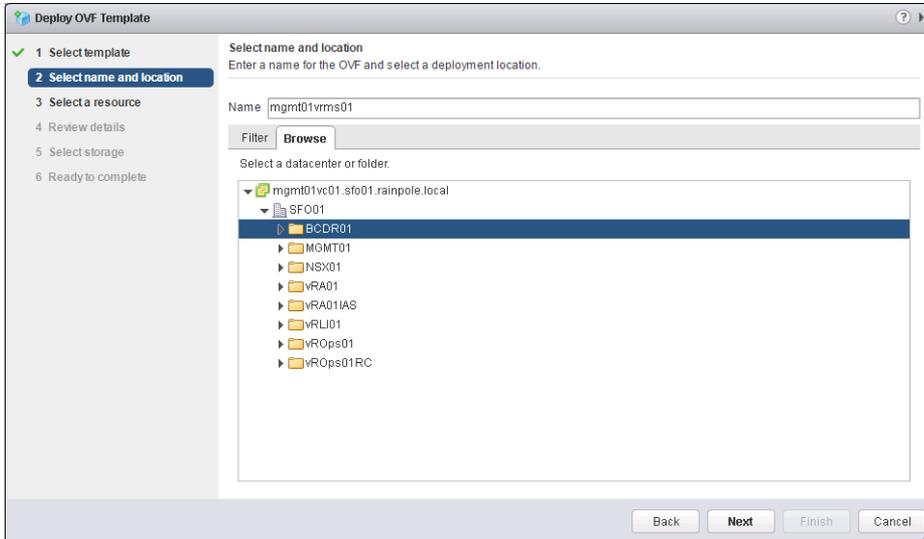
## Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

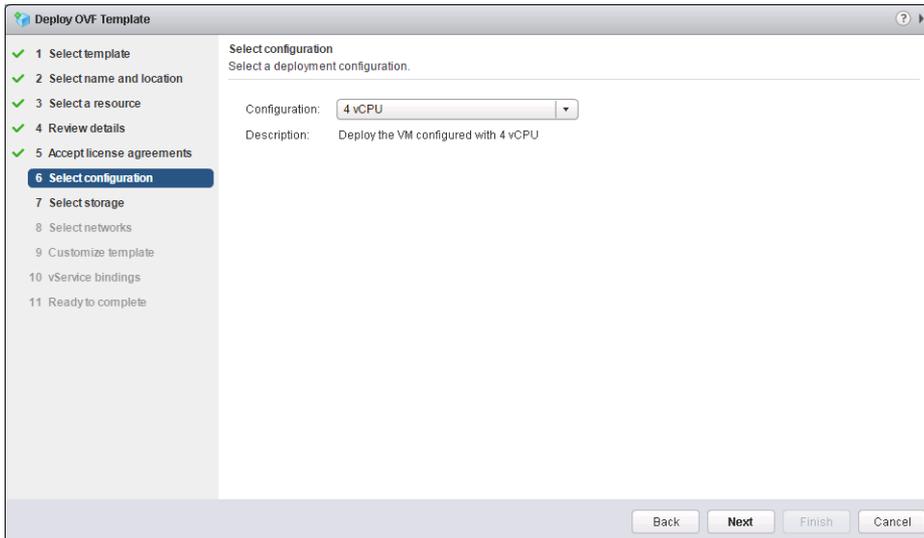
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Deploy the vSphere Replication appliance.
- 3 In the **Navigator**, click **Hosts and Clusters**.
- 4 Right-click **mgmt01vc01.sfo01.rainpole.local** and click **Deploy OVF Template**.
- 5 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
- 6 On the **Select name and location** page, enter a node name, select the inventory folder for the virtual appliance, and click **Next**.

Setting	Value
Name	mgmt01vrms01
vCenter Server	mgmt01vc01.sfo01.rainpole.local
Data center	SFO01
Folder	BCDR01

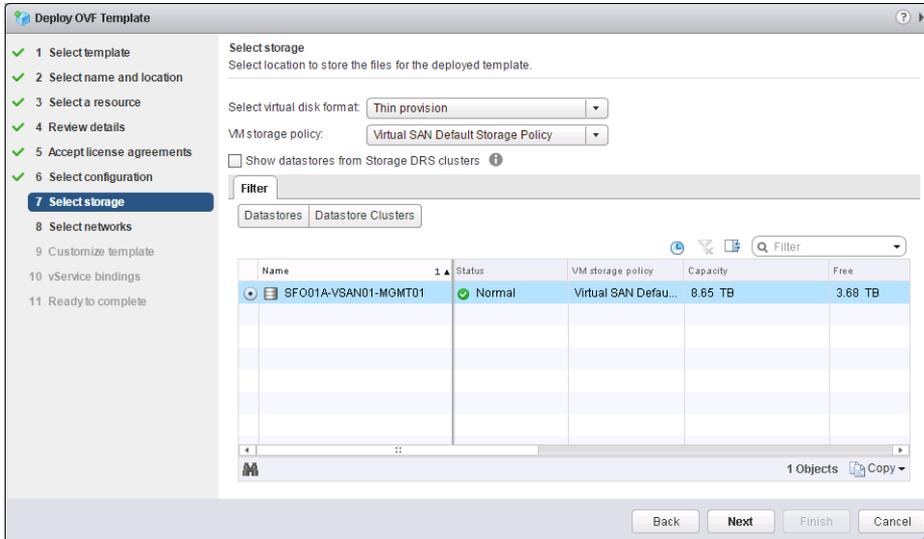


- 7 On the **Select a Resource** page, select the **SFO01-Mgmt01** cluster and click **Next**.
- 8 On the **Review Details** page, click **Next**.
- 9 On the **Accept License Agreements** page, click **Accept** and click **Next**.
- 10 On the **Select Configuration** page, leave the default **4 vCPU** configuration selected and click **Next**.



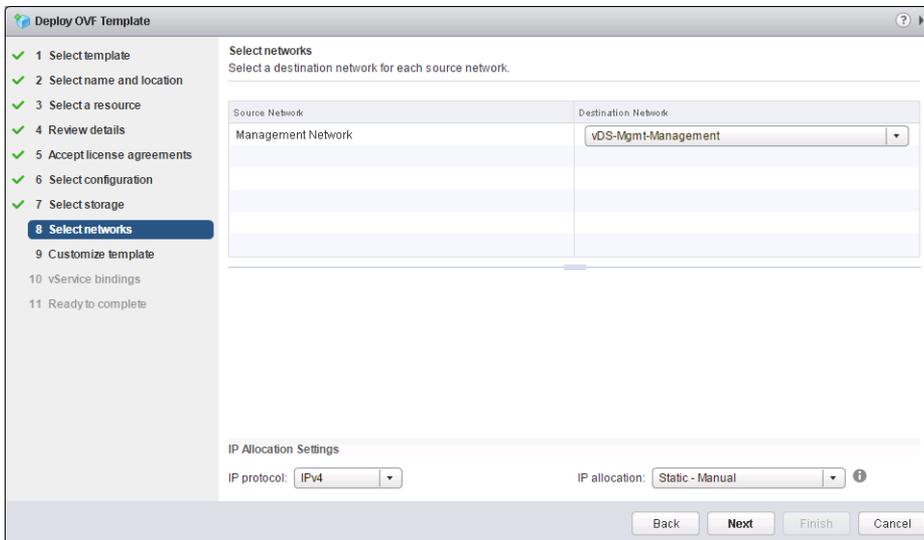
- 11 On the **Select Storage** page, enter the following settings and click **Next**.

Setting	Value
VM Storage Policy	Virtual SAN Default Storage Policy
Datastore	SFO01A-VSAN01-MGMT01



12 On the **Setup Networks** page, select the following settings and click **Next**.

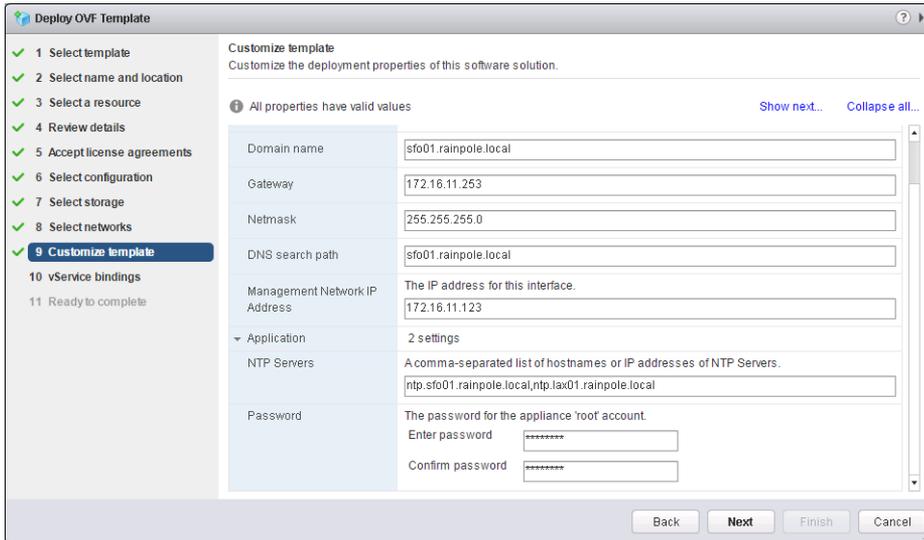
Setting	Value
Management Network Destination	vDS-Mgmt-Management
IP protocol	IPv4
IP allocation	Static - Manual



13 On the **Customize Template** page, enter the following settings and click **Next**.

Setting	Value
DNS servers	172.16.11.5,172.16.11.4
Domain name	sfo01.rainpole.local
Gateway	172.16.11.253
Netmask	255.255.255.0

Setting	Value
DNS search path	sfo01.rainpole.local
Management Network IP Address	172.16.11.123
NTP Servers	ntp.sfo01.rainpole.local,ntp.lax01.rainpole.local
Enter password	<i>vr_sfo_root_password</i>
Confirm password	<i>vr_sfo_root_password</i>



14 On the **vService Bindings** page, click **Next**.

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

16 In the **Navigator**, expand the entire `mgmt01vc01.sfo01.rainpole.local` tree, select the **mgmt01vrms01** 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 by using the vSphere Replication Management Interface..

### Procedure

- 1 Log in to the Management Interface of the vSphere Replication appliance.
  - a Open a Web browser and go to **https://mgmt01vrms01.sfo01.rainpole.local:5480**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vr_sfo_root_password</i>

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

Setting	Value
Configuration Mode	Configure using the embedded database
LookupService Address	sfo01psc01.sfo01.rainpole.local
SSO Administrative Account	svc-vr@rainpole.local
Password	svc-vr_password
VRM Host	172.16.11.123
VRM Site Name	mgmt01vc01.sfo01.rainpole.local
vCenter Server Address	mgmt01vc01.sfo01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	vcenter_server_admin_email

- In the **Confirm SSL Certificate** dialog box, click **Accept**.
- Wait for the vSphere Replication Management (VRM) server to save the configuration.

**vSphere Replication Appliance**

VR | Network | Update | System | Application Home | Help | Logout user root

Getting Started | **Configuration** | Security | Support

**Startup Configuration**  
 Successfully saved the configuration

**Configuration Mode:**

- Configure using the embedded database
- Manual configuration
- Configure from an existing VRM database

LookupService Address:

SSO Administrator:

Password:

VRM Host:

VRM Site Name:

vCenter Server Address:

vCenter Server Port:

vCenter Server Admin Mail:

IP Address for Incoming Storage Traffic:

SSL Certificate Policy

**Actions**

- 
- 
- 

- Under **Service Status**, verify that the status of the VRM service is running.
- Log out from the vSphere Replication 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.

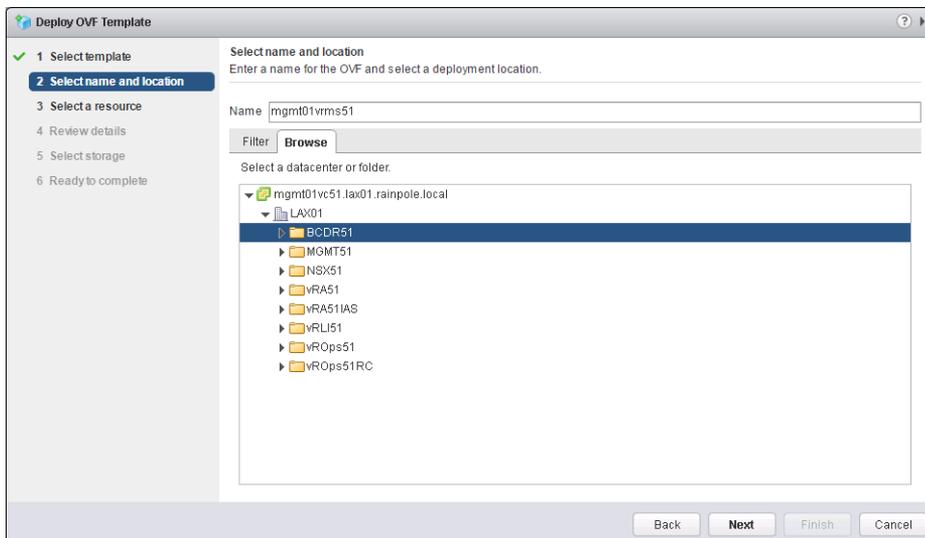
**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

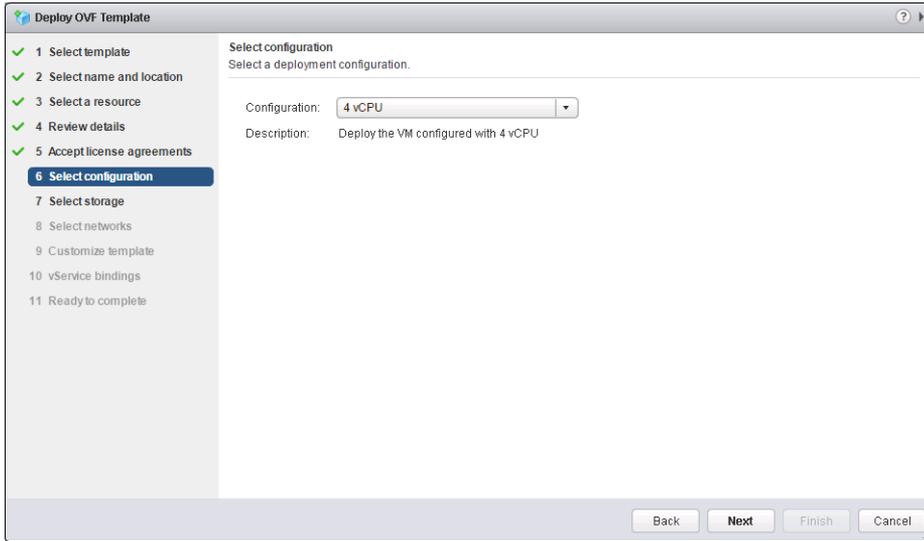
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Hosts and Clusters**.
- 3 Right-click **mgmt01vc51.lax01.rainpole.local**, and click **Deploy OVF Template**.
- 4 On the **Select template** page, click the **Browse** button, use a multiple selection to select the following files from the bin folder of the .iso mount for vSphere Replication on your computer, click **Open**, and click **Next**.
  - vSphere\_Replication\_OVF10.ovf
  - vSphere\_Replication-support.vmdk
  - vSphere\_Replication-system.vmdk
- 5 On the **Select name and location** page, enter a node name, select the inventory folder for the virtual appliance, and click **Next**.

Setting	Value
Name	mgmt01vrms51
vCenter Server	mgmt01vc51.lax01.rainpole.local
Data center	LAX01
Folder	BCDR51

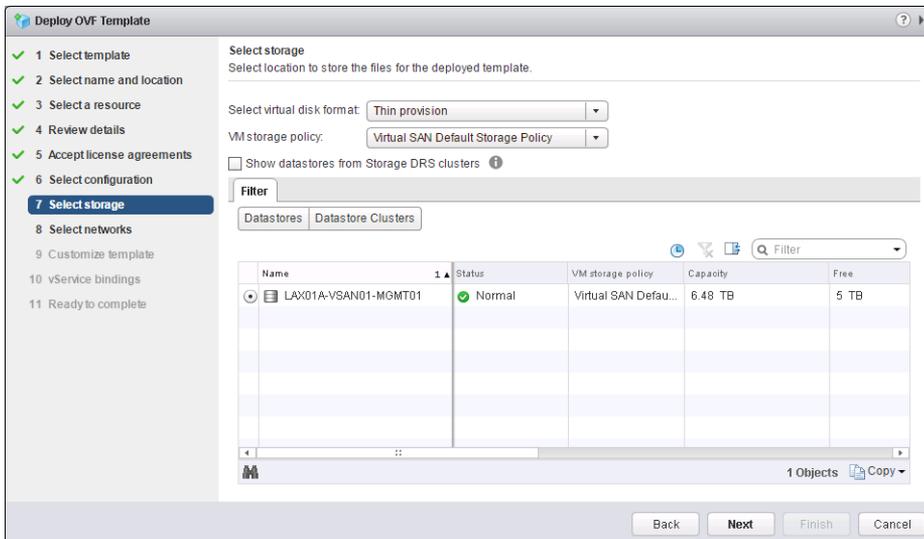


- 6 On the **Select a Resource** page, select the **LAX01-Mgmt01** cluster, and click **Next**.
- 7 On the **Review Details** page, click **Next**.
- 8 On the **Accept License Agreements** page, click **Accept**, and click **Next**.
- 9 On the **Select Configuration** page, leave the default **4 vCPU** configuration selected and click Next.



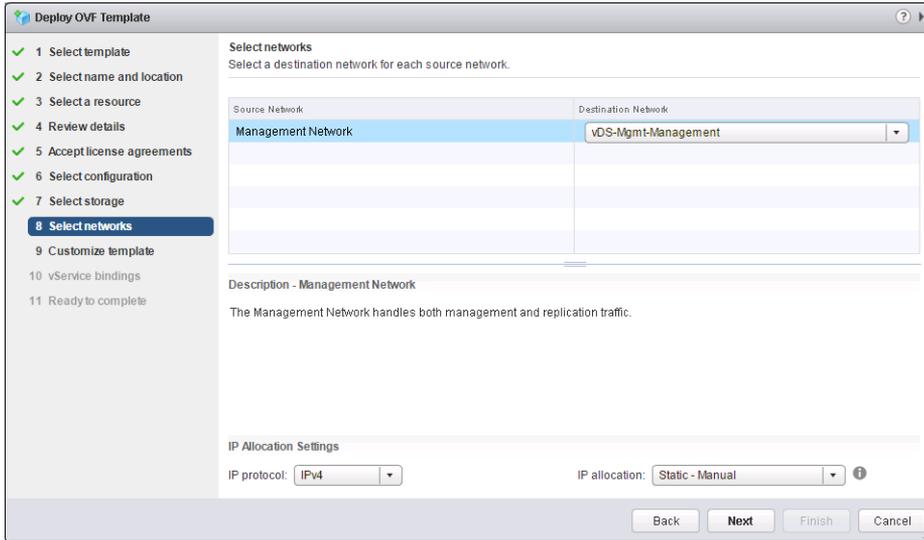
- 10 On the **Select Storage** page, enter the following settings, and click **Next**.

Setting	Value
VM Storage Policy	Virtual SAN Default Storage Policy
Datastore	LAX01A-VSAN01-MGMT01



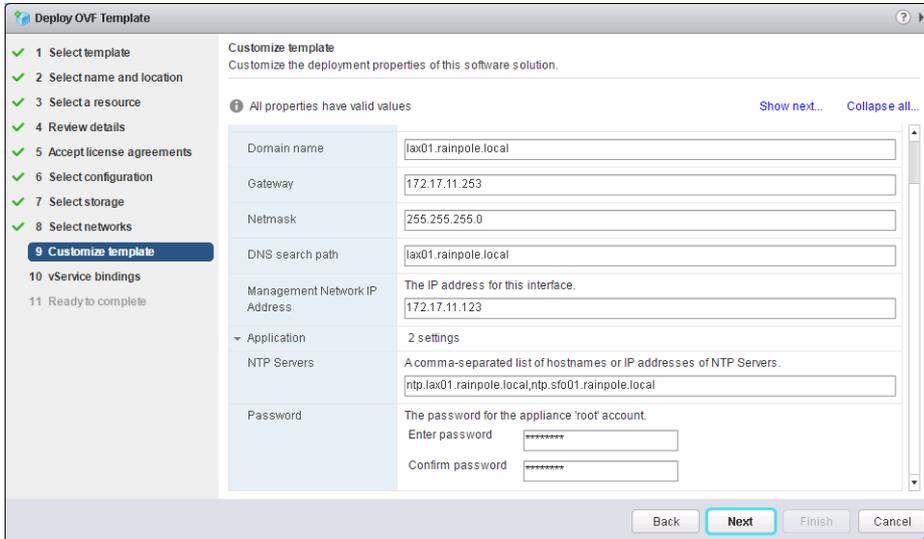
11 On the **Setup Networks** page, select the following settings, and click **Next**.

Setting	Value
Management Network Destination	vDS-Mgmt-Management
IP protocol	IPv4
IP allocation	Static - Manual



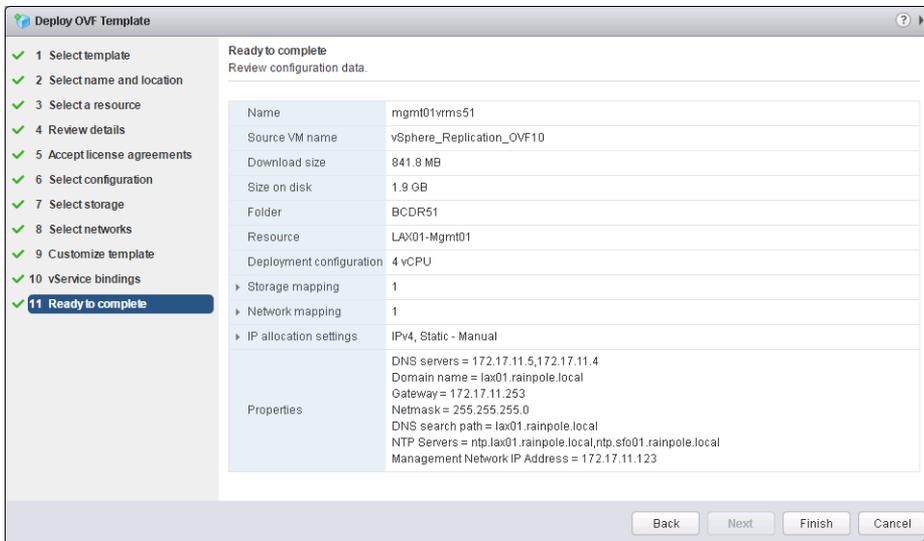
12 On the **Customize Template** page, enter the following settings, and click **Next**.

Setting	Value
DNS servers	172.17.11.5,172.17.11.4
Domain name	lax01.rainpole.local
Gateway	172.17.11.253
Netmask	255.255.255.0
DNS search path	lax01.rainpole.local
Management Network IP Address	172.17.11.123
NTP Servers	ntp.lax01.rainpole.local,ntp.sfo01.rainpole.local
Enter password	<i>vr_lax_root_password</i>
Confirm password	<i>vr_lax_root_password</i>



13 On the **vService Bindings** page, click **Next**.

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



15 In the **Navigator**, expand the entire `mgmt01vc51.lax01.rainpole.local` tree, select the **mgmt01vrms51** 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 by using the vSphere Replication Management Interface.

**Procedure**

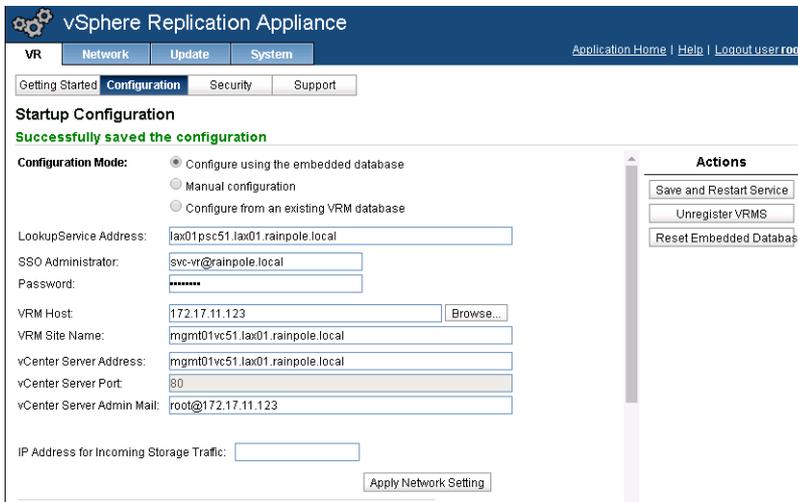
- 1 Log in to the Management Interface of the vSphere Replication.
  - a Open a Web browser and go to **https://mgmt01vrms51.lax01.rainpole.local:5480**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vr_lax_root_password

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

Setting	Value
Configuration Mode	Configure using the embedded database
LookupService Address	lax01psc51.lax01.rainpole.local
SSO Administrative Account	svc-vr@rainpole.local
Password	svc-vr_password
VRM Host	172.17.11.123
VRM Site Name	mgmt01vc51.lax01.rainpole.local
vCenter Server Address	mgmt01vc51.lax01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	vcenter_server_admin_email

- 3 In the **Confirm SSL Certificate** dialog box, click **Accept**.
- 4 Wait for the vSphere Replication Management (VRM) server to save the configuration.



- 5 Under **Service Status**, verify that the status of the VRM service is running.
- 6 Log out from the vSphere Replication Management Interface.

## Connect the vSphere Replication Instances

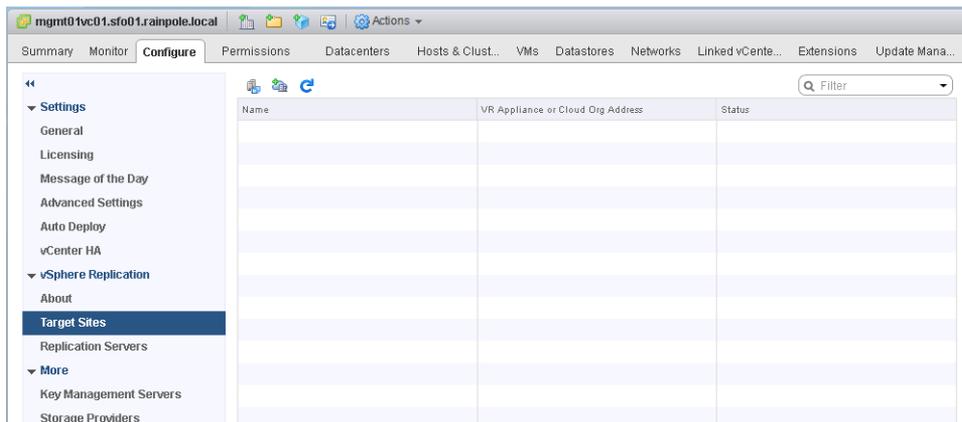
To use vSphere Replication between Region A and Region B, you must configure a connection between the two vSphere Replication appliances because each region is managed by a different vCenter Server instance.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Connect the two vSphere Replication instances.
  - a On the vSphere Web Client Home page, click **Hosts and Clusters**.
  - b In the **Navigator**, select the **mgmt01vc01.sfo01.rainpole.local** instance, click the **Configure** tab, and click **Target Sites** under **vSphere Replication**.
  - c Click the **Connect to target site to configure replications** icon.



- d In the **Connect to Target Site** dialog box, select **Connect to a remote site**, enter the following settings, and click the **Log In** button.

Setting	Value
PSC address of the remote site	lax01psc51.lax01.rainpole.local
User name	svc-vr@rainpole.local
Password	svc-vr_password

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

The **Connect to Target site** dialog box shows the **mgmt01vc51.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.

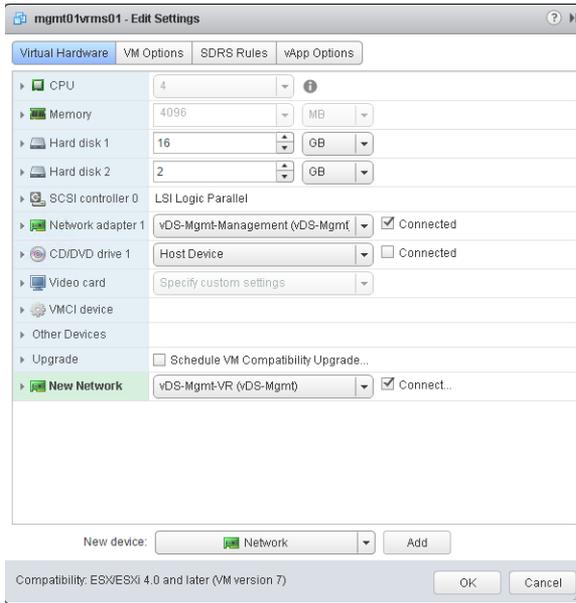
### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Shut down the vSphere Replication appliance to allow changes in the hardware configuration.
  - a In the **Navigator**, click **Hosts and Clusters**.
  - b Expand the entire **mgmt01vc01.sfo01.rainpole.local** tree.
  - c Right-click the **mgmt01vrms01** virtual appliance and select **Power > Shut Down Guest OS**.
  - d In the **Confirm Guest Shut Down** dialog box, click **Yes** to proceed.
- 3 Add a VM network adapter to the vSphere Replication virtual appliance that handles replication traffic only.
  - a Right-click the **mgmt01vrms01** virtual appliance and select **Edit Settings**.
  - b In the **Edit Settings** dialog box, click **Yes** to proceed.
  - c In the **mgmt01vrms01 - 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 **vDS-Mgmt-VR** and click **OK**.



- e Right-click the **mgmt01vrms01** 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 Management Interface.
- a Open a Web browser and go to **https://mgmt01vrms01.sfo01.rainpole.local:5480**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vr_sfo_root_password

5 Configure the network settings for the new network adapter eth1.

- a Click the **Network** tab and click **Address**.
- b Under **eth1 info**, enter the following settings and click **Save Settings**.

Setting	Value
IPv4 Address Type	Static
IPv4 Address	172.16.16.71
Netmask	255.255.255.0
IPv6 Address Type	Auto

The screenshot shows the 'vSphere Replication Appliance' interface. The 'Network' tab is selected, and the 'Address' sub-tab is active. The 'Network Address Settings' section includes fields for Nameserver Source, Hostname, IPv4 Default Gateway, IPv6 Default Gateway, Preferred DNS Server, Alternate DNS Server, Domain Name, and Domain Search Path. Below this, there are sections for 'eth0 info' and 'eth1 info'. The 'eth1 info' section is expanded, showing the following settings: IPv4 Address Type (Static), IPv4 Address (172.16.16.71), Netmask (255.255.255.0), and IPv6 Address Type (Auto). On the right side, there are 'Save Settings' and 'Cancel Changes' buttons. The footer of the page reads 'Powered by VMware Studio'.

- c Click the **VR** tab and click **Configuration**.
- d In the **IP Address for Incoming Storage Traffic** text box, enter **172.16.16.71** and click **Apply Network Setting**.

172.16.16.71 is the IP address of the new network adapter that will handle replication traffic.

- 6 Repeat the steps to reconfigure the vSphere Replication appliance **mgmt01vrms51** in Region B, use the values from the following table.

Setting	Value
Object to configure	mgmt01vrms51
Connect New Network Adapter To	vDS-Mgmt-VR
URL of vSphere Replication Appliance	https://mgmt01vrms51.lax01.rainpole.local:5480
IPv4 Address Type	Static
IPv4 Address	172.17.16.71
Netmask	255.255.255.0
IP Address For Incoming Storage Traffic	172.17.16.71

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

Appliance Host Name	Source Gateway	Target Network
mgmt01vrms01.sfo01.rainpole.local	172.16.16.253	172.17.16.0/24
mgmt01vrms51.lax01.rainpole.local	172.17.16.253	172.16.16.0/24

- a For each vSphere Replication appliance, open an SSH connection and log in using the following credentials.

Setting	Value
Appliance host name	<ul style="list-style-type: none"> <li>■ mgmt01vrms01.sfo01.rainpole.local for Region A</li> <li>■ mgmt01vrms51.lax01.rainpole.local for Region B</li> </ul>
User name	root
Password	<i>vr_root_password</i>

- b Run the following command to create a route to the recovery region for the hosts in Region A or to the protected region for the hosts in Region B.

Region of the vSphere Replication Appliance	Command
Region A	route add -net 172.17.16.0/24 gw 172.16.16.253 dev eth1
Region B	route add -net 172.16.16.0/24 gw 172.17.16.253 dev eth1

- c Repeat the step on the vSphere Replication appliance in the other region.

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

Host Name	Source Gateway	Target Network
mgmt01esx01.sfo01.rainpole.local	172.16.16.253	172.17.16.0/24
mgmt01esx02.sfo01.rainpole.local	172.16.16.253	172.17.16.0/24
mgmt01esx03.sfo01.rainpole.local	172.16.16.253	172.17.16.0/24
mgmt01esx04.sfo01.rainpole.local	172.16.16.253	172.17.16.0/24
mgmt01esx51.lax01.rainpole.local	172.17.16.253	172.16.16.0/24

Host Name	Source Gateway	Target Network
mgmt01esx52.lax01.rainpole.local	172.17.16.253	172.16.16.0/24
mgmt01esx53.lax01.rainpole.local	172.17.16.253	172.16.16.0/24
mgmt01esx54.lax01.rainpole.local	172.17.16.253	172.16.16.0/24

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

Setting	Value
User name	root
Password	<i>esxi_root_user_password</i>

- b Run the following command to create a route to the recovery region for the hosts in Region A or to the protected region for the hosts in Region B.

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

- c Repeat the step for all remaining ESXi hosts in the SFO01-Mgmt01 cluster in Region A and LAX01-Mgmt01 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
- NSX for vSphere
  - NSX Manager for the management cluster
  - NSX Manager for the shared compute and edge cluster
- vRealize Automation
- vRealize Operations Manager
- vRealize Log Insight

## 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 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 2-17. IP Addresses and Host Names for vSphere Data Protection in Region B**

Network Setting	Value
IP address	172.17.11.81
FQDN	mgmt01vdp51.lax01.rainpole.local
DNS servers	172.17.11.5, 172.16.11.4
Default gateway	172.17.11.253
Subnet mask	255.255.255.0

## Deployment Prerequisites

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

Prerequisite	Value
Initial Storage	<ul style="list-style-type: none"> <li>■ Virtual disk provisioning.               <ul style="list-style-type: none"> <li>■ Thin</li> </ul> </li> <li>■ Required storage               <ul style="list-style-type: none"> <li>■ 4 TB NFS</li> </ul> </li> </ul>
Software Features	<ul style="list-style-type: none"> <li>■ vSphere               <ul style="list-style-type: none"> <li>■ Management vCenter Server</li> <li>■ Management cluster with enabled DRS and HA.</li> <li>■ vSphere Distributed Switch configured for the vSphere management network</li> </ul> </li> </ul>
Installation Package	Download the .ova file of the vSphere Data Protection virtual appliance on the machine where you use the vSphere Web Client.

## 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the vSphere Web Client, navigate to the LAX01-Mgmt01 cluster object.

Inventory Object	Value
vCenter Server	mgmt01vc51.lax01.rainpole.local
Data center	LAX01
Cluster	LAX01-Mgmt01

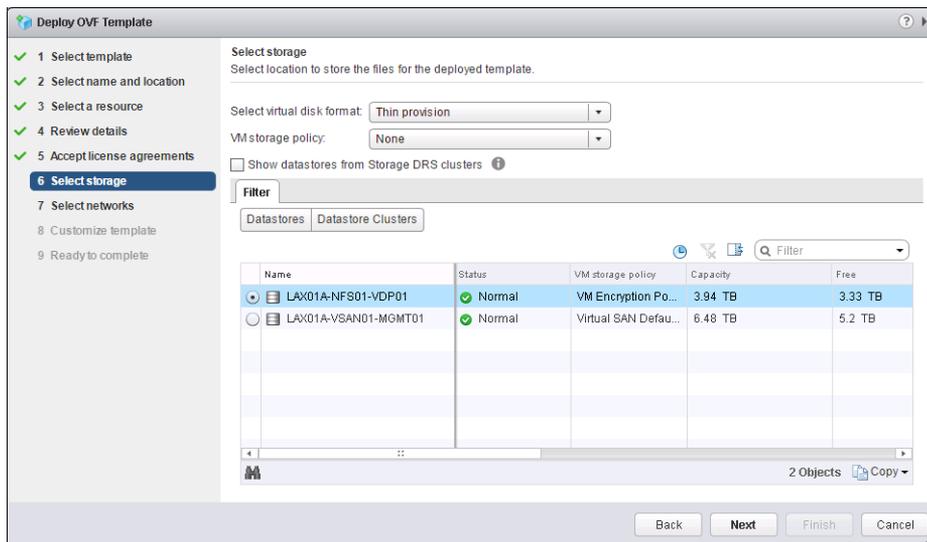
- 3 Right-click the **LAX01-Mgmt01** object and select **Deploy OVF Template**.
- 4 On the **Select template** page, select **Local file**, browse to the location of the vSphere Data Protection OVA file on your file system, and click **Next**.
- 5 On the **Select name and location** page, enter a node name, select the inventory folder for the virtual appliance, and click **Next**.

Setting	Value
Name	mgmt01vdp51
vCenter Server	mgmt01vc51.lax01.rainpole.local
Data center	LAX01

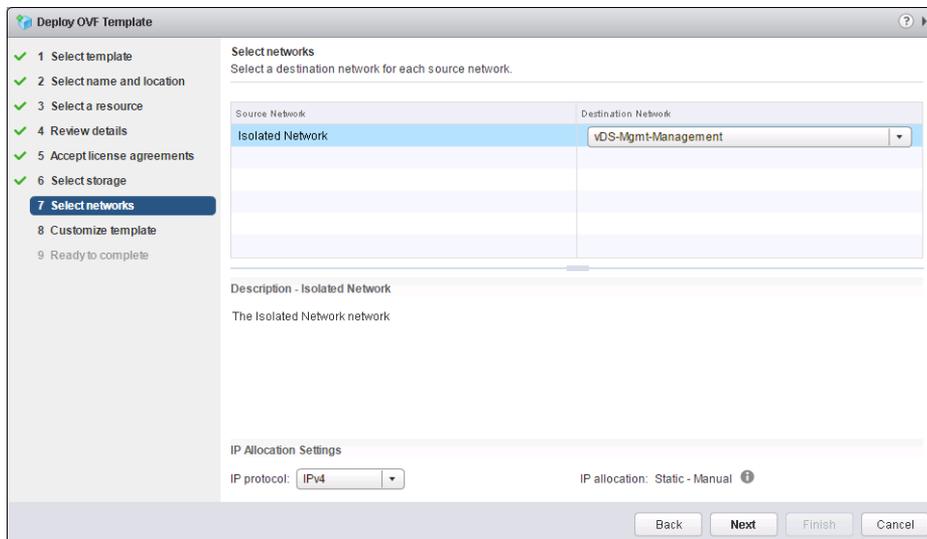
- 6 On the **Select a resource** page, click the **Browse** tab, select the **LAX01-Mgmt01** cluster, and click **Next**.
- 7 On the **Review details** page, examine the virtual appliance details, such as product, version, download size, and size on disk, and click **Next**.
- 8 On the **Accept license agreements** page, accept the end user license agreement and click **Next**.

