

# Operational Verification

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

About VMware Validated Design Operational Verification	5
Updated Information	6
<b>1 Validate vSphere Components</b>	<b>7</b>
Verify the Platform Services Controller Instances	7
Verify the vCenter Server Instances	12
Verify the ESXi Hosts	18
<b>2 Validate the Cloud Management Platform</b>	<b>23</b>
Verify the Power Status and Address of All vRealize Automation, vRealize Orchestrator and vRealize Business VMs	24
Verify the Version, Service Status and Configuration of vRealize Automation Appliances	25
Verify the Status of IaaS Web Server and Manager Service Nodes of vRealize Automation	29
Verify the Version and Service Status of vRealize Automation Windows Nodes	31
Verify the Version, Status, and Configuration of vRealize Orchestrator VMs	35
Verify the Status of the Distributed Execution Managers and vSphere Proxy Agents in vRealize Automation	43
Verify the Status of vRealize Automation Integration with Active Directory	45
Verify the Version, Service Status and Configuration of the vRealize Business VMs	47
Request a Single-Machine Blueprint from the Service Catalog of vRealize Automation	56
Verify the Cloud Management Platform Load Balancing	58
<b>3 Validate NSX for vSphere</b>	<b>60</b>
Verify the Version, Service Status and Configuration of the NSX Manager Appliances	61
Verify the Status of NSX Controller Instances and Host Components	65
Test VXLAN Connectivity of the Hosts in the Management Cluster	69
Test VXLAN Connectivity of the Hosts in the Shared Edge and Compute Cluster	72
Verify the Status of NSX Firewall, Service Composer, and Distributed Switches	75
Verify the Status of the NSX Edge Devices for North-South Routing	78
Verify the Status of the Universal Distributed Logical Router	83
Verify the Status of the NSX Load Balancer	86
<b>4 Validate vRealize Operations Manager</b>	<b>91</b>
Verify the Power Status of All vRealize Operations Manager VMs	91
Verify the Configuration of vRealize Operations Manager Cluster Nodes and Remote Collectors	92
Verify the vRealize Operations Manager Load Balancing	95

- Validate vRealize Operations Manager Adapters and Management Packs 97
  - Verify the Version, Status, and Configuration of the VMware vSphere Adapter in vRealize Operations Manager 98
  - Verify the Version and Configuration of the vRealize Operations Management Pack for Log Insight 100
  - Verify the Version, Status, and Configuration of vRealize Operations Manager Management Pack for NSX for vSphere 101
  - Verify the Version, Status, and Configuration of the vRealize Automation Management Pack 104
  - Verify the Version, Status, and Configuration of the Management Pack for Storage Devices in vRealize Operations Manager 106
- 5 Validate vRealize Log Insight 109**
  - Verify the Status of the vRealize Log Insight Nodes 109
- 6 Validate vSphere Data Protection 117**
  - Verify the Appliance Status and Version of vSphere Data Protection 117
  - Verify the Configuration and Service Status of vSphere Data Protection 118
- 7 Validate Site Recovery Manager 121**
  - Verify the Version and Service Status of Site Recovery Manager 121
- 8 Validate the vSphere Replication 126**
  - Verify the Version and Service Status of vSphere Replication 126
- 9 SDDC Startup and Shutdown 130**
  - Shutdown Order of the Management Virtual Machines 130
  - Startup Order of the Management Virtual Machines 132

# About VMware Validated Design Operational Verification

*VMware Validated Design Operational Verification* provides step-by-step instructions for verifying that the management components in the Software-Defined Data Center (SDDC) that is deployed according to VMware Validated Design™ for Software-Defined Data Center are operating as expected.

After performing a maintenance operation of the management components in the software-defined data center, verifying whether these components are running without any faults ensures continuous operation of the environment. Verify the operation of the SDDC after patching, updating, upgrading, restoring and recovering the SDDC management components.

## Intended Audience

The *VMware Validated Design Operational Verification* documentation is intended for cloud architects, infrastructure administrators, cloud administrators and cloud operators 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 Software

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

# Updated Information

This *VMware Validated Design Operational Verification* is updated with each release of the product or when necessary.

This table provides the update history of the *VMware Validated Design Operational Verification* documentation.

Revision	Description
EN-002464-01	<ul style="list-style-type: none"><li>■ <a href="#">Verify the ESXi Hosts</a> is added to provide verification instructions about ESXi hosts. You can use these instructions to verify the operation of the ESXi management hosts after upgrade.</li><li>■ The virtual machine name of the Platform Services Controller load balancer is updated to LAX01PSC51 in <a href="#">Chapter 9 SDDC Startup and Shutdown</a>.</li><li>■ <a href="#">Verify the Status of NSX Controller Instances and Host Components</a> now contains details about connecting to the NSX Controllers for the shared edge and compute cluster in Region B.</li><li>■ The virtual machine names of the vSphere Proxy Agents are replaced with the host names in <a href="#">Verify the Status of the Distributed Execution Managers and vSphere Proxy Agents in vRealize Automation</a>.</li></ul>
EN-002464-00	Initial release.

# Validate vSphere Components

After you perform maintenance in your environment, verify the version, service status and the configuration of each Platform Services Controller and vCenter Server Appliance instances, and of each ESXi management host.

## Procedure

### 1 Verify the Platform Services Controller Instances

Validate the functionality of the Platform Services Controller for the Management vCenter Server and of the Platform Services Controller for the Compute vCenter Server in Region A and Region B.

### 2 Verify the vCenter Server Instances

Validate the functionality of the vCenter Server instances in Region A and Region B.

### 3 Verify the ESXi Hosts

After you upgrade the ESXi hosts, validate the functionality of each host for management and compute clusters in region A and region B.

## Verify the Platform Services Controller Instances

Validate the functionality of the Platform Services Controller for the Management vCenter Server and of the Platform Services Controller for the Compute vCenter Server in Region A and Region B.

Start with the Platform Services Controller for the management cluster in Region A.

**Table 1-1. Platform Services Controller Instances in the Environment**

Region	Cluster	FQDN	VAMI	Administrative UI
Region A	Management	mgmt01psc01.sfo01.rainpole.local	https://fqdn:5480	https://fqdn/psc
	Shared edge and compute	comp01psc01.sfo01.rainpole.local	https://fqdn:5480	https://fqdn/psc
Region B	Management Cluster	mgmt01psc51.lax01.rainpole.local	https://fqdn:5480	https://fqdn/psc
	Shared edge and compute	comp01psc51.lax01.rainpole.local	https://fqdn:5480	https://fqdn/psc

## Procedure

- 1 Log in to the management interface of the Platform Services Controller virtual appliance.
  - a Open a Web browser and go to **https://mgmt01psc01.sfo01.rainpole.local:5480**.
  - b Log in using the following credentials.

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

- 2 Verify the Health Status and the Single Sign-On status for this Platform Services Controller.
  - a On the **Summary** page, under **Health Status**, verify that the Overall Health is Good.
  - b Verify that the Single Sign-On status is RUNNING.

The screenshot shows the VMware vCenter Server Appliance management interface. The browser address bar displays the URL: `https://mgmt01psc01.sfo01.rainpole.local:5480/#/appliance/summary?locale=en`. The page title is "vCenter Server Appliance".

**Summary**

- Hostname: mgmt01psc01.sfo01.rainpole.local
- Type: VMware Platform Services Controller
- Product: VMware vCenter Server Appliance
- Version: 6.5.0.5200

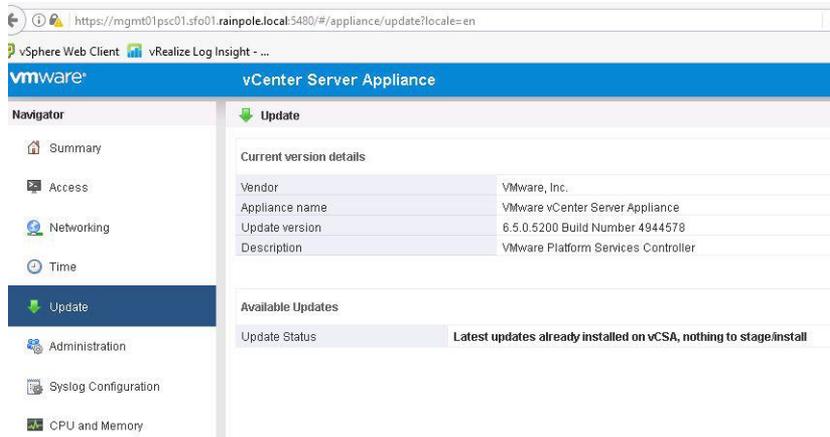
**Health Status**

Overall Health	Good
Last Health Check	2/7/2017, 9:15:26 PM
CPU	Good
Memory	Good

**Health Messages**

- The CPU is heavily loaded

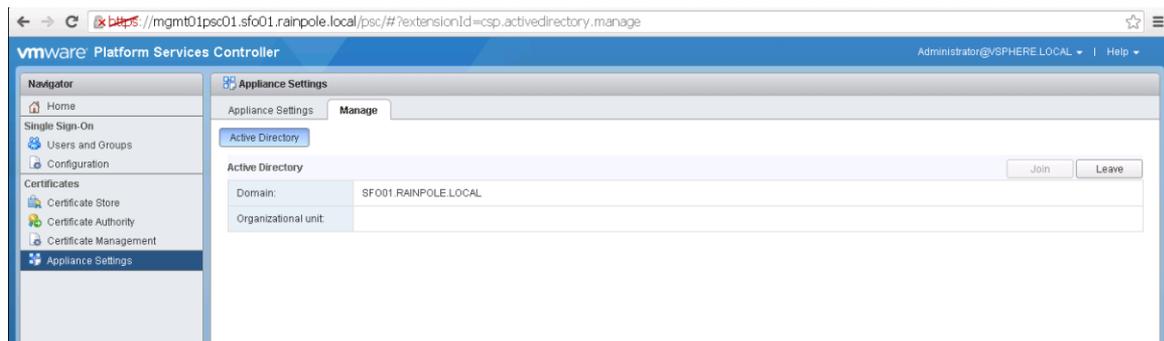
- 3 Verify the version of the Platform Services Controller.
  - a In the **Navigator**, click **Update**.
  - b On the **Update** page, verify that the Product Version is correct.



- 4 Verify the connection status between the Active Directory and the Platform Services Controller.
  - a Open a Web browser and go to <https://mgmt01psc01.sfo01.rainpole.local/psc>.
  - b Log in using the following credentials.