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

Setting	Value
Datastore	LAX01A-NFS01-VDP01
Select virtual disk format	Thin provision
VM storage policy	None



- On the **Select networks** page, select the **vDS-Mgmt-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**.

IPv4 Setting	Value
Default gateway	172.17.11.253
DNS server	172.17.11.5, 172.17.11.4
Static IPv4 address	172.17.11.81
Subnet mask	255.255.255.0

- 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**.

## 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://mgmt01vdp51.lax01.rainpole.local:8543/vdp-configure`**.
  - b Log in using the following credentials.

Setting	Value
Username	root
Password	changeme

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: ~!@#,.)

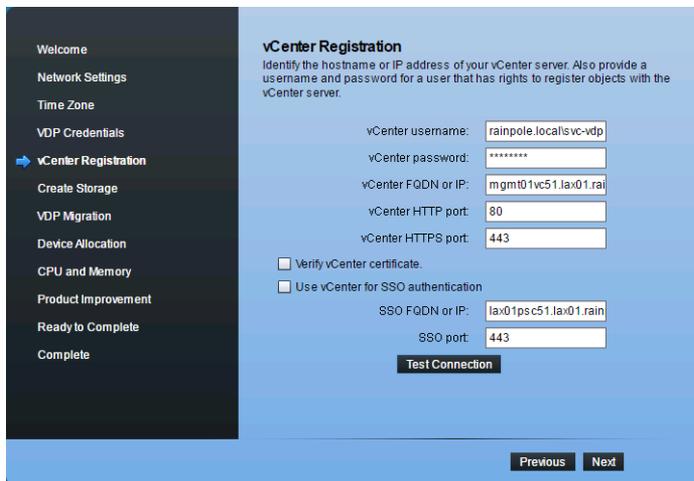
6 On the **vCenter Server Registration** page, configure the settings for registration with the Management vCenter Server.

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

vCenter Server Setting	Value
vCenter username	rainpole.local\svc-udp
vCenter password	svc-udp_password
vCenter FQDN or IP	mgmt01vc51.lax01.rainpole.local
vCenter HTTP port	80
vCenter HTTPS port	443
Verify vCenter Server certificate	Deselected

b Enter the settings for vCenter Single Sign-On on the Management Platform Services Controller.

Single Sign-On Setting	Value
Use vCenter for SSO authentication	Deselected
SSO FQDN or IP address	lax01psc51.lax01.rainpole.local
SSO port	443



- c Click **Test Connection** and in the **Connection success** message box, click **OK**.
- d On the *vCenter Registration* page, click **Next**.

- 7 On the **Create Storage** page, select **Create new storage**, in the **Capacity** text box enter 4 TiB, and click **Next**.
- 8 On the **Device Allocation** page, from the **Provision** drop-down menu select **Thin** and click **Next**.
- 9 On the **CPU and Memory** page, leave the default settings and click **Next**.
- 10 On the **Product Improvement** page, select **Enable Customer Experience Improvement Program** and click **Next**.
- 11 On the **Ready to Complete** page, select **Run performance analysis on storage configuration** and **Restart the appliance if successful**, and click **Next**.
- 12 In the warning message box about storage configuration, click **Yes**.  
vSphere Data Protection setup starts configuring data disks.
- 13 After disk configuration is complete, click **OK** in the success box.
- 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://mgmt01vc51.lax01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.
 

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password
  - 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:

Location	Replacement Order
Replace only in Region B	<ol style="list-style-type: none"> <li>1 Management Platform Services Controller</li> <li>2 Management vCenter Server</li> <li>3 Management NSX Manager</li> <li>4 Compute Platform Services Controller</li> <li>5 Compute vCenter Server</li> <li>6 Compute NSX Manager</li> <li>7 vSphere Data Protection</li> </ol>
Replace in both Region A and Region B	<ol style="list-style-type: none"> <li>1 Site Recovery Manager</li> <li>2 vSphere Data Protection</li> </ol>

## 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 certificates twice, once for each vCenter Server instance. You can start replacing certificates on Management vCenter Server `mgmt01vc51.lax01.rainpole.local` first.

**Table 2-18. Certificate-Related Files on the vCenter Server Instances**

vCenter Server FQDN	Files for Certificate Replacement	Replacement Order
mgmt01vc51.lax01.rainpole.local	<ul style="list-style-type: none"> <li>■ mgmt01vc51.lax01_ssl.key</li> <li>■ mgmt01vc51.lax01.1.cer</li> <li>■ chainRoot64.cer</li> </ul>	After you replace the certificate on the management Platform Services Controller.
comp01vc51.lax01.rainpole.local	<ul style="list-style-type: none"> <li>■ comp01vc51.lax01_ssl.key</li> <li>■ comp01vc51.lax01.1.cer</li> <li>■ chainRoot64.cer</li> </ul>	After you replace the certificate on the compute Platform Services Controller.

**Procedure**

- 1 Use the `scp` command, FileZilla, or WinSCP to copy the machine and CA certificate files to the `/tmp/ssl` directory on the Management vCenter Server.

Use the `scp` command, FileZilla, or WinSCP to copy the files.

- 2 Log in to the vCenter Server instance by using Secure Shell client.
  - a Open an SSH connection to the FQDN of the vCenter Server appliance.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vcenter_server_root_password</i>

- 3 Replace the CA-signed certificate on the vCenter Server instance.
  - a From the SSH client connected to the vCenter Server instance, add the Root certificate to the VMware Endpoint Certificate Store as a Trusted Root Certificate using following command and enter the vCenter Single Sign-On password when prompted.

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --chain --cert /tmp/ssl/chainRoot64.cer
```

- b Start the vSphere Certificate Manager utility on the vCenter Server instance.

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

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

vCenter Server	IP Address of Connected Platform Services Controller
mgmt01vc51.lax01.rainpole.local	172.17.11.61
comp01vc51.lax01.rainpole.local	172.17.11.63

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

vCenter Server	Path to Certificate-Related Files
mgmt01vc51.lax01.rainpole.local	Please provide valid custom certificate for Machine SSL. File: <code>/tmp/ssl/mgmt01vc51.lax01.1.cer</code> Please provide valid custom key for Machine SSL. File: <code>/tmp/ssl/mgmt01vc51.lax01.key</code> Please provide the signing certificate of the Machine SSL certificate File: <code>/tmp/ssl/chainRoot64.cer</code>
comp01vc51.lax01.rainpole.local	Please provide valid custom certificate for Machine SSL. File: <code>/tmp/ssl/comp01vc51.lax01.1.cer</code> Please provide valid custom key for Machine SSL. File: <code>/tmp/ssl/comp01vc51.lax01.key</code> Please provide the signing certificate of the Machine SSL certificate File: <code>/tmp/ssl/chainRoot64.cer</code>

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

```
Updated 21 service(s)
Status : 100% Completed [All tasks completed successfully]
```

- 5 After you replace the certificate on the mgmt01vc51.lax01.rainpole.local, repeat the procedure to replace the certificate on the compute vCenter Server comp01vc51.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 NSX Manager for the mgmt01nsxm51.lax01.rainpole.local management cluster.

**Table 2-19. Certificate-Related Files on the NSX Manager Instances in Region B**

NSX Manager FQDN	Certificate File Name	Replacement Time
mgmt01nsxm01.lax01.rainpole.local	<ul style="list-style-type: none"> <li>■ mgmt01nsxm51.lax01.chain.cer from manual generation</li> <li>■ mgmt01nsxm51.lax01.4.p12 from the CertGenVVD tool</li> </ul>	After you replace the certificate on the Management vCenter Server
comp01nsxm51.lax01.rainpole.local	<ul style="list-style-type: none"> <li>■ comp01nsxm51.lax01.cer.chain.cer from manual generation</li> <li>■ comp01nsxm51.lax01.4.p12 from the CertGenVVD tool</li> </ul>	After you replace the certificate on the Compute vCenter Server

**Procedure**

- 1 On the Windows host that has access to the data center, log in to the NSX Manager Web interface.
  - a Open a Web browser and go to following URL.

NSX Manager	URL
NSX Manager for the management cluster	https://mgmt01nsxm51.lax01.rainpole.local
NSX Manager for the shared compute and edge cluster	https://comp01nsxm51.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>nsx_manager_admin_password</i>

- 2 On the **Manage** tab, click **SSL Certificates**, click **Import** and provide the certificate chain file.
- 3 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**.
- 4 Re-register the NSX Manager to the Management vCenter Server.
  - a Open a Web browser and go to the NSX Manager Web interface.

NSX Manager	URL
NSX Manager for the management cluster	https://mgmt01nsxm51.lax01.rainpole.local
NSX Manager for the shared compute and edge cluster	https://comp01nsxm51.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>nsx_manager_admin_password</i>

- 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**.

Setting	Value
Lookup Service IP	lax01psc51.lax01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 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**.

Setting	Value for the NSX Manager for the Management Cluster	Value for the NSX Manager for the Shared Edge and Compute Cluster
vCenter Server	mgmt01vc51.lax01.rainpole.local	comp01vc51.lax01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local	
Password	svc-nsxmanager_password	

- 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.
- 5 Reconnect to the NSX Manager instances in Region A.
- a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local**
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 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 If primary and secondary nodes are not syncing correctly
- g Select **Actions > Disconnect from Primary NSX Manager**.
- h On the **Management** tab , select the **172.16.11.65** instance from the **NSX Manager** drop-down menu.
- i Select **Actions > Add Secondary NSX Manager**
- j In the **Add Secondary NSX Manager** dialog box, enter the following settings and click **OK**.

Setting	Value
NSX Manager	172.17.11.65
Username	admin
Password	mgmtnsx_admin_password
Confirm Password	mgmtnsx_admin_password

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

**6** Reconnect the NSX Manager instances to vRealize Operations Manager.

- a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- c In the left pane of vRealize Operations Manager, click **Administration** and click **Certificates**.
- d Select the row that contains CN=mgmt01nsxm51.lax01.rainpole.local and click the **Delete** icon.
- e Select the row that contains CN=comp01nsxm51.lax01.rainpole.local and click the **Delete** icon.
- f In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.
- g From the solution table on the **Solutions** page, select the **Management Pack for NSX-vSphere** solution, and click the **Configure** icon at the top.
- h In the **Manage Solutions** dialog box, from the **Adapter Type** table at the top, select **NSX-vSphere Adapter**.
- i Click the **mgmt01nsxm51-lax01** adapter instance, click **Test Connection**, accept the new certificate and click **Save settings**.
- j Click **comp01nsxm51-lax01** adapter instance, click **Test Connection**, accept the new certificate and click **Save settings**.

## Replace the VMware Site Recovery Manager Certificates

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

You replace certificates twice, once for each Site Recovery Manager. You will begin by replacing certificates on mgmt01srm01.sfo01.rainpole.local, the Site Recovery Manager in Region A.

**Table 2-20. Certificate-Related Files for Site Recovery Manager in Region A and Region B**

File Name	Site Recovery Manager in Region A	Site Recovery Manager in Region B
CA Certificate Chain	CACert.chain.cer	CACert.chain.cer
PKCS#12 File Name from Manual Generation	mgmt01srm01.sfo01.p12	mgmt01srm51.lax01.p12
PKCS#12 File Name from the CertGenVVD tool	mgmt01srm01.sfo01.5.p12	mgmt01srm51.lax01.5.p12

**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	mgmt01srm01.sfo01.rainpole.local
Region B	mgmt01srm51.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	windows_administrator_password

- 2 Install the CA certificates in the Windows trusted root certificate store of the Site Recovery Manager virtual machine.
  - a Locate CACert.chain.cer file in C:\certs folder.
  - b Double-click the CACert.chain.cer file 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 the **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 the one that you generated manually or by using the CertGenVVD tool.
  - 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 C:\certs, select the mgmt01srm01.sfo01.p12 or mgmt01srm51.lax01.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.

Region	URL
Region A	https://mgmt01vc01.sfo01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- c In the vSphere Web Client, click **Site Recovery > Sites**.
  - d Right-click the site **mgmt01vc01.sfo01.rainpole.local** and select **Reconfigure Pairing**.
  - e Enter the address of the Platform Services Controller **lax01psc51.lax01.rainpole.local** on the remote site and click **Next**.
  - f Select the vCenter Server instance **mgmt01vc51.lax01.rainpole.local** with which Site Recovery Manager is registered on the remote site, enter the vCenter Single Sign-On administrator user name **administrator@vsphere.local** and **vsphere\_admin\_password** password, and click **Finish**.
- 5 Repeat the steps to generate a CA-signed certificate and replace the default VMware-signed certificate with this one on mgmt01srm51.lax01.rainpole.local.

## Replace the vSphere Replication Certificates

After you replace the certificates of all Platform Services Controllers, vCenter Server instances and NSX Managers, and of the Site Recovery Manager instances, replace the certificates on vSphere Replication in Region A and Region B

A vSphere Replication appliance uses certificate-based authentication for all connections that it establishes with vCenter Server instances and remote site vSphere Replication instances. vSphere Replication does not use user name and password based authentication. vSphere Replication generates a standard SSL certificate when the appliance first boots and registers with vCenter Server. The default certificate policy uses trust by thumbprint. You change the certificate by using the virtual appliance management interface (VAMI) of the vSphere Replication appliance.

If you use the CertGenVVD tool, you skip creating a CSR file and a certificate signed by the Microsoft CA on the child AD server in Region A.

## Install the CA-Signed Certificate on vSphere Replication

After you generate a CA-signed PKCS#12 file manually or by using the CertGenVVD tool, replace the default VMware-signed certificate with this certificate on vSphere Replication in both regions.

You create certificates twice, once for each vSphere Replication. You can start replacing certificates on vSphere Replication in Region A `mgmt01vrms01.sfo01.rainpole.local` first.

**Table 2-21. PKCS#12 Files for vSphere Replication in Region A and Region B**

vSphere Replication Appliance Name	PKCS#12 File Name from Manual Generation	PKCS#12 File Name from the CertGenVVD Tool
mgmt01vrms01.sfo01.rainpole.local	mgmt01vrms01.sfo01.p12	mgmt01vrms01.sfo01.5.p12
mgmt01vrms51.lax01.rainpole.local	mgmt01vrms01.lax01.p12	mgmt01vrms51.lax01.5.p12

### Prerequisites

If you use the CertGenVVD tool to generate CA-signed certificates for the products in this validated design, generate the PEM file for vRealize Operations Manager and download it to your computer. See [VMware Knowledge Base article 2146215](#).

### Procedure

- 1 Upload the PKCS#12 file to vSphere Replication by using the vSphere Replication Appliance interface (VAMI).
  - a Open a Web browser and go to the following URL.

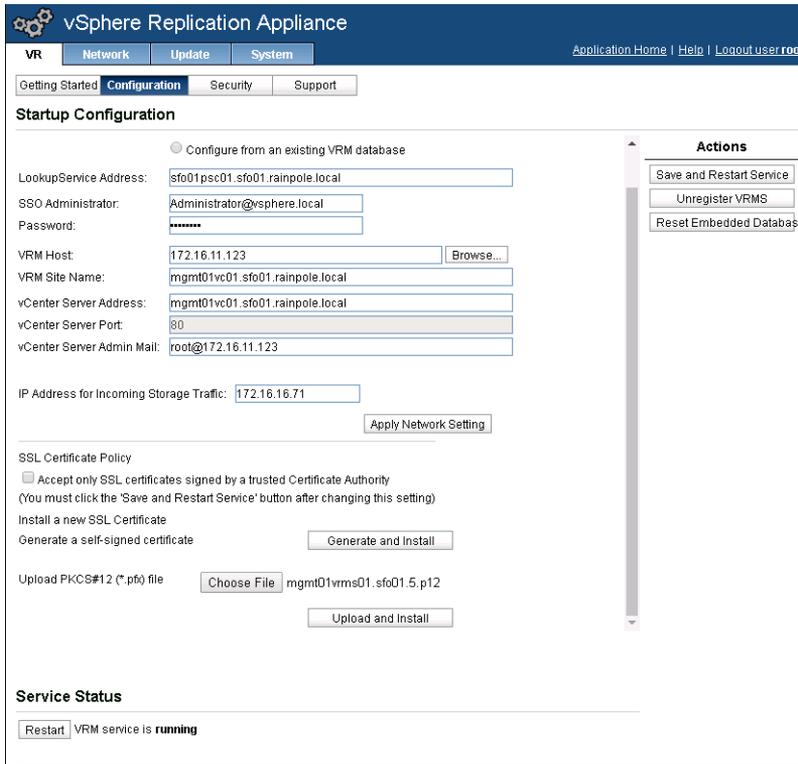
vSphere Replication	URL
vSphere Replication in Region A	<a href="https://mgmt01vrms01.sfo01.rainpole.local:5480">https://mgmt01vrms01.sfo01.rainpole.local:5480</a>
vSphere Replication in Region B	<a href="https://mgmt01vrms51.lax01.rainpole.local:5480">https://mgmt01vrms51.lax01.rainpole.local:5480</a>

- b Log in using the following credentials.

Setting	Value
User name	root
Password	<code>vr_root_password</code>

- c On the **VR** tab, click the **Configuration** tab.

- d Enter the vCenter Single Sign-On administrator password *vsphere\_admin\_password*.
- e Click **Choose File** next to **Upload PKCS#12 (\*.pfx)** file and locate the PKCS#12 file that you created.



- 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.

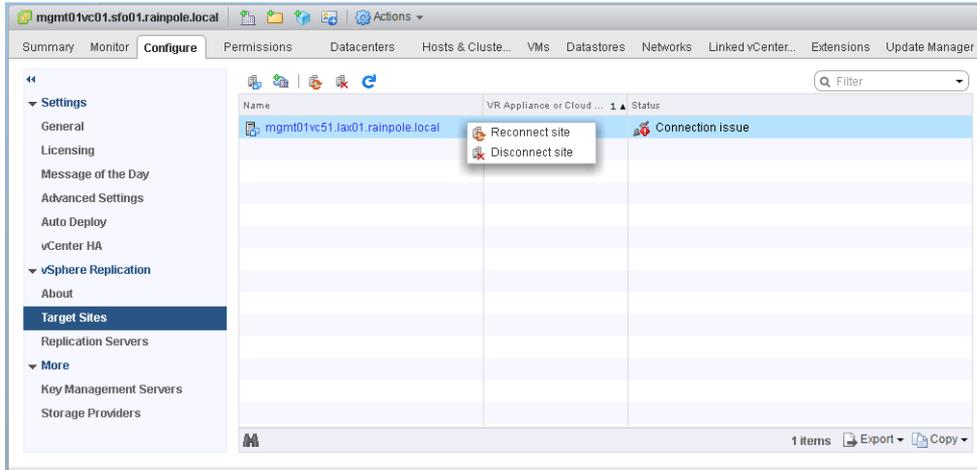
When you change the SSL certificate, the vSphere Replication status changes to disconnected state because new certificate is not validated by the vSphere Replication instance in other site.

- a Open a Web browser and go to **https://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- c On the vSphere Web Client **Home** page, click **vSphere Replication**.
- d Select **mgmt01vc01.sfo01.rainpole.local**, click **Manage**, and select **Target Sites**.

- e Right-click **mgmt01vc51.lax01.rainpole.local** and click **Reconnect site**.
- f In the **Reconnect Sites** dialog box, click **Yes** to proceed.



- 3 Repeat the steps to generate and install the CA-signed certificate on the other vSphere Replication instance.

## Install a CertGenVVD-Generated Certificate on vSphere Data Protection 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 Copy the .keystore file that CertGenVVD tool generated to the /root folder on the vSphere Data Protection virtual appliance.

You can use scp, FileZilla or WinSCP.

- 2 Log in to the vSphere Data Protection appliance.
  - a Open an SSH connection to the virtual machine **mgmt01vdp51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vdp_root_password

- 3 Restart all vSphere Data Protection services by running the following commands.