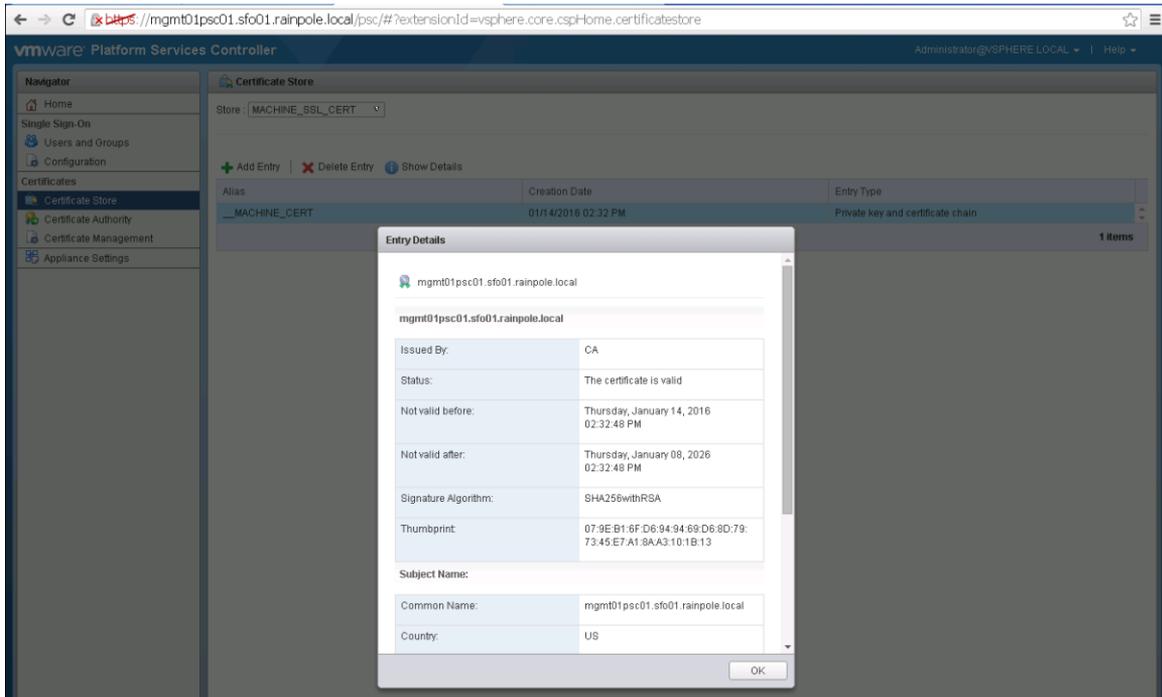
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- c In the **Navigator**, click **Appliance Settings** and click the **Manage** tab.
  - d Under Active Directory, verify that the Domain setting shows SF001.RAINPOLE.LOCAL as this is the Region A Active Directory FQDN.



- 5 Verify the Identity Sources for the Platform Services Controller.
  - a In the **Navigator**, click **Configuration**, and click the **Identity Sources** tab.
  - b Under **Domain**, verify that the vsphere.local, localos, and rainpole.local entries are listed.

- 6 Verify the certificate of the Platform Services Controller.
  - a In the **Navigator**, click **Certificate Store**.
  - b On the **Certificate Store** page, select the certificate and click **Show Details**.
  - c Verify that the value of the Status setting is **Valid**.



- 7 Verify that all Platform Services Controller services are available and running.
  - a Open an SSH connection to the virtual machine `mgmt01psc01.sfo01.rainpole.local`.
  - b Log in using the following credentials.

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

- c Run the following command to list the Platform Services Controller services.

```
service-control --list
```

d Verify that the following services are listed.

- vmcad
- vmafdd
- vmdnsd
- vmware-cm
- vmware-sca
- vmware-cis-license
- applmgmt
- vmware-statsmonitor
- vmdird
- pshealth
- vmware-vmon
- vmware-rhttpproxy
- vmware-vapi-endpoint
- vmware-stsd
- lwsmd
- vmware-psc-client
- vmware-sts-idmd
- vmonapi

e Run the following command to view the current status of the Platform Services Controller services and verify that status of all services is Running.

```
service-control --status
```

```

login as: root
VMware vCenter Server Appliance 6.5.0.5200
Type: VMware Platform Services Controller
Using keyboard-interactive authentication.
Password:
root@mgmt01psc01 [ ~ ]# service-control --list
vmcad (VMware Certificate Service)
vmxafdd (VMware Authentication Framework)
vmdnsd (VMware Domain Name Service)
vmware-cm (VMware Component Manager)
vmware-sca (VMware Service Control Agent)
vmware-cis-license (VMware License Service)
applmgmt (VMware Appliance Management Service)
vmware-statsmonitor (VMware Appliance Monitoring Service)
vmdir (VMware Directory Service)
pschealth (VMware Platform Services Controller Health Monitor)
vmware-vmcon (VMware Service Lifecycle Manager)
vmware-rhttpproxy (VMware HTTP Reverse Proxy)
vmware-vapi-endpoint (VMware vAPI Endpoint)
vmware-std (VMware Security Token Service)
lwsmd (Likewise Service Manager)
vmware-psc-client (VMware Platform Services Controller Client)
vmware-sts-idmd (VMware Identity Management Service)
vmonapi (VMware Service Lifecycle Manager API)
root@mgmt01psc01 [ ~ ]# service-control --status
Running:
applmgmt lwsmd pschealth vmafdd vmcad vmdir vmdnsd vmonapi vmware-cis-license vmware-cm vmware-psc-client vmware-rhttpproxy
vmware-sca vmware-statsmonitor vmware-sts-idmd vmware-std vmware-vapi-endpoint vmware-vmcon
root@mgmt01psc01 [ ~ ]#

```

- 8 Repeat the procedure for the remaining Platform Services Controller instances in Region A and Region B.

## Verify the vCenter Server Instances

Validate the functionality of the vCenter Server instances in Region A and Region B.

Start with the Management vCenter Server instance in Region A.

**Table 1-2. vCenter Server Instances in the Environment**

Region	Cluster	vCenter Server FQDN	VAMI	vSphere Web Client
Region A	Management	mgmt01vc01.sfo01.rainpole.local	https://fqdn:5480	https://fqdn/vsphere-client
	Shared edge and compute	comp01vc01.sfo01.rainpole.local	https://fqdn:5480	https://fqdn/vsphere-client
Region B	Management	mgmt01vc51.lax01.rainpole.local	https://fqdn:5480	https://fqdn/vsphere-client
	Shared edge and compute	comp01vc51.lax01.rainpole.local	https://fqdn:5480	https://fqdn/vsphere-client

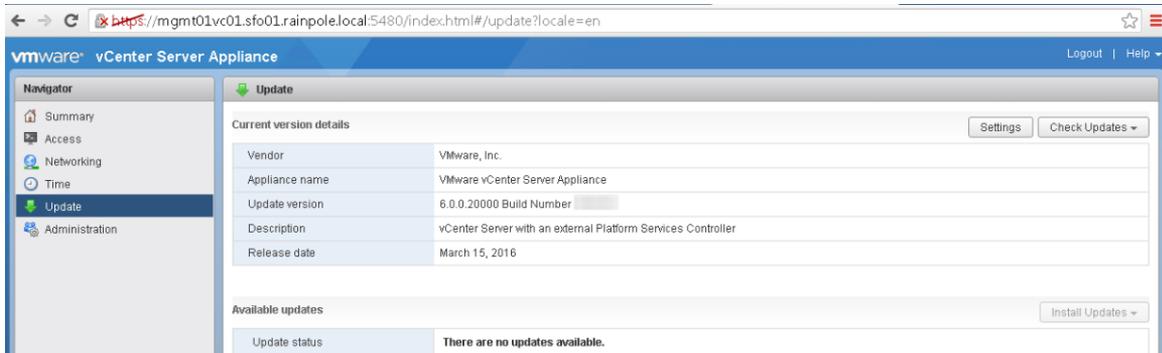
### Procedure

- 1 Log in to the Management 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 On the **Summary** page, under **Health Status**, verify that the Overall Health is Good.

- 3 If you have performed a patch or update, verify the version of the vCenter Server instance.
  - a In the **Navigator**, click **Update**.
  - b On the **Update** page, verify that the Product Version is correct.



- 4 Verify that all vCenter Server services are available and running.
  - a Open an SSH connection to the virtual machine `mgmt01vc01.sfo01.rainpole.local`.
  - b Log in using the following credentials.

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

- c Run the following command to list the vCenter Server services.

```
service-control --list
```

d Verify that the following services are listed.

- vmware-imagebuilder
- vmware-cm
- vmware-vpxd
- vmware-sps
- applmgmt
- vmware-statsmonitor
- vmware-rhttpproxy
- vmware-vapi-endpoint
- lwsmd
- vmafdd
- vmware-vsm
- vmonapi
- vmware-perfcharts
- vmware-updatemgr
- vmware-vmon
- vmware-vsan-health
- vsphere-client
- vmware-vpostgres
- vmware-eam
- vmcam
- vmware-mbcs
- vmware-vcha
- vsphere-ui
- vmware-content-library
- vmware-sca
- vmware-netdumper
- vmware-vpxd-svcs
- vmware-rbd-watchdog

```

mgmt01vc01.sfo01.rainpole.local - PuTTY
login as: root
VMware vCenter Server Appliance 6.5.0.5200
Type: vCenter Server with an external Platform Services Controller
root@mgmt01vc01.sfo01.rainpole.local's password:
root@mgmt01vc01 [ ~ ]# service-control --list
vmware-imagebuilder (VMware Image Builder Manager)
vmware-cm (VMware Component Manager)
vmware-vpxd (VMware vCenter Server)
vmware-sps (VMware vSphere Profile-Driven Storage Service)
applmgmt (VMware Appliance Management Service)
vmware-statsmonitor (VMware Appliance Monitoring Service)
vmware-rhttpproxy (VMware HTTP Reverse Proxy)
vmware-vapi-endpoint (VMware vAPI Endpoint)
lvsmd (Likewise Service Manager)
vmaidd (VMware Authentication Framework)
vmware-vsm (VMware vService Manager)
vmonapi (VMware Service Lifecycle Manager API)
vmware-perfcharts (VMware Performance Charts)
vmware-updatemgr (VMware Update Manager)
vmware-vmom (VMware Service Lifecycle Manager)
vmware-vsan-health (VMware VSAN Health Service)
vsphere-client (VMware vSphere Web Client)
vmware-vpostgres (VMware Postgres)
vmware-eam (VMware ESX Agent Manager)
vmcam (VMware vSphere Authentication Proxy)
vmware-mbcs (VMware Message Bus Configuration Service)
vmware-wcha (VMware vCenter High Availability)
vsphere-ui (VMware vSphere Client)
vmware-content-library (VMware Content Library Service)
vmware-sca (VMware Service Control Agent)
vmware-netdumper (VMware vSphere ESXi Dump Collector)
vmware-vpxd-svcs (VMware vCenter-Services)
vmware-rbd-watchdog (VMware vSphere Auto Deploy Waiter)
root@mgmt01vc01 [ ~ ]#