```
dpnctl stop all
dpnctl start all
```

- 4 Run the `addFingerprint.sh` script to update the vSphere Data Protection server thumbprint displayed in the VM console welcome screen.

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

# Region B Cloud Management Platform Implementation

# 3

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.

This chapter includes the following topics:

- [Prerequisites for Cloud Management Platform Implementation in Region B](#)
- [Configure Service Account Privileges in Region B](#)
- [vRealize Automation Installation in Region B](#)
- [vRealize Orchestrator Configuration in Region B](#)
- [vRealize Business Installation in Region B](#)
- [Create Anti-Affinity Rules for vRealize Automation Proxy Agent Virtual Machines in Region B](#)
- [Content Library Configuration in Region B](#)
- [Tenant Content Creation in Region B](#)

## 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 vRA Proxy Agents and vRB Data Collector in Region B**

Role	IP Address	FQDN
vRealize Automation Proxy Agents	192.168.32.52	vra01ias51.lax01.rainpole.local
	192.168.32.53	vra01ias52.lax01.rainpole.local
vRealize Business Data Collector	192.168.32.54	vra01buc51.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	
	172.17.11.251	ntp.lax01.rainpole.local
	172.17.11.252	

## 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.

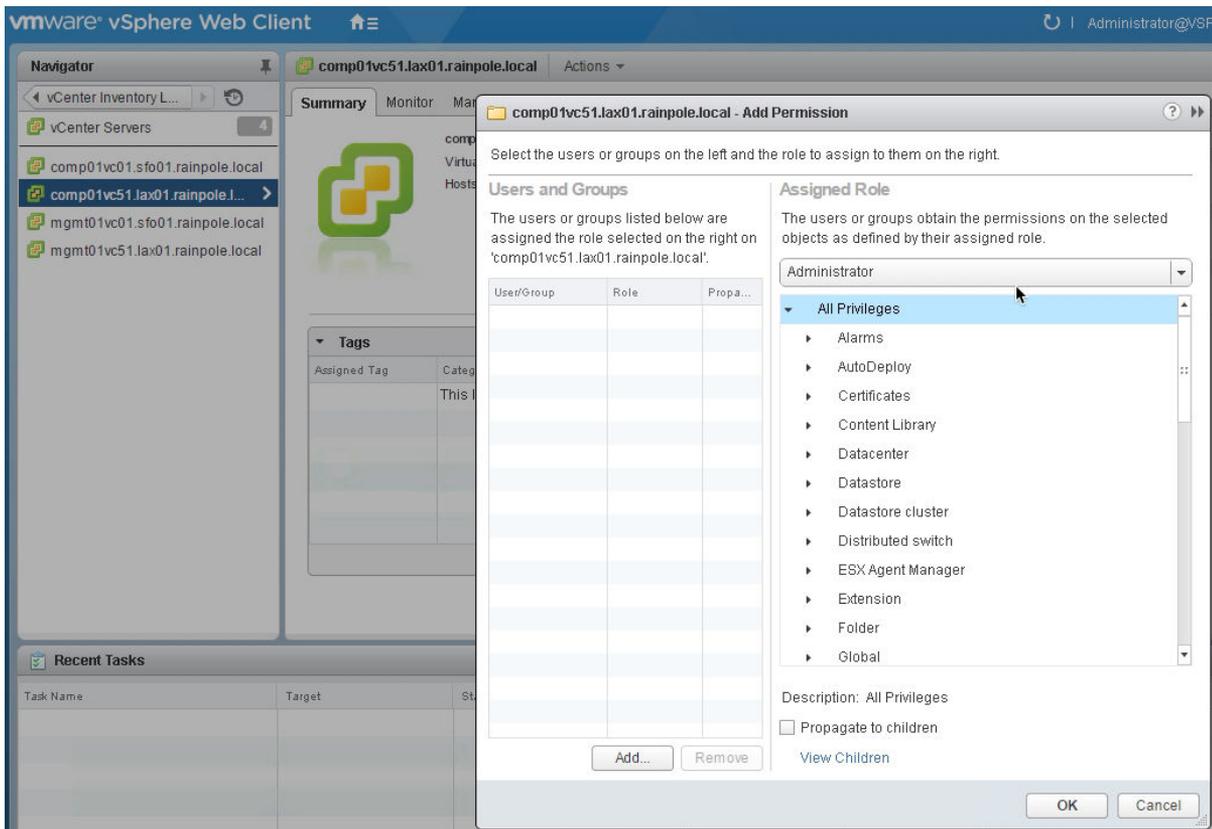
**Procedure**

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://comp01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

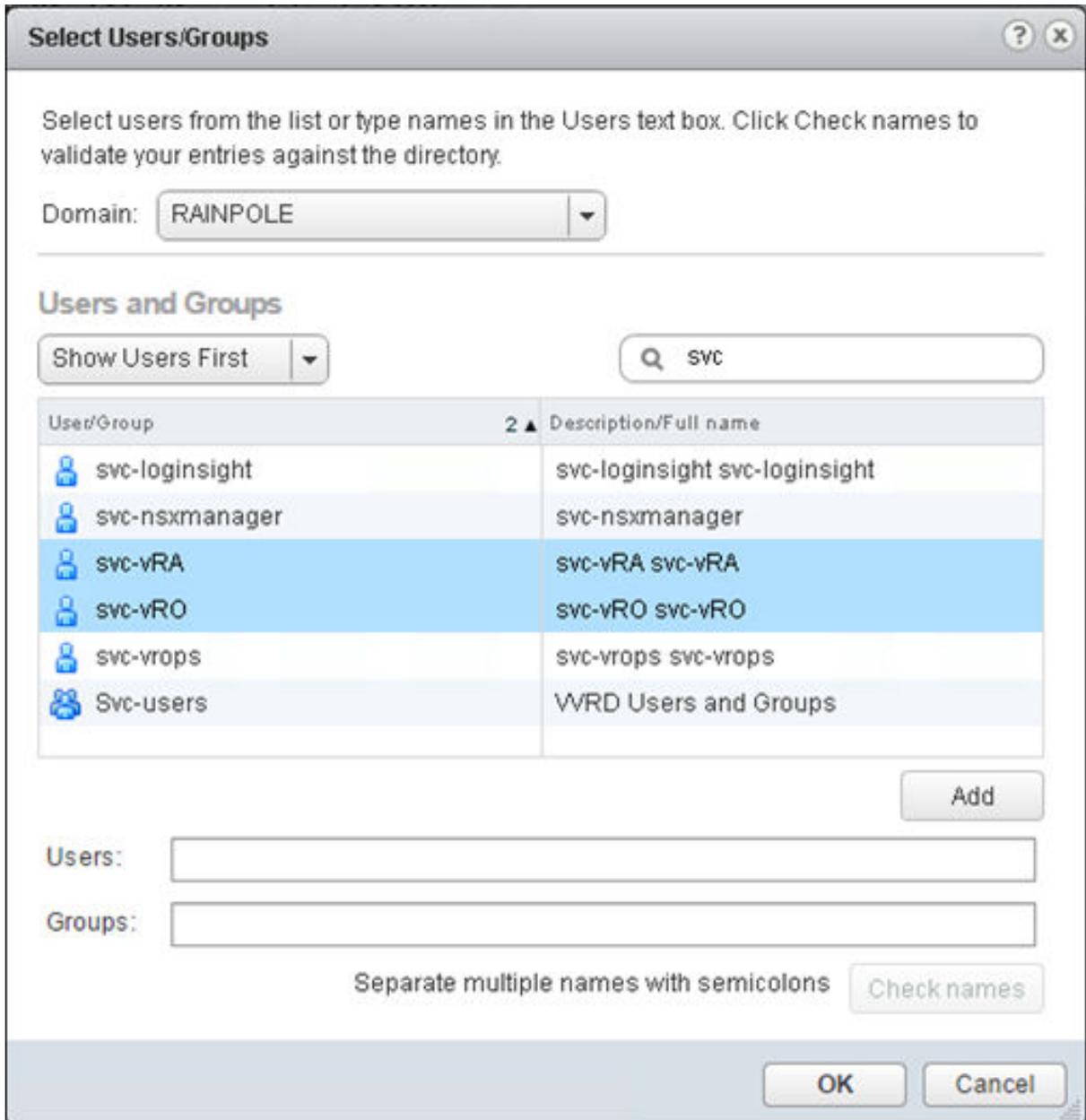
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator pane, select **vCenter Inventory Lists > vCenter Servers**.
- 3 Right-click the **comp01vc51.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.

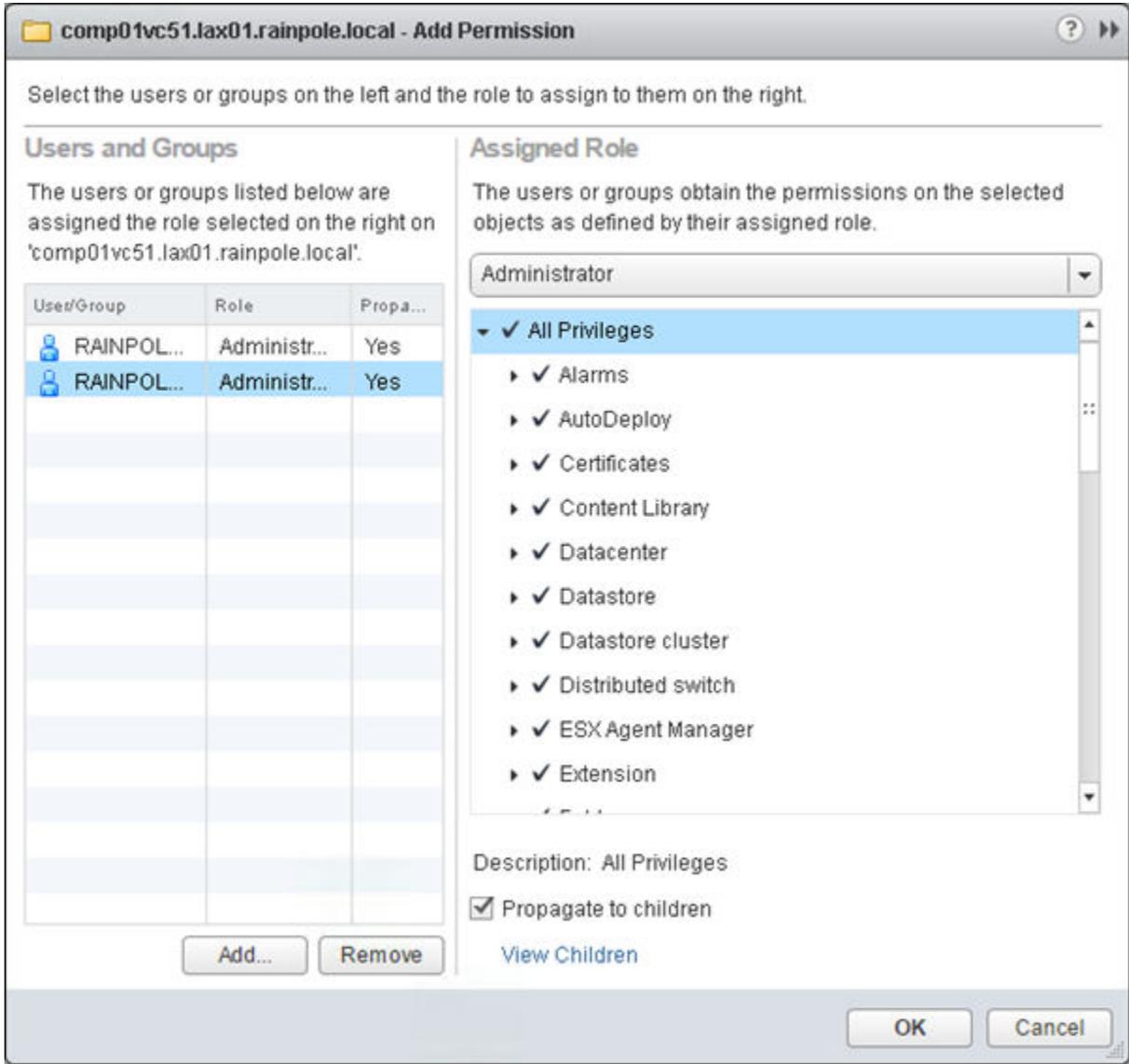


- 5 Select **RAINPOLE** from the **Domain** drop-down menu, and in the **Show Users First** text box enter **svc** to filter user and group names.
- 6 Select **svc-vra** and **svc-vro** from the **User/Group** list, click the **Add** button and click **OK**.



- 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.

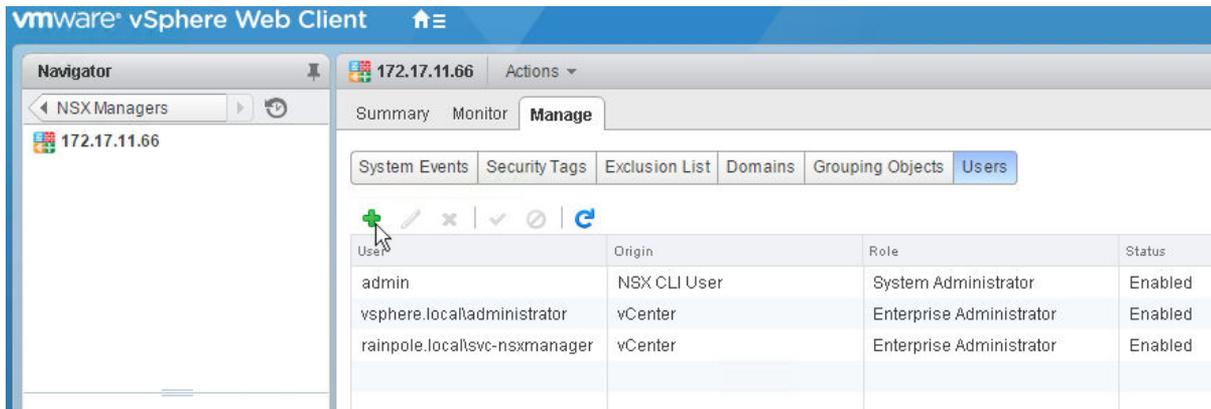
**Procedure**

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://comp01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

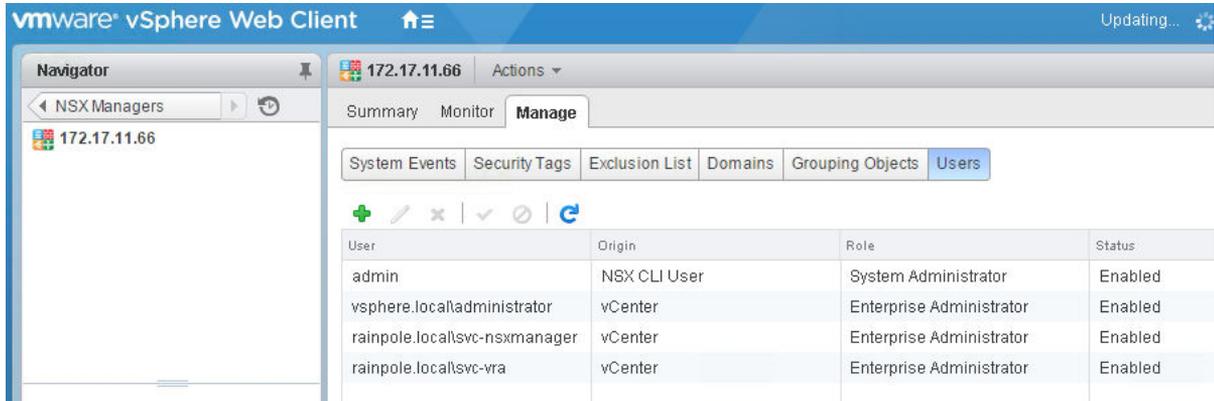
- 2 In the **Navigator** pane, select **Networking & Security > NSX Managers**.
- 3 Double-click the **172.17.11.66** Compute NSX Manager.
- 4 Click **Manage**, click **Users**, and click the **Add** icon.

The **Assign Role** wizard appears.



- 5 On the **Identify User** page, select the **Specify a vCenter User** radio button, enter **svc-vra@rainpole.local** in the **User** text box, and click **Next**.
- 6 On the **Select Roles** page, select the **Enterprise Administrator** radio button, and click **Finish**.

The svc-vra@rainpole.local user is now configured as an **Enterprise Administrator** for the compute cluster NSX instance, and appears in the lists of users and roles.



## 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://mgmt01vc51.lax01.rainpole.local/vsphere-client>.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 Click **Networking & Security**.

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

4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **LAXMGMT-LB01** NSX Edge to edit its network settings.

5 Click the **Manage** tab, click **Settings**, and select **Interfaces**.

- 6 Select the **OneArmLB** interface and click the **Edit** icon.
- 7 In the **Edit NSX Edge** Interface dialog box, add the VIP addresses of the vRealize Automation nodes in the **Secondary IP Addresses** text box.

**Note** The **Connectivity Status** should remain as **Disconnected**.

Setting	Value
Secondary IP Address	192.168.11.53,192.168.11.56,192.168.11.59,192.168.11.65

Edit NSX Edge Interface ?

vNIC#: 0

Name: \* OneArmLB

Type: Internal

Connected To: Mgmt-xRegion01-VXLAN Change Remove

Connectivity Status:  Connected  Disconnected

Configure Subnets:

+ ✂ ✖
Filter

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
192.168.11.2 ✖	.11.53,192.168.11.56,192.168.11.59,192.168.11.65 ✖	24 ✖

*Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.1.2,1.1.1.3*

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU:

Options:  Enable Proxy ARP  Send ICMP Redirect

Reverse Path Filter

Fence Parameters:

Example: ethernet0.filter1.param1=1

- 8 Click **OK** to save the configuration.

## Create Application Profiles in Region B

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

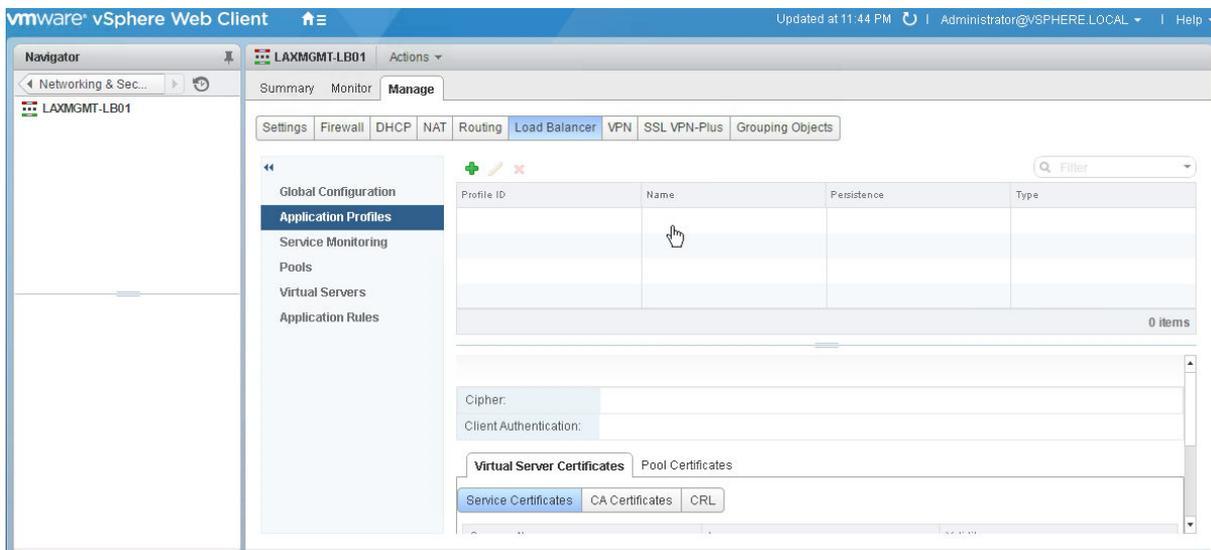
You repeat this procedure twice to create two application profiles.

### Procedure

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **LAXMGMT-LB01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Application Profiles**.



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

Setting	Value
Name	vRealize-https-persist
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	Source IP
Expires in (Seconds)	1800

**New Profile**

Name:

Type:

Enable SSL Passthrough

HTTP Redirect URL:

Persistence:

Cookie Name:

Mode:

Expires in (Seconds):

Insert X-Forwarded-For HTTP header

Enable Pool Side SSL

Virtual Server Certific... Pool Certificates

Service Certificates CA Certificates CRL

Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	VSM_SOLUTION_1744	VSM_SOLUTION_1744	Tue Nov 29 2016 - Thu Nc
<input type="radio"/>	VSM_SOLUTION_1744	VSM_SOLUTION_1744	Tue Nov 29 2016 - Thu Nc
<input type="radio"/>	VSM_SOLUTION_2c77	VSM_SOLUTION_2c77	Tue Nov 29 2016 - Thu Nc
<input type="radio"/>	VSM_SOLUTION_2c77	VSM_SOLUTION_2c77	Tue Nov 29 2016 - Thu Nc
<input type="radio"/>	sfo01psc01.sfo01.rainp	rainpole-DC01RPL-CA	Tue Nov 29 2016 - Thu Nc

Cipher:

Client Authentication:

OK Cancel

- 7 Click **OK** to save the configuration.
- 8 Repeat the same steps to create the following application profile.

Setting	Value
Name	vRealize-https
Type	HTTPS

Setting	Value
Enable SSL Passthrough	Selected
Persistence	None

## Create Service Monitoring in Region B

The service monitor defines health check parameters for the load balancer. You create a service monitor for each component.

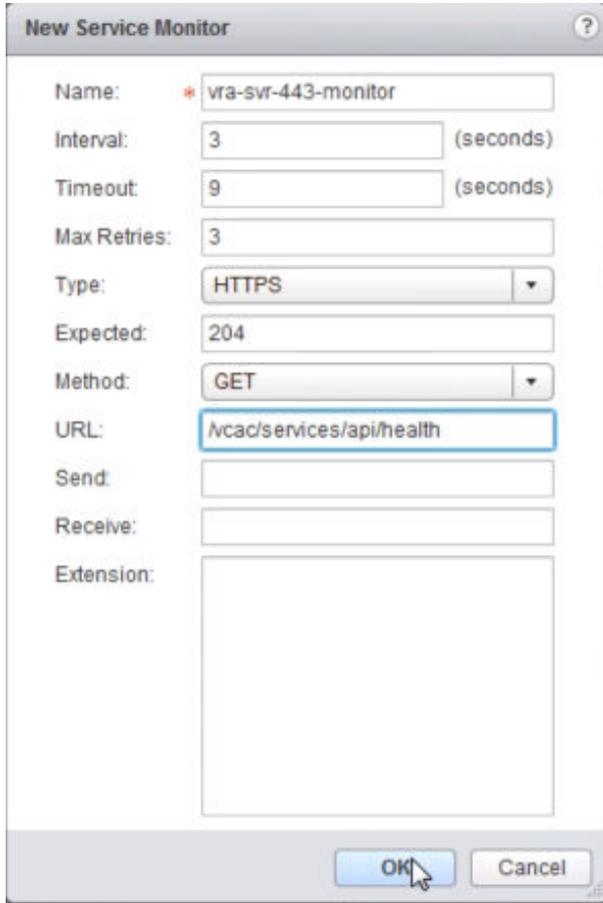
### Procedure

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://mgmt01vc51.lax01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **LAXMGMT-LB01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Service Monitoring**.
- 6 Click the **Add** icon and in the **New Service Monitor** dialog box, configure the values for the service monitor you are adding, and click **OK**.

Setting	vra-svr-443-monitor	vra-iaas-web-443-monitor	vra-iaas-mgr-443-monitor	vra-vro-8281-monitor
Name	vra-svr-443-monitor	vra-iaas-web-443-monitor	vra-iaas-mgr-443-monitor	vra-vro-8281-monitor
Interval	3	3	3	3
Timeout	9	9	9	9
Max Retries	3	3	3	3
Type	HTTPS	HTTPS	HTTPS	HTTPS
Expected	204			
Method	GET	GET	GET	GET
URL	/vcac/services/api/health	/wapi/api/status/web	/VMSPProvision	/vco/api/healthstatus
Receive		REGISTERED	ProvisionService	RUNNING



7 Repeat step 6 to create a service monitor for each component.

Upon completion, verify that you have successfully entered the monitor names and their respective configuration values.

### 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.

Repeat this procedure multiple five times to configure five different server pools.

**Table 3-2. Server Pools for the Cloud Management Platform in Region B**

Pool Name	Algorithm	Monitors	Members				Monitor Port	Weight
			Enable Member	Member Name	IP address	Port		
vra-svr-443	ROUND-ROBIN	NONE	Yes	vra01svr01a	192.168.11.51	443	443	1
			Yes	vra01svr01b	192.168.11.52			1
vra-iaas-web-443	ROUND-ROBIN	NONE	Yes	vra01iws01a	192.168.11.54	443	443	1
			Yes	vra01iws01b	192.168.11.55			1

**Table 3-2. Server Pools for the Cloud Management Platform in Region B (Continued)**

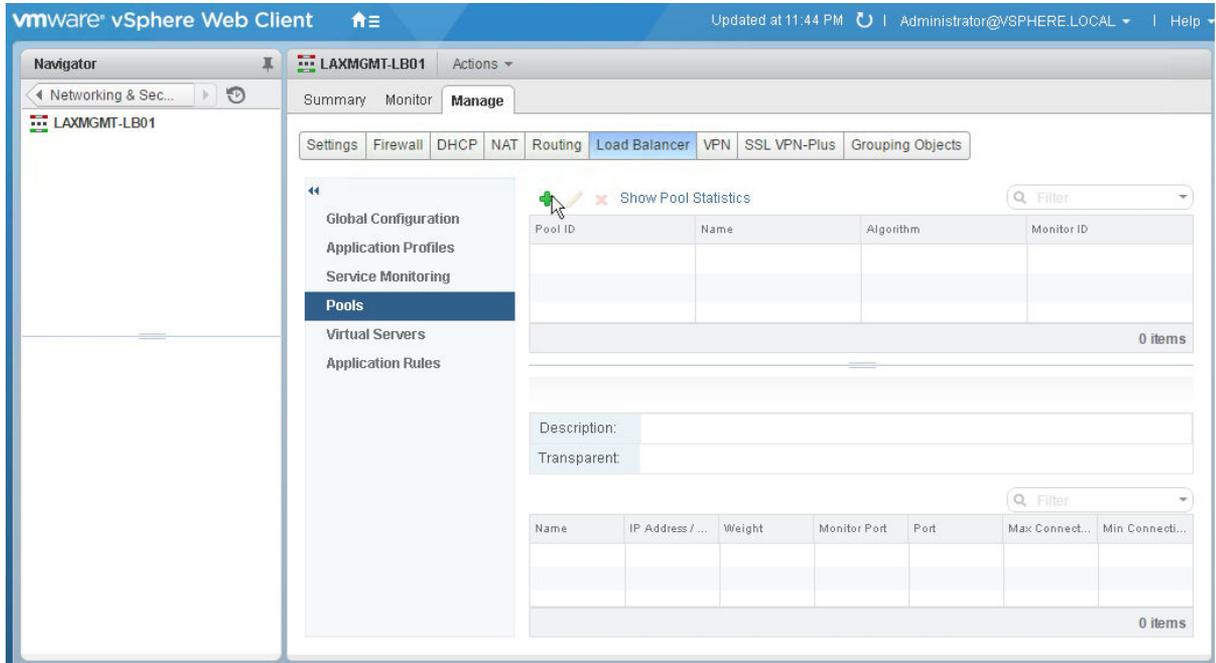
Pool Name	Algorithm	Monitors	Members				Port	Monitor Port	Weight
			Enable Member	Member Name	IP address	Port			
vra-iaas-mgr-443	ROUND-ROBIN	NONE	Yes	vra01ims01a	192.168.11.57	443	443	1	
			Yes	vra01ims01b	192.168.11.58			1	
vra-vro-8281	ROUND-ROBIN	NONE	Yes	vra01vro01a	192.168.11.63	8281	8281	1	
			Yes	vra01vro01b	192.168.11.64			1	
vra-svr-8444	ROUND-ROBIN	NONE	Yes	vra01svr01a	192.168.11.51	8444	443	1	
			Yes	vra01svr01b	192.168.11.52			1	

**Procedure**

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **LAXMGMT-LB01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.



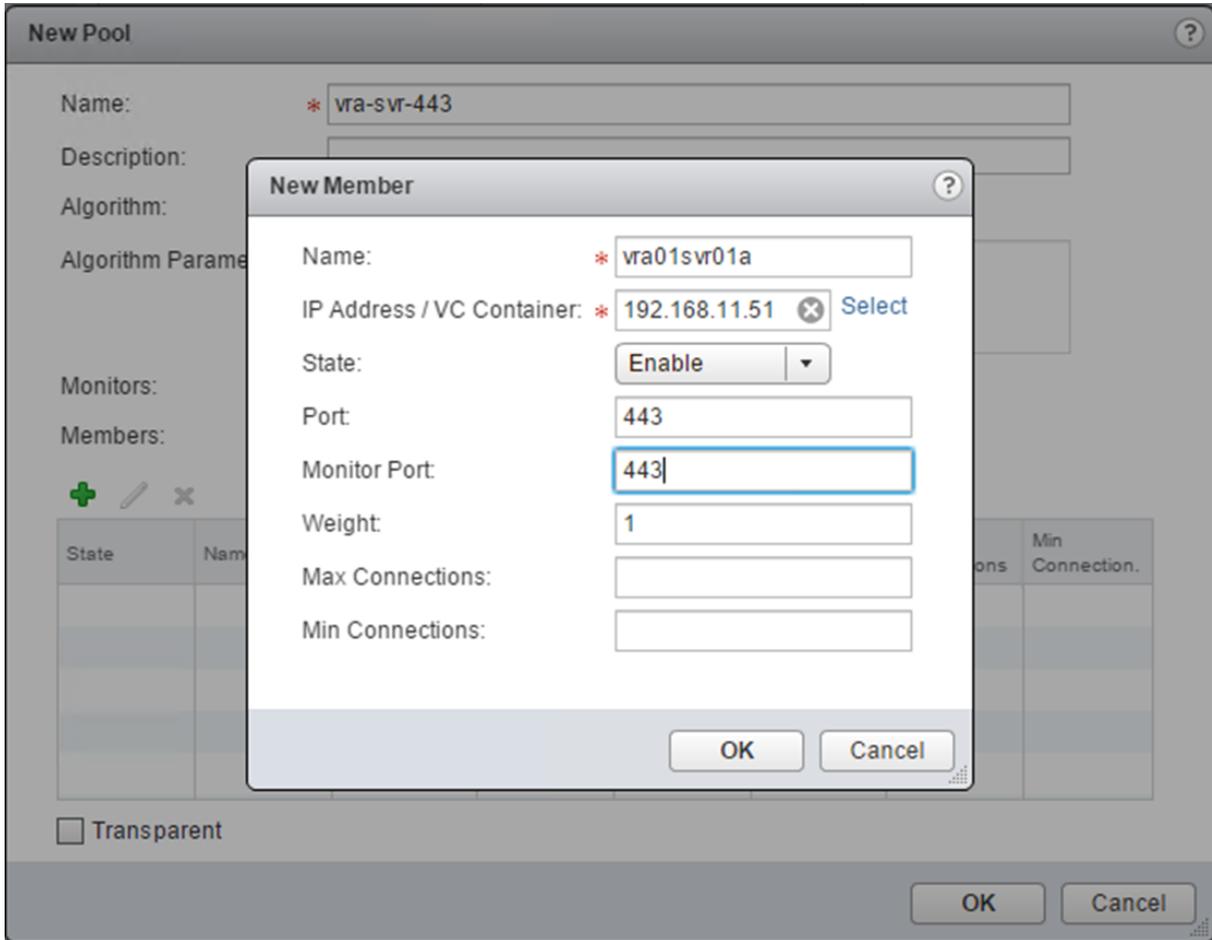
6 Click the **Add** icon, and in the **New Pool** dialog box configure the following values.

Setting	Value
Name	vra-svr-443
Algorithm	ROUND-ROBIN
Monitors	vra-svr-443-monitor

7 Under **Members**, click the **Add** icon to add the first pool member.

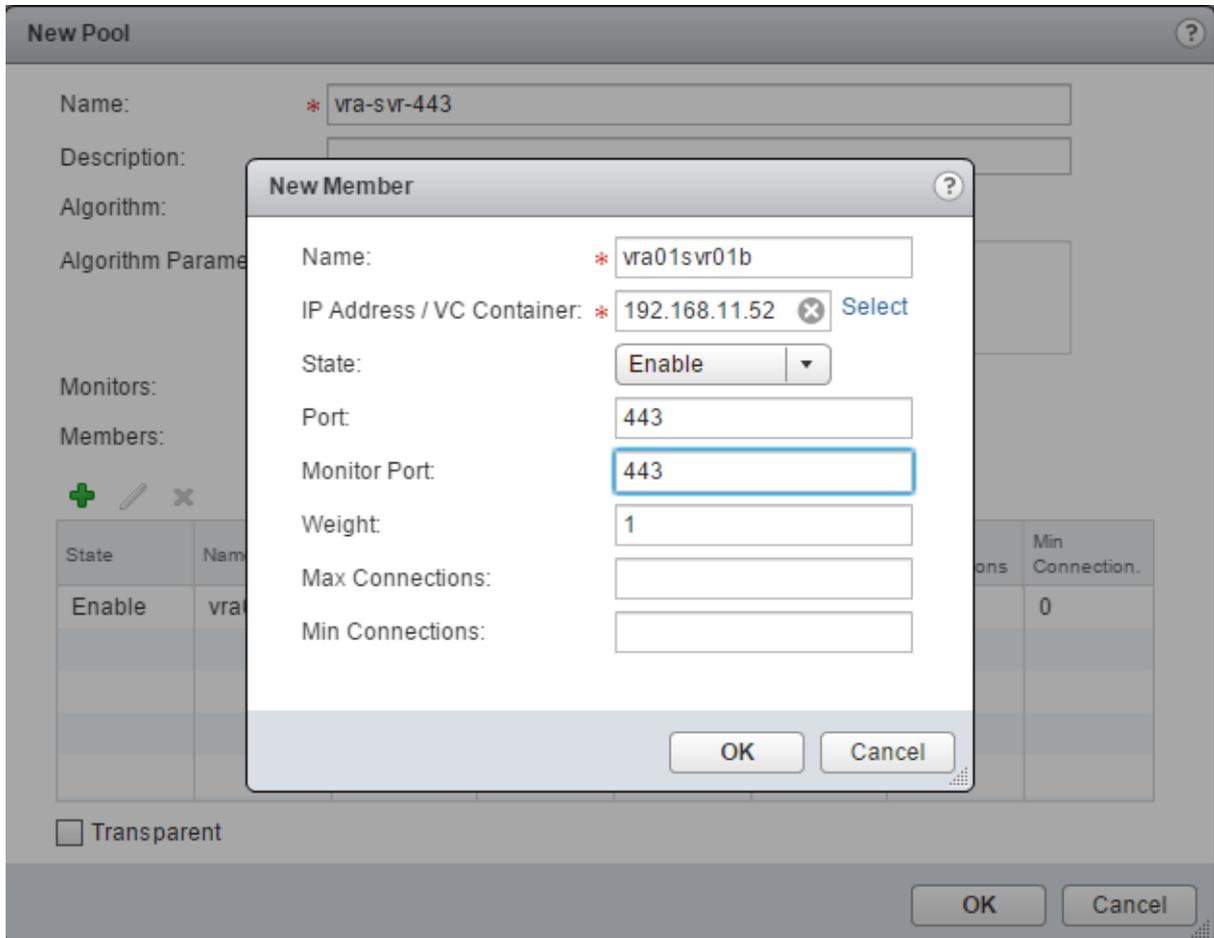
8 In the **New Member** dialog box configure the following values, and click **OK**.

Setting	Value
Name	vra01svr01a
IP Address/VC Container	192.168.11.51
State	Enable
Port	443
Monitor Port	443
Weight	1



- 9 Under **Members**, click the **Add** icon to add the second pool member.
- 10 In the **New Member** dialog box, configure the following values, click **OK**, and click **OK** again to save the vRealize Automation server pool.

Setting	Description
Name	vra01svr01b
IP Address/VC Container	192.168.11.52
State	Enabled
Port	443
Monitor Port	443
Weight	1



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.

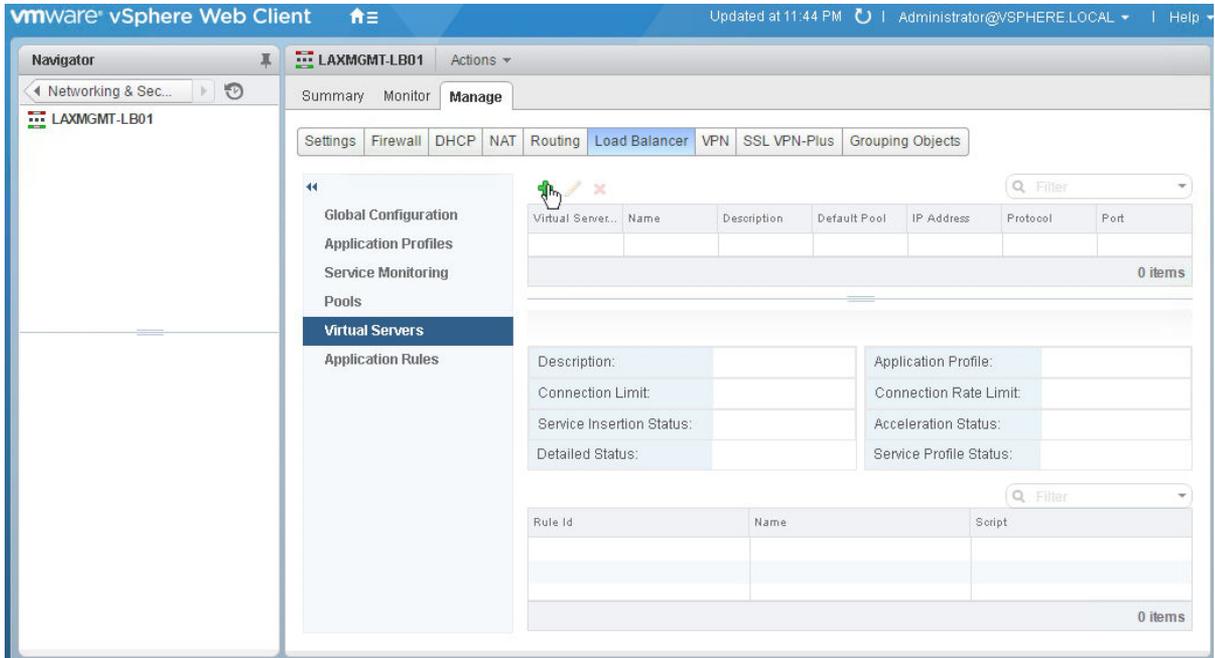
### Procedure

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://mgmt01vc51.lax01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click **Networking & Security**.

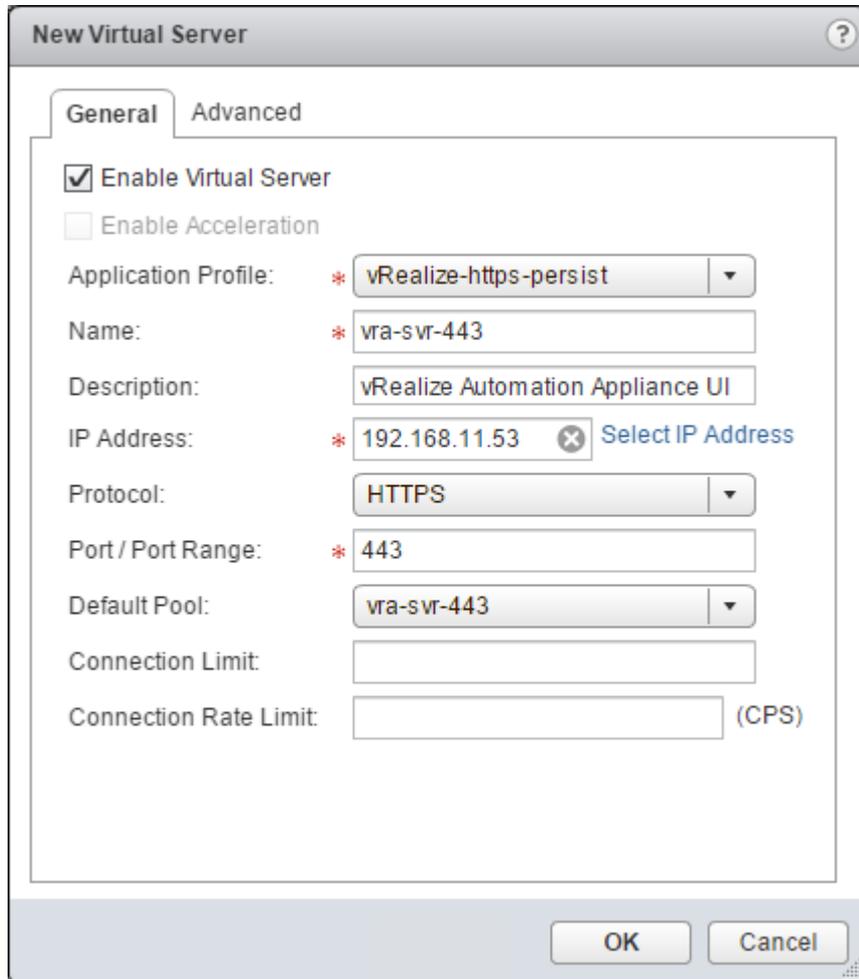
- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **LAXMGMT-LB01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Virtual Servers**.



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

Setting	vra-svr-443	vra-iaas-web-443	vra-iaas-mgr-443	vra-vro-8281	vra-svr-8444
Enable Virtual server	Selected	Selected	Selected	Selected	Selected
Application Profile	vRealize-https-persist	vRealize-https - persist	vRealize-https	vRealize-https	vRealize-https-persist
Name	vra-svr-443	vra-iaas-web-443	vra-iaas-mgr-443	vra-vro-8281	vra-svr-8444
Description	vRealize Automation Appliance UI	vRealize Automation IaaS Web UI	vRealize Automation IaaS Manager	vRealize Automation Orchestrator	vRealize Automation Remote Console Proxy
IP Address	192.168.11.53	192.168.11.56	192.168.11.59	192.168.11.65	192.168.11.53
Protocol	HTTPS	HTTPS	HTTPS	HTTPS	HTTPS

Setting	vra-svr-443	vra-iaas-web-443	vra-iaas-mgr-443	vra-vro-8281	vra-svr-8444
Port	443	443	443	8281	8444
Default Pool	vra-svr-443	vra-iaas-web-443	vra-iaas-mgr-443	vra-vro-8281	vra-svr-8444



- 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.

## 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

- [Create a Customization Specification for IaaS Proxy Agent Servers in Region B](#)

Create a vSphere Image Customization template to use with your vRealize Automation IaaS Proxy Agent deployment.

## 2 Create Windows Virtual Machines for vRealize Automation in Region B

vRealize Automation requires several Windows virtual machines to act as IaaS components in a distributed configuration. These redundant components provide high availability for the vRealize Automation infrastructure features.

## 3 Install vRealize Automation Management Agent on Windows IaaS Virtual Machines in Region B

For each Windows virtual machine deployed as part of the vRealize Automation installation, a management agent must be deployed to facilitate the installation of the Windows dependencies and vRealize Automation components.

## Create a Customization Specification for IaaS Proxy Agent Servers in Region B

Create a vSphere Image Customization template to use with your vRealize Automation IaaS Proxy Agent deployment.

### Procedure

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** page, click **Customization Specification Manager**.
- 3 Select **mgmt01vc51.lax01.rainpole.local** from the **vCenter Server** drop-down menu.
- 4 Click the **New** icon.

The **New VMGuest Customization Spec** wizard opens.

- 5 On the **Specify Properties** page, configure the following settings, and click **Next**.

Setting	Value
Target VM Operating System	Windows
Use custom SysPrep answer file	Deselected
Customization Spec Name	vra7-proxy-agent-template

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

Setting	Value
Name	Rainpole
Organization	Rainpole IT

- 7 On the **Set Computer Name** page, select the **Enter a name in the Clone/Deploy wizard** radio button, and click **Next**.

- 8 On the **Enter Windows License** page, enter the following settings, and click **Next**.

If you are using **Microsoft License Server**, or have multiple single license keys, leave the **Product Key** text box blank.

Setting	Value
Product Key	<i>volume_license_key</i>
Include Server License Information	Selected
Server License Mode	Per seat

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

Setting	Value
Password	<i>local_administrator_pwd</i>
Automatically logon as Administrator	Selected
Number of times to logon automatically	1

- 10 On the **Time Zone** page, select **(GMT) Coordinated Universal Time** from the **Time Zone** drop down menu, and click **Next**.

- 11 On the **Run Once** page, type `net localgroup administrators rainpole\svc-vra /add` in the text box and click **Add**. This command will add service account rainpole\svc-vra into virtual machine's local administrators group. Click **Next**.

- 12 On the **Configure Network** page, select the **Manually select custom settings** radio button, select **NIC1** from the list of network interfaces in the virtual machine, and click **Edit**.

The **Network Properties** dialog box displays.

- 13 In the **Edit Network** dialog box, on the **IPv4** page, configure the following settings and click **DNS**.

Setting	Value
Prompt the user for an address when the specification is used	Selected
Subnet Mask	255.255.255.0
Default Gateway	192.168.32.1

14 On the **DNS** page, provide DNS servers and search suffixes.

- a Configure the following DNS server settings.

Setting	Value
Use the following DNS server address	Selected
Preferred DNS Server	172.17.11.4
Alternate DNS Server	172.17.11.5

- b Enter **rainpole.local** in the **For all connections with TCP/IP enabled** text box and click the **Add** button.
- c Enter **lax01.rainpole.local** in the **For all connections with TCP/IP enabled** text box and click the **Add** button.
- d Enter **sfo01.rainpole.local** in the **For all connections with TCP/IP enabled** text box and click the **Add** button.
- e Click **OK** to save settings and close the **Edit Network** dialog box, and click **Next**.

15 On the **Set Workgroup or Domain** page, enter credentials that have administrative privileges in the domain, and click **Next**.

Setting	Value
Windows Server Domain	lax01.rainpole.local
Username	ad_admin_acct@lax01.rainpole.local
Password	ad_admin_password

16 On the **Set Operating System** options page, select the **Generate New Security ID (SID)** check box, and click **Next**.

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

The customization specification you created is listed in the **Customization Specification Manager**, and can be used to customize virtual machine guest operating systems.

## Create Windows Virtual Machines for vRealize Automation in Region B

vRealize Automation requires several Windows virtual machines to act as IaaS components in a distributed configuration. These redundant components provide high availability for the vRealize Automation infrastructure features.

To facilitate cloning, this design uses the `vra7-proxy-agent-template` image customization specification template and the `windows-2012r2-64` VM template. Two virtual machines that run on Windows will be required to install vRealize Automation Proxy Agents in Region B. Repeat this procedure twice by using the information in the following table to create two VMs.

Name for Virtual Machines	NetBIOS name	vCenter Folder	IP	vCPU number	Memory Size	Image Customization Specification Template	Network
vra01ias51.lax01.rainpole.local	vra01ias51	vRA01IAS	192.168.32.52	2	4 GB	vra7-proxy-agent-template	vxw-dvs-xxxx-Mgmt-RegionB01-VXLAN
vra01ias52.lax01.rainpole.local	vra01ias52	vRA01IAS	192.168.32.53	2	4 GB	vra7-proxy-agent-template	vxw-dvs-xxxx-Mgmt-RegionB01-VXLAN

### Prerequisites

Verify that you have created the Windows 2012 R2 template VM windows2012r2-template. See *Virtual Machine Template Specifications*.

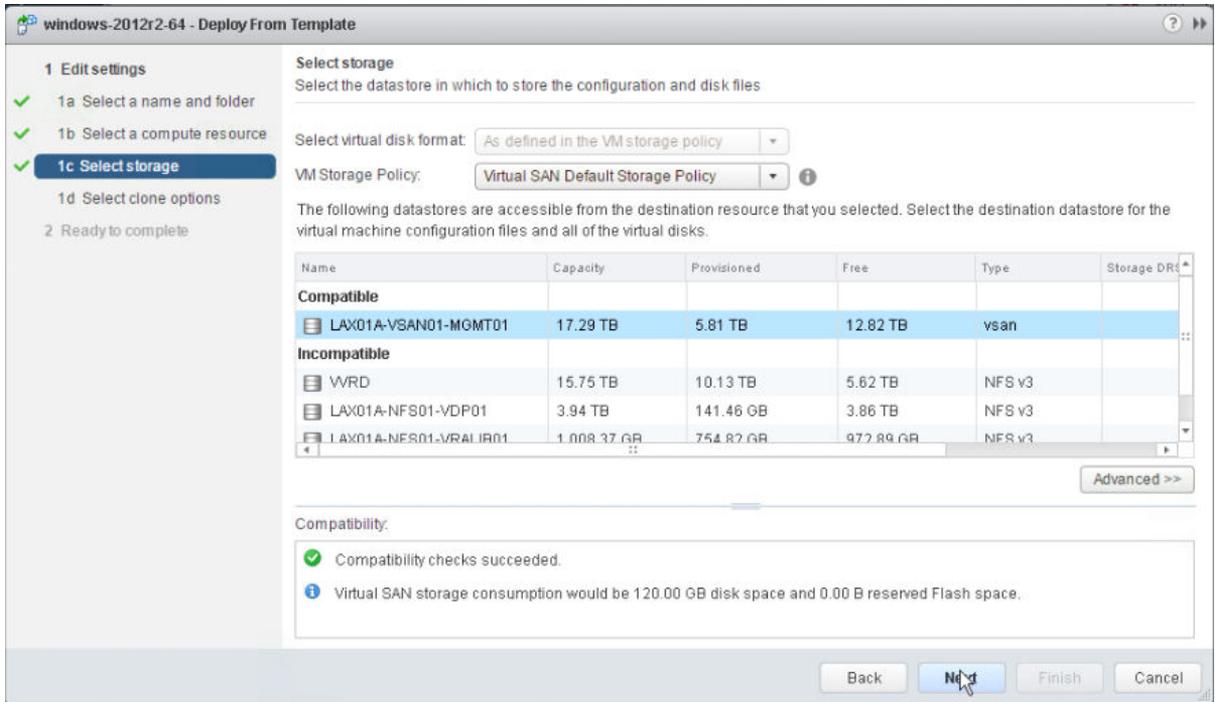
### Procedure

- 1 Log in to the vSphere Data Protection Configure Utility.
  - a Open a Web browser and go to **https://mgmt01vdp51.lax01.rainpole.local:8543/vdp-configure**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vdp_appliance_root_password

- 2 In the Navigator pane, select **Global Inventory Lists > vCenter Servers**. Click the **mgmt01vc51.lax01.rainpole.local** instance.
- 3 Select **VM Templates in Folders**, and from the VM Templates in Folders pane, right-click the IaaS windows template **win2012r2-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 **vra01ias51.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 **vRA01IAS** folder in the **LAX01** datacenter under **mgmt01vc51.lax01.rainpole.local**, and click **Next**.
- 5 On the **Select a compute resource** page, select **LAX01-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 **LAX01A-VSAN01-MGMT01** vSAN datastore from the datastore table and click **Next**.

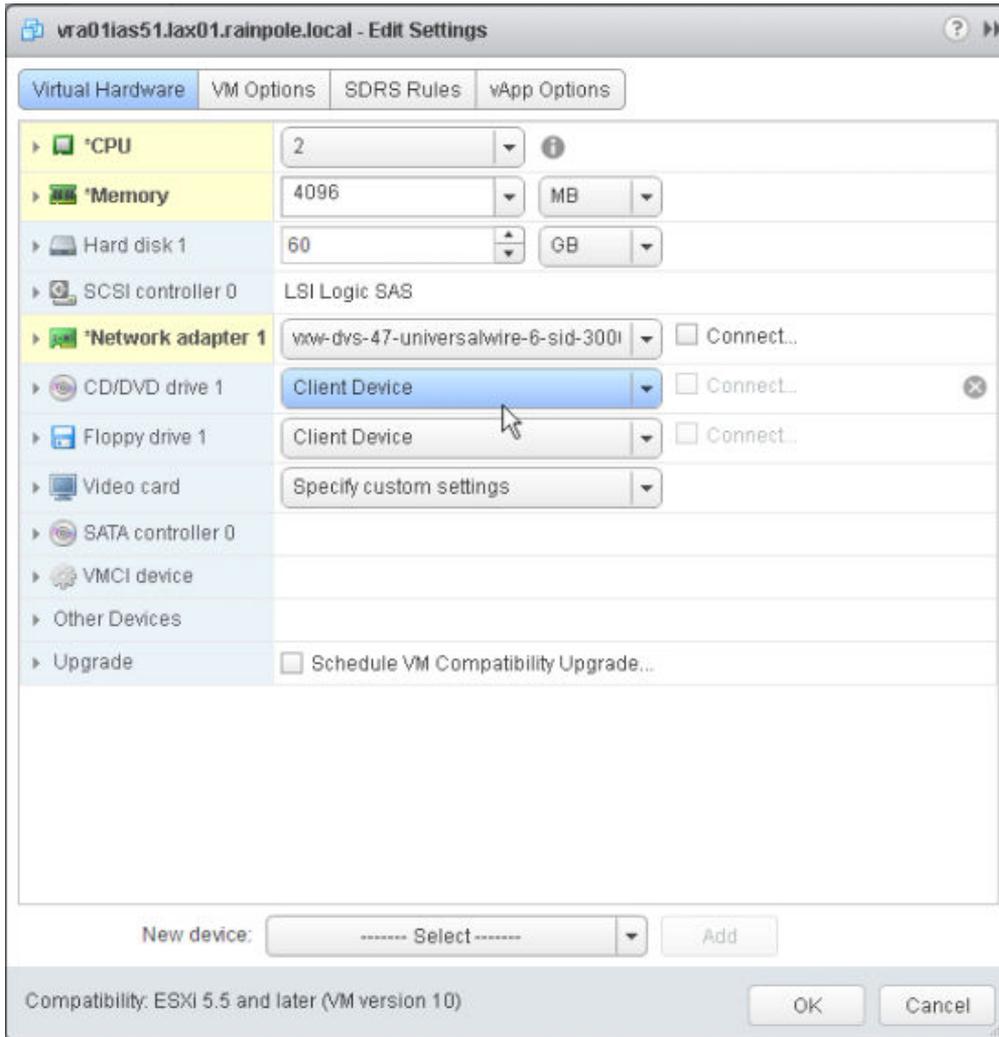


- 7 On the **Select Clone options** page, select the **Customize the operating system** check box, and click **Next**.
- 8 On the **Customize guest OS** page, select the **vra7-proxy-agent-template** from the table, and click **Next**.
- 9 On the **User Settings** page, enter the following values, and click **Next**.

Setting	Value
NetBIOS name	vra01ias51
IPv4 address	192.168.32.52
IPv4 subnet mask	255.255.255.0

- 10 On the **Ready to Complete** page, review your settings and click **Finish**.  
When the deployment of the virtual machine completes, you can customize the virtual machine.
- 11 In the **Navigator**, select **VMs and Templates**.
- 12 Right-click the **vra01ias51.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 **vxx-dvs-xxxx-Mgmt-RegionB01-VXLAN** from the drop-down menu and click **OK**.



- 14 Right-click the virtual machine **vra01ias51.lax01.rainpole.local**, and select **Power > Power on**.
  - 15 From the Virtual Machine Console, verify that **vra01ias51.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 vRealize Automation service account `svc-vra@rainpole.local` 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 `vra01ias51.lax01.rainpole.local` and `vra01ias52.lax01.rainpole.local`.

### Procedure

- 1 Log in to the Windows IaaS Proxy Agent virtual machine.
  - a Connect to `vra01ias51.lax01.rainpole.local` over RDP.
  - b Log in using the local administrator credentials that you specified during the creation of the customization specification process.
- 2 Download the vRealize Management Agent.
  - a Open a Web browser and go to `https://vra01svr01a.rainpole.local:5480/installer`.
  - b Download the Management Agent Installer.msi package.
- 3 Install the vRealize Management Agent.
  - a Start the `vCAC-IaaSManagementAgent-Setup.msi` installer.
  - b On the **Welcome** page, click **Next** to start the install process.
  - c On the **EULA** page, select the **I accept the terms of this agreement** check box and click **Next**.
  - d On the **Destination Folder** page, click **Next** to install in the default path.
  - e On the **Management Site Service** page, enter the following settings and click **Load**.

Setting	Value
vRA Appliance Address	<code>https://vra01svr01a.rainpole.local:5480</code>
Root username	<code>root</code>
Password	<code>vra_appA_root_password</code>

- f Select the **I confirm the fingerprint matches the Management Site Service SSL certificate** check box, and click **Next**.

- 4 On the **Management Agent Account Configuration** page, configure the following credentials and click **Next**.

Setting	Value
Username	rainpole\svc-vra
Password	<i>svc-vra_password</i>

- 5 On the **Ready to install** page, click **Install**.
- 6 Repeat the procedure to install the Management Agent in virtual machine vra01ias52.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 vra01ias51.lax01.rainpole.local and vra01ias52.lax01.rainpole.local.

### Procedure

- 1 Log in to the **vra01ias51.lax01.rainpole.local** virtual machine console using the vRealize Automation service account.

Setting	Value
Username	Rainpole\svc-vra
Password	<i>svc-vra_password</i>

- 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 **Log In** page, configure the following settings, and click **Next**.

Setting	Value
Appliance host name	vra01svr01a.rainpole.local:5480
User name	root
Password	<i>root_password</i>
Accept Certificate	Selected

- 6 On the **Installation Type** page, select **Custom Install**, select **Proxy Agents**, and click **Next**.

- 7 On the **Server and Account Settings** page, configure the following settings and click **Next**.

Setting	Value
Local server	Use the default host name
User name	RAINPOLE\svc-vra
Password	<i>svc-vra_password</i>

- 8 On the **Install Proxy Agent** page, configure the following values, and click **Add**.

**Note** If the Root CA certificate was used to sign the vRealize Automation certificate, is not be trusted by Proxy Agent Windows virtual machines. The Root CA certificate must be imported as the Trusted Root Certification Authority before you begin installation of the Proxy Agent.

Setting	Value
Agent type	vSphere
Agent name	VSPHERE-AGENT-51
Manager Service Host	vra01ims01.rainpole.local
Model Manager Web Service Host	vra01iws01.rainpole.local
vSphere Endpoint	comp01vc51.lax01.rainpole.local

**vRealize Automation Configuration**

**Install Proxy Agent**  
Install and configure Proxy Agent

Agent type: vSphere

Proxy Agent Details

Agent name: VSPHERE-AGENT-51

Manager Service Host: vra01ims01.rainpole.local [Test](#)

Model Manager Web Service Host: vra01iws01.rainpole.local [Test](#)

vSphere

Endpoint name: comp01vc51.lax01.rainpole.local  
This value must match the name of the vSphere endpoint in the vRealize Automation UI.

[Add](#) [Save](#)

Type	Name	Manager Service Host	Model Manager Web Service Host	Service User
vSphere	VSPHERE-AGE...	vra01ims01.rainpole.local	vra01iws01.rainpole.local	RAINPOLE\svc-vra

[Remove](#) [Edit](#)

[< Back](#) [Next >](#) [Cancel](#)

- 9 Click **Next**.

- 10 Verify the configuration, and click **Install** to install the proxy agent.
- 11 Repeat the procedure for virtual machine `vra01ias52.lax01.rainpole.local` to install another proxy agent for redundancy, using the following values.

Setting	Value
Agent Type	vSphere
Agent Name	VSPHERE-AGENT-51
Manager Service Host name	vra01ims01.rainpole.local
Model Manager Web Service Host name	vra01iws01.rainpole.local
vSphere Endpoint	comp01vc51.lax01.rainpole.local

## vRealize Orchestrator Configuration in Region B

VMware 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 that uses vRealize Orchestrator workflows to vRealize Orchestrator to allow vCenter Server and vRealize Orchestrator to communicate.

Install Java SE Development Kit that is required to run the vRealize Orchestrator Client.

## Procedure

- 1 Log in to the vRealize Orchestrator Client.
  - a Open a Web browser and go to **https://vra01vro01.rainpole.local:8281**.
  - b Click **Start Orchestrator Client**.
  - c On the VMware vRealize Orchestrator login page, log in to the vRealize Orchestrator Host A by using the following host name and credentials.

Setting	Value
Host name	vra01vro01.rainpole.local:8281
User name	svc-vra
Password	svc-vra_password

- 2 In the left pane, click **Workflows**, and navigate to **Library > vCenter > Configuration**.
- 3 Right-click the **Add a vCenter Server instance** workflow and click **Start Workflow**.
  - a On the **Set the vCenter Server Instance** page, configure the following settings and click **Next**.

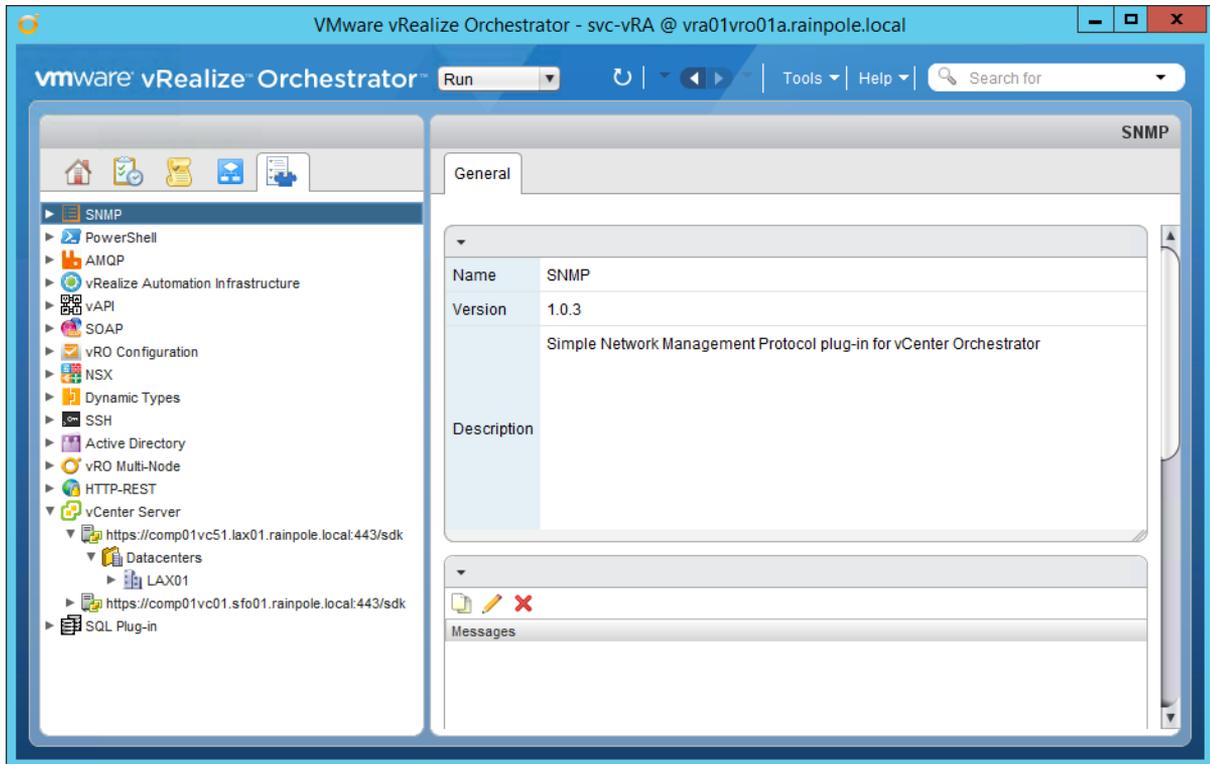
Setting	Value
IP or hostname of the vCenter Server instance to add	comp01vc51.lax01.rainpole.local
HTTPS port of the vCenter Server instance	443
Location of SDK that you use to connect	/sdk
Will you orchestrate this instance	Yes
Do you want to ignore certificate warnings	Yes

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

Setting	Value
Use a session per user	No
vCenter Server user name	svc-vro@rainpole.local
vCenter Server user password	svc-vro_password

- 4 To verify that the workflow completed successfully, click the **Inventory** tab and expand the **vCenter Server** 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.

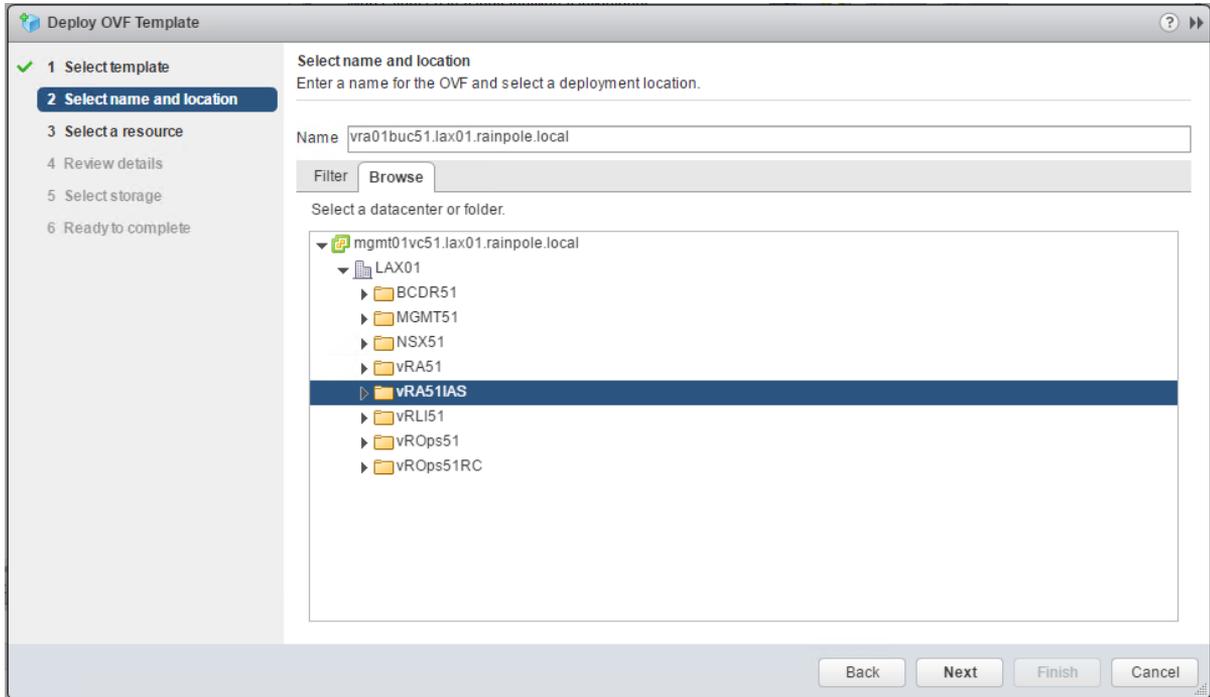
### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

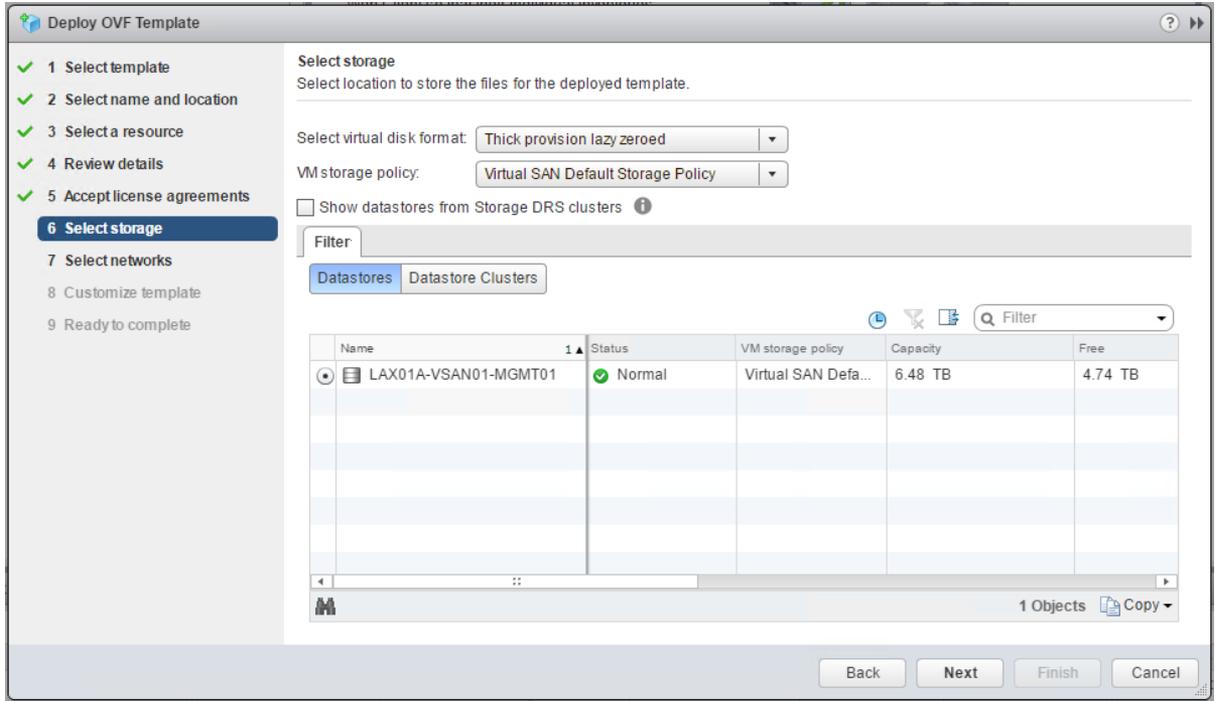
- 2 Click **Hosts and Clusters** and navigate to the **mgmt01vc51.lax01.rainpole.local** vCenter Server object.
- 3 Right-click the **mgmt01vc51.lax01.rainpole.local** object and select **Deploy OVF Template**.
- 4 On the **Select template** page, select **Local file**, browse to the location of the vRealize Business virtual appliance .ova file on your file system, and click **Next**.
- 5 On the **Select name and location** page, enter the following information and click **Next**.

Setting	Value
Name	vra01buc51.lax01.rainpole.local
Select a folder or datacenter	vRA51IAS

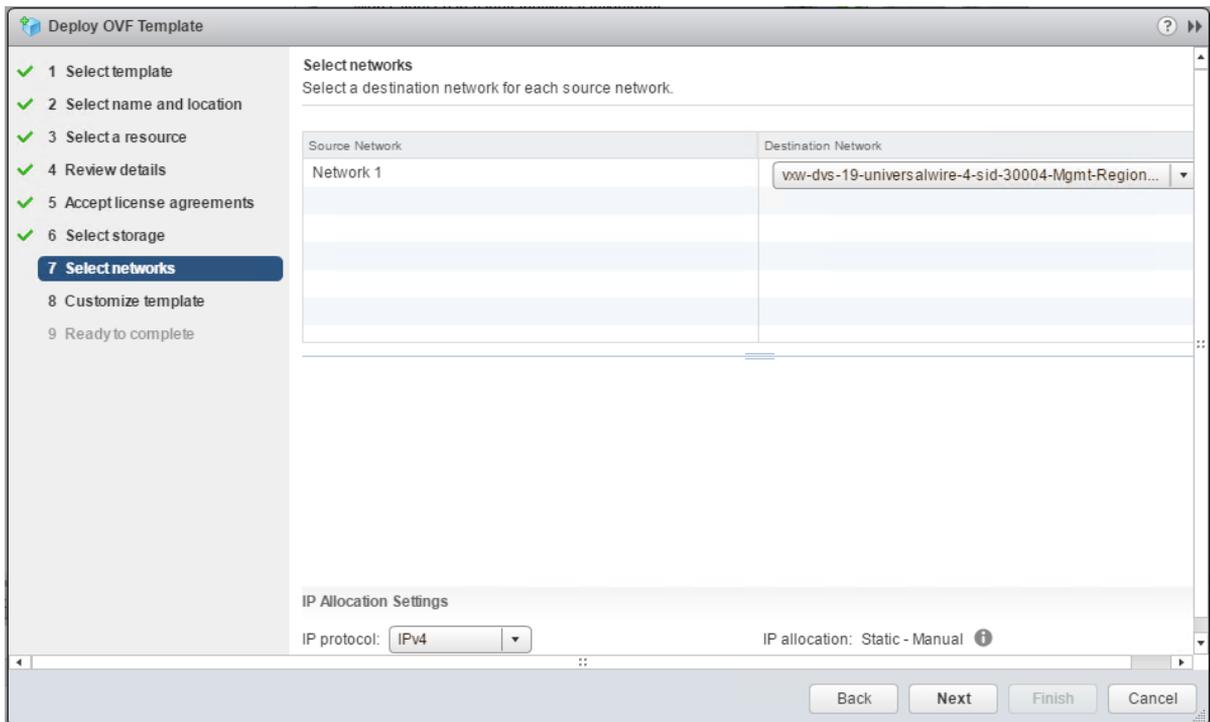


- 6 On the **Select a resource** page, select the **LAX01-Mgmt01** cluster and click **Next**.
- 7 On the **Review details** page, examine the virtual appliance details, such as product, version, download and disk size, and click **Next**.
- 8 On the **Accept license agreements** page, accept the end user license agreements and click **Next**.

- 9 On the **Select storage** page, select the datastore.
  - a Select **vSAN Default Storage Policy** from the **VM Storage Policy** drop-down menu.
  - b From the datastore table, select the **LAX01A-VSAN01-MGMT01** 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**.

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

Deploy OVF Template

1 Select template  
2 Select name and location  
3 Select a resource  
4 Review details  
5 Accept license agreements  
6 Select storage  
7 Select networks  
**8 Customize template**  
9 Ready to complete

**Customize template**  
Customize the deployment properties of this software solution.

All properties have valid values [Show next...](#) [Collapse all...](#)

Application	5 settings
Currency	Please select currency. USD - US D...
Enable SSH service	This will be used as an initial status of the SSH service in the appliance. You can change it later from the appliance Web console. <input type="checkbox"/>
Enable Server	This will enable the server components of vRealize Business for Cloud. <input type="checkbox"/>
Join the VMware Customer Experience Improvement Program	VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual. Additional information regarding the data collected through CEIP and the purposes for which it is used by VMware is set forth in the Trust and Assurance Center at <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> . If you prefer not to participate in VMware's CEIP for this product, you should uncheck the box below. You may join or leave VMware's CEIP for this product at any time. <input checked="" type="checkbox"/>
Root user password	Please enter the password for root user of the virtual appliance. Enter password: ***** Confirm password: *****
Networking Properties	6 settings
Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired. 192.168.32.1
Domain Name	The domain name of this VM. Leave blank if DHCP is desired. lax01.rainpole.local
Domain Name Servers	The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired. 172.17.11.5,172.17.11.4
Domain Search Path	The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired. lax01.rainpole.local
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. 192.168.32.54
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired. 255.255.255.0

Back Next Finish Cancel

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 **vra01buc51.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://vra01buc51.lax01.rainpole.local:5480**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vrb_collector_root_password

- 2 Configure the appliance to use a time server.
  - a Click the **Administration** tab and click **Time Settings**.
  - b On the **Time Settings** page, enter the following settings and click **Save Settings**.

Setting	Description
Time Sync. Mode	Use Time Server
Time Server #1	ntp.lax01.rainpole.local
Time Server #2	ntp.sfo01.rainpole.local

**vRealize Business for Cloud**

Administration System Telemetry Network Update [Logout user root](#)

Administration **Time Settings** SSL

### Time Settings

Time Sync. Mode	Use Time Server	<b>Actions</b> Save Settings Refresh
Time Server #1	ntp.lax01.rainpole.local	
Time Server #2	ntp.sfo01.rainpole.local	
Time Server #3		
Time Server #4		
Time Server #5		
Current Time	15 Jul, 2016 04:11:01 UTC +0000	

## Register the vRealize Business Data Collector with the Server in Region B

As part of vRealize Business installation in Region B, you connect the Region B vRealize Business Data Collector with the vRealize Business Server previously deployed in Region A.

Because the tenant is configured in vRealize Automation, you register the vRealize Business Data Collector appliance with the vRealize Business Server using the following procedure.

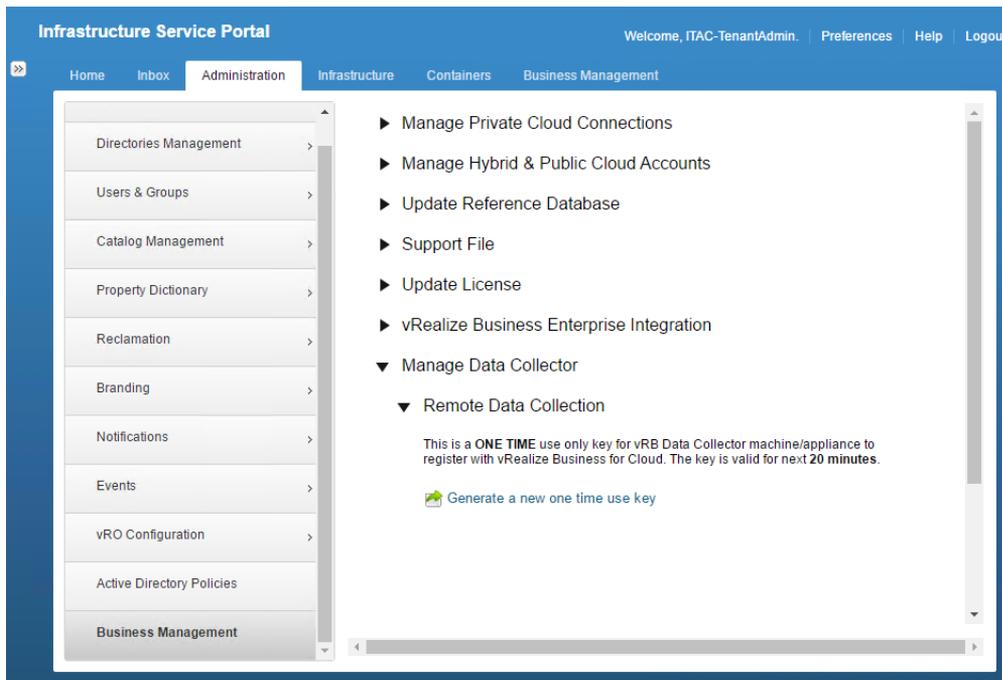
- Generate a one-time key from vRealize Automation.
- Register the Data Collector to the vRealize Business Server.

**Procedure**

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	Rainpole.local

- 2 Generate a one-time use key for connecting vRealize Business Data Collector.
  - a Navigate to **Administration > Business Management**.
  - b Expand the **Manage Data Collector > Remote Data Collection** section.
  - c Click **Generate a new one time use key**.
  - d Save the one time use key as you need it later.



- 3 Log in to the vRealize Business Data Collector console.
  - a Open a Web browser and go to **https://vra01buc51.lax01.rainpole.local:9443/dc-ui**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrb_collector_root_password</i>

- 4 Register the Data Collector with the vRealize Business Server.
  - a Expand the **Registration with the vRealize Business Server** section.
  - b Enter the following values and click **Register**.

After you click **Register**, a warning message informs you that the certificate is not trusted.

Setting	Value
Enter the vRB Server Url:	https://vra01bus01.rainpole.local
Enter the One Time Key:	<i>one_time_use_key</i>

## vRealize Business for Cloud Data Collector

- ▶ Manage Private Cloud Connections
- ▶ Manage Hybrid & Public Cloud Accounts
- ▼ Registration with vRealize Business Server

You can connect your data collector with an existing vRB Server. You can have only one vRB server registered at a time.

**Registered vRB URL :** vra01bus01.rainpole.local

### Register with vRealize Business

Enter the vRB Server Url :

The server URL must begin with https://

Enter the One Time Key :

The OTK is found in the One Time Key tab in the vRB Server

- ▶ Support File

- 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://vra01buc51.lax01.rainpole.local:9443/dc-ui**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrb_collector_root_password</i>

- 2 Click **Manage Private Cloud Connections**, select **vCenter Server**, and click the **Add** icon.
- 3 In the **Add vCenter Server Connection** dialog box, enter the following settings and click **Save**.

Setting	Value
Name	comp01vc51.lax01.rainpole.local
vCenter Server	comp01vc51.lax01.rainpole.local
Username	svc-vra@rainpole.local
Password	<i>svc_vra_password</i>

- 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://mgmt01vc51.lax01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** page, click **Hosts and Clusters**.

- 3 Under **mgmt01vc51.lax01.rainpole.local**, click **LAXO01**, and click **LAX01-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 **vra01ias51.lax01.rainpole.local** and **vra01ias52.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://comp01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 From the **Home** page, click **Content Libraries** and click content library **SFO01-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://comp01vc51.lax01.rainpole.local/vsphere-client**.

b Log in using the following credentials.

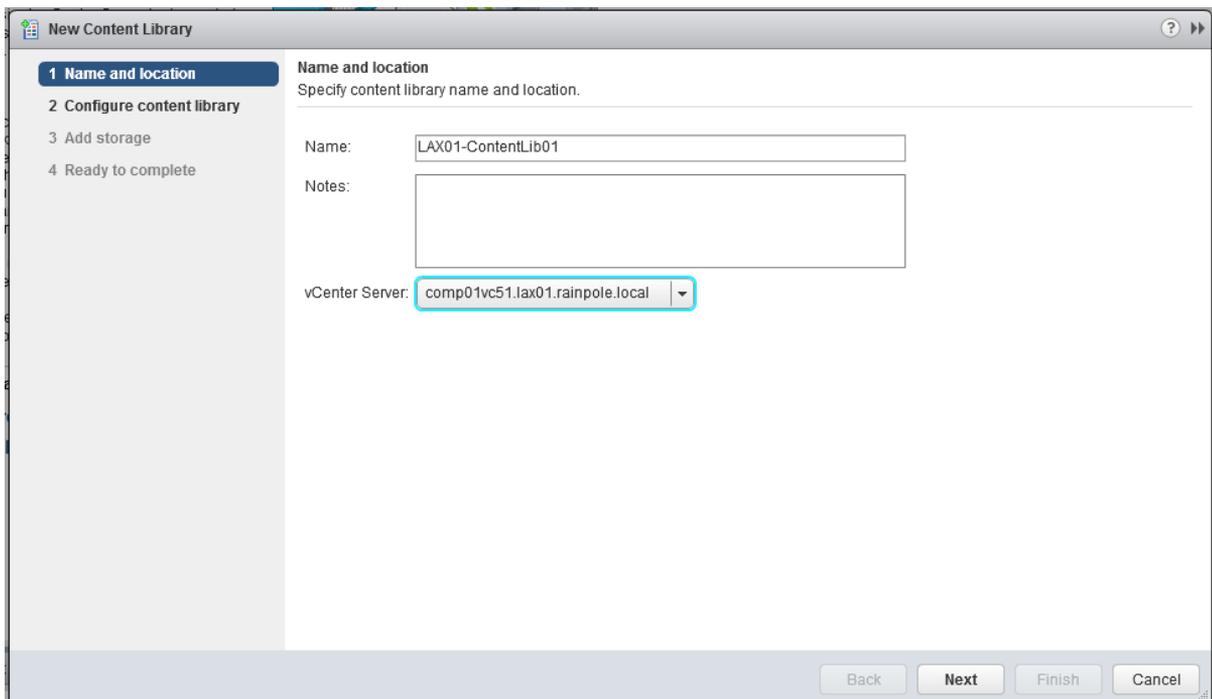
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

6 From the **Home** page, click **Content Libraries**, and click the **Create new library** icon.

The **New Content Library** wizard opens.

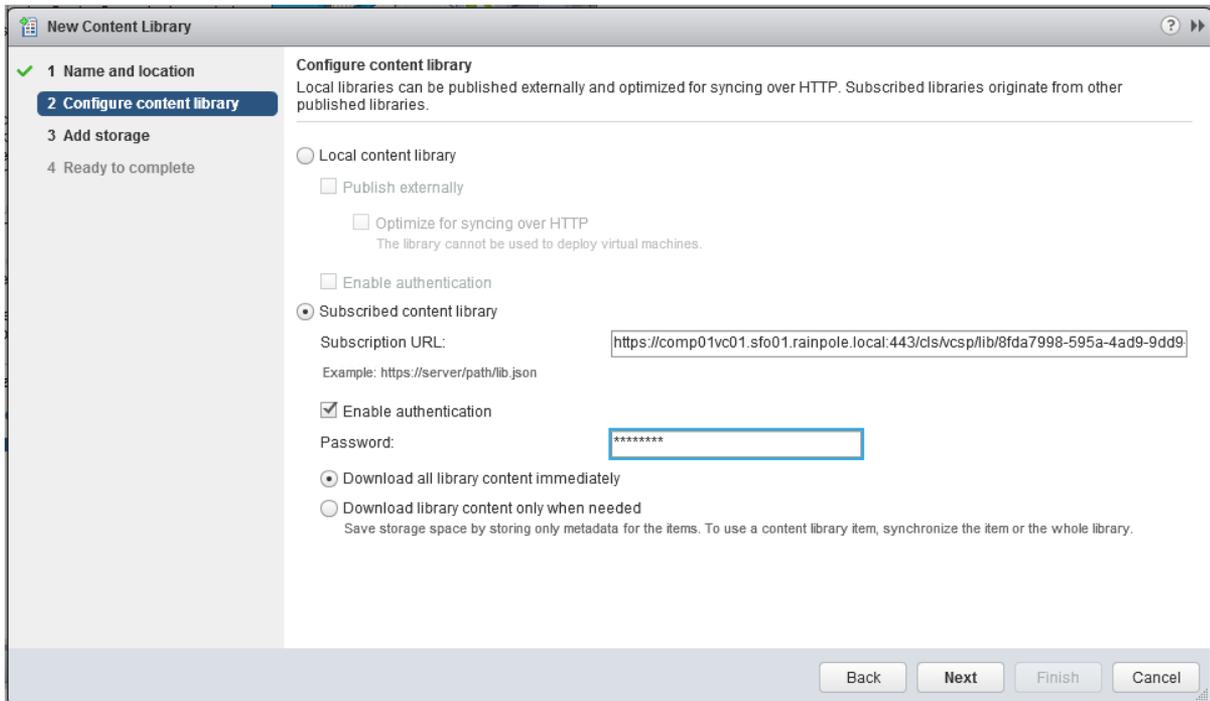
7 On the **Name and location** page, specify the following settings and click **Next**.

Setting	Value
Name	LAX01-ContentLib01
vCenter Server	comp01vc51.lax01.rainpole.local

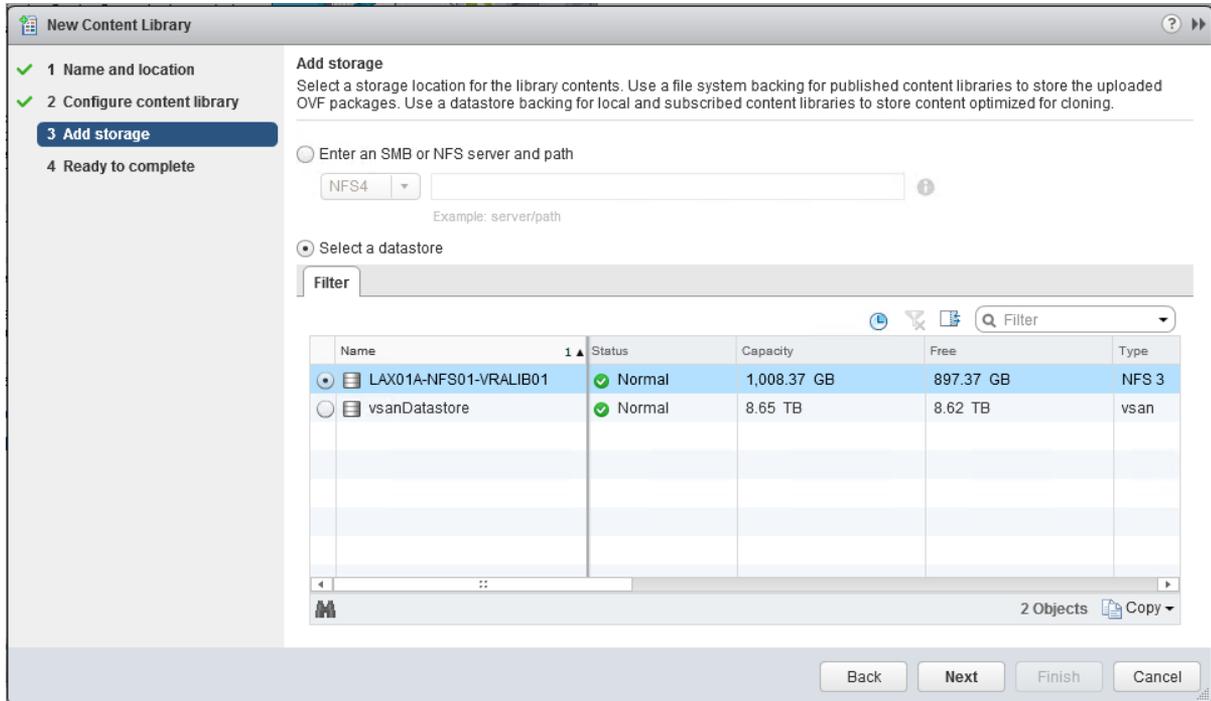


- 8 On the **Configure content library** page, select **Subscribed content library** specify the following settings, and click **Next**.

Setting	Value
Subscribed content library	Selected
Subscription URL	<i>SFO01-ContentLib01_subscription_URL</i>
Enable authentication	Selected
Password	<i>SFO01-ContentLib01_password</i>
Download all library content immediately	Selected



- 9 On the **Add storage** page, click the **Select a datastore** radio button, select the **LAX01A-NFS01-VRALIB01** 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 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 will deploy. Customization specifications are XML files that contain system configuration settings for the guest operating systems used by virtual machines. When you apply a specification to a guest operating system during virtual machine cloning or deployment, you prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names.

## 8 [Create Virtual Machines Using VM Templates in the Content Library in Region B](#)

vRealize Automation cannot directly access virtual machine templates in the content library. You must create a virtual machine using the virtual machine templates in the content library, then convert the template in vCenter Server. Perform this procedure on all vCenter Servers compute clusters you add to vRealize Automation, including the first vCenter Server compute instance.

## 9 [Convert the Virtual Machine to a VM Template in Region B](#)

You can convert a virtual machine directly to a template instead of making a copy by cloning.

## 10 [Configure Single Machine Blueprints in Region B](#)

Virtual machine blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

## 11 Configure Unified Single Machine Blueprints for Cross-Region Deployment in Region B

To provision blueprints from a specific vRealize Automation deployment to multiple regions, you define the additional regions in vRealize Automation, and associate the blueprints with those locations.

### Create Fabric Groups in Region B

IaaS administrators can organize virtualization compute resources and cloud endpoints into fabric groups by type and intent. One or more fabric administrators manage the resources in each fabric group. Fabric administrators are responsible for creating reservations on the compute resources in their groups to allocate fabric to specific business groups. Fabric groups are created in a specific tenant, but their resources can be made available to users who belong to business groups in all tenants.

#### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

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

Setting	Value
Name	LAX Fabric Group
Fabric administrators	ug-ITAC-TenantAdmins@rainpole.local

**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**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	Rainpole.local

- 2 Navigate to **Infrastructure > Reservation > Reservation Policies**.
- 3 Click the **New** icon, configure the following settings, and click the **Save** icon.

Setting	Value
Name	LAX-Production-Policy
Description	Reservation policy for Production Business Group in LAX

- 4 Click the **New** icon, configure the following settings, and click the **Save** icon.

Setting	Value
Name	LAX-Development-Policy
Description	Reservation policy for Development Business Group in LAX

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

Setting	Value
Name	LAX-Edge-Policy
Description	Reservation policy for Tenant Edge resources in LAX

## Create a vSphere Endpoint in vRealize Automation in Region B

To allow vRealize Automation to manage the infrastructure, IaaS administrators create endpoints and configure user-credentials for those endpoints. When you create a vSphere Endpoint, vRealize Automation can communicate with the vSphere environment and discover compute resources that are managed by vCenter Server, collect data, and provision machines.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Endpoints > Credentials** and click **New**.
- 3 On the **Credentials** page, configure the vRealize Automation credential for the administrator of comp01vc51.lax01.rainpole.local with the following settings, and click **Save**.

Setting	Value
Name	comp01vc51lax01 admin
Description	Administrator of comp01vc51.lax01.rainpole.local
User Name	svc-vra@rainpole.local
Password	<i>svc_vra_password</i>

- 4 Remain on the **Credentials** page and click **New** once again.
- 5 Configure the NSX administrator credentials of comp01nsxm51.lax01.rainpole.local with the following settings, and click the **Save** icon.

Setting	Value
Name	comp01nsxm51lax01 admin
Description	Administrator of NSX Manager comp01nsxm51.lax01.rainpole.local
User Name	svc-vra@rainpole.local
Password	<i>svc_vra_password</i>

- 6 Navigate to **Infrastructure > Endpoints > Endpoints** and click **New > Virtual > vSphere (vCenter)**.

- 7 On the **New Endpoint - vSphere (vCenter)** page, create a vSphere Endpoint with the following settings, and click **OK**.

**Note** The vSphere Endpoint Name must be identical to the name that you used to install the proxy agents.

Setting	Value
Name	comp01vc51.lax01.rainpole.local
Address	https://comp01vc51.lax01.rainpole.local/sdk
Credentials	comp01vc51lax01 admin
Specify manager for network and security platform	Selected
Address	https://comp01nsxm51.lax01.rainpole.local
Credentials	comp01nsxm51lax01 admin

## Add Compute Resources to a Fabric Group in Region B

You allocate compute resources to fabric groups so that vRealize Automation can use the resources in that compute resource for that fabric group when provisioning virtual machines.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 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**.

The screenshot shows the 'Fabric Groups' page in the Infrastructure Service Portal. The page title is 'Fabric Groups' and it includes a sub-header: 'Place compute resources in fabric groups and assign fabric administrators to manage them.' Below this is a table with the following data:

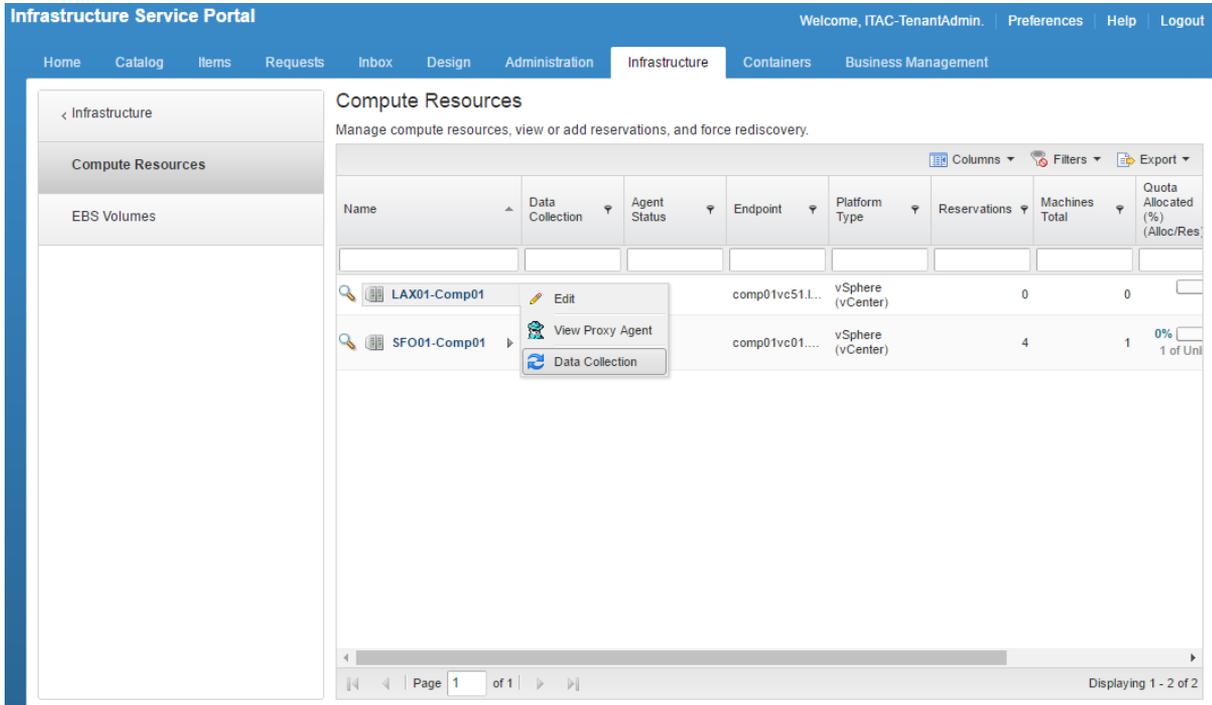
Name	Fabric Administrators	Description	Compute Resources
LAX Fabric Group	ntAdmins@rainpole.local		
SFO Fabric Group	ntAdmins@rainpole.local		SFO01-Comp01

A context menu is open over the 'LAX Fabric Group' row, showing 'Edit' and 'Delete' options. The page footer indicates 'Page 1 of 1' and 'Displaying 1 - 2 of 2'.

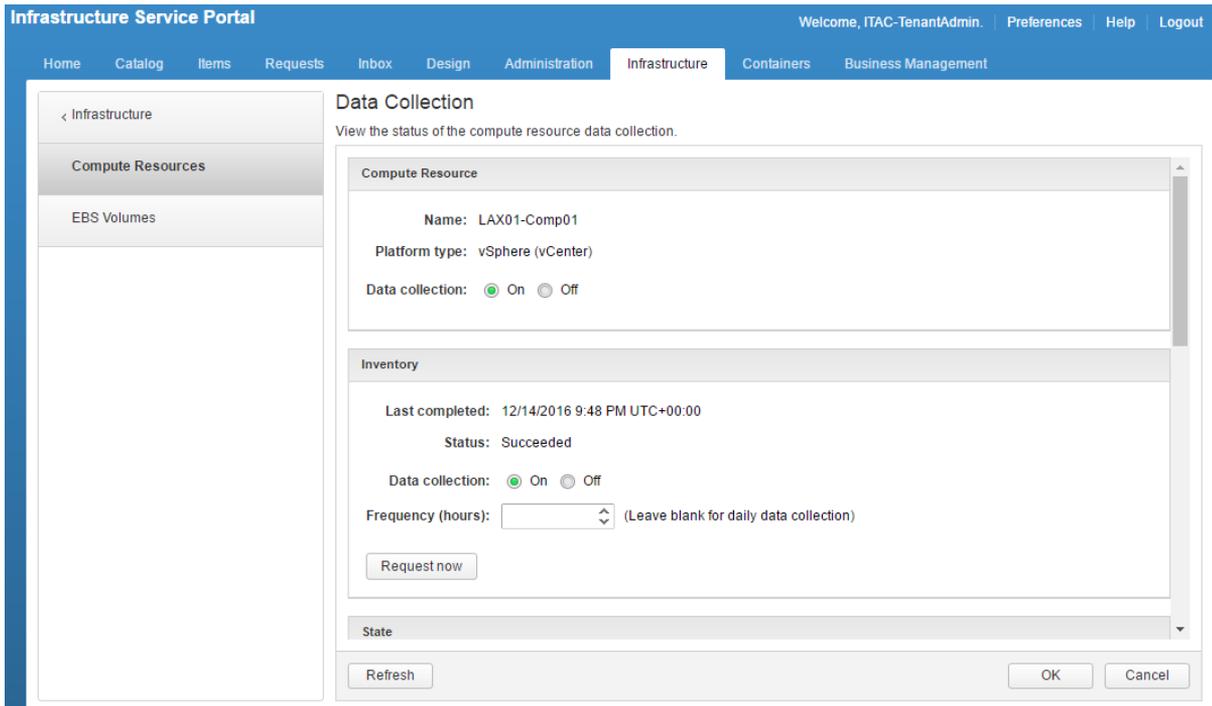
- On the **Edit Fabric Group** page, select **LAX01-Comp01** from the **Compute resources** table, and click **OK**.

**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 `vra01ias51.lax01.rainpole.local` and `vra01ias52.lax01.rainpole.local`.

- Navigate to **Infrastructure > Compute Resources > Compute Resources**.
- In the **Compute Resource** column, hover the mouse pointer over the compute cluster **LAX01-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**

Group	Name
Production	LAX01-Comp01-Prod-Res01
Development	LAX01-Comp01-Dev-Res01

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to <https://vra01svr01.rainpole.local/vcac/org/rainpole>.
  - b Log in using the following credentials.

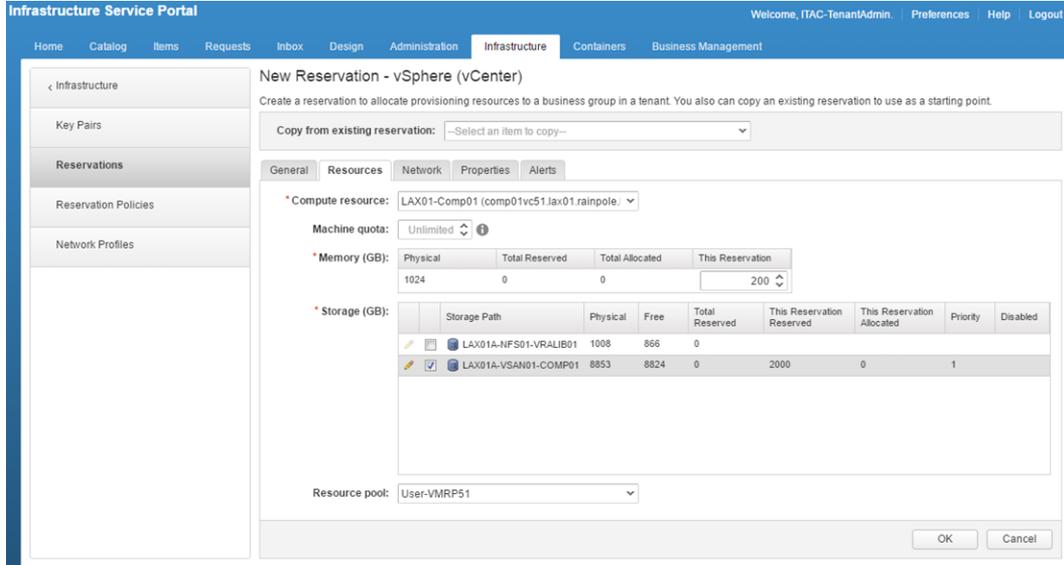
Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Reservations > Reservations** and select **New > vSphere (vCenter)**.
- 3 On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values for each group.

Setting	Production Group Value	Development Group Value
Name	LAX01-Comp01-Prod-Res01	LAX01-Comp01-Dev-Res01
Tenant	rainpole	rainpole
Business Group	Production	Development
Reservation Policy	LAX-Production-Policy	LAX-Development-Policy
Priority	100	100
Enable This Reservation	Selected	Selected

- 4 On the **New Reservation - vSphere (vCenter)** page, click the **Resources** tab.
  - a Select **LAX01-Comp01 (comp01vc51.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 datastore **LAX01A-VSAN01-COMP01**, and enter **2000** in the **This Reservation Reserved** text box, enter **1** in the **Priority** text box, and click **OK**.
- d Select **User-VMRP51** from the **Resource pool** drop-down menu.

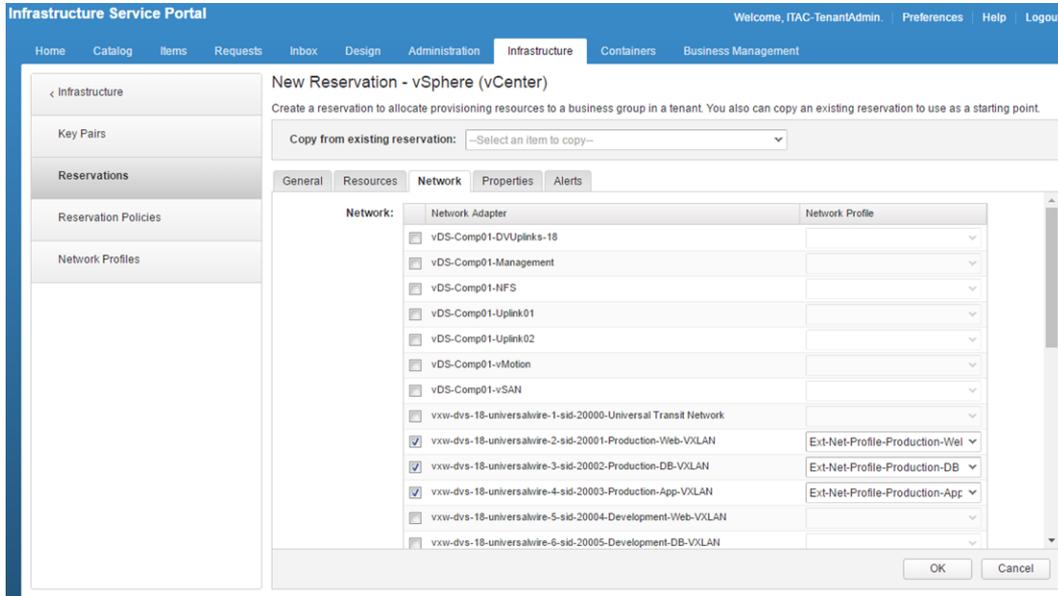


- 5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.
- 6 On the **Network** tab, select the network path check boxes listed in the table below from the **Network Paths** list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.
  - a Configure the Production Business Group with the following values.

Production Network Path	Production Group Network Profile
vxx-dvs-xxxxx-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxx-dvs-xxxxx-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxx-dvs-xxxxx-Production-App-VXLAN	Ext-Net-Profile-Production-App

- b Configure the Development Business Group with the following values.

Development Network Path	Development Group Network Profile
vxx-dvs-xxxxx-Development-Web-VXLAN	Ext-Net-Profile-Development-Web
vxx-dvs-xxxxx-Development-DB-VXLAN	Ext-Net-Profile-Development-DB
vxx-dvs-xxxxx-Development-App-VXLAN	Ext-Net-Profile-Development-App



- 7 Click **OK** to save the reservation.
- 8 Repeat this procedure to create a reservation for the Development Business Group.

## Create Reservations for the User Edge Resources in Region B

Before members of a business group can request virtual machines, fabric administrators must allocate resources to that business group by creating a reservation. Each reservation is configured for a specific business group to grant them access to request virtual machines on a specified compute resource.

Perform this procedure twice to create Edge reservations for both the Production and Development business groups.

**Table 3-4. Business Group Names**

Group	Name
Production	LAX01-Edge01-Prod-Res01
Development	LAX01-Edge01-Dev-Res01

### Procedure

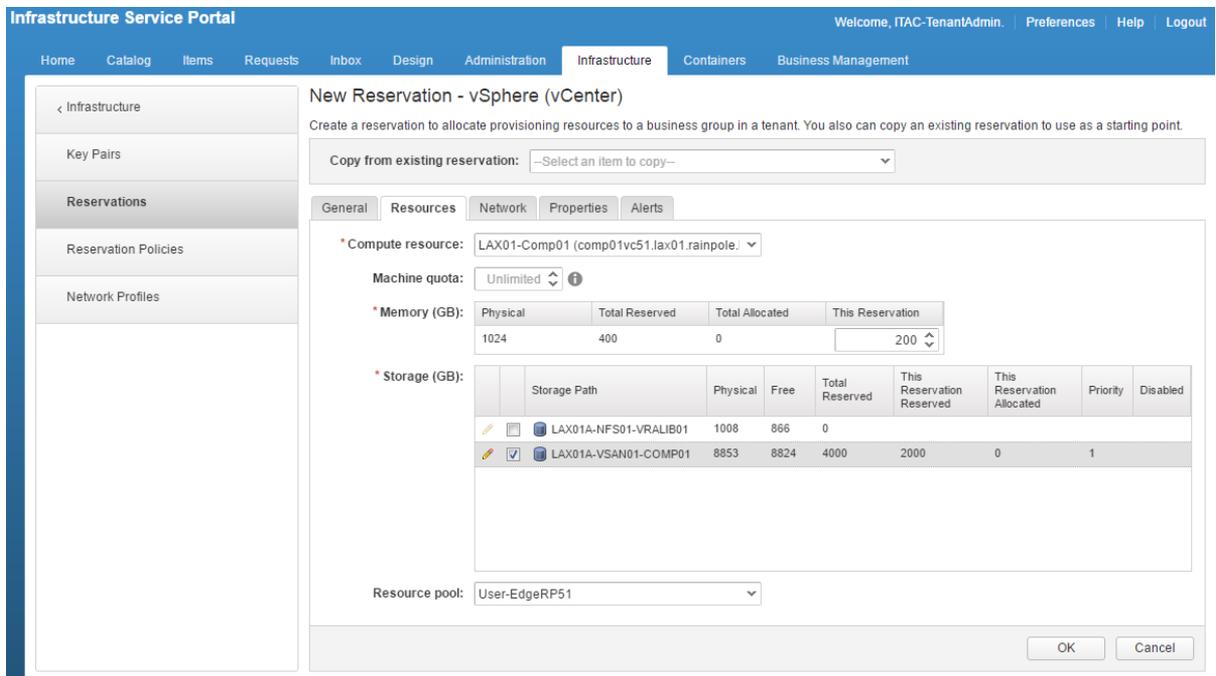
- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Reservations > Reservations**, and click **New vSphere (vCenter)**.
- 3 On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values for your business group.

Setting	Production Group Value	Development Group Value
Name	LAX01-Edge01-Prod-Res01	LAX01-Edge01-Dev-Res01
Tenant	rainpole	rainpole
Business Group	Production	Development
Reservation Policy	LAX-Edge-Policy	LAX-Edge-Policy
Priority	100	100
Enable This Reservation	Selected	Selected

- 4 On the **New Reservation - vSphere (vCenter)** page, click the **Resources** tab.
  - a Select **LAX01-Comp01(comp01vc51.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 datastore **LAX01A-VSAN01-COMP01**, enter **2000** in the **This Reservation Reserved** text box, enter **1** in the **Priority** text box, and click **OK**.
  - d Select **User-EdgeRP51** from the **Resource pool** drop-down menu.



- 5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.

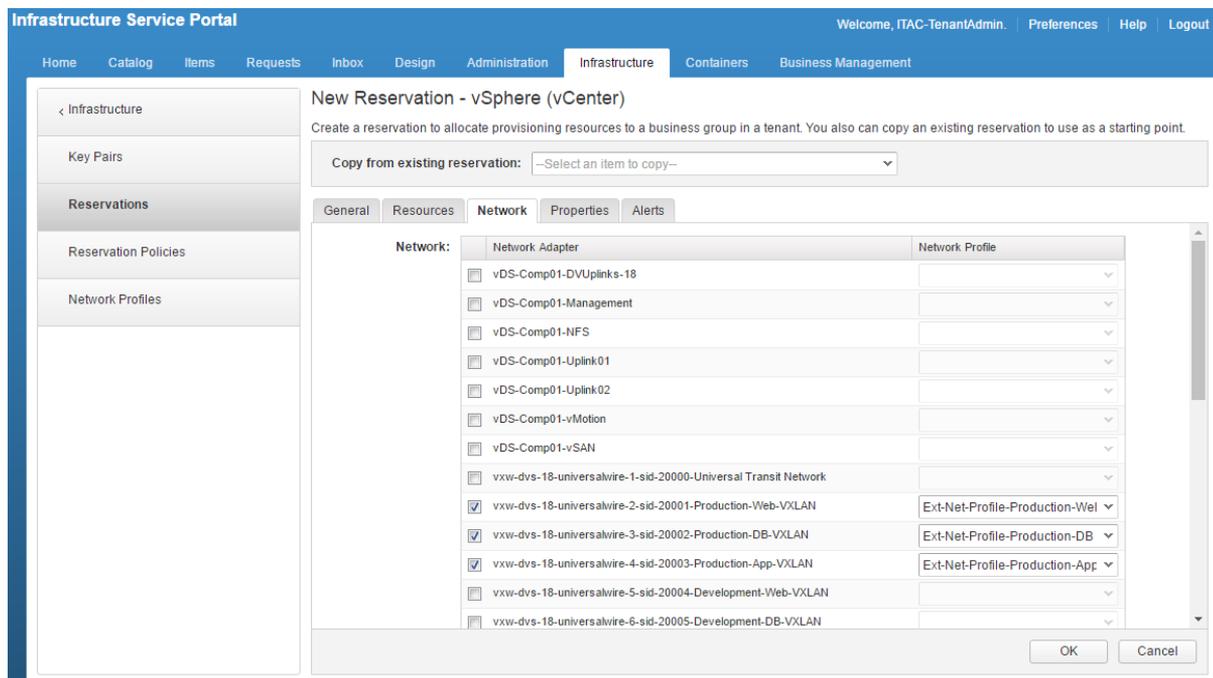
- On the **Network** tab, select the network path check boxes listed in the table below from the **Network Paths** list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.

Production Business Group

Production Port Group	Production Network Profile
vxw-dvs-xxxxx-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxw-dvs-xxxxx-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxw-dvs-xxxxx-Production-App-VXLAN	Ext-Net-Profile-Production-App

Development Business Group

Development Port Group	Development Network Profile
vxw-dvs-xxxxx-Development -Web-VXLAN	Ext-Net-Profile-Development -Web
vxw-dvs-xxxxx-Development -DB-VXLAN	Ext-Net-Profile-Development -DB
vxw-dvs-xxxxx-Development -App-VXLAN	Ext-Net-Profile-Development -App



- Click **OK** to save the reservation.
- Repeat the procedure to create a Edge reservation for the Development Business Group.

## Create 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 will 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 will later use the customization specifications that you create when you create 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://comp01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to **Home > Operations and Policies > Customization Specification Manager**.
- 3 Select the vCenter Server **comp01vc51.lax01.rainpole.local** from the drop-down menu.

- 4 Click the **Create a new specification** icon.

The **New VM Guest Customization Spec** wizard appears.

- 5 On the **Specify Properties** page, select **Linux** from the **Target VM Operating System** drop-down menu, enter **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**.

Setting	Value
Area	America
Location	Los Angeles
Hardware Clock Set To	Local Time

- 8 On the **Configure Network** page, click **Next**.
- 9 On the **Enter DNS and domain settings** page, leave the default settings, and click **Next**.
- 10 Click **Finish** to save your changes.

The customization specification that you created is listed in the **Customization Specification Manager**.

## Create a Customization Specification for Windows in Region B

Create a Windows guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://comp01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to **Home > Operations and Policies > Customization Specification Manager**.
- 3 Select the vCenter Server **comp01vc51.lax01.rainpole.local** from the drop-down menu.
- 4 Click the **Create a new specification** icon.

The **New VM Guest Customization Spec** wizard appears.

- 5 On the **Specify Properties** page, select **Windows** from the **Target VM Operating System** drop-down menu, enter `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**.

Setting	Value
Domain	lax01.rainpole.local
User name	LAX01\administrator
Password	<code>admin_pwd</code>

- 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**

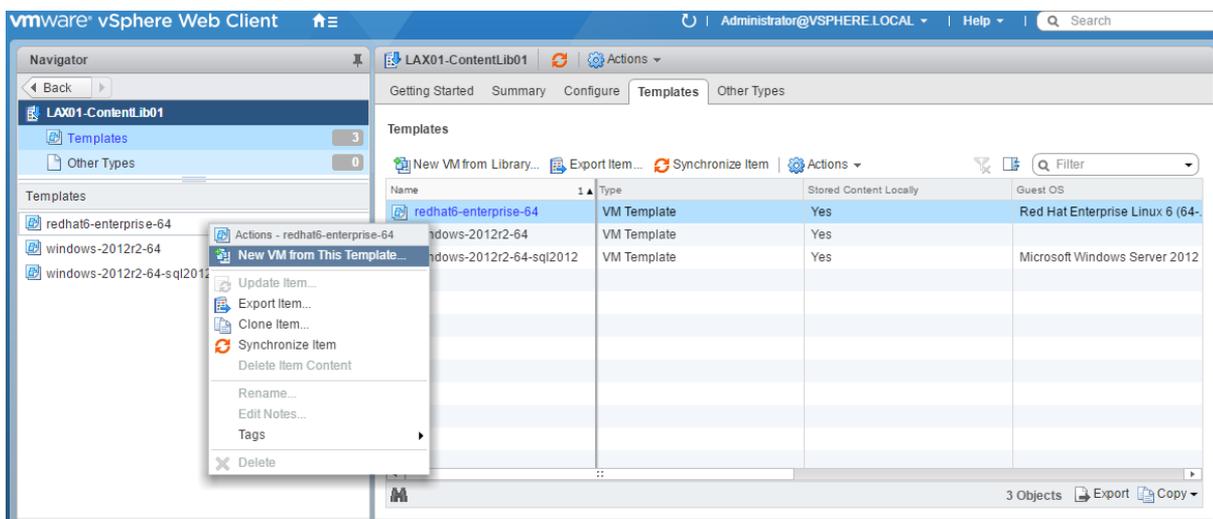
VM Template Name	Guest OS
redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)
windows-2012r2-64	Windows Server 2012 R2 (64-bit)
windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)

**Procedure**

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://comp01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to **Home > VMs and Templates**.
- 3 Expand the **comp01vc51.lax01.rainpole.local** vCenter Server.
- 4 Right-click the **LAX01** data center and select **New Folder > New VM and Template Folder**.
- 5 Create a new folder and label it **VM Templates**.
- 6 Navigate to **Home > Content Libraries**.
- 7 Click **LAX01-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-Comp01** and select resource pool **User-VMRP51**.
- 12 On the **Review details** page, verify the template details, and click **Next**.
- 13 On the **Select storage** page, select the **LAX01A-NFS01-VRALIB01** datastore and **Thin Provision** from the **Select virtual disk format** drop-down menu.
- 14 On the **Select networks** page, select **vDS-Comp01-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 the Virtual Machine to a VM Template 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**

VM Template Name	Guest OS
redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)
windows-2012r2-64	Windows Server 2012 R2 (64-bit)
windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)

**Procedure**

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://comp01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to **Home > VMs and Templates**.
- 3 In the **Navigator** pane, expand **comp01vc51.lax01.rainpole.local > LAX01 > 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.

**Create a Service Catalog in Region B**

A service catalog provides a common interface for consumers of IT services to request services, track their requests, and manage their provisioned service items.

## Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Administration** tab, click **Catalog Management > Services**, and click **New**.  
The **New Service** page appears.
- 3 In the **New Service** page, configure the following settings, and click **OK**.

Setting	Value
Name	LAX Service Catalog
Description	Default setting (blank)
Status	Active
Icon	Default setting (blank)
Status	Default setting (blank)
Hours	Default setting (blank)
Owner	Default setting (blank)
Support Team	Default setting (blank)
Change Window	Default setting (blank)

## Create a Single Machine Blueprint in Region B

Create a blueprint for cloning the windows-2012r2-64 virtual machine using the specified resources on the Compute vCenter Server. Tenants can later use this blueprint for automatic provisioning. A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

Repeat this procedure to create six blueprints.

Blueprint Name	VM Template	Reservation Policy	Service Catalog	Add to Entitlement
Windows Server 2012 R2 - LAX Prod	windows-2012r2-64 (comp01vc51.lax01.rainpole.local)	LAX-Production-Policy	LAX Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 - LAX Dev	windows-2012r2-64 (comp01vc51.lax01.rainpole.local)	LAX-Development-Policy	LAX Service Catalog	Dev-SingleVM-Entitlement

Blueprint Name	VM Template	Reservation Policy	Service Catalog	Add to Entitlement
Windows Server 2012 R2 With SQL2012 - LAX Prod	windows-2012r2-64-sql2012(comp01vc51.lax01.rainpole.local)	LAX-Production-Policy	LAX Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - LAX Dev	windows-2012r2-64-sql2012(comp01vc51.lax01.rainpole.local)	LAX-Development-Policy	LAX Service Catalog	Dev-SingleVM-Entitlement
Redhat Enterprise Linux 6 - LAX Prod	redhat6-enterprise-64(comp01vc51.lax01.rainpole.local)	LAX-Production-Policy	LAX Service Catalog	Prod-SingleVM-Entitlement
Redhat Enterprise Linux 6 - LAX Dev	redhat6-enterprise-64(comp01vc51.lax01.rainpole.local)	LAX-Development-Policy	LAX Service Catalog	Dev-SingleVM-Entitlement

**Procedure**

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

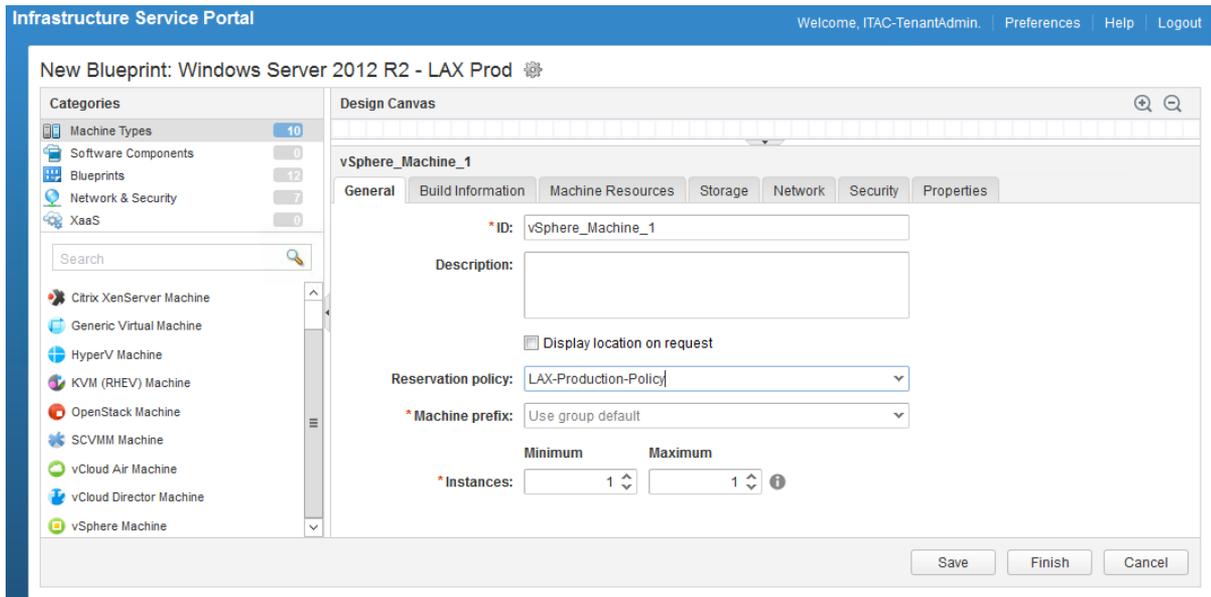
- 2 Navigate to **Design > Blueprints**.
- 3 Click **New**.
- 4 In the **New Blueprint** dialog box, configure the following settings on the **General** tab, and click **OK**.

Setting	Value
Name	Windows Server 2012 R2 - LAX Prod
Archive (days)	15
Deployment limit	Default setting (blank)
Minimum	30
Maximum	270

- 5 Select and drag the **vSphere Machine** icon to the **Design Canvas**.
- 6 Click the **General** tab, configure the following settings, and click **Save**.

Setting	Default
ID	Default setting (vSphere_Machine_1)
Description	Default setting (blank)

Setting	Default
Display location on request	Deselected
Reservation policy	LAX-Production-Policy
Machine prefix	Default setting (blank)
Minimum	Default setting (blank)
Maximum	Default setting (blank)



7 Click the **Build Information** tab, configure the following settings, and click **Save**.

Setting	Value
Blueprint type	Server
Action	Clone
Provisioning workflow	CloneWorkflow
Clone from	windows-2012r2-64 template
Customization spec	itac-windows-joindomain-custom-spec

8 Click the **Machine Resources** tab, configure the following settings, and click **Save**.

Setting	Minimum	Maximum
CPU	2	4
Memory (MB):	4096	16384
Storage	Default setting (blank)	Default setting (60)

9 Click the **Network** tab.

- a Select **Network & Security** in the **Categories** section to display the list of available network and security components.
- b Select the **Existing Network** component and drag it onto the **Design Canvas**.
- c Click in the **Existing network** text box and select the **Ext-Net-Profile-Production-Web** network profile.

Blueprint Name	Existing network
Windows Server 2012 R2 - LAX Prod	Ext-Net-Profile-Production-Web
Windows Server 2012 R2 - LAX Dev	Ext-Net-Profile-Development-Web
Windows Server 2012 R2 With SQL2012 - LAX Prod	Ext-Net-Profile-Production-DB
Windows Server 2012 R2 With SQL2012 - LAX Dev	Ext-Net-Profile-Development-DB
Redhat Enterprise Linux 6 - LAX Prod	Ext-Net-Profile-Production-App
Redhat Enterprise Linux 6 - LAX Dev	Ext-Net-Profile-Development-App

- d Click **Save**.
- e Select **vSphere\_machine** properties from the design canvas.
- f Select the **Network** tab, click **New**, configure the following settings, and click **OK**.

Network	Assignment Type	Address
ExtNetProfileProductionWeb	Static IP	Default setting (blank)
ExtNetProfileDevelopmentWeb	Static IP	Default setting (blank)
ExtNetProfileProductionDB	Static IP	Default setting (blank)
ExtNetProfileDevelopmentDB	Static IP	Default setting (blank)
ExtNetProfileProductionApp	Static IP	Default setting (blank)
ExtNetProfileDevelopmentApp	Static IP	Default setting (blank)

- g Click **Finish** to save the blueprint.

10 Select the blueprint **Windows Server 2012 R2 - LAX Prod** and click **Publish**.

11 Repeat this procedure to create additional blueprints.

## Configure Entitlements of Blueprints in Region B

You entitle users to the actions and items that belong to the service catalog by associating each blueprint with an entitlement.

Repeat this procedure to associate the six blueprints with their entitlement.

Blueprint Name	VM Template	Reservation Policy	Service Catalog	Add to Entitlement
Windows Server 2012 R2 - LAX Prod	windows-2012r2-64 (comp01vc51.lax01.rainpole.local)	LAX-Production-Policy	LAX Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 - LAX Dev	windows-2012r2-64 (comp01vc51.lax01.rainpole.local)	LAX-Development-Policy	LAX Service Catalog	Dev-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - LAX Prod	windows-2012r2-64-sql2012(comp01vc51.lax01.rainpole.local)	LAX-Production-Policy	LAX Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - LAX Dev	windows-2012r2-64-sql2012(comp01vc51.lax01.rainpole.local)	LAX-Development-Policy	LAX Service Catalog	Dev-SingleVM-Entitlement
Redhat Enterprise Linux 6 - LAX Prod	redhat6-enterprise-64(comp01vc51.lax01.rainpole.local)	LAX-Production-Policy	LAX Service Catalog	Prod-SingleVM-Entitlement
Redhat Enterprise Linux 6 - LAX Dev	redhat6-enterprise-64(comp01vc51.lax01.rainpole.local)	LAX-Development-Policy	LAX Service Catalog	Dev-SingleVM-Entitlement

## Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to <https://vra01svr01.rainpole.local/vcac/org/rainpole>.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Select the **Administration** tab and navigate to **Catalog Management > Catalog Items**.
- 3 On the **Configure 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**.

The screenshot shows the 'Configure Catalog Item' dialog in the Infrastructure Service Portal. The dialog is titled 'Configure Catalog Item' and has two tabs: 'General' and 'Entitlements'. The 'General' tab is active. The configuration details are as follows:

- Name:** Windows Server 2012 R2 - LAX Prod
- Source:** Blueprint Service
- Resource type:** Deployment
- Description:** (Empty text box)
- Icon:** (Empty text box) with a 'Browse...' button. Below it, it says 'Recommended size: 100 x 100 pixels'.
- Preview:** Three preview thumbnails are shown: 'List view', 'Catalog view', and 'Detail view'. The 'Detail view' thumbnail is the largest and most prominent.
- Status:** Active (dropdown menu)
- Quota:** Unlimited (dropdown menu)
- Service:** LAX Service Catalog (dropdown menu)

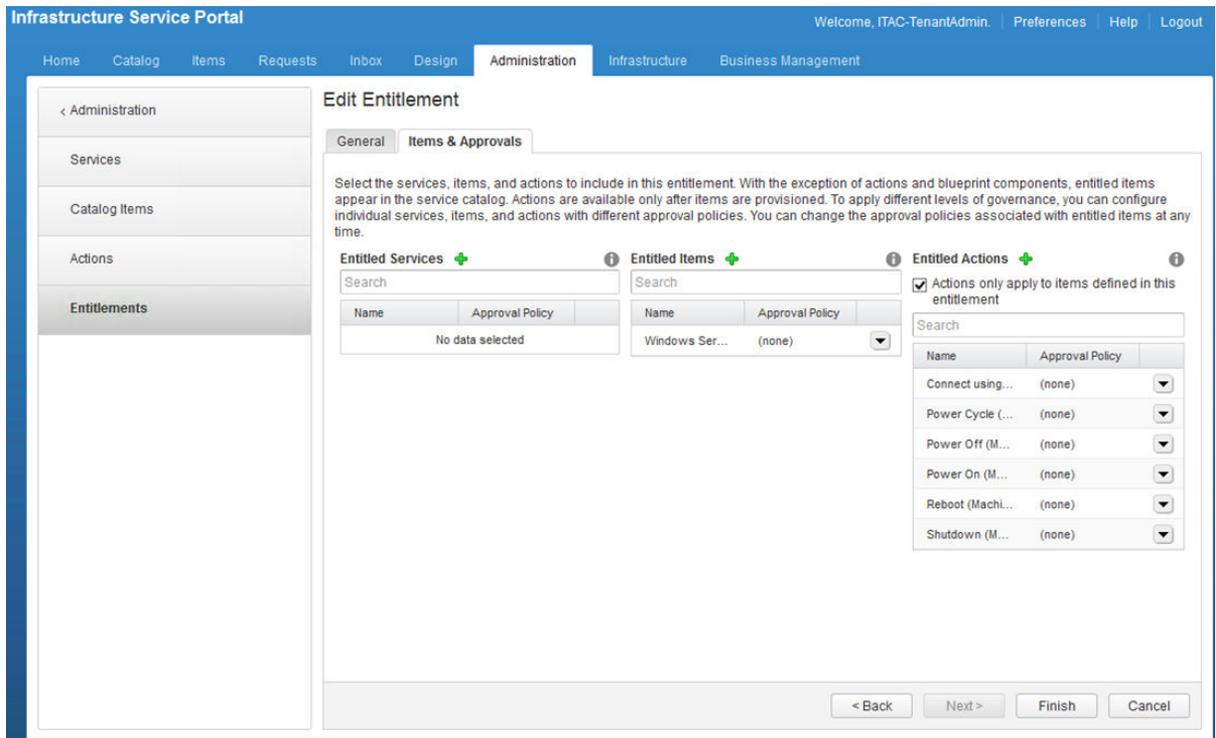
At the bottom right of the dialog, there are 'OK' and 'Cancel' buttons. The left sidebar of the portal shows a navigation menu with 'Administration' selected, and sub-items for 'Services', 'Catalog Items', 'Actions', and 'Entitlements'.

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 Select the **Catalog** tab and verify that the blueprint is listed in the **Service Catalog**.

7 Click **Request** button to request a virtual machine using **Windows Server 2012 R2 - LAX Prod** blueprint.

8 Click **Requests** tab to monitor the status of the provision request. Verify the request completes successfully.

9 Repeat this procedure to associate all of the blueprints with their entitlement.

## 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 in Region B](#)

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 and Development business groups. 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 in Region B

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 and vra01iws01b.

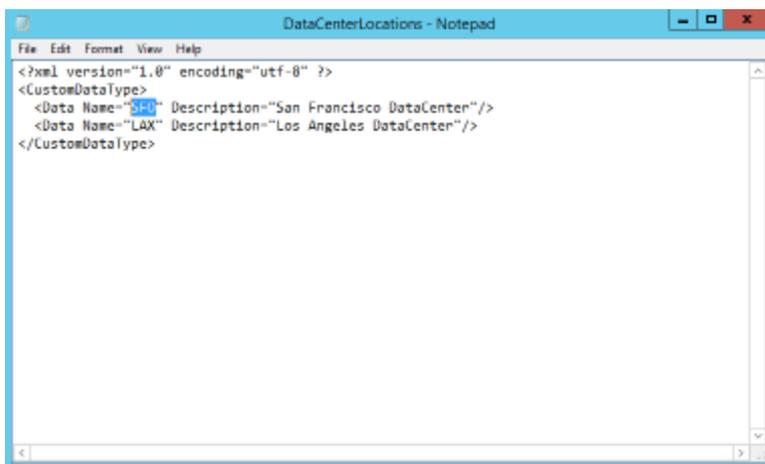
### Procedure

- 1 Log in to the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vcenter_admin_password

- 2 Open a VM console to the IaaS Web server virtual machine **vra01iws01a**, and log in using administrator credentials.
  - a Open the file C:\Program Files (x86)\VMware\VCAC\Server\Website\XmlData\DataCenterLocations.xml in a text editor.
  - b Update the Data Name and Description attributes to use the following settings.

Data Name	Description
SFO	San Francisco DataCenter
LAX	Los Angeles DataCenter



- 3 Save and close the file.

- 4 Restart the IaaS Web server virtual machine `vra01iws01a`.  
Wait until the virtual machine restarts and is successfully running.
- 5 Repeat this procedure for the IaaS web server virtual machine `vra01iws01b`.

## Associate Compute Resources with a Location in Region B

Each data center location has its own compute resources, which you associate with that site for its dedicated use.

Repeat this procedure twice, once for each vCenter Server compute cluster and region.

Location	vCenter Server Compute Cluster
SFO	SFO01-Comp01
LAX	LAX01-Comp01

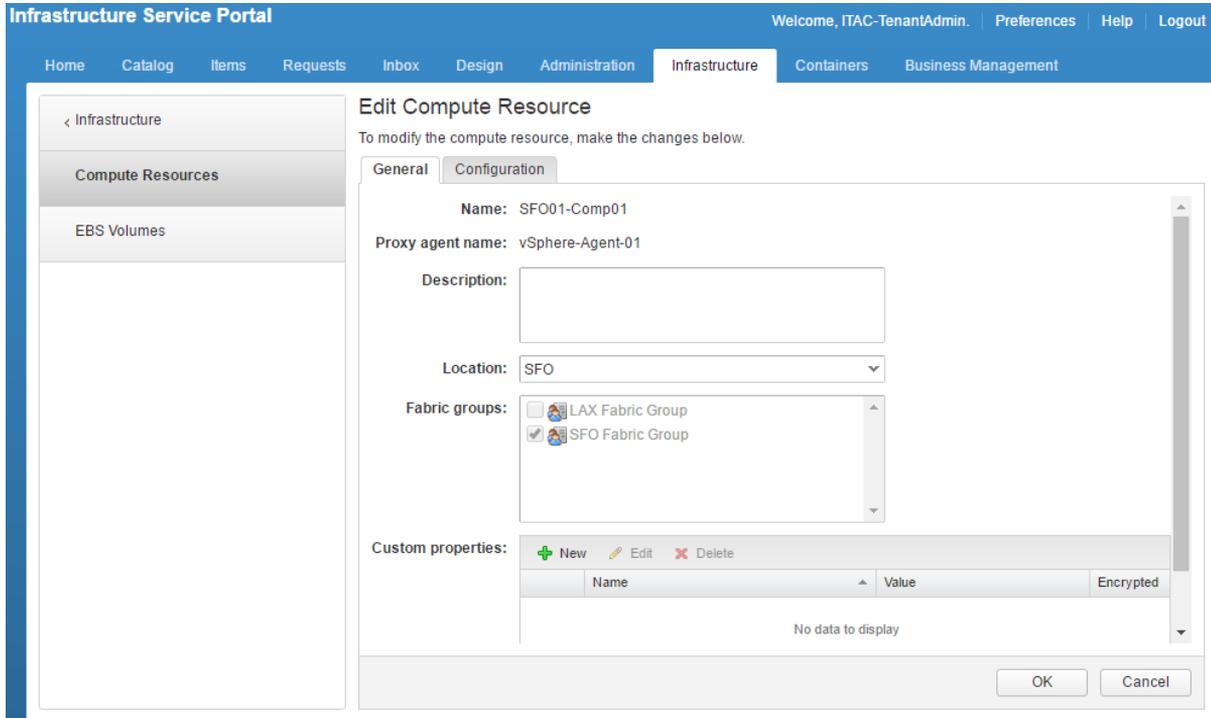
### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.
  - b Log in using the following credentials.

Setting	Value
User name	<code>itac-tenantadmin</code>
Password	<code>itac-tenantadmin_password</code>
Domain	<code>rainpole.local</code>

- 2 Select **Infrastructure > Compute Resources > Compute Resources**.
- 3 Using the mouse pointer, point to the compute resource **SFO01-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-Comp01** compute cluster.



- 5 Click **OK**.
- 6 Repeat this to set data center location for **LAX01-Comp01** compute cluster.

## Add a Property Group and a Property Definition for Data Center Location in Region B

Property definitions let you more easily control which location to deploy a blueprint, and based upon that choice, which storage and network resources to use with that blueprint.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to <https://vra01svr01.rainpole.local/vcac/org/rainpole>.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Select **Administration > Property Dictionary > Property Definitions**.

3 Click **New** to create a property definition.

- a Enter **Vrm.DataCenter.Location** in the **Name** text box.

---

**Note** The property definition name is case sensitive, and must exactly match the property name used in the blueprint or build profile.

---

- b Enter **Select a Region** in the **Label** text box.
- c In the **Visibility** section, select the **All Tenants** radio button and specify to which tenant the property is available.
- d (Optional) Enter a property description in the **Description** text box.

Describe the intent of the property and any information that might help the consumer best use the property.

- e Leave default setting for **Display order**.
- f Select **String** from the **Data type** drop-down menu.
- g Select **Yes** from the **Required** drop-down menu.
- h Select **Dropdown** from the **Display advice** drop-down menu.
- i Select **Static list** radio button for **Values**.
- j Deselect **Enable custom value entry**.
- k Click **New** in the **Static list** area and enter a property name and value from the following table.

Name	Value
San Francisco	SFO
Los Angeles	LAX

- l Click **OK** to save both predefined values.
- m Click **OK** to save the property definition.

The property is created and available on the **Property Definitions** page.

4 Select **Administration > Property Dictionary > Property Groups**. Click **New**.

5 Enter **Select Location** in the **Name** text box.

6 If you enter the **Name** value first, the **ID** text box is populated with the same value.

7 In the **Visibility** section, select the **All Tenants** radio button to specify with which tenant the property is to be available.

8 (Optional) Enter a description of the property group.

9 Add a property to the group by using the **Properties** box.

- a Click **New**.
- b Select **Vrm.DataCenter.Location** as the property name.

- c Deselect the **Encrypted** check box.
- d Select the **Show in Request** check box.
- e Click **OK** to add the property to the group.

10 Click **OK** to save the property group.