```

- e Run the following command to view the current status of the vCenter Server services and verify that status of all services is Running.

```
service-control --status
```

```

mgmt01vc01.sfo01.rainpole.local - PuTTY
root@mgmt01vc01:~ # service-control --status
INFO:root:Service: vmware-rhttpproxy, Action: status
Service: vmware-rhttpproxy, Action: status
2016-04-04T23:22:25.032Z Running command: ['/sbin/service', 'vmware-rhttpproxy', 'status']
2016-04-04T23:22:25.073Z Done running command
INFO:root:Service: vmware-sca, Action: status
Service: vmware-sca, Action: status
2016-04-04T23:22:25.074Z Running command: ['/sbin/service', 'vmware-sca', 'status']
2016-04-04T23:22:25.167Z Done running command
INFO:root:Service: vmware-netdumper, Action: status
Service: vmware-netdumper, Action: status
2016-04-04T23:22:25.167Z Running command: ['/sbin/service', 'vmware-netdumper', 'status']
2016-04-04T23:22:25.206Z Done running command
INFO:root:Service: vmware-syslog, Action: status
Service: vmware-syslog, Action: status
2016-04-04T23:22:25.207Z Running command: ['/sbin/service', 'vmware-syslog', 'status']

```

- 5 Verify the connection between the vCenter Server instance and the Platform Services Controller 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

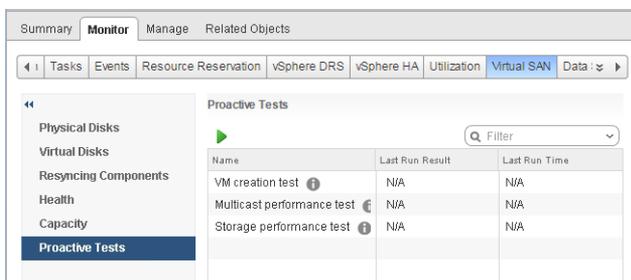
- c From the **Home** menu, select **Hosts and Clusters**.
- d In the **Navigator**, verify that all four vCenter Server instances are present in the list.  
This operation validates that the Enhanced Linked Mode is intact and active for all vCenter Server instances.

- 6 Verify the vMotion functionality.

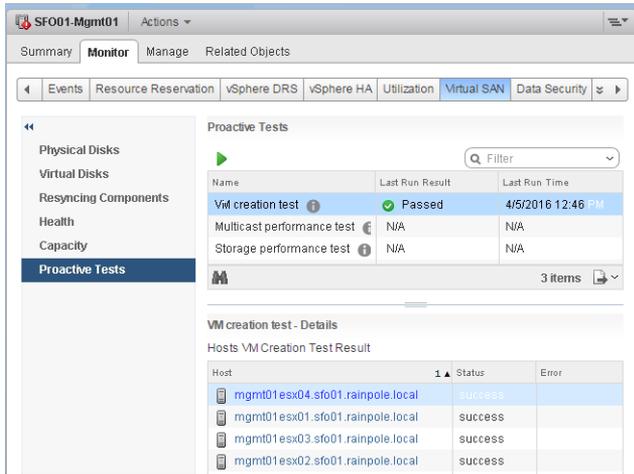
- a Navigate to **Home > Hosts and Clusters**.
- b Right-click the **mgmt01esx01** host and select **Maintenance Mode > Enter Maintenance Mode**.
- c Verify that the VMs from this host migrate to the other host in the cluster.
- d Right-click the **mgmt01esx01** host and select **Maintenance Mode > Exit Maintenance Mode**.
- e Repeat this step for the other clusters in the environment.

- 7 Verify vSAN health with proactive health checks by creating a simple VM on every ESXi host in the vSAN cluster.

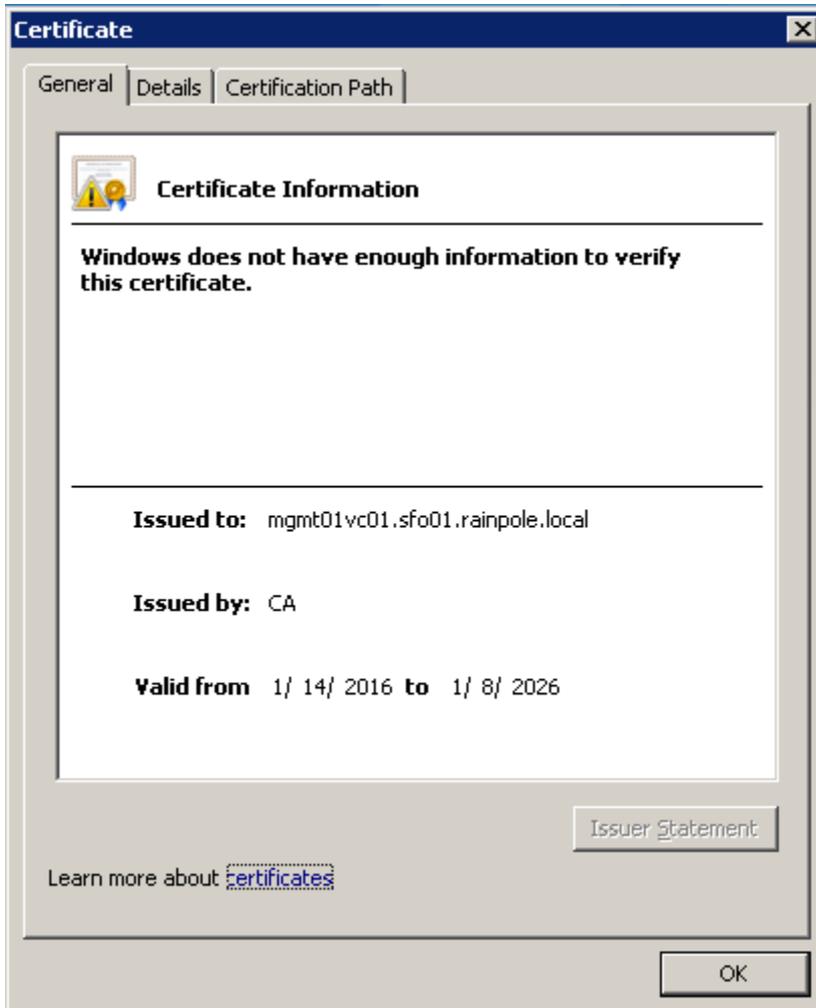
- a Navigate to **Home > Hosts and Clusters** and select the **SFO01-Mgmt01** cluster.
- b Click the **Monitor** tab, click **Virtual SAN** and select **Proactive Tests**.
- c Under **Proactive Tests**, select **VM creation test** and click the **Run Test Now** icon.



- d In the **Run VM creation test** dialog box, click **Yes**.
- e After the test completes, verify that the **VM Creation test-details** table shows Success status for all hosts in the cluster.



- 8 Verify the certificate of the vCenter Server instance.
  - a In your Web browser address bar, click the **Padlock** icon and view the details for the certificate.
  - b Verify that the certificate is valid.



- 9 Repeat the procedure for the remaining vCenter Server instances in Region A and Region B.

## Verify the ESXi Hosts

After you upgrade the ESXi hosts, validate the functionality of each host for management and compute clusters in region A and region B.

**Table 1-3. ESXi hosts in the test environment**

Region	Cluster	ESXi Hosts FQDN
Region A	Management Cluster	mgmt01esx01.sfo01.rainpole.local
		mgmt01esx02.sfo01.rainpole.local
		mgmt01esx03.sfo01.rainpole.local

**Table 1-3. ESXi hosts in the test environment (Continued)**

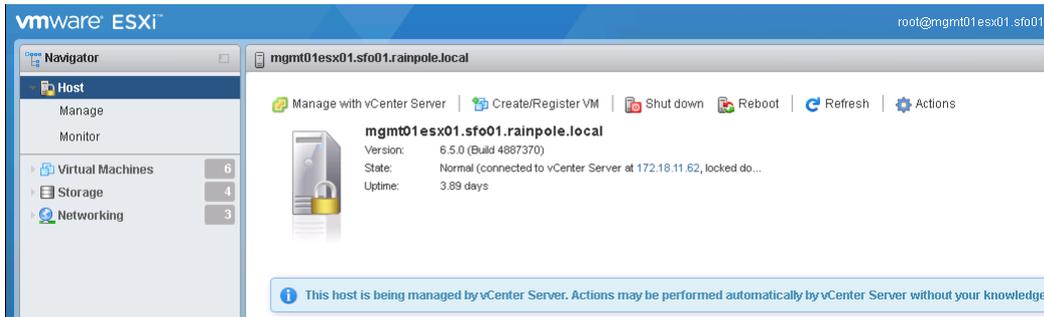
Region	Cluster	ESXi Hosts FQDN
Region B	Compute Cluster	mgmt01esx04.sfo01.rainpoel.local
		comp01esx01.sfo01.rainpoel.local
		comp01esx02.sfo01.rainpoel.local
		comp01esx03.sfo01.rainpoel.local
	Management Cluster	comp01esx04.sfo01.rainpoel.local
		mgmt01esx51.lax01.rainpoel.local
		mgmt01esx52.lax01.rainpoel.local
		mgmt01esx53.lax01.rainpoel.local
	Compute Cluster	mgmt01esx54.lax01.rainpoel.local
		comp01esx51.lax01.rainpoel.local
comp01esx52.lax01.rainpoel.local		
comp01esx53.lax01.rainpoel.local		
		comp01esx54.lax01.rainpoel.local

**Procedure**

- 1 Log in to the VMware Host Client interface of a management ESXi host mgmt01esx01.
  - a Open a Web browser and go to **https://mgmt01esx01.sfo01.rainpoel.local/ui**.
  - b Log in using the following credentials.

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

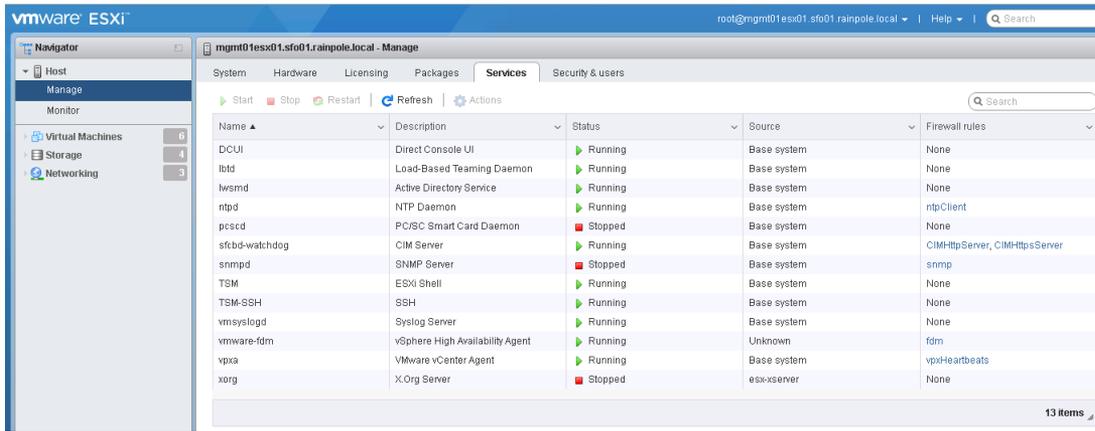
- 2 Verify the Version, the Build number and the State of ESXi host.
  - a In the **Navigator** section, click **Host**.
  - b On the host page, verify that the ESXi Version and Build number are correct in relation to the VMware Validated Design build numbers.
  - c Verify that the State of the host is Normal and ensure that the host is connected to vCenter Server.