## Create a Reservation Policy for the Unified Blueprint in Region B

When tenant administrators and business group managers create a 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.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Reservations > Reservation Policies**.
  - 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 and Development business groups.

Region	Business Group	Reservation Name	Reservation Policy	Compute Resource
Region A	Production	SFO01-Comp01-Prod-UnifiedBlueprint	UnifiedBlueprint-Policy	SFO01-Comp01(comp01vc01.sfo01.rainpole.local)
	Development	SFO01-Comp01-Dev-UnifiedBlueprint	UnifiedBlueprint-Policy	SFO01-Comp01(comp01vc01.sfo01.rainpole.local)
Region B	Production	LAX01-Comp01-Prod-UnifiedBlueprint	UnifiedBlueprint-Policy	LAX01-Comp01(comp01vc51.lax01.rainpole.local)
	Development	LAX01-Comp01-Dev-UnifiedBlueprint	UnifiedBlueprint-Policy	LAX01-Comp01(comp01vc51.lax01.rainpole.local)

**Procedure**

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

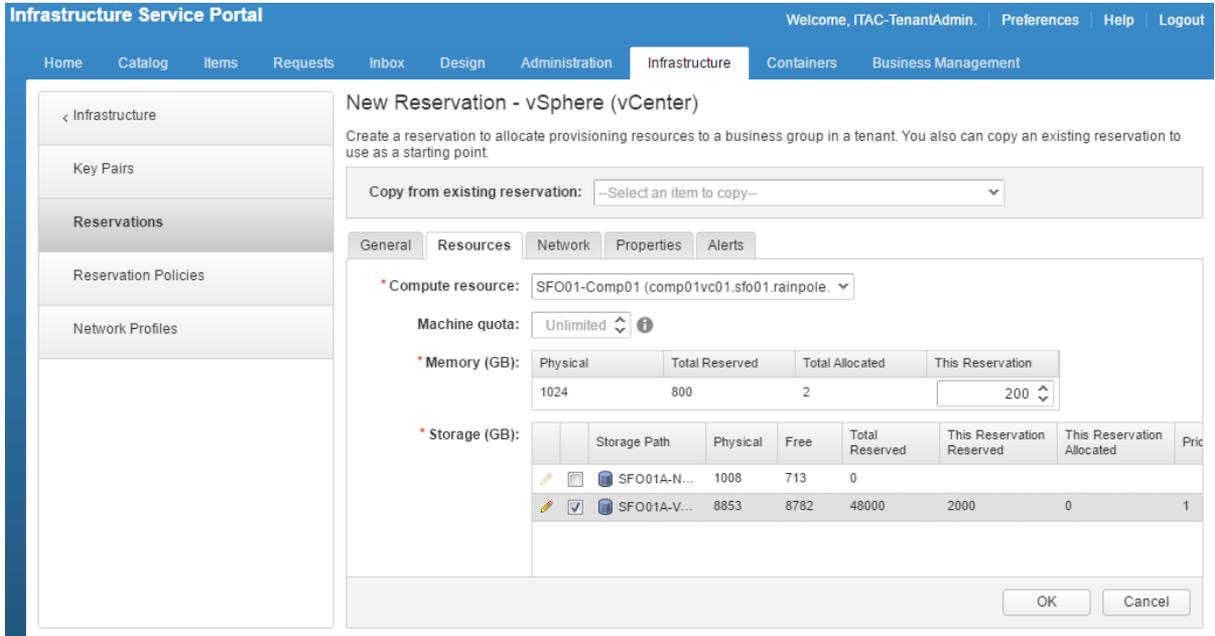
Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Reservations > Reservations** and click **New > vSphere (vCenter)**.
- 3 On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values.

Setting	Production Business Group Value	Development Business Group Value
Name	SFO01-Comp01-Prod-UnifiedBlueprint	SFO01-Comp01-Dev-UnifiedBlueprint
Tenant	rainpole	rainpole
Business Group	Production	Development
Reservation Policy	UnifiedBlueprint-Policy	UnifiedBlueprint-Policy
Priority	100	100
Enable This Reservation	Selected	Selected

- 4 On the **New Reservation - vSphere** page, click the **Resources** tab.
  - a Select **SFO01-Comp01(comp01vc01.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 the check box for datastore **SFO01A-VSAN01-COMP01**, and enter **2000** in the **This Reservation Reserved** text box, enter **1** in the **Priority** text box, and click **OK**.
- d Select **User-VMRP01** from the **Resource Pool** drop-down menu.



- 5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.
- 6 On the **Network** tab, select the network path check boxes listed in the table below from the **Network Paths** list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.

Production Business Group

Production Network Path	Production Group Network Profile
vxw-dvs-xxxxx-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxw-dvs-xxxxx-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxw-dvs-xxxxx-Production-App-VXLAN	Ext-Net-Profile-Production-App

Development Business Group

Development Network Path	Development Group Network Profile
vxw-dvs-xxxxx-Development-Web-VXLAN	Ext-Net-Profile-Development-Web
vxw-dvs-xxxxx-Development-DB-VXLAN	Ext-Net-Profile-Development-DB
vxw-dvs-xxxxx-Development-App-VXLAN	Ext-Net-Profile-Development-App

- 7 Click **OK** to save the reservation.
- 8 Repeat this procedure to create reservations for the Development Business Group.

## Create a Service Catalog for the Unified Blueprint in Region B

The service catalog provides a common interface for consumers of IT services to request and manage the services and resources they need. Users can browse the catalog to request services, track their requests, and manage their provisioned service items.

After the service catalog is created, business group managers can create entitlements for services, catalog items, and resource actions to groups of users. The entitlement allows members of a particular business group, for example, the Production business group, to use the blueprint. Without an entitlement, users cannot use the blueprint.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Click the **Administration** tab, and select **Catalog Management > Services**.
- 3 Click **New**.
  - a In the **New Service** dialog box type **Unified Single Machine Catalog** in the **Name** text box.
  - b Select **Active** from the **Status** drop-down menu.
  - c Click **OK**.

## Create an Entitlement for the Unified Blueprint Catalog in Region B

Entitle all blueprints in the Unified Blueprint Catalog to the Production and Development business groups. 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 twice, first to associate the Unified Blueprint Catalog with the Prod-SingleVM-Entitlement entitlement, and then once again to associate the Unified Blueprint Catalog with the Dev-SingleVM-Entitlement entitlement.

## Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Associate the **Unified Blueprint Catalog** with the **Prod-SingleVM-Entitlement** entitlement that you created earlier.
  - a Select **Administration > Catalog Management > Entitlements**.
  - b Click **Prod-SingleVM-Entitlement**.  
The **Edit Entitlement** pane appears.
  - c Select the **Items & Approvals** tab.
  - d Navigate to **Entitled Services** and click the **Add** icon.
  - e Check the box next to **Unified Single Machine Catalog** and click **OK**.
  - f Click **Finish** to save your changes.

## Create Unified Single Machine Blueprints in Region B

A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings. Create three blueprints from which to clone the virtual machine for your environment using pre-configured resources on the vCenter Server compute cluster in both Region A and Region B. Tenants use these blueprints to automatically provision virtual machines.

Repeat this procedure to create three Unified Single Machine blueprints, one for each blueprint name listed in the following table.

Blueprint Name	VM Template	Reservation Policy	Service Catalog
Windows Server 2012 R2 - Unified	windows-2012r2-64 (comp01vc01.sfo01.rainpole.local)	UnifiedBlueprint-Policy	Unified Single Machine Catalog
Windows Server 2012 R2 With SQL2012 - Unified	windows-2012r2-64- sql2012(comp01vc01.sfo01.rainpole.local)	UnifiedBlueprint-Policy	Unified Single Machine Catalog
Redhat Enterprise Linux 6 - Unified	redhat6- enterprise-64(comp01vc01.sfo01.rainpole.local)	UnifiedBlueprint-Policy	Unified Single Machine Catalog

**Procedure**

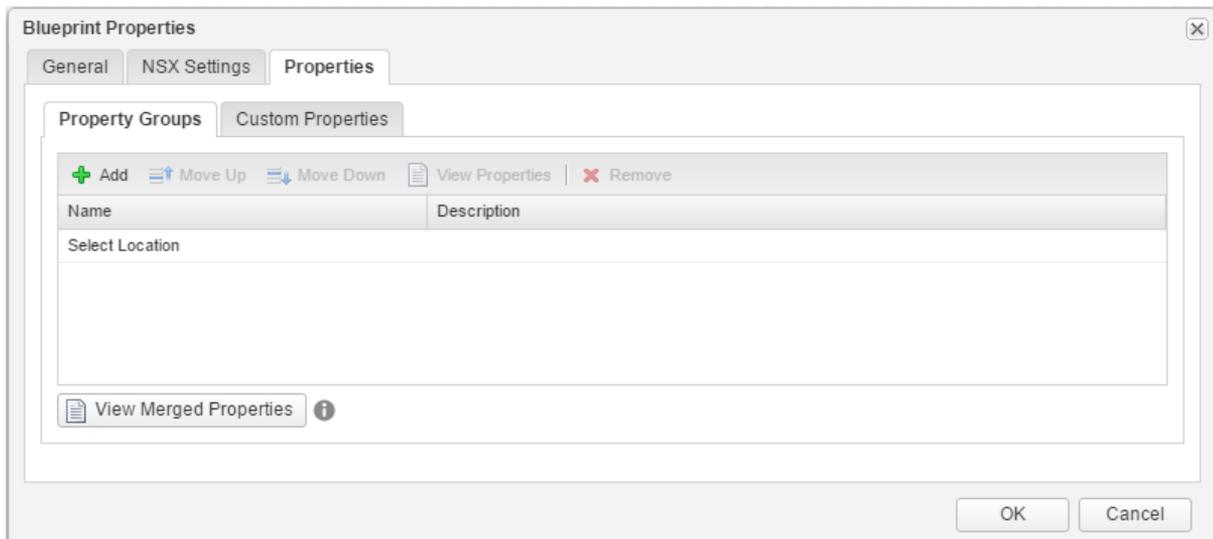
- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Design > Blueprints**.
- 3 Click **New**.
- 4 In the **New Blueprint** dialog box, configure the following settings on the **General** tab.

Setting	Value
Name	Windows Server 2012 R2 - Unified
Archive (days)	15
Deployment limit	Default setting (blank)
Minimum	30
Maximum	270

- 5 Click the **Properties** tab.
  - a Click **Add** on the **Property Groups** tab.
  - b Select the property group **Select Location** and click **OK**.



- 6 Click **OK**.

- 7 Select and drag the **vSphere Machine** icon to the Design Canvas.
- 8 Click the **General** tab, configure the following settings, and click **Save**.

Setting	Value
ID	Unified_Win2012R2_VM
Reservation Policy	UnifiedBlueprint-Policy
Machine Prefix	Use group default
Minimum	Default setting
Maximum	Default setting

- 9 Click the **Build Information** tab, configure the following settings, and click **Save**.

Setting	Value
Blueprint Type	Server
Action	Clone
Provisioning Workflow	CloneWorkflow
Clone from	windows-2012r2-64
Customization spec	itac-windows-joindomain-custom-spec

- 10 Click the **Machine Resources** tab, configure the following settings, and click **Save**.

Setting	Minimum	Maximum
CPU	1	4
Memory (MB):	4096	16384
Storage	50	60

- 11 Click the **Network** tab.
  - a Select **Network & Security** in the **Categories** section to display the list of available network and security components.
  - b Select the **Existing Network** component and drag it onto the design canvas.
  - c Click in the **Existing network** text box and select the **Ext-Net-Profile-Production-Web** network profile.
  - d Click **Save**.
  - e Select **vSphere\_Machine** properties from the design canvas.
  - f Select the **Network** tab, click **New**, and configure the following settings. Click **OK**.

Setting	Value
Network	ExtNetProfileProductionWeb
Assignment Type	Static IP
Address	Default setting (blank)

- 12 Select the blueprint **Windows Server 2012 R2 - Unified** and click **Publish**.
- 13 Navigate to **Administration > Catalog Management > Catalog Items** and add the blueprint to the **Unified Single Machine Catalog**.
  - a In the **Catalog Items** list, click the blueprint labelled **Windows Server 2012 R2 - Unified**.
  - b In the **Configure Catalog Items** dialog box, set **Service** to **Unified Single Machine Catalog**, and click **OK**.

## Test the Cross-Region Deployment of the Single Machine Blueprints in Region B

The data center environment is now ready for the multi-site deployment of virtual machines using vRealize Automation. Test your environment and confirm the successful provisioning of virtual machines using the blueprints you created to both Region A and Region B.

Repeat this procedure twice to provision virtual machines in both the Region A and Region B Compute vCenter Server instances.

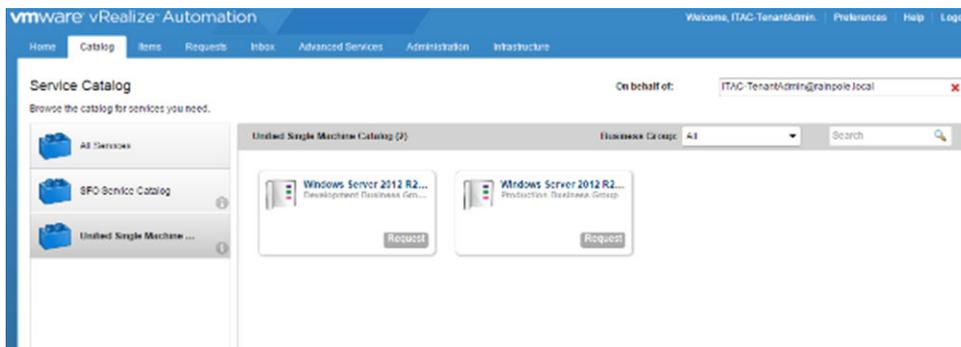
Region	Compute vCenter Server
San Francisco	comp01vc01.sfo01.rainpole.local
Los Angeles	comp01vc51.lax01.rainpole.local

### Procedure

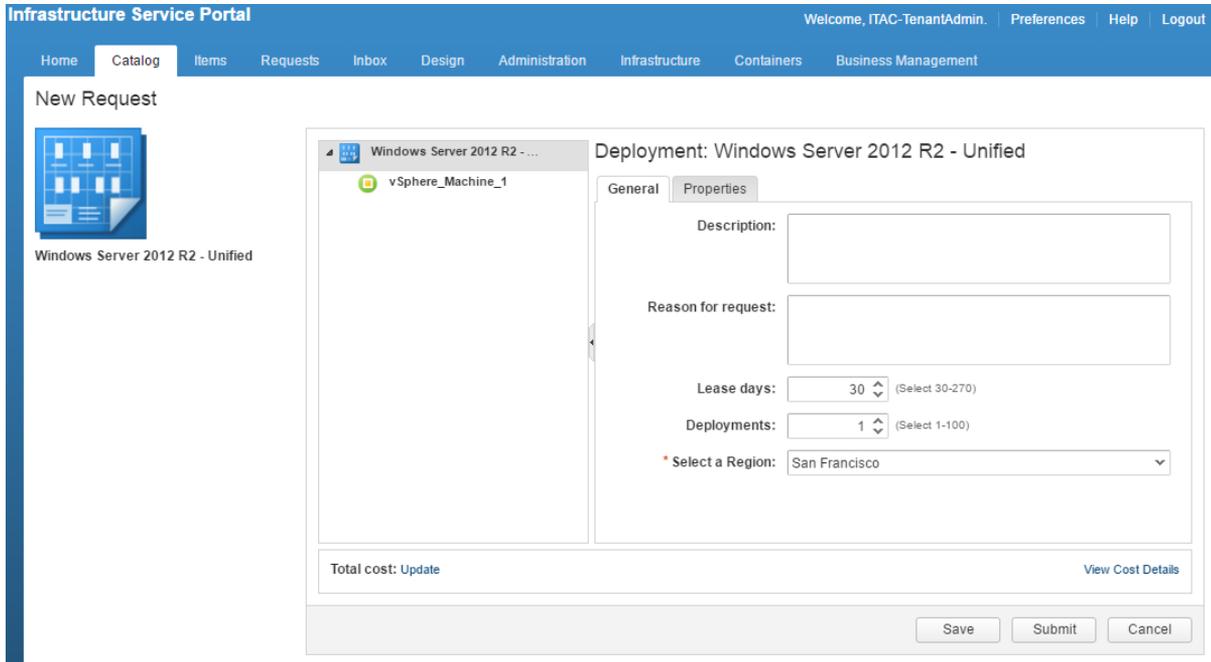
- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	Rainpole.local

- 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://comp01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in as the vCenter Server administrator using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vcenter_admin_password

- c Select **Home > VMs and Templates**.
  - d In the **Navigator** panel, expand the vCenter Server compute cluster **comp01vc01.sfo01.rainpole.local > SFO01 > 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.

# Region B Operations Implementation

# 4

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.

This chapter includes the following topics:

- [Region B vRealize Operations Manager Implementation](#)
- [Region B vRealize Log Insight Implementation](#)
- [Region B vSphere Update Manager Download Service Implementation](#)

## 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 LAXMGMT-LB01 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 [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.

# 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. IP Addresses and Host Names for the Remote Collector Nodes in Region B**

Role	IP Address	FQDN
Remote collector 1	192.168.32.31	vrops-rmtcol-51.lax01.rainpole.local
Remote collector 2	192.168.32.32	vrops-rmtcol-52.lax01.rainpole.local
Default gateway	192.168.32.1	-
DNS server	172.17.11.5	-
Subnet mask	255.255.255.0	-

#### Deployment Prerequisites

Verify that your environment satisfies the following prerequisites to deployment vRealize Operations Manager Remote Collector Nodes.

Prerequisite	Value
Storage	<ul style="list-style-type: none"> <li>■ Virtual disk provisioning. <ul style="list-style-type: none"> <li>■ Thin</li> </ul> </li> <li>■ Required storage per node <ul style="list-style-type: none"> <li>■ Initial storage for node deployment: 1.6 GB</li> </ul> </li> </ul>
Software Features	<ul style="list-style-type: none"> <li>■ vSphere <ul style="list-style-type: none"> <li>■ Management vCenter Server</li> <li>■ Client Integration Plugin on the machine where you use the vSphere Web Client</li> <li>■ Management cluster with enabled DRS and HA</li> </ul> </li> <li>■ NSX for vSphere <ul style="list-style-type: none"> <li>■ Application virtual network for the 3-node analytics cluster for failover of the analytics cluster by using vCenter Site Recovery Manager</li> <li>■ Application virtual network for the 2-node remote collector cluster</li> </ul> </li> <li>■ vRealize Operations Manager <ul style="list-style-type: none"> <li>■ 3-node analytics cluster in Region A</li> <li>■ 2-node remote collector cluster in Region A</li> </ul> </li> </ul>
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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to the mgmt01vc51.lax01.rainpole.local vCenter Server object.
- 3 Right-click the **mgmt01vc51.lax01.rainpole.local** object and select **Deploy OVF Template**.
- 4 On the **Select template** page, select **Local file**, browse to the location of the vRealize Operations Manager OVA file on your file system, and click **Next**.

- 5 On the **Select name and location** page, enter a node name, select the inventory folder for the virtual appliance, and click **Next**.

Setting	Value
Name	<ul style="list-style-type: none"> <li>■ vrops-rmtcol-51 for remote collector 1</li> <li>■ vrops-rmtcol-52 for remote collector 2</li> </ul>
Name of remote collector 2	
vCenter Server	mgmt01vc51.lax01.rainpole.local
Data center	LAX01
Folder	vROps51RC

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

Setting	Value
Datacenter	LAX01
Cluster	LAX01-Mgmt01

- 7 On the **Review details** page, examine the virtual appliance details, such as product, version, download and disk size, and click **Next**.
- 8 On the **Accept license agreements** page, accept the end user license agreements and click **Next**.
- 9 On the **Select configuration** page, from the **Configuration** drop-down menu, select **Remote Collector (Standard)** deployment configuration of the virtual appliance, and click **Next**.
- 10 On the **Select storage** page, select the datastore indicated in the table below, and click **Next**.

Setting	Value
Select virtual disk format	Thin provision
VM Storage Policy	vSAN Default Storage Policy
Datastore table	LAX01A-VSAN01-MGMT01

- 11 On the **Setup networks** page, select the distributed port group on the vDS-Mgmt distributed switch that ends with Mgmt-RegionB01-VXLAN and click **Next**.

12 On the **Customize template** page, set the IPv4 settings and select the time zone for the virtual appliance and click **Next**.

- a In the **Networking Properties** section, configure the following IPv4 settings.

Setting	Value
DNS server	172.17.11.5
Default gateway	192.168.32.1
Static IPv4 address	<ul style="list-style-type: none"> <li>■ 192.168.32.31 for remote collector 1</li> <li>■ 192.168.32.32 for remote collector 2</li> </ul> 192.168.32.31
Subnet mask	255.255.255.0

- b From the **Timezone setting** drop-down menu, select the **Etc/UTC** time zone.

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

14 After the virtual appliance is deployed, right-click the virtual appliance object and select **Power > Power On**.

15 Change the default empty password for the root user.

- a In the vSphere Web Client, right-click the remote collector virtual appliance and select **Open Console** to open the remote console to the appliance.

Name	Role
vrops-rmtcol-51	Remote collector 1
vrops-rmtcol-52	Remote collector 2

- b Press ALT+F1 to switch to the command prompt.
- c At the command prompt, log in as the **root** user using empty password.
- d At the command prompt, change the default empty password for the root user account with a new *vrops\_root\_password* password.
- e Close the virtual appliance console.

16 Repeat the steps to deploy the second remote collector appliance.

## Connect the Remote Collector Nodes to the Analytics Cluster in Region B

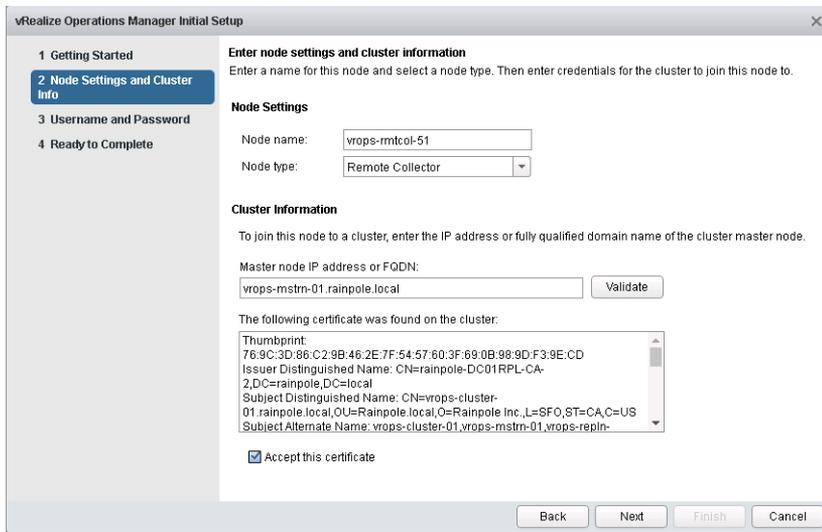
After you deploy the virtual appliances for the remote collector nodes on the Management vCenter Server in Region B, configure the settings of the remote collectors and connect them to the analytics cluster.

**Procedure**

- 1 Open a Web browser, and go to the initial setup user interface of each remote collector node virtual appliance.

Remote Collector Node	URL for Setup Interface
Remote collector 1	https://vrops-rmtcol-51.lax01.rainpole.local
Remote collector 2	https://vrops-rmtcol-52.lax01.rainpole.local

- 2 On the initial setup 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 node in the analytics cluster.



- a Configure the name, type and master address of the node.

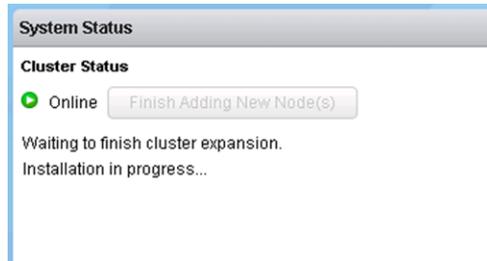
Setting	Value
<b>Node name</b>	<ul style="list-style-type: none"> <li>■ vrops-rmtcol-51 for remote collector 1</li> <li>■ vrops-rmtcol-52 for remote collector 2</li> </ul>
<b>Node type</b>	Remote Collector
<b>Master node IP address or FQDN</b>	vrops-mstrn-01.rainpole.local

- b Click **Validate** next to the **Master node IP address or FQDN** text box.  
The certificate of the master node appears in the text box.
  - c Validate that the master certificate is correct, and click **Accept this certificate**.
  - d Click **Next**.
- 5 On the **Username and Password** page, select **Use cluster administrator user name and password**, enter the *vrops\_admin\_password* password for the admin user, and click **Next**.

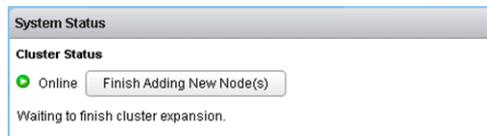
- On the **Ready to Complete** page, click **Finish**.

Wait for the node to finish installation operation.

The **System Status** page of vRealize Operations Manager appears. The cluster admin interface displays that the configuration of the node is in progress.



- Repeat the steps to configure the second remote collector node.
- 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:

- vrops-mstrn-01
- vrops-repln-02
- vrops-datan-03
- Two remote collectors for Region A vrops-rmtcol-01 and vrops-rmtcol-02
- Two remote collectors for Region B vrops-rmtcol-51 and vrops-rmtcol-52

Nodes in the vRealize Operations Manager Cluster							
Node Name	Node Address	Cluster Role	State	Status	Objects In Process	Objects Being C.	Metrics In Proce.
vrops-mstrn-01	vrops-mstrn-01.rainpole.local	Master	Running	Online	147	71	35903 14756
vrops-repln-02	vrops-repln-02.rainpole.local	Master Replica	Running	Online	150	34	35960 6107
vrops-datan-03	vrops-datan-03.rainpole.local	Data	Running	Online	148	50	42383 10516
vrops-rmtcol-01	vrops-rmtcol-01.sfo01.rainpole.local	Remote Collector	Running	Online	-	100	- 15180
vrops-rmtcol-02	vrops-rmtcol-02.sfo01.rainpole.local	Remote Collector	Running	Online	-	83	- 7554
vrops-rmtcol-51	vrops-rmtcol-51.lax01.rainpole.local	Remote Collector	Running	Online	-	-	- -
vrops-rmtcol-52	vrops-rmtcol-52.lax01.rainpole.local	Remote Collector	Running	Online	-	-	- -

## 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to the **mgmt01vc51.lax01.rainpole.local** vCenter Server object, and under the **LAX01** data center object select the **LAX01-Mgmt01** cluster.
- 3 Click **Configure** tab.
- 4 Under the **Configuration** group of settings, select **VM/Host Rules**.
- 5 On the **VM/Host Rules** page, click the **Add** button above the rules list.
- 6 In the **Create VM/Host Rule** dialog box, add a new anti-affinity rule for the virtual machines of the two remote collectors using the following values, and click **OK**.

Setting	Value
Name	anti-affinity-rule-vropsr
Enable rule	Selected
Type	Separate Virtual Machines
Members	<ul style="list-style-type: none"> <li>■ vrops-rmtcol-51</li> <li>■ vrops-rmtcol-52</li> </ul>

## 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.

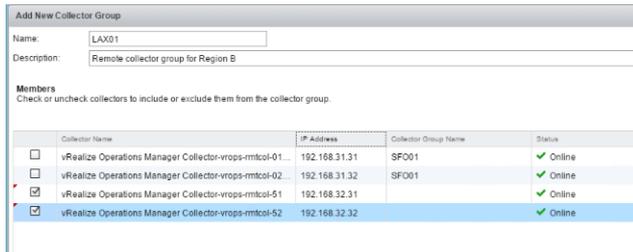
**Procedure**

- 1 Log in to vRealize Operations Manager by using the administration console.
  - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
  - b Log in using the following credentials.

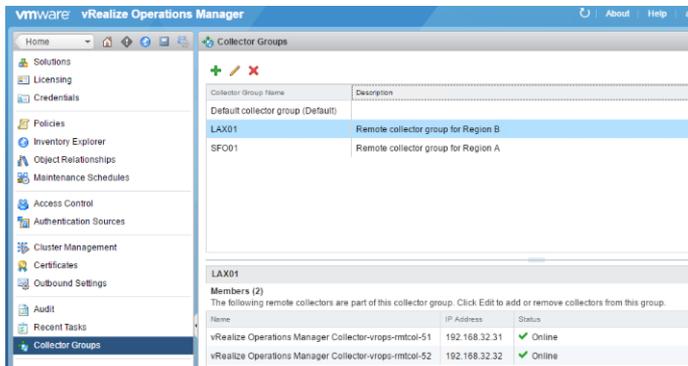
Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the **Home** page, click **Administration > Collector Groups**.
- 3 Click the **Add** icon.
- 4 In the **Add New Collector Group** dialog box, configure the following settings, and click **Save**.

Setting	Value
Name	LAX01
Description	Remote collector group for Region B
vrops-rmtcol-51	Selected
vrops-rmtcol-52	Selected



The **LAX01** 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 LAXMGMT-LB01 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.

### Prerequisites

- Verify that the NSX Manager for the management cluster in Region B has the management virtual application network for the analytics cluster configured.
- Verify that the Load Balancer service is enabled and interface is disconnected on the NSX Edge service gateway 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Networking & Security**.  
The vSphere Web Client displays the **NSX Home** page.
- 3 On the **NSX Home** page, click **NSX Edges** and select **172.17.11.65** from the **NSX Manager** drop-down menu at the top of the **NSX Edges** page.
- 4 On the **NSX Edges** page, double-click the **LAXMGMT-LB01** 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** icon.
  - c In the **Edit NSX Edge Interface** dialog box, click the **Edit** icon 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 LAXMGMT-LB01 device, click the **Load Balancer** tab.
- b Click **Application Profiles**, and click the **Add** icon.
- c In the **New Profile** dialog box, configure the profile using the following configuration settings, and click **OK**.

Setting	Value
Name	VROPS_HTTPS
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	Source IP
Expires in (Seconds)	1800
Client Authentication	Ignore

**New Profile**

Name:

Type:

Enable SSL Passthrough

HTTP Redirect URL:

Persistence:

Cookie Name:

Mode:

Expires In (Seconds):

Insert X-Forwarded-For HTTP header

Enable Pool Side SSL

Virtual Server Certifica... Pool Certificates

Service Certificates CA Certificates CRL

Configure Service Certificate

Common Name	Issuer	Validity

Cipher:

Client Authentication:

OK Cancel

7 Create a service monitoring entry.

- a On the **Load Balancer** tab of the LAXMGMT-LB01 device, click **Service Monitoring** and click the **Add** icon.
- b In the **New Service Monitor** dialog box, configure the health check parameters using the following configuration settings, and click **OK**.

Setting	Value
Name	VROPS_MONITOR
Interval	3
Timeout	5
Max Retries	2
Type	HTTPS
Method	GET
URL	/suite-api/api/deployment/node/status
Receive	ONLINE (must be upper case)

**New Service Monitor** ?

Name: \* VROPS\_MONITOR

Interval: 3 (seconds)

Timeout: 5 (seconds)

Max Retries: 2

Type: HTTPS

Expected:

Method: GET

URL: /suite-api/api/deployment/node/status

Send:

Receive: ONLINE

Extension:

OK Cancel

8 Add a server pool.

- a On the **Load Balancer** tab of the LAXMGMT-LB01 device, select **Pools**, and click the **Add** icon.
- b In the **New Pool** dialog box, configure the load balancing profile using the following configuration settings.

Setting	Value
Name	VROPS_POOL
Algorithm	LEASTCONN
Monitors	VROPS_MONITOR

The screenshot shows a 'New Pool' dialog box with the following fields and values:

- Name: VROPS\_POOL
- Description: (empty)
- Algorithm: LEASTCONN
- Algorithm Parameters: (empty)
- Monitors: VROPS\_MONITOR
- Members: (empty)

- c Under **Members**, click the **Add** icon to add the pool members.
- d In the **New Member** dialog box, add one member for each node of the analytics cluster and click **OK**.

Setting	Value
Enable Member	Selected
Name	<ul style="list-style-type: none"> <li>■ vroops-mstrn-01</li> <li>■ vroops-repln-02</li> <li>■ vroops-datan-03</li> </ul>
IP Address	<ul style="list-style-type: none"> <li>■ 192.168.11.31</li> <li>■ 192.168.11.32</li> <li>■ 192.168.11.33</li> </ul>
State	Enable
Port	443
Monitor Port	443
Weight	1
Max Connections	8
Min Connections	8

After you add the analytics cluster nodes to the pool, they will appear in the Members table.

- e In the **New Pool** dialog box, click **OK**.

## 9 Add a virtual server.

- a On the **Load Balancer** tab of the LAXMGMT-LB01 device, select **Virtual Servers** and click the **Add** icon.
- b In the **New Virtual Server** dialog box, configure the settings of the virtual server for the analytics cluster and click **OK**.

Setting	Value
Enable Virtual Server	Selected
Application Profile	VROPS_HTTPS
Name	VROPS_VIRTUAL_SERVER
IP Address	192.168.11.35
Protocol	HTTPS
Port	443
Default Pool	VROPS_POOL
Connection Limit	0
Connection Rate Limit	0

## 10 Configure auto-redirect from HTTP to HTTPS requests.

The NSX Edge can redirect users from HTTP to HTTPS without entering another URL in the browser.

- a On the **Load Balancer** tab of the LAXMGMT-LB01 device, select **Application Profiles** and click the **Add** icon.
- b In the **New Profile** dialog box, configure the application profile settings and click **OK**.

Setting	Value
Name	VROPS_REDIRECT
Type	HTTP
HTTP Redirect URL	https://vrops-cluster-01.rainpole.local/vcops-web-ent/login.action
Persistence	Source IP
Expires in (Seconds)	1800

- c On the **Load Balancer** tab of the LAXMGMT-LB01 device, select **Virtual Servers** and click the **Add** icon.
- d Configure the settings of the virtual server for HTTP redirects and click **OK**.

Setting	Value
Enable Virtual Server	Selected
Application Profile	VROPS_REDIRECT
Name	VROPS_REDIRECT
IP Address	192.168.11.35
Protocol	HTTP
Port	80
Default Pool	NONE
Connection Limit	0
Connection Rate Limit	0

## Add an Authentication Source for the Child Active Directory in Region B

Connect vRealize Operations Manager to the child Active Directory lax01.rainpole.local for central user management and access control in Region B.

### Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
  - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 In the left pane of vRealize Operations Manager, click **Administration** and click **Authentication Sources**.
- 3 On the **Authentication Sources** page, click the **Add**.
- 4 In the **Add Source for User and Group Import** dialog box, enter the settings for the LAX01.RAINPOLE.LOCAL child Active Directory in Region B, and click **OK**.

Active Directory Setting	Value
Source Display Name	LAX01.RAINPOLE.LOCAL
Source Type	Active Directory
Integration Mode	Basic
Domain/Subdomain	LAX01.RAINPOLE.LOCAL
Use SSL/TLS	Deselected
User Name	svc-vrops@rainpole.local
Password	svc-vrops_password
Settings under the <b>Details</b> section	
Automatically synchronize user membership for configured groups	Selected
Host	dc51lax.lax01.rainpole.local
Port	389
Base DN	dc=LAX01,dc=RAINPOLE,dc=LOCAL
Common Name	userPrincipalName

- 5 Click the **Test** button to test the connection to the domain controller, and in the **Info** success message click **OK**.

- 6 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.

### Prerequisites

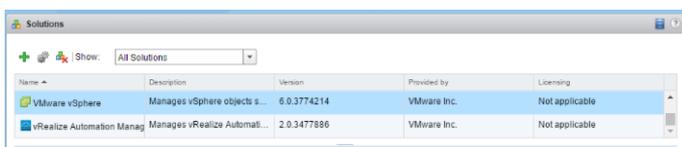
- Verify that the Management vCenter Server and Compute vCenter Server are running.
- Verify that the Management vCenter Server and Compute vCenter Server are configured with the rainpole.local Active Directory domain.
- Create a custom read-only role for user svc-vrops.

### Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
  - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.
- 3 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.

- 4 On the **Configure Adapters** page, from the **Adapter Type** table at the top, select **vCenter Adapter**.  
The **Instance Name** list contains the instances of the vCenter adapter for Region A.

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 name, description and FQDN of vCenter Server.

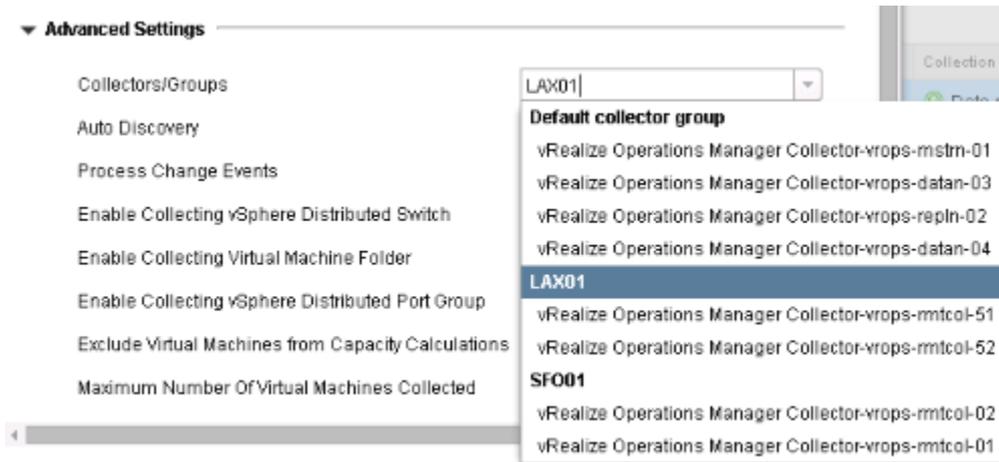
Setting	Value for Management vCenter Server	Value for Compute vCenter Server
Name	mgmt01vc51-lax01	comp01vc51-lax01
Description	Management vCenter Server for Region B	Compute vCenter Server for Region B
vCenter Server	mgmt01vc51.lax01.rainpole.local	comp01vc51.lax01.rainpole.local

- c Click the **Add** icon on the right side, configure the collection credentials for connection to the vCenter Server instances, and click **OK**.

Management vCenter Server Credentials Attribute		Value
Credential name	■	mgmt01vc51-lax01-credentials for Management vCenter Server
	■	comp01vc51-lax01-credentials for Compute vCenter Server
User Name		svc-vrops@rainpole.local
Password		svc-vrops-password

- d Leave **Enable Actions** set to **Enable** so that vCenter Adapter can run actions on objects in the vCenter Server from vRealize Operations Manager.
- e Click **Test Connection** to validate the connection to vCenter Server instance.  
The vCenter Server certificate appears.
- f In the **Review and Accept Certificate** dialog box, verify the certificate information and click **OK**.
- g Click **OK** in the **Test Connection Info** dialog box.
- h Expand the **Advanced Settings** section of settings.

- i From the **Collectors/Groups** drop-down menu, select the **LAX01** group.

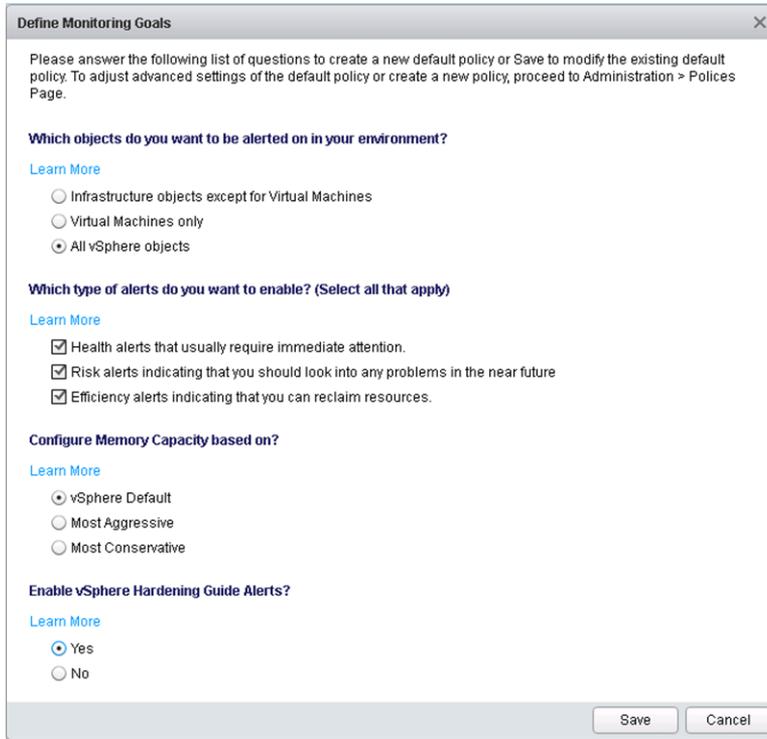


- j Specify a user account with administrator privileges to register vRealize Operations Manager with the vCenter Server instance.

Setting	Value
Registration user	administrator@vsphere.local
Registration password	vsphere_admin_password

After the registration, vCenter Server users can launch vRealize Operations Manager from and use health badges on the inventory objects in the vSphere Web Client.

- 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 **Default Policy Info** dialog box.
- 9 Click **Save Settings**.
- 10 In the **Review and Accept Certificate** dialog box, verify the certificate information and click **OK**.
- 11 Click **OK** in the **Adapter Instance Information** dialog box.
- 12 Repeat [Step 5](#) to [Step 11](#) for the Compute vCenter Server.
- 13 In the **Manage Solution - VMware vSphere** dialog box, click **Close**.
- 14 On the **Solutions** page, select **VMware vSphere** from the solution table to view the collection state and the collection status.

The **Collection State** column for the vCenter Adapters displays **Collecting**, and the **Collection Status** column displays **Data receiving**.

Name	Description	Provided by	Licensing	Adapter Status
vRealize Automation Management Pack	Manages vRealize Auto...	VMware Inc.	Not applicable	✔ Data receiving (1)
VMware vSphere	Manages vSphere object...	VMware Inc.	Not applicable	✔ Data receiving (4)

VMware vSphere Solution Details					
Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
vCenter Adapter	comp01vc51-lax01	comp01vc51-lax01-credentials	vRealize Operations Manage...	🟢 Collecting	🟢 Data receiving
vCenter Adapter	mgmt01vc51-lax01	mgmt01vc51-lax01-credentials	vRealize Operations Manage...	🟢 Collecting	🟢 Data receiving
vCenter Adapter	mgmt01vc01-sfo01	mgmt01vc01-sfo01-credentials	vRealize Operations Manage...	🟢 Collecting	🟢 Data receiving
vCenter Adapter	comp01vc01-sfo01	comp01vc01-sfo01-credentials	vRealize Operations Manage...	🟢 Collecting	🟢 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.

### Prerequisites

- Ensure that SSH has been enabled on the Management NSX Manager and Compute NSX Manager in Region B.
- On a Windows host that has access to you data center, install a REST client, such as the RESTClient add-on for Firefox.

## Procedure

- 1 Log in to the NSX Manager by using a Secure Shell (SSH) client.

- a Open an SSH connection to the NSX Manager virtual machine.

NSX Manager	Host name
NSX Manager for the management cluster	mgmt01nsxm51.lax01.rainpole.local
NSX Manager for the shared compute and edge cluster	comp01nsxm51.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<ul style="list-style-type: none"> <li>▪ <i>mngnsx_admin_password</i></li> <li>▪ <i>compnsx_admin_password</i></li> </ul>

- 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 admin password when prompted and press Enter.
- c Switch to Configuration mode.

```
configure terminal
```

- d Create the service account svc-vrops-nsx.

```
user svc-vrops-nsx password plaintext svc-vrops-nsx_password
```

- e Assign the svc-vrops-nsx user access to NSX Manager from the vSphere Web Client.

```
user svc-vrops-nsx privilege web-interface
```

- f 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 Firefox browser, go to **chrome://restclient/content/restclient.html**

- c From the **Authentication** drop-down menu, select **Basic Authentication**
- d In the **Basic Authorization** dialog box, enter the following credentials, select **Remember me** and click **Okay**.

Setting	Value
User name	admin
Password	<ul style="list-style-type: none"> <li>■ <i>mngnsx_admin_password</i></li> <li>■ <i>compnsx_admin_password</i></li> </ul>

The Authorization: Basic XXX header appears in the Headers pane.

- e In the Request pane, enter the following header details and click Okay.

Request Header Attribute	Value
Name	Content-Type
Value	Application/xml

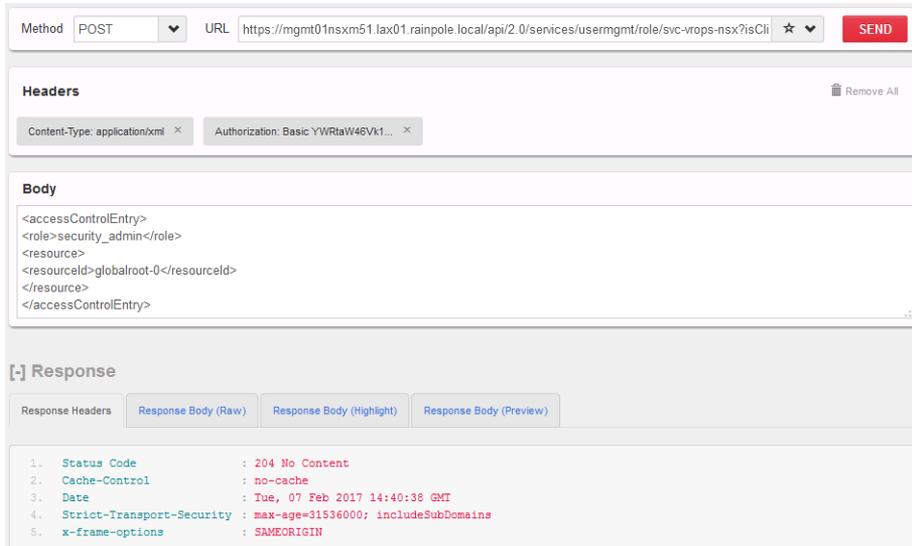
The Content-Type:application/xml header appears in the **Headers** pane.

- f In the **Request** pane, from the **Method** drop-down menu, select **POST**, and in the **URL** text box, enter the following URL.

NSX Manager	POST URL
NSX Manager for the management cluster	<a href="https://mgmt01nsxm51.lax01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true">https://mgmt01nsxm51.lax01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true</a>
NSX Manager for the shared edge and compute cluster	<a href="https://comp01nsxm51.lax01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true">https://comp01nsxm51.lax01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true</a>

- g In the **Request** pane, paste the following request body in the **Body** text box and click **Send**.