- 3 Verify the NTP status.
  - a In the **Navigator**, click **Manage**.
  - b On manage page, click **System**.
  - c Click **Time & date**.
  - d Verify that the NTP client status is enabled.
  - e Verify that the NTP service status is running.
  - f Verify that the displayed list of NTP servers is correct as per your VMware Validated Design environment.
- 4 Verify the license information.
  - a On the manage page, click **Licensing**.
  - b Verify that the license information is correct, .  
You can see the license key, expiration date, and all the available features and assets
- 5 Verify the ESXi packages.
  - a On the manage page, click **Packages**.
  - b Verify that the `esx-vsip` and `esx-vxlan` VIBs are installed and are of the correct version.

## 6 Verify the status of ESXi services.

- a On the manage page, click **Services**.
- b Verify that the services, such as VMware vCenter Agent, Direct Console UI, NTP Daemon, and so on, are running.



## 7 Verify the security and users related information.

- a On the manage page, click **Security & users**.
- b Click **Acceptance level** and ensure that the Acceptance Level is set to Partner or VMware Certified.
- c Click **Authentication**.
- d Ensure that Active directory is enabled.
- e Ensure that the Domain membership status reports are in OK state.
- f Ensure that the host is still joined to the Active Directory Domain as it was before the upgrade.
- g Click **Certificates** and ensure that the certificates on the ESXi host are still valid.  
If the ESXi host certificates are invalid, you must replace the certificates.
- h Click **Users** and ensure that any users that might have been directly added to the ESXi host are still there.
- i Click **Lockdown mode** and ensure that the Lockdown mode has been re-enabled after all upgrade activities are completed.

## 8 Verify the ESXi host monitoring services.

- a In the **Navigator**, click **Monitor**.
- b On the monitor page, click **Hardware**.
- c Ensure that all of the hardware sensors on the ESXi host in the Health column are in green status.

- d Click **Notifications**.
  - e Review any warnings that might have been generated after the upgrade.
- 9 Verify the storage information.
- a In the **Navigator**, click **Storage**.
  - b On storage page, click **Datastores**.
  - c Verify that all the configured datastores are displayed with proper disk space information.
- 10 Verify the network information.
- a In the **Navigator**, click **Networking**.
  - b On the network page, click **Port groups**.
  - c Verify that all the configured port groups are intact.

The screenshot shows the VMware ESXi interface for the host 'mgmt01esx02.sfo01.rainpole.local'. The 'Networking' section is selected in the left-hand 'Navigator' pane. The main area displays the 'Port groups' tab, which contains a table of port group configurations. The table has columns for Name, Active ports, VLAN ID, Type, vSwitch, and VMs. There are 13 items listed in the table.

Name	Active ports	VLAN ID	Type	vSwitch	VMs
vDS-Mgmt-DVUplinks-43	2	Unknown	Distributed virtual port group	vDS-Mgmt	0
vDS-Mgmt-Management	7	Unknown	Distributed virtual port group	vDS-Mgmt	9
vDS-Mgmt-NFS	1	Unknown	Distributed virtual port group	vDS-Mgmt	0
vDS-Mgmt+Motion	1	Unknown	Distributed virtual port group	vDS-Mgmt	0
vDS-Mgmt+VR	2	Unknown	Distributed virtual port group	vDS-Mgmt	1
vDS-Mgmt+VSAN	1	Unknown	Distributed virtual port group	vDS-Mgmt	0
vww-dvs-43-universa1wire-1-sid-30000...	7	Unknown	Distributed virtual port group	vDS-Mgmt	7
vww-dvs-43-universa1wire-2-sid-30001...	1	Unknown	Distributed virtual port group	vDS-Mgmt	1
vww-dvs-43-universa1wire-4-sid-30003...	3	Unknown	Distributed virtual port group	vDS-Mgmt	3
vww-vmkn1cPg-dvs-43-3034-4262d2cd...	2	Unknown	Distributed virtual port group	vDS-Mgmt	0
VMKernel	0	3104	Standard port group	vSwitch0	0
VM Network	0	3031	Standard port group	vSwitch0	0
Management Network	0	3031	Standard port group	vSwitch0	0

- d Click **Virtual switches** and verify that the configured distributed switch is displayed.
  - e Click **VMkernel NICs** and verify that the virtual adapters and port groups are intact.
  - f Click **TCP/IP stacks** and verify that the IPv4 gateway information for vxlan, vMotion stack and Default TCP/IP stack is intact.
- 11 Repeat the steps for all the remaining ESXi hosts and verify that all parameters are intact.

# Validate the Cloud Management Platform

# 2

After a maintenance like patch, update, restore, failover, or failback, validate the Cloud Management Platform (vRealize Automation, vRealize Orchestrator and vRealize Business components) and make sure they work as expected.

## Procedure

### 1 [Verify the Power Status and Address of All vRealize Automation, vRealize Orchestrator and vRealize Business VMs](#)

All virtual machines of vRealize Automation, vRealize Orchestrator and vRealize Business must be running for a fully-functional cloud platform.

### 2 [Verify the Version, Service Status and Configuration of vRealize Automation Appliances](#)

After you perform software maintenance in the Software-Defined Data Center (SDDC), verify that the version and the configuration of the two vRealize Automation server appliances are intact.

### 3 [Verify the Status of IaaS Web Server and Manager Service Nodes of vRealize Automation](#)

After you perform software maintenance in the Software-Defined Data Center (SDDC), verify that the IaaS Web Server and the IaaS Manager Service nodes are accessible.

### 4 [Verify the Version and Service Status of vRealize Automation Windows Nodes](#)

After you patch, update, restore, failover, or failback the vRealize Automation Windows nodes, such as Infrastructure as a Service (IaaS) Web Servers, IaaS Manager Service nodes, Distributed Execution Manager (DEM) Workers, vSphere Proxy Agents and Microsoft SQL Server, for each of them verify the version and the service status of its components.

### 5 [Verify the Version, Status, and Configuration of vRealize Orchestrator VMs](#)

Make sure that the two servers in the vRealize Orchestrator cluster are operational after a patch, update, restore, failover, or failback operation.

### 6 [Verify the Status of the Distributed Execution Managers and vSphere Proxy Agents in vRealize Automation](#)

After you perform software maintenance, verify that status the Distributed Execution Manager (DEM) and IaaS vSphere Proxy Agents components

### 7 [Verify the Status of vRealize Automation Integration with Active Directory](#)

Verify that vRealize Automation is connected to the Active Directory domain after patch, update, restore, failover or failback.

**8** [Verify the Version, Service Status and Configuration of the vRealize Business VMs](#)

After you perform software maintenance in the Software-Defined Data Center, verify that both the vRealize Business Server and Data Collector are operational.

**9** [Request a Single-Machine Blueprint from the Service Catalog of vRealize Automation](#)

Request a single-machine blueprint item from the service catalog to verify that vRealize Automation provisions items to the cloud environment.

**10** [Verify the Cloud Management Platform Load Balancing](#)

If you have performed an update, restore, failover or failback of the vRealize Automation, vRealize Orchestrator and vRealize Business VMs, verify the load balancing of the cluster.

## Verify the Power Status and Address of All vRealize Automation, vRealize Orchestrator and vRealize Business VMs

All virtual machines of vRealize Automation, vRealize Orchestrator and vRealize Business must be running for a fully-functional cloud platform.

### Prerequisites

Verify that all virtual machines of vRealize Automation, vRealize Orchestrator and vRealize Business are started in the order defined in the SDDC Startup and Shutdown section.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to the following URL.

Region	Management vCenter Server URL
Region A	<a href="https://mgmt01vc01.sfo01.rainpole.local/vsphere-client">https://mgmt01vc01.sfo01.rainpole.local/vsphere-client</a>
Region B	<a href="https://mgmt01vc51.lax01.rainpole.local/vsphere-client">https://mgmt01vc51.lax01.rainpole.local/vsphere-client</a>

- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Verify that all virtual machines of vRealize Automation, vRealize Orchestrator and vRealize Business are powered on, and have the FQDNs and IP addresses assigned according to this design.
  - a On the **Home** page, click **VMs and Templates**.
  - b In the **Navigator**, go to the following folder names on the Management vCenter Server and verify that the virtual machines are configured in the following way.

Region	Folder Name	VM Name	FQDN	IP Address		
Region A	vRA01	vra01mssql01.rainpole.local	vra01mssql01.rainpole.local	192.168.11.62		
		vra01vro01a.rainpole.local	vra01vro01a.rainpole.local	192.168.11.63		
		vra01vro01b.rainpole.local	vra01vro01b.rainpole.local	192.168.11.64		
		vra01bus01.rainpole.local	vra01bus01.rainpole.local	192.168.11.66		
		vra01svr01a.rainpole.local	vra01svr01a.rainpole.local	192.168.11.51		
		vra01svr01b.rainpole.local	vra01svr01b.rainpole.local	192.168.11.52		
		vra01iws01a.rainpole.local	vra01iws01a.rainpole.local	192.168.11.54		
		vra01iws01b.rainpole.local	vra01iws01b.rainpole.local	192.168.11.55		
		vra01ims01a.rainpole.local	vra01ims01a.rainpole.local	192.168.11.57		
		vra01ims01b.rainpole.local	vra01ims01b.rainpole.local	192.168.11.58		
		vra01dem01.rainpole.local	vra01dem01.rainpole.local	192.168.11.60		
		vra01dem02.rainpole.local	vra01dem02.rainpole.local	192.168.11.61		
		vRA01IAS	vRA01IAS	vra01ias01.sfo01.rainpole.local	vra01ias01.sfo01.rainpole.local	192.168.31.52
				vra01ias02.sfo01.rainpole.local	vra01ias02.sfo01.rainpole.local	192.168.31.53
vra01buc01.sfo01.rainpole.local	vra01buc01.sfo01.rainpole.local			192.168.31.54		
Region B	vRA51IAS	vra01ias51.lax01.rainpole.local	vra01ias51.lax01.rainpole.local	192.168.32.52		
		vra01ias52.lax01.rainpole.local	vra01ias52.lax01.rainpole.local	192.168.32.53		
		vra01buc51.lax01.rainpole.local	vra01buc51.lax01.rainpole.local	192.168.32.54		

## Verify the Version, Service Status and Configuration of vRealize Automation Appliances

After you perform software maintenance in the Software-Defined Data Center (SDDC), verify that the version and the configuration of the two vRealize Automation server appliances are intact.