```
<accessControlEntry>
  <role>security_admin</role>
  <resource>
    <resourceId>globalroot-0</resourceId>
  </resource>
</accessControlEntry>
```



The Status changes to 204 No Content.

- h Repeat the step for the other NSX Manager.

## 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.

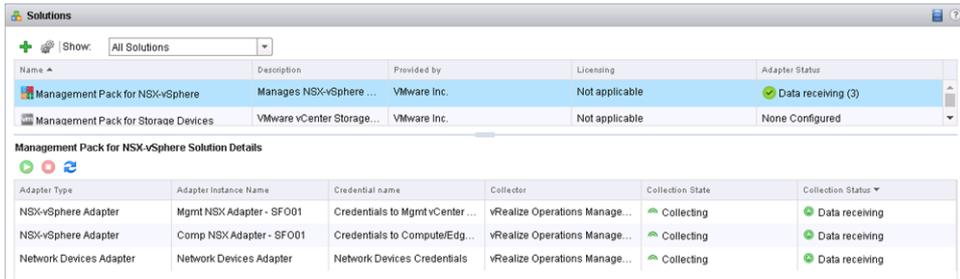
### Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
  - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.

- On the **Solutions** page, select the **Management Pack for NSX-vSphere** from the solution table, and click **Configure**.



- In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, from the **Adapter Type** table at the top, select **NSX-vSphere Adapter**.
- 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.
  - If you already have added another NSX-vSphere Adapter, click the **Add** icon to add an adapter settings.
  - Enter the name, the FQDN of the NSX Manager and the FQDN of the vCenter Server instance that is connected to the NSX Manager.

Setting	Value for the NSX Manager for the Management Cluster	Value for the NSX Manager for the Shared Edge and Compute Cluster
Display Name	Mgmt NSX Adapter - LAX01	Comp NSX Adapter - LAX01
Description	-	-
NSX Manager Host	mgmt01nsxm51.lax01.rainpole.local	comp01nsxm51.lax01.rainpole.local
VC Host	mgmt01vc51.lax01.rainpole.local	comp01vc51.lax01.rainpole.local
Enable Log Insight integration if configured	false	false

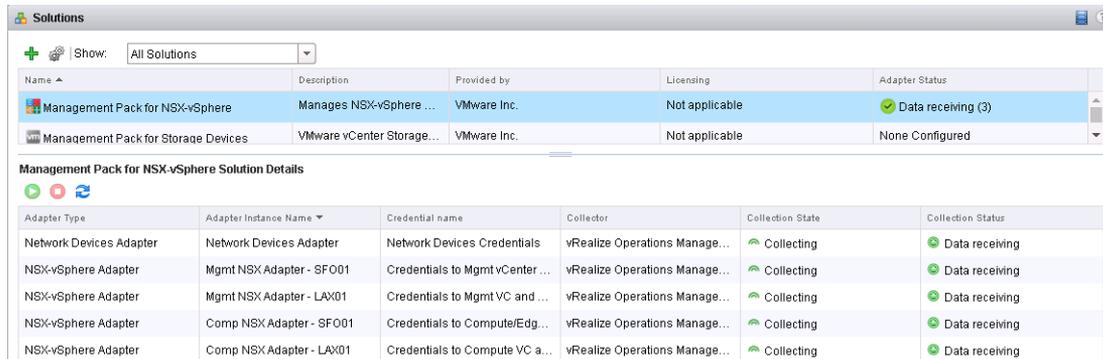
- Click the **Add** icon next to the **Credential** text box, configure the credentials for the connection to NSX Manager and vCenter Server, and click **OK**.

Setting	Value for the NSX Manager for the Management Cluster	Value for the NSX Manager for the Shared Edge and Compute Cluster
Credential name	Credentials to Mgmt VC and NSX Manager - LAX01	Credentials to Compute VC and NSX Manager - LAX01
NSX User Name	svc-vrops-nsx	svc-vrops-nsx
NSX Manager Password	<i>mgmt_nsx_manager_password</i>	<i>comp_nsx_manager_password</i>
vCenter User Name	svc-vrops@rainpole.local	svc-vrops@rainpole.local
vCenter Password	<i>svc-vrops-password</i>	<i>svc-vrops-password</i>

- d Expand the **Advanced Settings** pane.
- e In the **Advanced Settings** pane, click the **Collectors/Groups** drop-down menu, select **LAX01**
- f Click **Test Connection** to validate the connection to the Management NSX Manager or Compute NSX Manager.  
The NSX Manager certificate appears.
- g Click **Save Settings**.
- h In the **Review and Accept Certificate** dialog box, verify the certificate information and click **OK**.
- i Click **OK** in the **Adapter Instance** dialog box.
- j Repeat these steps to create an NSX-vSphere Adapter for the NSX Manager for the shared edge and compute cluster.

6 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, click **Close**.

The two NSX-vSphere Adapters for Region B are available 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 in vRealize Automation for Integration with vRealize Operations Manager in Region B

Assign the permissions that are required to access monitoring data from vRealize Automation in vRealize Operations Manager to the svc-vrops-vra operations service account.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	itac-tenantadmin_password
Domain	Rainpole.local

- 2 Navigate to **Infrastructure > Endpoints > Fabric Groups** to assign 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.

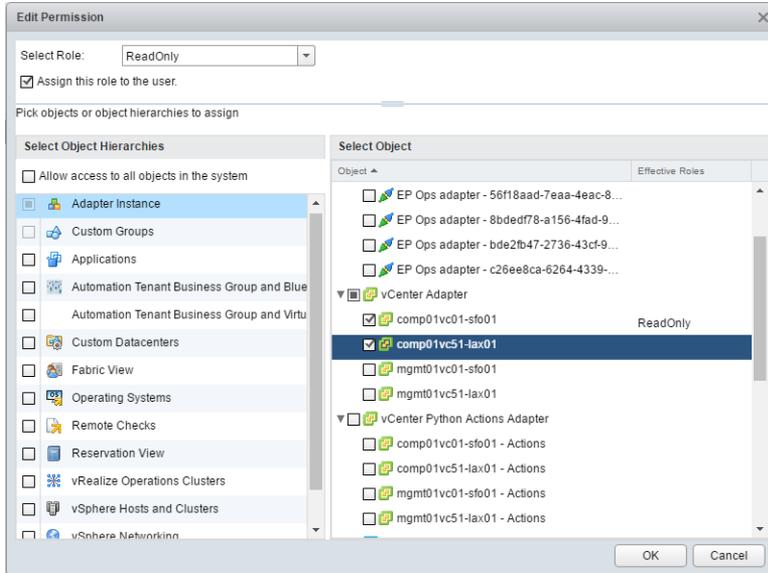
### Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
  - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 In the left pane of vRealize Operations Manager, click **Administration**, and click **Access Control**.
- 3 On the **Access Control** page, click the **User Accounts** tab.

- 4 Select the **svc-vra-vrops@rainpole.local** service account, and click **Edit** icon.
- 5 On the **Assign Groups and Permissions** page, to assign the ReadOnlly role to the svc-vra-vrops@rainpole.local service account, configure the following settings.
  - a Click the **Objects** tab.
  - b Under **Select Object**, select **vCenter Adapter > comp01vc51-lax01** .
  - c Click **OK**.



## Add Storage Devices Adapters in vRealize Operations Manager for Region B

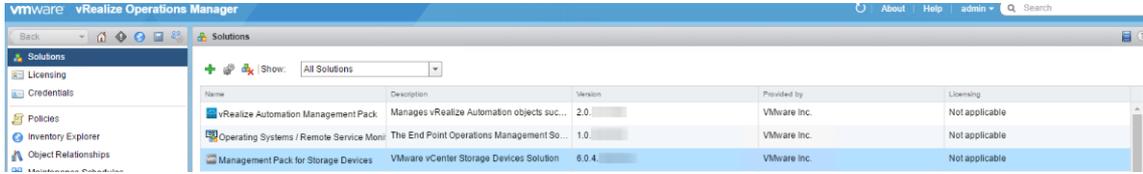
Configure a Storage Devices adapter for Region B to collect monitoring data about the storage devices in the SDDC.

### Procedure

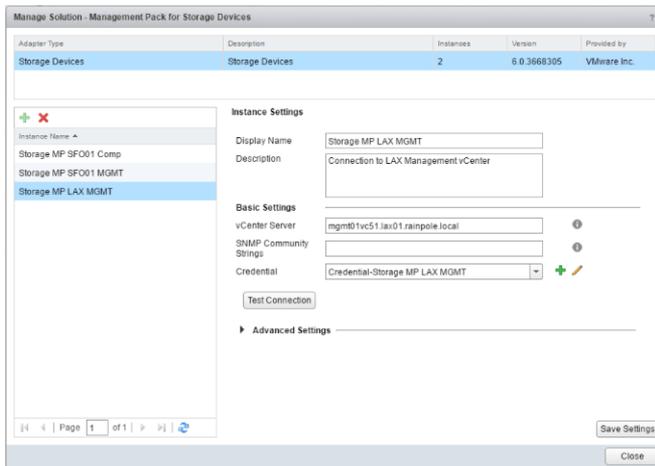
- 1 Log in to vRealize Operations Manager by using the administration console.
  - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.
- 3 On the **Solutions** page, select **Management pack for Storage Devices** from solution table and click **Configure**.



- 4 In the **Manage Solution - Management Pack for Storage Devices** dialog box, from the **Adapter Type** table at the top, select **Storage Devices**.
- 5 Under **Instance Settings**, enter the settings for connection to the Management vCenter Server or to the Compute vCenter Server.
  - a Click the **Add** icon to add an adapter settings.
  - b Enter the name, description, and FQDN of the vCenter Server instance.



Setting	Value for the Management Cluster	Value for the Shared Edge and Compute Cluster
Name	Storage MP LAX MGMT	Storage MP LAX Compute
Description	Connection to LAX Management vCenter	Connection to LAX Compute vCenter
vCenter Server	mgmt01vc51.lax01.rainpole.local	comp01vc51.lax01.rainpole.local
SNMP Community Strings	-	-

- c Click the **Add** icon, configure the credentials for connection to the Management vCenter Server to the Compute vCenter Server, and click **OK**.

Setting	Value for the Management Cluster	Value for the Shared Edge and Compute Cluster
Credential name	Credential-Storage MP LAX MGMT	Credential-Storage MP LAX Compute
User Name	svc-mpsd-vrops@rainpole.local	svc-mpsd-vrops@rainpole.local
Password	<i>svc-mpsd-vrops-password</i>	<i>svc-mpsd-vrops-password</i>

- d Click **Test Connection** to validate the connection to the Management vCenter Server or the Compute vCenter Server.

- e In the **Review and Accept Certificate** dialog box, verify the vCenter Server certificate information and click **OK**.
  - f Click **OK** in the **Test Connection** dialog box.
  - g Expand the **Advanced Settings** section of settings, and from the **Collectors/Groups** drop-down menu, select the **LAX01** remote collector group.
  - h Click **Save Settings** and click **OK** in the information box that appears.
  - i Repeat the steps for the other vCenter Server instance.
- 6 In the **Manage Solution - Management Pack for Storage Devices** dialog box, click **Close**.

The two 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**.

The screenshot shows the 'Solutions' page in vRealize Operations Manager. It displays a table of installed management packs and a detailed view of the 'Management Pack for Storage Devices'.

Name	Description	Version	Provided by	Licensing
Management Pack for Storage Devices	VMware vCenter Storage De...	6.0 4.3668305	VMware Inc.	Not applicable
Management Pack for NSX-vSphere	Manages NSX-vSphere obje...	3.0 2.3765807	VMware Inc.	Not applicable
VMware vSphere	Manages vSphere objects s...	6.0 3774214	VMware Inc.	Not applicable

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
Storage Devices	Storage MP LAX Compute	Credential-Storage MP LAX...	vRealize Operations Manag...	Collecting	Data receiving
Storage Devices	Storage MP LAX MGMT	Credential-Storage MP LAX...	vRealize Operations Manag...	Collecting	Data receiving
Storage Devices	Storage MP SFO01 Comp	Storage MP SFO01 Comp...	vRealize Operations Manag...	Collecting	Data receiving
Storage Devices	Storage MP SFO01 MGMT	Storage MP SFO01 MGMT...	vRealize Operations Manag...	Collecting	Data receiving

## 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 Install a CA-Signed Certificate on vRealize Log Insight in Region B

vRealize Log Insight comes with a default self-signed certificate that is generated and signed at installation time. After you start vRealize Log Insight in Region B, install a CA-signed certificate to secure the communication of vRealize Log Insight.

#### 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](#)

Install and configure vRealize Log Insight Content Pack for vRealize Operations Manager in Region B for troubleshooting vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight UI.

#### 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 vRealize Log Insight Content Pack for vSAN in Region B](#)

Install the content pack for VMware vSAN to add the dashboards for viewing log information 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 will not be failed over to the recovery region, Region B. 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) for balancing 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 4-2. IP Addresses and Host Name for the vRealize Log Insight Cluster in Region B**

Role	IP Address	FQDN
Integrated load balancer VIP address	192.168.32.10	vrli-cluster-51.lax01.rainpole.local
Master node	192.168.32.11	vrli-mstr-51.lax01.rainpole.local
Worker node 1	192.168.32.12	vrli-wrkr-51.lax01.rainpole.local
Worker node 2	192.168.32.13	vrli-wrkr-52.lax01.rainpole.local
Default gateway	192.168.32.1	-
DNS servers	<ul style="list-style-type: none"> <li>■ 172.17.11.5</li> <li>■ 172.16.11.5</li> </ul>	-

---

**Table 4-2. IP Addresses and Host Name for the vRealize Log Insight Cluster in Region B (Continued)**

Role	IP Address	FQDN
Subnet mask	255.255.255.0	-
NTP servers	<ul style="list-style-type: none"> <li>■ 172.16.11.251</li> <li>■ 172.16.11.252</li> <li>■ 172.17.11.251</li> <li>■ 172.17.11.252</li> </ul>	<ul style="list-style-type: none"> <li>■ ntp.sfo01.rainpole.local</li> <li>■ ntp.lax01.rainpole.local</li> </ul>

## Deployment Prerequisites

Prerequisite	Value
Storage	<ul style="list-style-type: none"> <li>■ Virtual disk provisioning               <ul style="list-style-type: none"> <li>■ Thin</li> </ul> </li> <li>■ Required storage per node               <ul style="list-style-type: none"> <li>■ Initial storage for node deployment:510 GB</li> </ul> </li> </ul>
Software Features	<ul style="list-style-type: none"> <li>■ vSphere               <ul style="list-style-type: none"> <li>■ Management vCenter Server</li> <li>■ Management cluster with DRS and HA enabled.</li> </ul> </li> <li>■ NSX for vSphere               <ul style="list-style-type: none"> <li>■ Application virtual network for the 3-node vRealize Log Insight cluster</li> </ul> </li> </ul>
Installation Package	Download the .ova file of the vRealize Log Insight virtual appliance on the machine where you use the vSphere Web Client.
License	Obtain a license that covers the use of vRealize Log Insight.
Active Directory	Verify that you have a parent and child Active Directory domain controllers configured with the role-specific SDDC users and groups for the rainpole.local domain.
Certification Authority	Configure the Active Directory domain controller as a certificate authority for the environment.
E-mail account	Provide an email account to send vRealize Log Insight notifications from.

## Deploy the Virtual Appliance for Each Node in the vRealize Log Insight Cluster in Region B

Use the vSphere Web Client to deploy each vRealize Log Insight node as a virtual appliance on the management cluster in Region B.

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to the mgmt01vc51.lax01.rainpole.local vCenter Server object.
- 3 Right-click **mgmt01vc51.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
vrii-mstr-51	Master node
vrii-wrkr-51	Worker node 1
vrii-wrkr-52	Worker node 2

- b Select the inventory folder for the virtual appliance.

Object	Value
vCenter Server	mgmt01vc51.lax01.rainpole.local
Data center	LAX01
Folder	vRLI51

- 6 On the **Select a resource** page, select the **LAX01-Mgmt01** management cluster as the resource to run the virtual appliance on, and click **Next**.
- 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, 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 datastore for the vRealize Log Insight node.

By default, the virtual appliance disk is thin provisioned.

a From the **VM Storage Policy** drop-down menu, select **Virtual SAN Default Storage Policy**.

b From the datastore table, select the **LAX01A-VSAN01-MGMT01** vSAN datastore and click **Next**.

**11** On the **Setup networks** page, select the distributed port group on the vDS-Mgmt distributed switch that ends with Mgmt-RegionB01-VXLAN, and click **Next**.

**12** On the **Customize template** page, set the networking settings and the root user credentials for the virtual appliance.

- a In the **Networking Properties** section, configure the following networking settings.

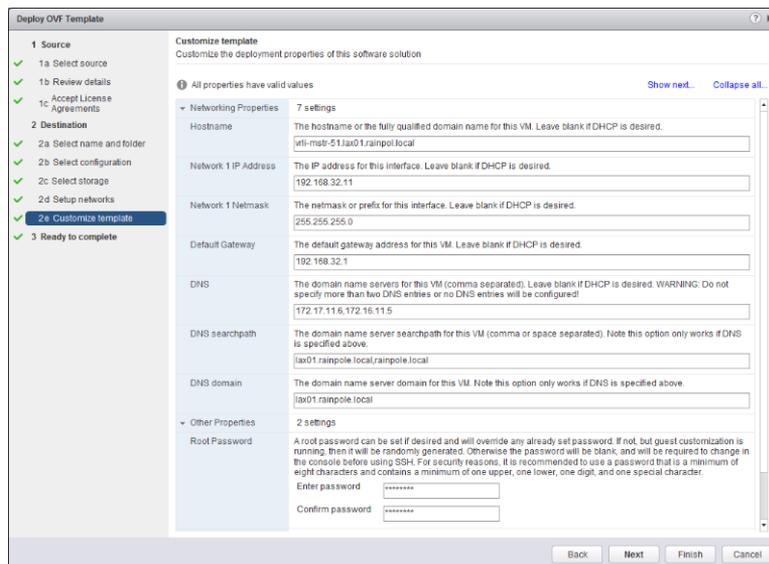
Property	Value
Host name	<ul style="list-style-type: none"> <li>■ vrl-i-mstr-51.lax01.rainpole.local for the master node</li> <li>■ vrl-i-wrkr-51.lax01.rainpole.local for the worker node 1</li> <li>■ vrl-i-wrkr-52.lax01.rainpole.local for the worker node 2</li> </ul>
Default gateway	192.168.32.1
DNS server	172.17.11.5,172.16.11.5
DNS searchpath	lax01.rainpole.local,rainpole.local
DNS domain	lax01.rainpole.local
Static IPv4 address	<ul style="list-style-type: none"> <li>■ 192.168.32.11 for the master node</li> <li>■ 192.168.32.12 for the worker node 1</li> <li>■ 192.168.32.13 for the worker node 2</li> </ul>
Subnet mask	255.255.255.0

- b In the **Other Properties** section, enter and confirm a password for the root user and click **Next**.

The password must contain at least 8 characters, and must include:

- One uppercase character
- One lowercase character
- One digit
- One special character

Use this password if you log in to the console of the vRealize Log Insight virtual appliance.



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

The deployment of the virtual appliance starts.

**14** Right-click the virtual appliance object and select the **Power > Power On** menu item.

**15** Repeat the procedure to deploy the vRealize Log Insight virtual appliances for the remaining two nodes in the cluster.

## Configure a DRS Anti-Affinity Rule for vRealize Log Insight in Region B

To protect the vRealize Log Insight cluster in Region B from a host-level failure, configure vSphere DRS to run the worker virtual appliances on different hosts in the management cluster.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to the mgmt01vc51.lax01.rainpole.local vCenter Server object, and under the **LAX01** data center object select the **LAX01-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 called **vrli-antiaffinity-rule** for the vrli-mstr-51, vrli-wrkr-51 and vrli-wrkr-52 virtual machines, and click **OK**.

Rule Attribute	Value
Name	anti-affinity-rule-vrli
Enable rule	Yes
Type	Separate Virtual Machines
Members	<ul style="list-style-type: none"> <li>■ vrli-mstr-51</li> <li>■ vrli-wrkr-51</li> <li>■ vrli-wrkr-52</li> </ul>

## 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://vrli-mstr-51.lax01.rainpole.local>**.

The initial configuration wizard opens.

- 2 On the **Setup** page, click **Next**.
- 3 On the **Choose Deployment Type** page, click **Start New Deployment**.
- 4 After the deployment is launched, on the **Admin Credentials** page, set the email address and the password of the admin user, and click **Save and Continue**.

The password must contain at least 8 characters, and contain one uppercase character, one lowercase character, one number, and one special character.

- 5 On the License page, enter the license key, click **Add New License Key**, and click **Continue**.
- 6 On the **General Configuration** page, enter the following settings and click **Save and Continue**.

Setting	Value
Email System Notifications to	<i>email address to receive system notifications</i>
Send HTTP Post System Notifications To	<a href="https://vrli-cluster-51.lax01.rainpole.local">https://vrli-cluster-51.lax01.rainpole.local</a>

- 7 On the **Time Configuration** page, enter the following settings, click **Test** and click **Save and Continue**.

Setting	Value
Sync Server Time With	NTP Server (recommended)
NTP Servers	ntp.lax01.rainpole.local, ntp.sfo01.rainpole.local

- 8 On the **SMTP Configuration** page, specify the properties of an SMTP server to enable outgoing alerts and system notification emails, and to test the email notification.
  - a Set the connection setting for the SMTP server that will send the email messages from vRealize Log Insight.

Contact your system administrator for details about the email server.

SMTP Option	Description
SMTP Server	FQDN of the SMTP server
Port	Server port for SMTP requests
SSL (SMTPS)	Sets whether encryption should be enabled for the SMTP transport option connection.
STARTTLS Encryption	Enable or disable the STARTTLS encryption.
Sender	Address that appears as the sender of the email.
Username	User name on the SMTP server.
Password	Password for the SMTP server you specified in Username.

- b To verify that the SMTP configuration is correct, enter a valid email address and click **Send > Test Email**.

vRealize Log Insight sends a test email to the address that you provided.

- 9 On the **Setup Complete** page, click **Finish**.

vRealize Log Insight starts operating in standalone mode.

## Join the Worker Nodes to vRealize Log Insight in Region B

After you deploy the virtual appliances for vRealize Log Insight and start the vRealize Log Insight instance on the master node in Region B, join the two worker nodes to form a cluster.

### Procedure

- 1 For each worker node appliance, go to the initial setup UI in your Web browser.

Worker Node	HTTP URL
Worker node 1	https://vrli-wrkr-51.lax01.rainpole.local
Worker node 2	https://vrli-wrkr-52.lax01.rainpole.local

The initial configuration wizard opens.

- 2 Click the **Next** button on the **Welcome** page.
- 3 On the **Choose Deployment Type** page, click **Join Existing Deployment**.
- 4 On the **Join Existing Deployment** page, enter the master node FQDN `vrli-mstr-51.lax01.rainpole.local` and click **Go**.

The worker node sends a request to the vRealize Log Insight master node to join the existing deployment.

- 5 After the worker node contacts the master node, click the **Click here to access the Cluster Management page** link.

The login page of the vRealize Log Insight user interface opens.

- 6 Log in to the vRealize Log Insight UI by using the following credentials.

Setting	Value
User name	admin
Password	<i>vrl_i_admin_password</i>

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) for balancing 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://vrl\_i-mstr-51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrl_i_admin_password</i>

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Management**, click **Cluster**.
- 4 Under **Integrated Load Balancer**, click **New Virtual IP Address**.
- 5 In the **New Virtual IP** dialog box, enter the following settings and click **Save**.

Setting	Value
IP	192.168.32.10
FQDN	vrl_i-cluster-51.lax01.rainpole.local

## Join vRealize Log Insight to the Active Directory in Region B

To propagate user roles in vRealize Log Insight that are maintained centrally and are inline with the other solutions in the SDDC, configure vRealize Log Insight in Region B to use the Active Directory (AD) domain as an authentication source.

### Figure 4-1. Procedure

#### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://vrli-cluster-51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 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.

Setting	Value
Enable Active Directory support	Selected
Default Domain	RAINPOLE.LOCAL
User Name	svc-loginsight
Password	<i>svc_loginsight_password</i>
Connection Type	Standard
Require SSL	Yes or No according to the instructions from the IT administrator

- b Click **Test Connection** to verify the connection, and click **Save**.

## Install a CA-Signed Certificate on vRealize Log Insight in Region B

vRealize Log Insight comes with a default self-signed certificate that is generated and signed at installation time. After you start vRealize Log Insight in Region B, install a CA-signed certificate to secure the communication of vRealize Log Insight.

vRealize Log Insight uses a certificate for the following communication:

- Connection to the vRealize Log Insight UI
- SSL syslog transfers

- Communication from the Log Insight agents through the Ingestion API

vRealize Log Insight accepts only PEM encoded certificates that include the complete certification chain. The private key must not be encrypted by a pass phrase.

## Replace the Certificate to vRealize Log Insight in Region B

After you generate the PEM certificate chain file that contains the own certificate, the signer certificate and the private key file, upload the certificate chain to 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://vrli-cluster-51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 2 In the vRealize Log Insight UI, click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Configuration**, click **SSL**.
- 4 On the **SSL Configuration** page, next to **New Certificate File (PEM format)** click **Choose File**, browse to the location of the `vrli.lax01.2.chain.pem` file on your computer, and click **Save**.  
The certificate is uploaded to vRealize Log Insight.
- 5 In a Web browser, go to **https://vrli-cluster-51.lax01.rainpole.local**.  
A warning message that the connection is not trusted appears.
- 6 To review the certificate, click the padlock  icon in the address bar of the browser, and verify that the **Subject Alternative Name** contains the names of the vRealize Log Insight cluster nodes.
- 7 Import the certificate in your Web browser.  
For example, in Google Chrome under the **HTTPS/TLS** settings click the **Manage certificates** button, and in the **Certificates** dialog box import `vrli.lax01.2.chain.pem`.

You can also use Certificate Manager on Windows or Keychain Access on MAC OS X.

## Connect vRealize Log Insight to the vSphere Environment in Region B

Start collecting log information about the ESXi and vCenter Server instances in the SDDC in Region B.

## Procedure

### 1 Connect vRealize Log Insight to vSphere in Region B

After you configure the svc-loginsight AD user with the vSphere privileges that are required for retrieving log information from the vCenter Server instances and ESXi hosts, in Region B 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.

## Connect vRealize Log Insight to vSphere in Region B

After you configure the svc-loginsight AD user with the vSphere privileges that are required for retrieving log information from the vCenter Server instances and ESXi hosts, in Region B connect vRealize Log Insight to vSphere.

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://vrli-cluster-51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Integration**, click **vSphere**.

4 In the **vCenter Servers** pane, enter the connection settings for the Management vCenter Server and for the Compute vCenter Server.

a Enter the host name, user credentials, and collection options for the vCenter Server instances, and click **Test Connection**.

vCenter Server Option	Value
Hostname	<ul style="list-style-type: none"> <li>■ mgmt01vc51.lax01.rainpole.local</li> <li>■ comp01vc51.lax01.rainpole.local</li> </ul>
Username	svc-loginsight@rainpole.local
Password	<i>svc-loginsight_user_password</i>
Collect vCenter Server events, tasks and alarms	Selected
Configure ESXi hosts to send logs to Log Insight	Selected

b Click **Advanced Options** and examine the list of ESXi hosts that are connected to the vCenter Server instance to verify that you connect to the correct vCenter Server .

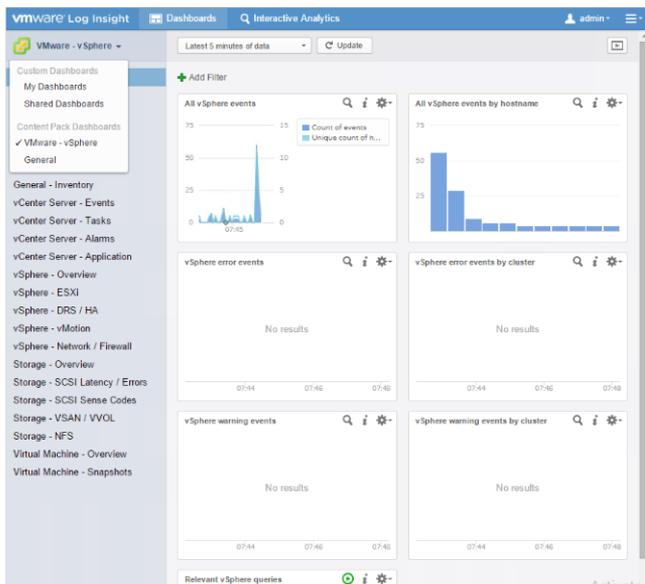
c Click **Add vCenter Server** to add a new settings form and repeat the steps to add the settings for the second vCenter Server instance in Region B.

5 Click **Save**.

A progress dialog box appears.

6 Click **OK** in the confirmation dialog box that appears after vRealize Log Insight contacts the vCenter Server instances.

You see the vSphere dashboards under the VMware - vSphere content pack dashboard category.



## Configure vCenter Server to Forward Log Events to vRealize Log Insight in Region B

You can configure each vCenter Server and Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster. You can then view and analyze all syslog information in the vRealize Log Insight web interface.

In Region B, you configure the following vCenter Server and Platform Services Controller instances:

Appliance Type	Appliance Management Interface URL
vCenter Server instances	<ul style="list-style-type: none"> <li>▪ <a href="https://mgmt01vc51.lax01.rainpole.local:5480">https://mgmt01vc51.lax01.rainpole.local:5480</a></li> <li>▪ <a href="https://comp01vc51.lax01.rainpole.local:5480">https://comp01vc51.lax01.rainpole.local:5480</a></li> </ul>
Platform Services Controller instances	<ul style="list-style-type: none"> <li>▪ <a href="https://mgmt01psc51.lax01.rainpole.local:5480">https://mgmt01psc51.lax01.rainpole.local:5480</a></li> <li>▪ <a href="https://comp01psc51.lax01.rainpole.local:5480">https://comp01psc51.lax01.rainpole.local:5480</a></li> </ul>

### Procedure

- 1 Redirect the log events from the appliance to vRealize Log Insight.
  - a Open a Web browser and go to **<https://mgmt01vc51.lax01.rainpole.local:5480>**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>mgmtvc_root_password</i>

- c In the **Navigator**, click **Syslog Configuration**.
  - d On the **Syslog Configuration** page, click **Edit**, configure the following settings, and click **OK**.

Setting	Value
Common Log Level	*
Remote Syslog Host	vrli-cluster-51.lax01.rainpole.local
Remote Syslog Port	514
Remote Syslog Protocol	UDP

- e Repeat the steps for the other vCenter Server Appliance and Platform Services Controller Appliances.
- 2 Verify that the appliances are forwarding their syslog traffic to vRealize Log Insight.
  - a Open a Web browser and go to **<https://vrli-cluster-51.lax01.rainpole.local>**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- c In the vRealize Log Insight user interface, click **Dashboards** and select **VMware - vSphere** from the content pack dashboard drop-down menu.
- d Verify that the vCenter Server and Platform Services Controller nodes are presented on the **All vSphere events by hostname** widget of the **General Overview** dashboard.

## Connect vRealize Log Insight to vRealize Operations Manager in Region B

Install and configure vRealize Log Insight Content Pack for vRealize Operations Manager in Region B for troubleshooting vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight UI.

### Procedure

#### 1 Install the vRealize Log Insight Content Pack for vRealize Operations Manager in Region B

Install the content pack for vRealize Operations Manager to add the dashboards for viewing log information in vRealize Log Insight.

#### 2 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.

## Install the vRealize Log Insight Content Pack for vRealize Operations Manager in Region B

Install the content pack for vRealize Operations Manager to add the dashboards for viewing log information in vRealize Log Insight.

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://vrli-cluster-51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under **Content Pack Marketplace**, select **Marketplace**.
- 4 In the list of content packs, locate the **VMware - vRops 6.x** content pack and click its icon.

5 In the **Install Content Pack** dialog box, click **Install**.

After the installation is complete, the VMware - vRops 6.x content pack appears in the **Installed Content Pack** list on the left.

### **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 On your computer, create a `liagent.ini` file for each of the 2 remote collector nodes of vRealize Operations Manager in Region B.

You can place each file in a node-specific folder.

- a Create an empty `liagent.ini` file and paste the following template configuration.