After you patch, update, restore, failover, or fallback the vRealize Automation appliances vra01svr01a.rainpole.local and vra01svr01b.rainpole.local, verify the version, the service status and the configuration of each of them. The two appliances share the same configuration except for static IP address and host name.

**Table 2-1. Network Parameters for the vRealize Automation Appliances**

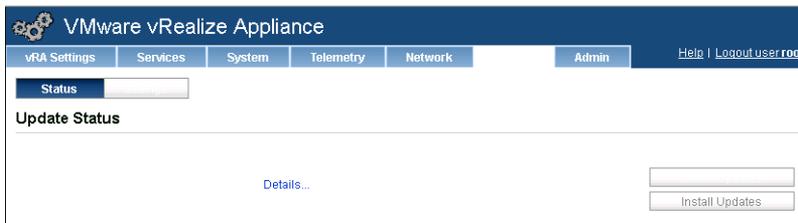
vRealize Appliance	Appliance Management Console URL	IP Address	FQDN
vRealize Appliance A	https://vra01svr01a.rainpole.local:5480	192.168.11.51	vra01svr01a.rainpole.local
vRealize Appliance B	https://vra01svr01b.rainpole.local:5480	192.168.11.52	vra01svr01b.rainpole.local

**Procedure**

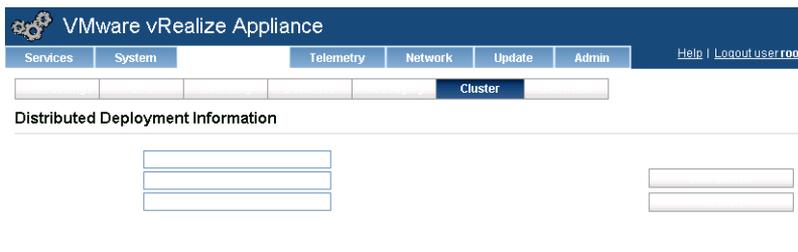
- 1 Verify the authentication of vRealize Automation appliance to the appliance management console.
  - a Open a Web browser and go to **https://vra01svr01a.rainpole.local:5480**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vra_appliance_root_password

- c Verify that authentication is successful.
- 2 If you have performed a patch or update, verify the version of the vRealize Automation appliance.
  - a In the appliance management console, click the **Update** tab and click the **Status** tab.
  - b Verify that the Appliance Version property shows the target appliance version.



- 3 Verify the cluster status of the vRealize Automation appliance.
  - a In the appliance management console, click the **vRA Settings** tab and click the **Cluster** tab.
  - b Under **Distributed Deployment Information**, verify that the status shows Current node in cluster mode.



- 4 Verify the Single Sign-On connection settings.
  - a In the appliance management console, click the **vRA Settings** tab and click the **SSO** tab.
  - b Verify the following settings for Single Sign-on.

Single Sign-On Setting	Expected Value
SSO Default Tenant	vsphere.local
SSO Info	Configured - working connected

- 5 In the appliance management console, click the **vRA Settings** tab, click the **Licensing** tab, and verify that the license key and expiration date are valid.
- 6 Verify the database settings of the vRealize Automation appliance.
  - a In the appliance management console, click the **vRA Settings** tab and click the **Database** tab.
  - b Verify that the connection status of the internal PostgreSQL database shows **CONNECTED**.
  - c Verify that the status of vRealize Automation appliance master and replica nodes is **Up**.

VMware vRealize Appliance

Services System Telemetry Network Update Admin Help | Logout user root

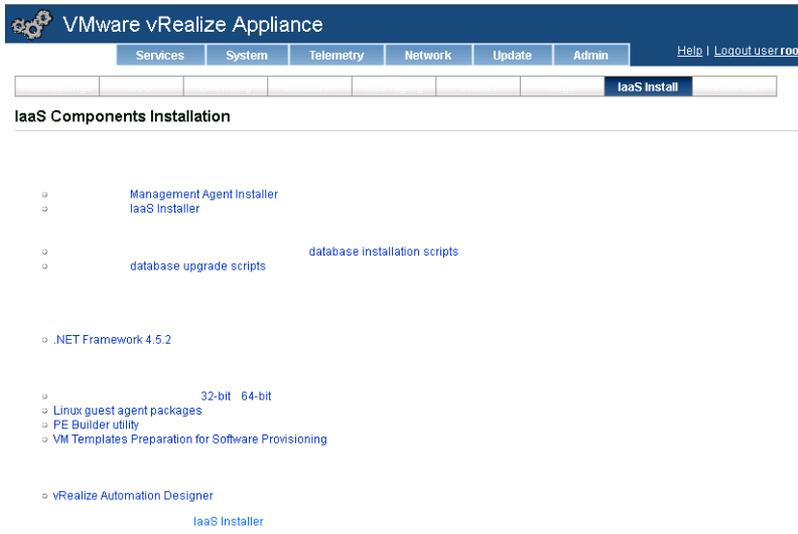
Database

Configure vRA Postgres Database

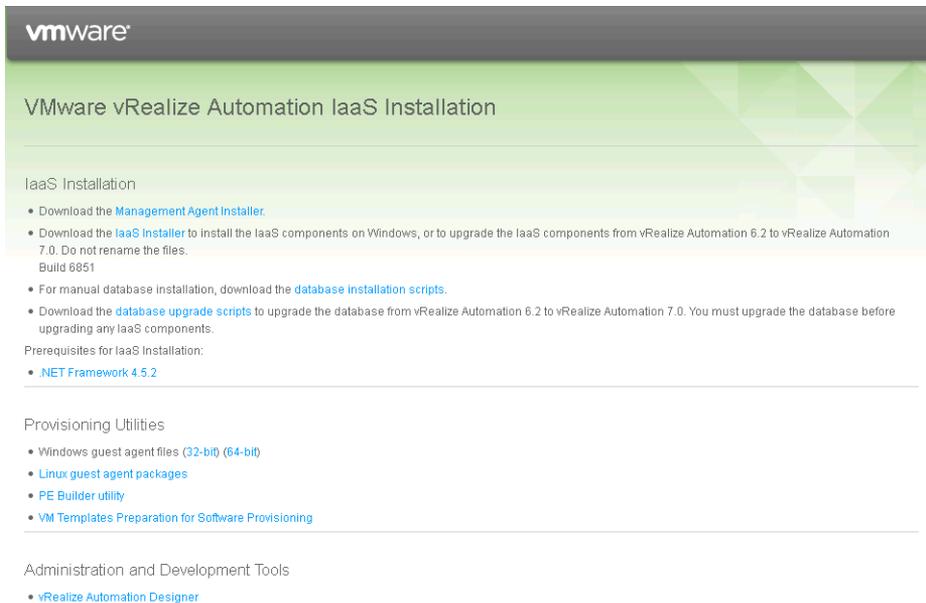
Database node host Mode Status Sync State\* Valid\* Priority\*

Add New Database Node Refresh

- 7 Verify the Infrastructure as a Service (IaaS) installation link.
  - a In the appliance management console, click the **vRA Settings** tab and click the **IaaS install** tab.
  - b Click the **IaaS Installer** link at the bottom of the page.



- c Verify that a new page that provides all the required components to the install IaaS components opens.



- 8 Click the **Services** tab and verify that the status of all the services is REGISTERED.

The screenshot shows the VMware vRealize Appliance interface. The 'Services' tab is selected, displaying a table of registered services. The table has four columns: Service, Service Type, Last Updated, and Status. All services listed are in a 'REGISTERED' status. The table is paginated to show 1-31 of 31 items.

Service	Service Type	Last Updated	Status
advanced-designer-service	com.vmware.csp.core.designer.service	2015 Oct 27 18:01:04	REGISTERED
approval-service	com.vmware.csp.core.cafe.approvals	2015 Oct 27 18:02:04	REGISTERED
artifact-management-service	com.vmware.devops.artifactmanagement	2015 Oct 27 18:01:11	REGISTERED
authentication	com.vmware.csp.cafe.authentication	2015 Oct 28 08:22:04	REGISTERED
authorization	com.vmware.csp.cafe.authorization	2015 Oct 28 22:06:05	REGISTERED
branding-service	com.vmware.csp.core.branding.service	2015 Oct 27 18:00:33	REGISTERED
catalog-service	com.vmware.csp.core.cafe.catalog	2015 Oct 27 18:02:04	REGISTERED
component-registry	com.vmware.csp.core.cafe.componentregistry	2015 Oct 27 17:59:27	REGISTERED
console-proxy-service	com.vmware.csp.component.console.proxy.service	2015 Oct 27 18:01:04	REGISTERED
content-management	com.vmware.csp.core.content.service	2015 Oct 27 18:01:04	REGISTERED
dashboard-service	com.vmware.devops.dashboard	2015 Oct 28 20:04:04	REGISTERED
eventlog-service	com.vmware.csp.cafe.eventlog	2015 Oct 27 17:59:10	REGISTERED
fabric-service	com.vmware.csp.fabric.cafe.fabric	2015 Oct 27 17:59:44	REGISTERED
files-service	com.vmware.csp.core.cafe.files	2015 Oct 27 17:59:55	REGISTERED
iaas-proxy-provider	com.vmware.csp.component.iaas.proxy.provider	2015 Oct 27 17:59:40	REGISTERED
iaas-service	com.vmware.csp.iaas.blueprint.service	2015 Oct 30 04:16:01	REGISTERED
identity	com.vmware.csp.core.cafe.identity	2015 Oct 28 22:34:04	REGISTERED
licensing-service	com.vmware.csp.core.cafe.licensing	2015 Oct 27 17:59:26	REGISTERED
management-service	com.vmware.csp.component.management.service	2015 Oct 27 18:00:25	REGISTERED
notification-service	com.vmware.csp.cafe.notification	2015 Oct 27 18:02:04	REGISTERED
plugin-service	com.vmware.csp.core.plugin.service	2015 Oct 27 17:59:27	REGISTERED
portal-service	com.vmware.csp.core.portal.service	2015 Oct 27 18:00:33	REGISTERED
release-management	com.vmware.csp.component.devops.release.managem	2015 Oct 27 18:00:00	REGISTERED
reservation-service	com.vmware.vcac.core.cafe.reservation	2015 Oct 27 18:00:04	REGISTERED
resource-service	com.vmware.csp.core.cafe.resource	2015 Oct 27 18:00:55	REGISTERED
shell-ui-app	com.vmware.csp.core.cafe.shell	2015 Oct 28 20:22:04	REGISTERED
sts-service	com.vmware.cis.core.sso	2015 Oct 27 17:20:05	REGISTERED
vco	com.vmware.vco.o11n	2015 Oct 27 18:02:04	REGISTERED
vco	com.vmware.vco.o11n	2015 Oct 28 15:12:04	REGISTERED
vco	com.vmware.vco.o11n	2015 Oct 28 15:12:04	REGISTERED
workitem-service	com.vmware.csp.core.cafe.workitem	2015 Oct 28 21:08:04	REGISTERED

- 9 Repeat the procedure for other appliance `vra01svr01b.rainpole.local` to verify the version and configuration status.

## Verify the Status of IaaS Web Server and Manager Service Nodes of vRealize Automation

After you perform software maintenance in the Software-Defined Data Center (SDDC), verify that the IaaS Web Server and the IaaS Manager Service nodes are accessible.

After you patch, update, upgrade, restore, failover, or failback the vRealize Automation IaaS Web Server nodes and the IaaS Manager Service nodes, verify that the nodes are available by checking that you can access the following points:

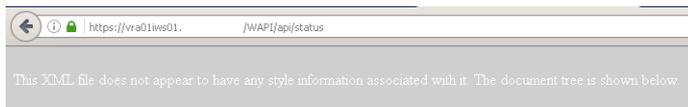
- Web Services API of the IaaS Web Server nodes `vra01iws01a.rainpole.local` and `vra01iws01b.rainpole.local`
- VM provisioning service (VMPS) of the IaaS Manager Service nodes `vra01ims01a.rainpole.local` and `vra01ims01b.rainpole.local`.

You access the points over the URLs for the nodes and the URL for the vRealize Automation load balancer.

## Procedure

- 1 In a Web browser, go to each of the following URLs and verify the `ServiceInitializationStatus` of the vRealize Automation IaaS Web server node in the response.

Node	URL	Expected Service Initialization Status
Virtual IP (VIP)	<a href="https://vra01iws01.rainpole.local/WAPI/api/status">https://vra01iws01.rainpole.local/WAPI/api/status</a>	REGISTERED
IaaS Web Server 1	<a href="https://vra01iws01a.rainpole.local/WAPI/api/status">https://vra01iws01a.rainpole.local/WAPI/api/status</a>	REGISTERED
IaaS Web Server 2	<a href="https://vra01iws01b.rainpole.local/WAPI/api/status">https://vra01iws01b.rainpole.local/WAPI/api/status</a>	REGISTERED



```

ServiceRegistryStatus
  DefaultServiceEndpointType           DefaultServiceEndpointType
  ErrorMessage "true"
  IdentityCertificateInfo "true"
  Initialized           Initialized
  ServiceInitializationStatus           ServiceInitializationStatus
  ServiceName           ServiceName
  ServiceRegistrationId "true"
  SolutionUser "true"
  SslCertificateInfo "true"
  StartedTime "true"
ServiceRegistryStatus

```

- 2 (Optional) Stop the World Wide Web Publishing Services on the IaaS Web Server nodes and open the vCloud Automation Center Web API Web page to verify that the load balancer redirects the traffic to the other IaaS Web Server node.
  - a Log in to the Windows virtual machine `vra01iws01a.rainpole.local` as an administrator.
  - b Open a command prompt and run the following command to stop the World Wide Web Publishing Services.

```
net stop w3svc
```

- c In a Web browser, go to the VIP URL **`https://vra01iws01.rainpole.local/WAPI/api/status`** and verify that the service registry status page loads.
- d Back in the command prompt, run the following command to start the World Wide Web Publishing Services.

```
net start w3svc
```

- e Repeat the step for the other IaaS Web Server `vra01iws01b.rainpole.local` to verify that the load balancer redirects the traffic.

- 3 In a Web browser, go to each of the following URLs to open the ProvisionService Service Web page and verify the connection to the IaaS Manager Service VM provisioning service (VMPS).

You do not verify the `vra01ims01b.rainpole.local` node because `vra01ims01a.rainpole.local` and `vra01ims01b.rainpole.local` are in active-passive mode.

Node	URL
Virtual IP (VIP)	<a href="https://vra01ims01.rainpole.local/VMPS">https://vra01ims01.rainpole.local/VMPS</a>
IaaS Manager Service 1	<a href="https://vra01ims01a.rainpole.local/VMPS">https://vra01ims01a.rainpole.local/VMPS</a>

**ProvisionService Service**

You have created a service.

To test this service, you will need to create a client and use it to call the service. You can do this using the `svcutil.exe` tool from the command line with the following syntax:

```
svcutil.exe https://vra01ims01a.rainpole.local/VMPSProvision?w=dl
```

You can also access the service description as a single file:

```
https://vra01ims01a.rainpole.local/VMPSProvision?single=w=dl
```

This will generate a configuration file and a code file that contains the client class. Add the two files to your client application and use the generated client class to call the Service. For example:

```
C#
class Test
{
    static void Main()
    {
        ProvisionClient client = new ProvisionClient();

        // Use the 'client' variable to call operations on the service.

        // Always close the client.
        client.Close();
    }
}

Microsoft Basic
Class Test
Shared Sub Main()
    Dim client As ProvisionClient = New ProvisionClient()
    ' Use the 'client' variable to call operations on the service.

    ' Always close the client.
    client.Close()
End Sub
End Class
```

## Verify the Version and Service Status of vRealize Automation Windows Nodes

After you patch, update, restore, failover, or failback the vRealize Automation Windows nodes, such as Infrastructure as a Service (IaaS) Web Servers, IaaS Manager Service nodes, Distributed Execution Manager (DEM) Workers, vSphere Proxy Agents and Microsoft SQL Server, for each of them verify the version and the service status of its components.

**Table 2-2. Program Names and Services to Verify on the Windows Nodes of vRealize Automation**

Role	VM Name/Host Name	Program Names for Version Check	Services for Availability Check
IaaS Web Server	vra01iws01a.rainpole.local	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center Management Agent</li> <li>■ VMware vCloud Automation Center Server</li> <li>■ VMware vCloud Automation Center WAPI</li> </ul>	VMware vCloud Automation Center Management Agent
IaaS Web Server	vra01iws01b.rainpole.local	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center Management Agent</li> <li>■ VMware vCloud Automation Center Server</li> <li>■ VMware vCloud Automation Center WAPI</li> </ul>	VMware vCloud Automation Center Management Agent
IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center DEM-Orchestrator - vra01ims01a.rainpole.local DEO</li> <li>■ VMware vCloud Automation Center Management Agent</li> <li>■ VMware vCloud Automation Center Server</li> </ul>	<ul style="list-style-type: none"> <li>■ VMware DEM-Orchestrator - vra01ims01a.rainpole.local DEO</li> <li>■ VMware vCloud Automation Center Management Agent</li> <li>■ VMware vCloud Automation Center Service</li> </ul>
IaaS Manager Service and DEM Orchestrator	vra01ims01b.rainpole.local	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center DEM-Orchestrator - vra01ims01b.rainpole.local DEO</li> <li>■ VMware vCloud Automation Center Management Agent</li> <li>■ VMware vCloud Automation Center Server</li> </ul>	<ul style="list-style-type: none"> <li>■ VMware DEM-Orchestrator - vra01ims01b.rainpole.local DEO</li> <li>■ VMware vCloud Automation Center Management Agent</li> <li>■ VMware vCloud Automation Center Service (Manual)</li> </ul>
vRealize Automation DEM Worker	vra01dem01.rainpole.local	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-01</li> <li>■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-02</li> <li>■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-03</li> <li>■ VMware vCloud Automation Center Management Agent</li> </ul>	<ul style="list-style-type: none"> <li>■ VMware DEM-Worker - DEM-WORKER-01</li> <li>■ VMware DEM-Worker - DEM-WORKER-02</li> <li>■ VMware DEM-Worker - DEM-WORKER-03</li> <li>■ VMware vCloud Automation Center Management Agent</li> </ul>
vRealize Automation DEM Worker	vra01dem02.rainpole.local	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-04</li> <li>■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-05</li> <li>■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-06</li> <li>■ VMware vCloud Automation Center Management Agent</li> </ul>	<ul style="list-style-type: none"> <li>■ VMware DEM-Worker - DEM-WORKER-04</li> <li>■ VMware DEM-Worker - DEM-WORKER-05</li> <li>■ VMware DEM-Worker - DEM-WORKER-06</li> <li>■ VMware vCloud Automation Center Management Agent</li> </ul>

**Table 2-2. Program Names and Services to Verify on the Windows Nodes of vRealize Automation (Continued)**

Role	VM Name/Host Name	Program Names for Version Check	Services for Availability Check
vRealize Automation Proxy Agent	vra01ias01.sfo01.rainpole.local	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center Agents - vSphere-Agent-01</li> <li>■ VMware vCloud Automation Center Management Agent</li> </ul>	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center Agent - vSphere-Agent-01</li> <li>■ VMware vCloud Automation Center Management Agent</li> </ul>
vRealize Automation Proxy Agent	vra01ias02.sfo01.rainpole.local	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center Agents - vSphere-Agent-02</li> <li>■ VMware vCloud Automation Center Management Agent</li> </ul>	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center Agent - vSphere-Agent-02</li> <li>■ VMware vCloud Automation Center Management Agent</li> </ul>
vRealize Automation Proxy Agent	vra01ias51.lax01.rainpole.local	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center Agents - vSphere-Agent-51</li> <li>■ VMware vCloud Automation Center Management Agent</li> </ul>	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center Agent - vSphere-Agent-51</li> <li>■ VMware vCloud Automation Center Management Agent</li> </ul>
vRealize Automation Proxy Agent	vra01ias52.lax01.rainpole.local	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center Agents - vSphere-Agent-52</li> <li>■ VMware vCloud Automation Center Management Agent</li> </ul>	<ul style="list-style-type: none"> <li>■ VMware vCloud Automation Center Agent - vSphere-Agent-52</li> <li>■ VMware vCloud Automation Center Management Agent</li> </ul>
Microsoft SQL Server	vra01mssql01.rainpole.local	-	MSSQLSERVER

**Note** vSphere Proxy Agent nodes are region-specific. Failover or failback operations are not applicable for these nodes.