```

; Client-side configuration of VMware Log Insight Agent
; See liagent-effective.ini for the actual configuration used by VMware Log Insight Agent

[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
hostname=<YOUR LOGINSIGHT HOSTNAME HERE>

; 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

[storage]
;max_disk_buffer - max disk usage limit (data + logs) in MB:
; 100 - 2000 MB, default 200
;max_disk_buffer=200

[logging]
;debug_level - the level of debug messages to enable:
; 0 - no debug messages
; 1 - trace essential debug messages
; 2 - verbose debug messages (will have negative impact on performance)
;debug_level=0

[filelog|messages]
directory=/var/log
include=messages;messages.?

[filelog|syslog]

```

```

directory=/var/log
include=syslog;syslog.?

[filelog|COLLECTOR-collector]
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"COLLECTOR","vmw_vr_ops_clustername":"<YOUR CLUSTER NAME HERE>",
"vmw_vr_ops_clusterrole":"Master","vmw_vr_ops_nodename":"<YOUR NODE NAME HERE>",
"vmw_vr_ops_hostname":"<YOUR VROPS HOSTNAME HERE>"}
directory = /data/vcops/log
include = collector.log*
exclude_fields=hostname
event_marker=^\\d{4}-\\d{2}-\\d{2}[\\s]\\d{2}:\\d{2}:\\d{2}\\.\d{3}

[filelog|COLLECTOR-collector_wrapper]
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"COLLECTOR","vmw_vr_ops_clustername":"<YOUR CLUSTER NAME HERE>",
"vmw_vr_ops_clusterrole":"Master","vmw_vr_ops_nodename":"<YOUR NODE NAME HERE>",
"vmw_vr_ops_hostname":"<YOUR VROPS HOSTNAME HERE>"}
directory = /data/vcops/log
include = collector-wrapper.log*
exclude_fields=hostname
event_marker=^\\d{4}-\\d{2}-\\d{2}[\\s]\\d{2}:\\d{2}:\\d{2}\\.\d{3}

[filelog|COLLECTOR-collector_gc]
directory = /data/vcops/log
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"COLLECTOR","vmw_vr_ops_clustername":"<YOUR CLUSTER NAME HERE>",
"vmw_vr_ops_clusterrole":"Master","vmw_vr_ops_nodename":"<YOUR NODE NAME HERE>",
"vmw_vr_ops_hostname":"<YOUR VROPS HOSTNAME HERE>"}
include = collector-gc*.log*
exclude_fields=hostname
event_marker=^\\d{4}-\\d{2}-\\d{2}[\\w]\\d{2}:\\d{2}:\\d{2}\\.\d{3}

[filelog|CALL_STACK-call_stack]
tags = {"vmw_vr_ops_appname":"vROps","vmw_vr_ops_logtype":"CALL_STACK",
"vmw_vr_ops_clustername":"<YOUR CLUSTER NAME HERE>","vmw_vr_ops_clusterrole":"Master",
"vmw_vr_ops_nodename":"<YOUR NODE NAME HERE>","vmw_vr_ops_hostname":"<YOUR VROPS HOSTNAME

```

```
HERE>"}
directory = /data/vcops/log/callstack
include = collector*.txt
exclude_fields=hostname
```

- b In the node-specific `liagent.ini` file, change the following parameters and save the file.

Parameter	Description	Location in <code>liagent.ini</code>	Configuration Instructions
<code>hostname</code>	IP address or FQDN of the Log Insight VIP	[server] section	Replace <YOUR LOGINSIGHT HOSTNAME HERE> with <code>vrli-cluster-51.lax01.rainpole.local</code> .
<code>proto</code>	Protocol that the agent uses to send events to the Log Insight server.	[server] section	Remove the ; comment in front of the parameter to set the log protocol to <code>cfapi</code> .
<code>port</code>	Communication port that the agent uses to send events to the vRealize Log Insight server.	[server] section	Remove the ; comment in front of the parameter to set the port to <code>9000</code> .
<code>vmw_vr_ops_clustername</code>	Name of the vRealize Operations Manager cluster	each [filelog  <i>section_name</i> ] section	Replace each <YOUR CLUSTER NAME HERE> with <code>vrops-cluster-01</code> .
<code>vmw_vr_ops_clusterrole</code>	Role of the vRealize Operations Manager node	each [filelog  <i>section_name</i> ] section	Set to <b>Remote Collector</b> .
<code>vmw_vr_ops_hostname</code>	IP address or FQDN of the vRealize Operations Manager node	each [filelog  <i>section_name</i> ] section	Replace each <YOUR VROPS HOSTNAME NAME HERE> with the following FQDN: <ul style="list-style-type: none"> <li>■ <code>vrops-rmtcol-51.lax01.rainpole.local</code> for remote collector 1</li> <li>■ <code>vrops-rmtcol-52.lax01.rainpole.local</code> for remote collector 2</li> </ul>
<code>vmw_vr_ops_nodename</code>	Name of the vRealize Operations Manager node that is set during node initial configuration	each [filelog  <i>section_name</i> ] section	Replace each <YOUR NODE NAME HERE> with the following name: <ul style="list-style-type: none"> <li>■ <code>vrops-rmtcol-51</code> for remote collector 1</li> <li>■ <code>vrops-rmtcol-52</code> for remote collector 2</li> </ul>

You change the [server] section as follows.

```
[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
hostname=vrl-cluster-51.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
```

For example, on the remote collector node vrops-rmtcol-51 you change the [filelog|ANALYTICS-analytics] section that is related to the logs files of the analytics module as follows.

```
[filelog|ANALYTICS-analytics]
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"COLLECTOR","vmw_vr_ops_clustername":"vrops-cluster-51",
"vmw_vr_ops_clusterrole":"Remote Collector","vmw_vr_ops_nodename":"vrops-rmtcol-51",
"vmw_vr_ops_hostname":"vrops-rmtcol-51.lax01.rainpole.local"}
directory = /data/vcops/log
include = analytics*.log*
exclude_fields=hostname
```

## 2 Enable SSH on each node of vRealize Operations Manager.

- a Open a Web browser and go to <https://mgmt01vc51.lax01.rainpole.local/vsphere-client> .
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- c Under the mgmt01vc51.lax51.rainpole.local vCenter Server, navigate to the virtual appliance for the node.

Virtual Appliance Name	Role
vrops-rmtcol-51	Remote collector 1
vrops-rmtcol-52	Remote collector 2

- d Right-click the appliance node and select **Open Console** to open the remote console to the appliance.
- e Press ALT+F1 to switch to the command prompt.
- f Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrops_root_password</i>

- g Start the SSH service by running the command.

```
service sshd start
```

- h Close the virtual appliance console.

### 3 Apply the Log Insight agent configuration.

- a On the appliance, replace the `liagent.ini` file in the `/var/lib/loginsight-agent` folder with the node-specific file on your computer.

You can use `scp`, FileZilla or WinSCP.

- b Restart the Log Insight agent on node by running the following console command as the root user.

```
/etc/init.d/liagentd restart
```

- c Stop the SSH service on the virtual appliance by running the following command.

```
service sshd stop
```

### 4 Repeat the steps for the second remote collector node.

5 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://vrli-cluster-51.lax01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- c Click the configuration drop-down menu icon and select Administration.
- d Under Management, click Agents.
- e From the drop-down menu on the top, select **vRops 6.x - 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 field and click **Copy**.
- h In the **agent filter** fields, enter the following values pressing Enter after each host name.

Filter	Operator	Value
Hostname	matches	■ vrops-rmtcol-51.lax01.rainpole.local
		■ vrops-rmtcol-52.lax01.rainpole.local

- i Click **Refresh** and verify that all the agents in the filter appear in the **Agents** list.
- j Click **Save New Group** at the bottom of the page.
- k Click the **Dashboard** tab and select the **VMware - vRops 6.x** dashboard from the drop-down 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 the shared compute and edge cluster to forward log information to vRealize Log Insight in Region B by using the NSX REST API. You can use a REST client, such as the RESTClient add-on for Firefox, to enable log forwarding.

## 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://vrli-cluster-51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under **Content Pack Marketplace**, select **Marketplace**.
- 4 In the list of content packs, locate the **VMware - NSX-vSphere** content pack and click its icon.
- 5 In the **Install Content Pack** dialog box, accept the **License Agreement** and click **Install**.

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.

NSX Manager	URL
NSX Manager for the management cluster	https://mgmt01nsxm51.lax01.rainpole.local
NSX Manager for the shared compute and edge cluster	https://comp01nsxm51.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	nsx_manager_admin_password

- 2 On the main page of the appliance user interface, click **Manage Appliance Settings**.
- 3 Under **Settings**, click **General**, and in the **Syslog Server** pane, click **Edit**.
- 4 In the **Syslog Server** dialog box, configure vRealize Log Insight as a syslog server by specifying the following settings and click **OK**.

Syslog Server Setting	Value
Syslog Server	vrli-cluster-51.lax01.rainpole.local
Port	514
Protocol	UDP

- 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 the shared compute and edge cluster to forward log information to vRealize Log Insight in Region B by using the NSX REST API. You can use a REST client, such as the RESTClient add-on for Firefox, to enable log forwarding.

**Prerequisites**

On a Windows host that has access to your data center, install a REST client, such as the RESTClient add-on for Firefox.

**Procedure**

- 1 Log in to the Windows host that has access to your data center.
- 2 In a Firefox browser, go to **chrome://restclient/content/restclient.html**.

### 3 Specify the request headers for requests to the NSX Manager.

- a From the **Authentication** drop-down menu, select **Basic Authentication**.
- b In the **Basic Authorization** dialog box, enter the following credentials, select **Remember me** and click **Okay**.

Authentication Attribute	Value
Username	admin
Password	<i>mngnsx_admin_password</i> <i>compnsx_admin_password</i>

The `Authorization:Basic XXX` header appears in the **Headers** pane.

- c From the **Headers** drop-down menu, select **Custom Header**.
- d In the **Request Header** dialog box, enter the following header details and click **Okay**.

Request Header Attribute	Value
Name	Content-Type
Value	application/xml

The `Content-Type:application/xml` header appears in the **Headers** pane.

### 4 Contact the NSX Manager to retrieve the IDs of the associated NSX Controllers.

- a In the **Request** pane, from the **Method** drop-down menu, select **GET**.
- b In the **URL** text box, enter the following URL, and click **Send**.

NSX Manager	URL
NSX Manager for the management cluster	<code>https://mgmt01nsxm51.lax01.rainpole.local/api/2.0/vdn/controller</code>
NSX Manager for the shared compute and edge cluster	<code>https://comp01nsxm51.lax01.rainpole.local/api/2.0/vdn/controller</code>

The RESTClient sends a query to the NSX Manager about the installed NSX controllers.

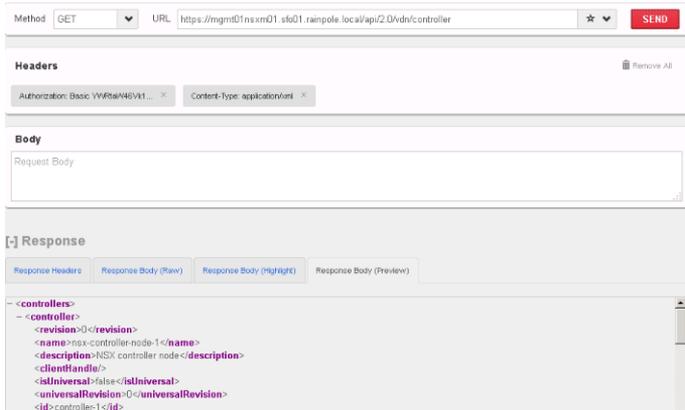
- c After the NSX Manager sends a response back, click the **Response Body (Preview)** tab under Response.

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-2`.

- e Repeat the steps for the other NSX Manager.



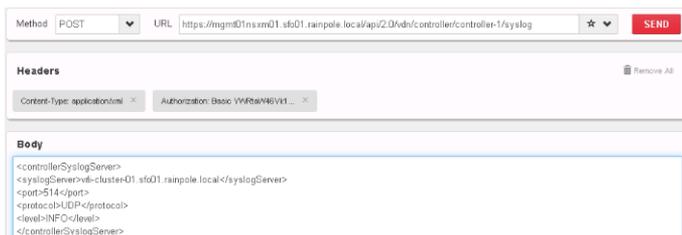
- 5 For each NSX Controller, send a request to configure vRealize Log Insight as a remote syslog server.
  - a In the **Request** pane, from the **Method** drop-down menu, select **POST**, and in the **URL** text box, enter the following URL.

NSX Manager	NSX Controller in the Controller Cluster	POST URL
NSX Manager for the management cluster	NSX Controller 1	https://mgmt01nsxm51.lax01.rainpole.local/api/2.0/vdn/controller/controller-1/syslog
	NSX Controller 2	https://mgmt01nsxm51.lax01.rainpole.local/api/2.0/vdn/controller/controller-2/syslog
	NSX Controller 3	https://mgmt01nsxm51.lax01.rainpole.local/api/2.0/vdn/controller/controller-3/syslog
NSX Manager for the shared edge and compute cluster	NSX Controller 1	https://comp01nsxm51.lax01.rainpole.local/api/2.0/vdn/controller/controller-1/syslog
	NSX Controller 2	https://comp01nsxm51.lax01.rainpole.local/api/2.0/vdn/controller/controller-2/syslog
	NSX Controller 3	https://comp01nsxm51.lax01.rainpole.local/api/2.0/vdn/controller/controller-3/syslog

- b In the **Request** pane, paste the following request body in the **Body** text box and click **Send**.

```
<controllerSyslogServer>
  <syslogServer>vrli-cluster-51.lax01.rainpole.local</syslogServer>
  <port>514</port>
  <protocol>UDP</protocol>
  <level>INFO</level>
</controllerSyslogServer>
```

- c Repeat the steps for the next NSX Controller.



- 6 Verify the syslog configuration on each NSX Controller.
  - a In the **Request** pane, from the **Method** drop-down menu, select **GET**, and in the **URL** text box, enter the controller-specific syslog URL from [Step 5](#).

- b After the NSX Manager sends a response back, click the **Response Body (Preview)** 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 `vrli-cluster-51.lax01.rainpole.local`.
  - d Repeat the steps for the next NSX Controller.

## 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://mgmt01vc51.lax01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Networking & Security**.
- 3 From the **Networking & Security** menu on the left, click **NSX Edges**.
- 4 On the **NSX Edges** page, select the NSX Manager instance from the **NSX Manager** drop-down menu.

NSX Manager Instance	IP Address
NSX Manager for the management cluster	172.17.11.65
NSX Manager for the shared edge and compute cluster	172.17.11.66

The edge devices in the scope of the NSX Manager appear.

## 5 Configure the log forwarding on each edge service gateway.

- a Double-click the edge device to open its user interface.

Management NSX Edge Service Gateway	Compute NSX Edge Service Gateway
LAXMGMT-ESG01	LAXCOMP-ESG01
LAXMGMT-ESG02	LAXCOMP-ESG02
LAXMGMT-LB01	-

- b On the NSX edge device page, click the **Manage** tab, click **Settings** and click **Configuration**.
- c In the **Details** panel, click **Change** next to **Syslog servers**.
- d In the **Edit Syslog Servers Configuration** dialog box, configure the following settings and click **OK**.

Setting	Value
Syslog server 1	192.168.32.10
Protocol	udp

- e Repeat the steps for the next NSX edge device.

The vRealize Log Insight user interface in Region B starts showing log data in the NSX-vSphere-Overview dashboard available under the VMware - NSX-vSphere group of content pack dashboards.

## 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.

### 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://vrli-cluster-51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under **Content Pack Marketplace**, select **Marketplace**.
- 4 In the list of content packs, locate the **VMware - vRA 7** content pack and click its icon.
- 5 In the **Install Content Pack** dialog box, click **Install**.
- 6 Repeat the procedure to install the VMware - Orchestrator 7.0.1+ and Microsoft - SQL Server content pack

After the installation is complete, the VMware - vRA 7, VMware - Orchestrator and Microsoft - SQL Server content packs appear in the **Installed Content Packs** list on the left.

## 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.

vRealize Automation Component	Host Name/VM Name
vSphere Proxy Agent	vra01ias51.lax01.rainpole.local
vSphere Proxy Agent	vra01ias52.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	<i>windows_administrator_password</i>

- c On the Windows host, open a Web browser and go to **<https://vrli-cluster-51.lax01.rainpole.local>**.
- d Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 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 Log Insight Agent.msi file to the Windows host.
- i Double-click the .msi file to run the installer.
- j In the **VMware vRealize Log Insight Agent Setup** wizard, accept the license agreement and click **Next**.
- k With the Log Insight host name vrli-cluster-51.lax01.rainpole.local shown in the **Host** text box, click **Install**.
- l When the installation is complete, click **Finish**.

- 2 Configure the Log Insight Windows Agents Group from the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://vrli-cluster-51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

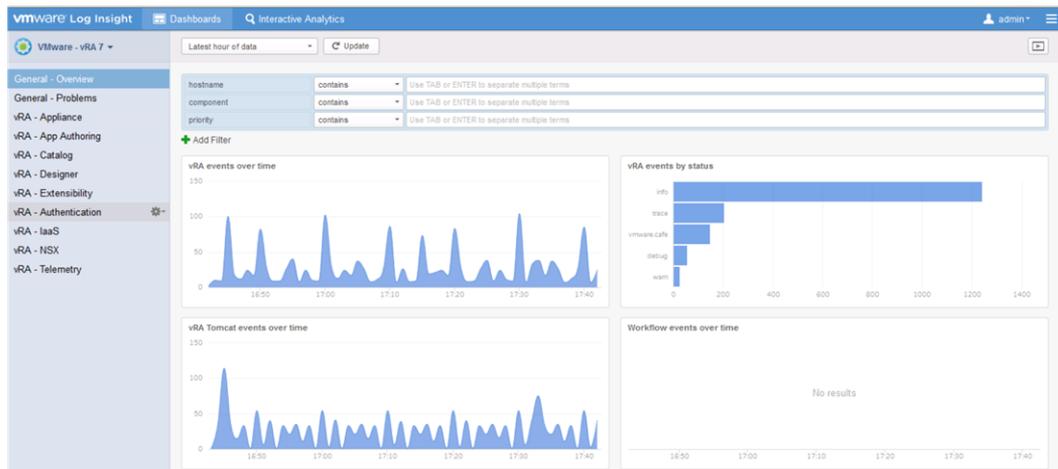
- c Click the configuration drop-down menu icon  and select **Administration**.
- d Under **Management**, click **Agents**.
- e From the drop-down on the top, select **vRealize Automation 7 - Windows** from the **Available Templates** section.
- f Click **Copy Template**.
- g In the **Copy Agent Group** 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.

Filter	Operator	Values
Hostname	matches	vr01ias51 vr01ias52

- 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.



## Install the vRealize Log Insight Content Pack for vSAN in Region B

Install the content pack for VMware vSAN to add the dashboards for viewing log information in vRealize Log Insight.

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://vrli-cluster-51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 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 - vSAN** content pack and click its icon.
- 5 In the **Install Content Pack** dialog box, click **Install**.

After the installation is complete, the VMware - vSAN content pack appears in the **Installed Content Packs** list on the left.

vSAN log information becomes available without additional configuration. The integration between vRealize Log Insight and vSphere accommodates the transfer of vSAN log information automatically.

## 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 and export it as `/V2D_vRLI_MgmtB_1TB`.
- 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://vrli-cluster-51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.
- 3 Configure retention threshold notification.
 

Log Insight continually estimates how long data can be retained with the currently available pool of storage. If the estimation drops below the retention threshold of one week, Log Insight immediately notifies the administrator that the amount of searchable log data is likely to drop.

  - a Under **Configuration**, click **General**.
  - b On the **General Configuration** page, under the **Alerts** section select the **Send a notification when capacity drops below** check box next to the **Retention Notification Threshold** settings, and enter a 1-week period in the text box underneath.
  - c Click **Save**.
- 4 Configure data archiving.
  - a Under **Configuration**, click **Archiving**.
  - b Select the **Enable Data Archiving** check box.
  - c In the **Archive Location** text box, enter the path in the form of **nfs://nfs-server-address/V2D\_vRLI\_MgmtB\_1TB** 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 will not be failed over to the recovery region, Region B. 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 from losing Region A related logs in the event of 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 from losing Region B related logs in the event of disaster.

### 3 Add a Log Filter in Region A

Add a filter to avoid forwarding Region B log events forwarded to Region A back to the Log Insight deployment in Region B. Using a filter prevents from 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 from losing Region A related logs in the event of disaster.

You provide the following settings for log forwarding to vRealize Log Insight in Region B:

- SSL certificate for Region B in the Java keystore of each vRealize Log Insight node in Region A.
- Target URL, protocol and tagging
- Disk cache

Disk cache represents the amount of local disk space to reserve for buffering events that you configure to be forwarded. Buffering is used when the remote destination is unavailable or unable to process the events being sent to it. If the local buffer becomes full and the remote destination is still unavailable, then the oldest local events are dropped and not forwarded to the remote destination even when the remote destination is back online.

## Procedure

### 1 Copy the certificate PEM file for vRealize Log Insight in Region B to the root directory of vrli-mstr-51.lax01.rainpole.local

- a Use the `scp` command, FileZilla, or WinSCP to connect to `vrli-mstr-51.lax01.rainpole.local`
- b Log in using the following credentials.

Setting	Value
user name	root
Password	<i>vrli_regionB_root_password</i>

- c Navigate to the `\root` directory on `vrli-mstr-51.lax01.rainpole.local`
- d Copy the certificate PEM file `vrli.lax01.2.chain.pem` from your computer to the `\root` directory on the master node.

## 2 Import the root certificate in the Java keystore on each vRealize Log Insight node in Region A.

- a Open an SSH session to the vRealize Log Insight node.

Name	Role
vrli-mstr-01.sfo01.rainpole.local	Master node
vrli-wrkr-01.sfo01.rainpole.local	Worker node 1
vrli-wrkr-02.sfo01.rainpole.local	Worker node 2

- b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrli_regionA_root_password</i>

- c By using `scp` copy the SSL certificate from the master node of vRealize Log Insight in Region B.

```
scp root@vrli-
mstr-51.lax01.rainpole.local:/root/vrli.lax01.2.chain.pem /root/vrli.lax01.2.chain.pem
```

- d When prompted to accept the certificate, type **yes**
- e When prompted for the root password, use the following credentials.

Setting	Value
User name	root
Password	<i>vrli_regionB_root_password</i>

- f Convert the `vrli.lax01.2.chain.pem` file to a `vrli.lax01.2.chain.crt` file.

```
openssl x509 -in /root/vrli.lax01.2.chain.pem -inform PEM -out /root/vrli.lax01.2.chain.crt
```

- g Import the `vrli.lax01.2.chain.crt` in the Java keystore of the vRealize Log Insight node:

```
cd /usr/java/default/lib/security/

../../bin/keytool -import -alias loginsight -file /root/vrli.lax01.2.chain.crt -keystore
cacerts
```

- h When prompted for a keystore password, type **changeit**
- i When prompted to accept the certificate, type **yes**
- j Repeat this operation on all vRealize Log Insight nodes in Region A and restart them.

- 3 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://vrli-cluster-01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 4 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.
- 5 Under **Management**, click **Event Forwarding**.
- 6 On the **Event Forwarding** page, click **New Destination** and enter the following forwarding settings in the **New Destination** dialog box.

Forwarding Destination Setting	Value
Name	SFO01 to LAX01
Host	vrli-cluster-51.lax01.rainpole.local
Protocol	Ingestion API
Use SSL	Selected
Tags	tag='SFO01'
Advanced Settings	
Port	9543
Disk Cache	2000 MB
Worker Count	8

New Destination

Name

Host

Protocol   Use SSL ⓘ

Tags  ⓘ

Forward complementary tags ⓘ

Filter *Forward all events* ⓘ

[+ ADD FILTER](#)

[Hide Advanced Settings](#)

Port  ⓘ

Disk Cache  MB ⓘ

Worker Count  ⓘ

Test event forwarded successfully

- 7 In the **New Destination** dialog box, click **Test** to verify that the connection settings are correct.
- 8 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 from losing Region B related logs in the event of disaster.

You provide the following settings for log forwarding to vRealize Log Insight in Region A:

- SSL certificate from Region A in the Java keystore of each 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 to reserve for buffering events that you configure to be forwarded. Buffering is used when the remote destination is unavailable or unable to process the events being sent to it. If the local buffer becomes full and the remote destination is still unavailable, then the oldest local events are dropped and not forwarded to the remote destination even when the remote destination is back online.

### Procedure

- 1 Copy the certificate PEM file for vRealize Log Insight in Region A to the root directory of vrli-mstr-01.sfo01.rainpole.local.
  - a Use the `scp` command, FileZilla, or WinSCP to connect to vrli-mstr-01.sfo01.rainpole.local
  - b Log in using the following credentials.

Setting	Value
user name	root
Password	<i>vrli_regionA_root_password</i>

- c Navigate to the `\root` directory on vrli-mstr-01.sfo01.rainpole.local.
- d Copy the certificate PEM file `vrli.sfo01.2.chain.pem` on your computer to the `\root` directory on the master node.

## 2 Import the root certificate in the Java keystore on each vRealize Log Insight node in Region B.

- a Open an SSH session and go to the vRealize Log Insight node.

Name	Role
vrli-mstr-51.lax01.rainpole.local	Master node
vrli-wrkr-51.lax01.rainpole.local	Worker node 1
vrli-wrkr-52.lax01.rainpole.local	Worker node 2

- b Log in using the following credentials.

Name	Role
User name	root
Password	<i>vrli_regionB_root_password</i>

- c Using `scp`, remotely copy the the SSL certificate from the master node in Region A.

```
scp root@vrli-
mstr-01.sfo01.rainpole.local:/root/vrli.sfo01.2.chain.pem /root/vrli.sfo01.2.chain.pem
```

- d When prompted to accept the certificate, type **yes**.

- e When prompted for the root password, type the following

Setting	Value
User name	root
Password	<i>vrli_regionA_root_password</i>

- f Convert the `vrli.sfo01.2.chain.pem` file into a `vrli.sfo01.2.chain.crt` file:

```
openssl x509 -in /root/vrli.sfo01.2.chain.pem -inform PEM -out /root/vrli.sfo01.2.chain.crt
```

- g Import the `vrli.sfo01.2.chain.crt` in the Java keystore of the vRealize Log Insight node.

```
cd /usr/java/default/lib/security/

../../bin/keytool -import -alias loginsight -file /root/vrli.sfo01.2.chain.crt -keystore
cacerts
```

- h When prompted for a keystore password, type **changeit**.

- i When prompted to accept the certificate, type **yes**.

- j Repeat this operation on all vRealize Log Insight nodes and restart them.

- 3 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://vrli-cluster-51.lax01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 4 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.
- 5 Under **Management**, click **Event Forwarding**.
- 6 On the **Event Forwarding** page, click **New Destination** and enter the following forwarding settings in the New Destination dialog box.

Forwarding Destination Option	Value
Name	LAX01 to SFO01
Host	vrli-cluster-01.sfo01.rainpole.local
Protocol	Ingestion API
Use SSL	Selected
Tags	tag='LAX01'
Filter	
Filter Type	tag
Operator	does not match
Value	'SFO01'
Advanced Settings	
Port	9543
Disk Cache	2000 MB
Worker Count	8

New Destination

Name

Host

Protocol   Use SSL [?](#)

Tags  [?](#)

Forward complementary tags [?](#)

Filter    [?](#)

[+ ADD FILTER](#) [x CLEAR ALL FILTERS](#) [Run in Interactive Analytics](#) [?](#)

[Hide Advanced Settings](#)

Port  [?](#)

Disk Cache  MB [?](#)

Worker Count  [?](#)

Test event forwarded successfully

- 7 In the **New Destination** dialog box, click **Test** to verify that the connection settings are correct.
- 8 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 Region B log events forwarded to Region A back to the Log Insight deployment in Region B. Using a filter prevents from 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://vrli-cluster-01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Management**, click **Event Forwarding**.

#### 4 Add a filter to prevent from forwarding loops.

- a In the **Event Forwarding** page of the vRealize Log Insight user interface, click the **Edit** icon of the SFO01 to LAX01 destination.
- b In the **Edit Destination** dialog box, click **Add Filter** and enter the following filter attributes.

Filter Attribute	Value
Filter Type	tag
Operator	does not match
Value	'LAX01'

#### Edit Destination

Name SFO01 to LAX01

Host vrli-cluster-51.lax01.rainpole.local

Protocol Ingestion API  Use SSL ⓘ

Tags tag='SFO01' ⓘ

Forward complementary tags ⓘ

Filter X tag does not match 'LAX01' ⓘ

+ ADD FILTER X CLEAR ALL FILTERS Run in Interactive Analytics ⓘ

Show Advanced Settings

TEST

Test event forwarded successfully

CANCEL SAVE

#### 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

You 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.
- Verify you have PostgreSQL database user credentials.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://mgmt01vc51.lax01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the vSphere Web Client, right-click the mgmt01umds51.lax01.rainpole.local 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 VMtools and Secure Shell (SSH) server, and end the session.

```
sudo apt-get update
sudo apt-get -y install SSH
exit
```

- 5 Log back into the UMDS virtual machine using SSH and the **svc-umds** service account credentials.

## 6 Install and start PostgreSQL and its dependencies:

```
sudo apt-get -y install vim perl tar sed psmisc unixodbc postgresql postgresql-contrib odbc-
postgresql
sudo service postgresql start
```

## 7 Log in as a PostgreSQL user, and create a database instance and a database user, by running the following commands.

When prompted, enter and confirm the *umds\_db\_user\_password* password.

```
sudo su - postgres
createdb umds_db
createuser -d -e -r umds_db_user -P
```

## 8 Enable password authentication for the database user.

- a Navigate to the folder that contains the PostgreSQL configuration file *pg\_hba.conf*.

Linux system	Default Location
Ubuntu 14.04	<i>/etc/postgresql/postgres_version/main</i>

```
cd /etc/postgresql/postgres_version/main
```

- b In the PostgreSQL configuration file, enable password authentication for the database user by inserting the following line right above *local all all peer*.

You can use the *vi* editor to make and save the changes.

#TYPE	DATABASE	USER	ADDRESS	METHOD
local	<i>umds_db</i>	<i>umds_db_user</i>		md5

- c Log out as a PostgreSQL user by running the following command.

```
logout
```

**9** Configure the PostgreSQL driver and the data source name (DSN) for connection to the UMDS database.

- a Edit the ODBC configuration file.

```
sudo vi /etc/odbcinst.ini
```

- b Replace the file with the following content and save the change using :wq.

```
[PostgreSQL]
Description=PostgreSQL ODBC driver (Unicode version)
Driver=/usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so
Debug=0
CommLog=1
UsageCount=1
```

- c Edit the system file /etc/odbc.ini.

```
sudo vi /etc/odbc.ini
```

- d Replace the file with the following content and save the change using :wq,

```
[UMDS_DSN]
;DB_TYPE = PostgreSQL
;SERVER_NAME = localhost
;SERVER_PORT = 5432
;TNS_SERVICE = <database_name>
;USER_ID = <database_username>
Driver = PostgreSQL
DSN = UMDS_DSN
ServerName = localhost
PortNumber = 5432
Server = localhost
Port = 5432
UserID = umds_db_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 `mgmt01umds51.lax01.rainpole.local`.
  - b Log in using the following credentials.

Setting	Value
User name	<code>svc-umds</code>
Password	<code>svc-umds_password</code>

- 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 patch location to `/var/lib/vmware-umds` and enter **yes** to confirm directory creation.
- 9 Provide the database details.

Option	Description
Provide the database DSN	<code>UMDS_DSN</code>
Provide the database username	<code>umds_db_user</code>
Provide the database password	<code>umds_db_user_password</code>

- 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 UMDS virtual machine by using a Secure Shell (SSH) client.
  - a Open an SSH connection to `mgmt01umds51.lax01.rainpole.local`.
  - b Log in using the following credentials.

Setting	Value
User name	<code>svc-umds</code>
Password	<code>svc-umds_password</code>

- 2 Navigate to the directory where UMDS is installed.

```
cd /usr/local/vmware-umds/bin
```

- 3 Disable the updates for older hosts and virtual appliances.

```
sudo ./vmware-umds -S -n
sudo ./vmware-umds -S -d embeddedEsx-5.5.0
sudo ./vmware-umds -S -d embeddedEsx-6.0.0
```

- 4 Configure automatic daily downloads by creating a cron job file.

```
cd /etc/cron.daily/
sudo touch umds-download
sudo chmod 755 umds-download
```

- 5 Edit the download command 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
```

- 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 the Nginx Web server.

### Procedure

- 1 Log in to UMDS virtual machine by using a Secure Shell (SSH) client.
  - a Open an SSH connection to `mgmt01umds51.lax01.rainpole.local`.
  - b Log in using the following credentials.

Setting	Value
User name	<code>svc-umds</code>
Password	<code>svc-umds_password</code>

- 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 mgmt01umds51 mgmt01umds51.lax01.rainpole.local;

    location / {
        # First attempt to serve request as file, then
        # as directory, then fall back to displaying a 404.
        try_files $uri $uri/ =404;
```

```

        # Uncomment to enable naxsi on this location
        # include /etc/nginx/naxsi.rules
        autoindex on;
    }

```

- 6 Disable the existing default site.

```
sudo rm /etc/nginx/sites-enabled/default
```

- 7 Enable the new UMDS site.

```
sudo ln -s /etc/nginx/sites-available/umds /etc/nginx/sites-enabled/
```

- 8 Restart the Nginx Web service to apply the new configuration.

```
sudo service nginx restart
```

- 9 Ensure you can browse the files of the UMDS Web server by opening a web browser to <http://mgmt01umds51.lax01.rainpole.local>.

## Use the UMDS Shared Repository as the Download Source in Update Manager in Region B

You 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://mgmt01vc51.lax01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 On the **Home** page of the vSphere Web Client, click the **Update Manager** icon.
- 3 From the **Objects** tab, click the **mgmt01vc51.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**.

Setting	Value
Use a shared repository	Selected
URL	http://mgmt01umds51.lax01.rainpole.local

The vSphere Web Client performs validation of the URL.

- 7 In the **Download Sources** page, click **Download Now** to run the download patch definitions.
- 8 If you are deploying the management components in Region B, repeat the procedure to configure the http://mgmt01umds51.lax01.rainpole.local repository for the comp01vc51.lax01.rainpole.local vCenter Server.