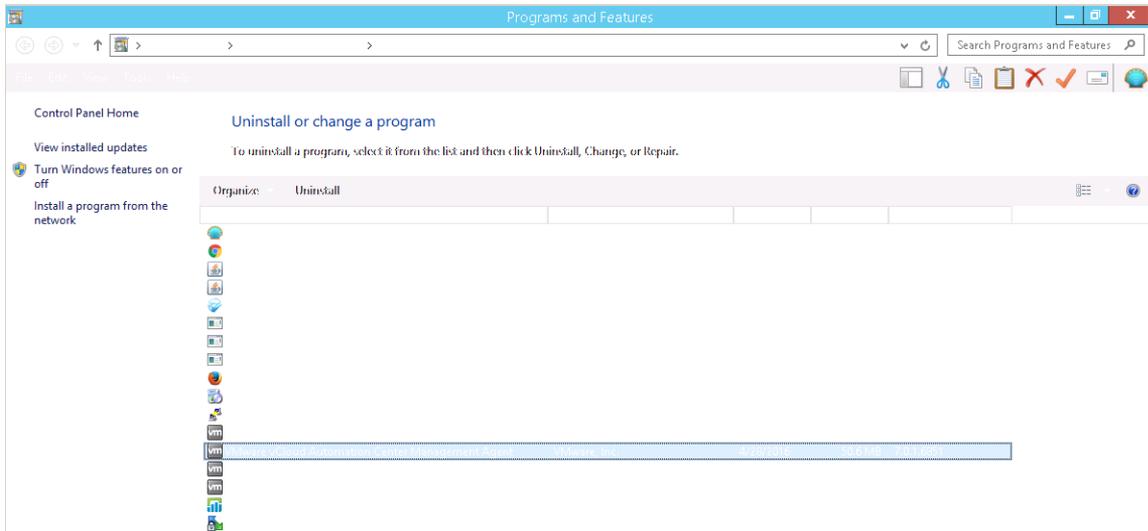
Verify the configuration of the IaaS Web Server vra01iws01a.rainpole.local first.

### Procedure

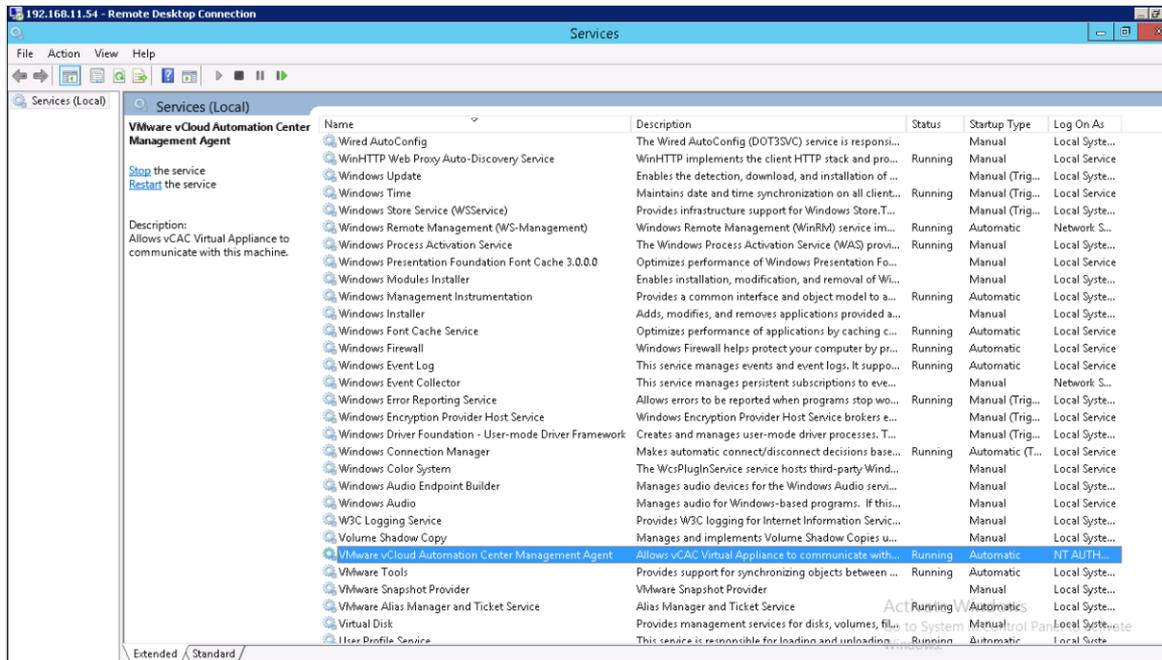
- 1 Log in to the vra01iws01a.rainpole.local Windows virtual machine by using a Remote Desktop Protocol (RDP) client.
  - a Open an RDP connection to the virtual machine vra01iws01a.rainpole.local.
  - b Log in using the following credentials.

Credential	Value
User name	svc-vra@rainpole.local
Password	svc-vra_password

- 2 If you have performed a patch or update, verify the version of IaaS Web Server programs.
  - a From the Windows **Start** menu, select **Control Panel > Programs and Features**.
  - b Verify that the version of the following programs is successfully updated.
    - VMware vCloud Automation Center Management Agent
    - VMware vCloud Automation Center Server
    - VMware vCloud Automation Center WAPI



- 3 Verify the status of IaaS Web Server services.
  - a From the Windows **Start** menu, select **Administrative Tools > Services**.
  - b Verify that the status of the VMware vCloud Automation Center Management Agent service is **Running**.



- 4 Repeat the procedure for each of the other Windows nodes of vRealize Automation from the table to verify the version and services availability.

## Verify the Version, Status, and Configuration of vRealize Orchestrator VMs

Make sure that the two servers in the vRealize Orchestrator cluster are operational after a patch, update, restore, failover, or fallback operation.

### Procedure

- 1 Verify that the vRealize Orchestrator appliance management interface is operational and that its version is correct.
  - a Open a Web browser and go to **https://vra01vro01a.rainpole.local:5480**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vro_appliance_A_root_pwd

- c On **System** tab, click to **Information** tab and verify that the version is correct
  - d (Optional) Log in to the second vRealize Orchestrator appliance  
**https://vra01vro01b.rainpole.local:5480** and verify the version.
- 2 Verify the status of the vRealize Orchestrator server service in the Control Center.
- a Open a Web browser and go to  
**https://vra01vro01a.rainpole.local:8283/vco-controlcenter.**
  - b Log in using the following credentials.

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

- c On the **Home** page, under **Manage**, click **Startup Options**.
- d On the **Startup Options** page, verify that Current Status is RUNNING.

The screenshot shows the VMware vRealize Orchestrator Control Center interface. The page title is "VMware vRealize Orchestrator" and "Control Center". The main content area is titled "Startup Options" and includes a power icon and the text "Control the Orchestrator server service." Below this, the "Current Status" is displayed as "RUNNING". There are three buttons: "Start", "Stop", and "Restart". A detailed status box shows the following information:

```

Status-Ing tcServer
Instance name:    app-server
Runtime version: 6.0.30.C.RELEASE
tc Runtime Base: /var/lib/vco/app-server
Status:          RUNNING as PID=3605
  
```

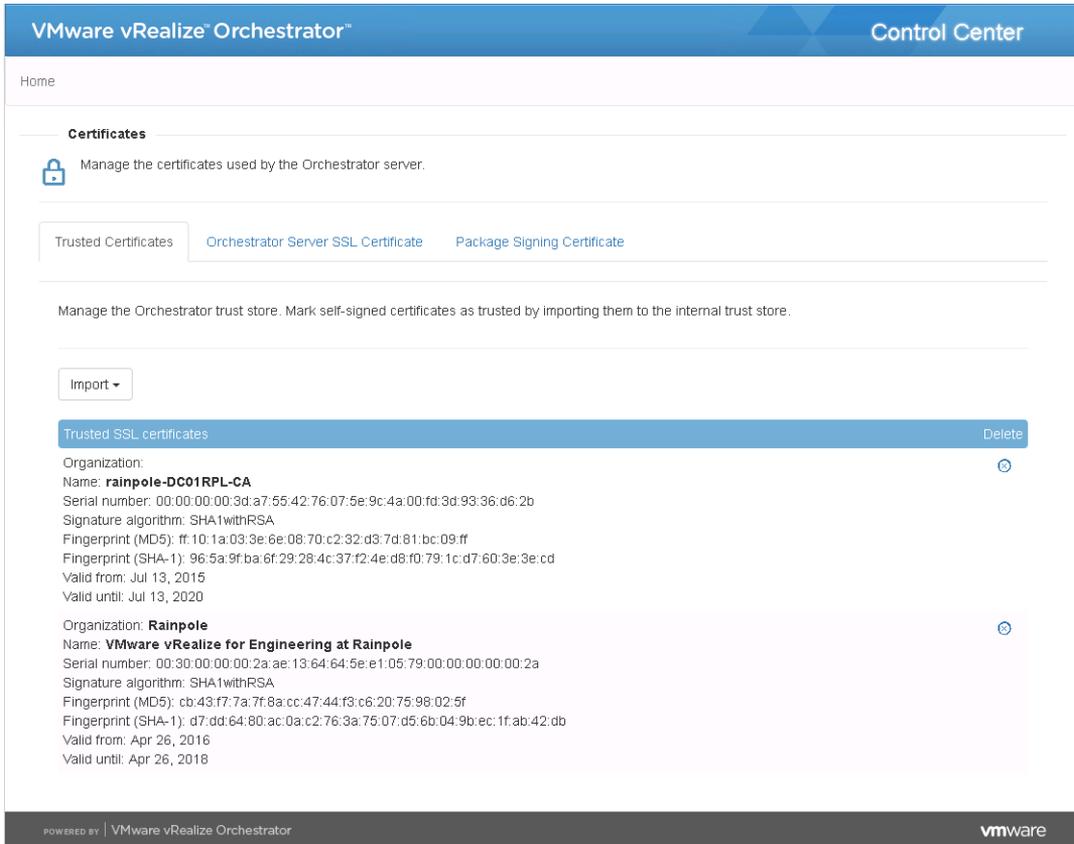
Below the status box, the following version and build information is displayed:

```

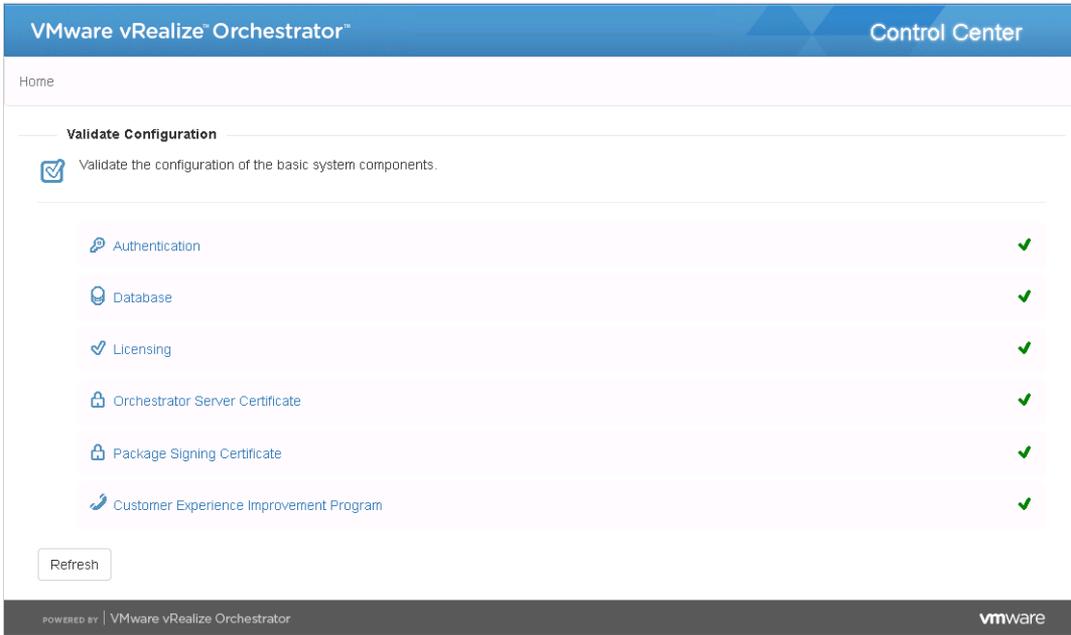
Version: 7.0.1
Build number: 3533702
Build date: Feb 9, 2016
Database version: 1.71
Install path: /var/lib/vco
  
```

The footer of the page includes "POWERED BY VMware vRealize Orchestrator" and the VMware logo.

- 3 Verify that all imported SSL certificates are intact.
  - a On the **Home** page, under **Manage**, click **Certificates**.
  - b Verify that the **Certificates** page shows the Microsoft CA certificate and issuer certificate, and that the certificates are not expired.



- 4 Validate the vRealize Orchestrator configuration in the vRealize Orchestrator Control Center.
  - a On the **Home** page, under **Manage**, click **Validate Configuration**.
  - b Verify that each system component configuration has a green check mark.



- 5 Verify that the authentication configuration is correct.
  - a On the **Home** page, under **Manage**, click **Configure Authentication Provider**.
  - b Click the **Test Login** tab, enter the following user credentials, and click **Test**.

Setting	Value
User name	svc-vra@rainpole.local
Password	svc-vra_password

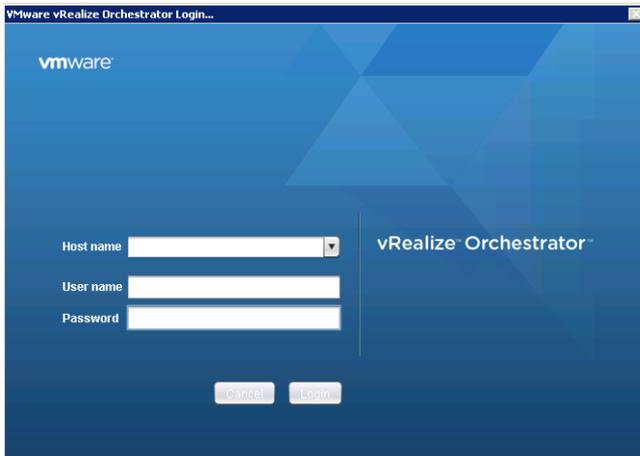
- c Verify that the user interface shows the message The User has administrative rights in vRealize Orchestrator.

The screenshot shows the VMware vRealize Orchestrator Control Center interface. The page title is "VMware vRealize Orchestrator" and the sub-header is "Control Center". The main content area is titled "Configure Authentication Provider" and includes a sub-header "Configure the authentication parameters and test your login credentials." Below this, there are two tabs: "Authentication Provider" and "Test Login". The "Test Login" tab is active. A message states: "After configuring your authentication provider, you can test if a user has administrative rights in the Orchestrator." Below this, a green info box displays: "Info. The user has administrative rights in vRealize Orchestrator." At the bottom, there are input fields for "User name" (containing "svc-vra@rainpole.local") and "Password" (containing "(Required)"). A "Test" button is located below the password field. The footer of the page reads "POWERED BY VMware vRealize Orchestrator" and the VMware logo is in the bottom right corner.

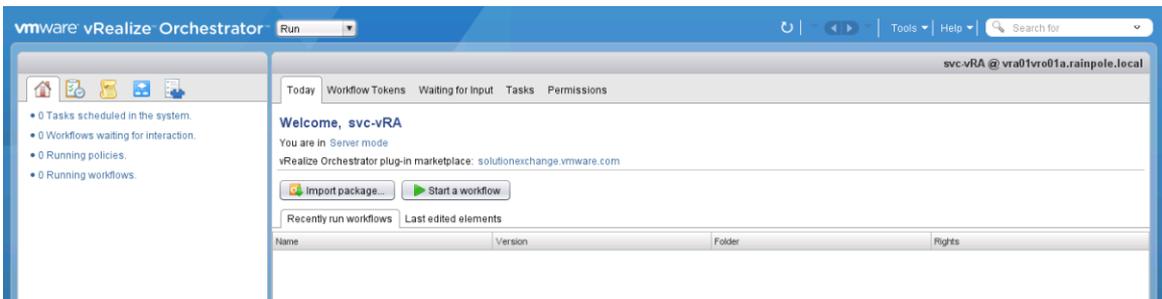
- 6 Repeat [Step 2](#) to [Step 5](#) for the other vRealize Orchestrator appliance at <https://vra01vro01b.rainpole.local:8283/vco-controlcenter/>.
- 7 Verify that you can log in to the vRealize Orchestrator servers by using the vRealize Orchestrator client.
  - a Open a Web browser and go to <https://vra01vro01a.rainpole.local:8281/vco/>.
  - b On the main page of vRealize Orchestrator, click the **Start Orchestrator Client** link and open the `client.jnlp` file.

- c Log in using the following credentials.

Setting	Value
User name	svc-vra@rainpole.local
Password	svc-vra_password



- d If a certificate warning appears, ignore it.
- e Verify that the login is successful.

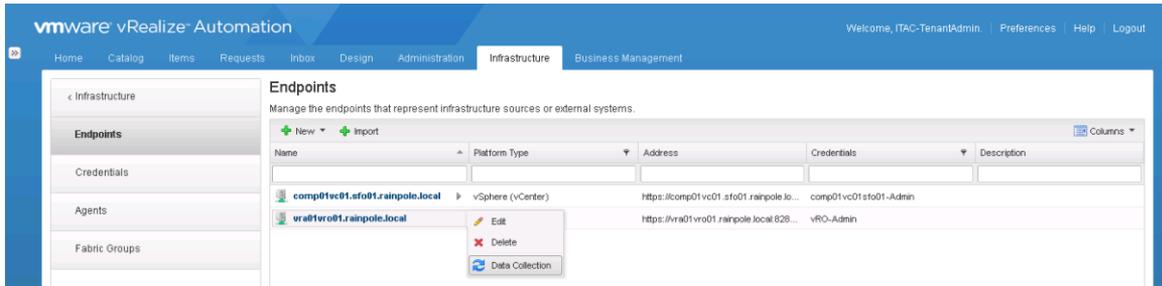


- f Repeat the step for the other vRealize Orchestrator appliance at **https://vra01vro01b.rainpole.local:8281/vco/** to verify that the login is successful.
- 8 Verify the vRealize Orchestrator endpoint data collection status in the vRealize Automation Rainpole portal.
- a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

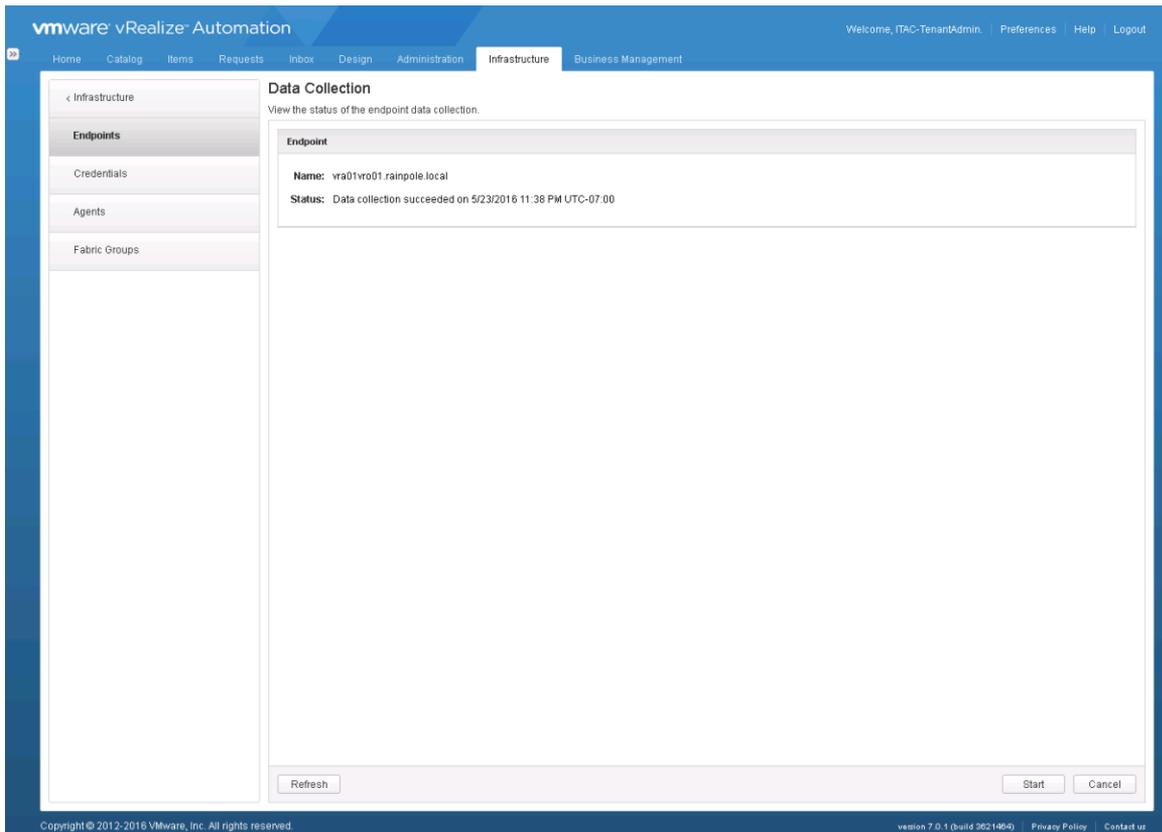
Setting	Value
User name	ITAC-TenantAdmin
Password	rainpole_tenant_admin_password
Domain	rainpole.local

- c Click the **Infrastructure** tab and click **Endpoints > Endpoints**.

- d Hover the vRealize Orchestrator endpoint and select **Data Collection**.

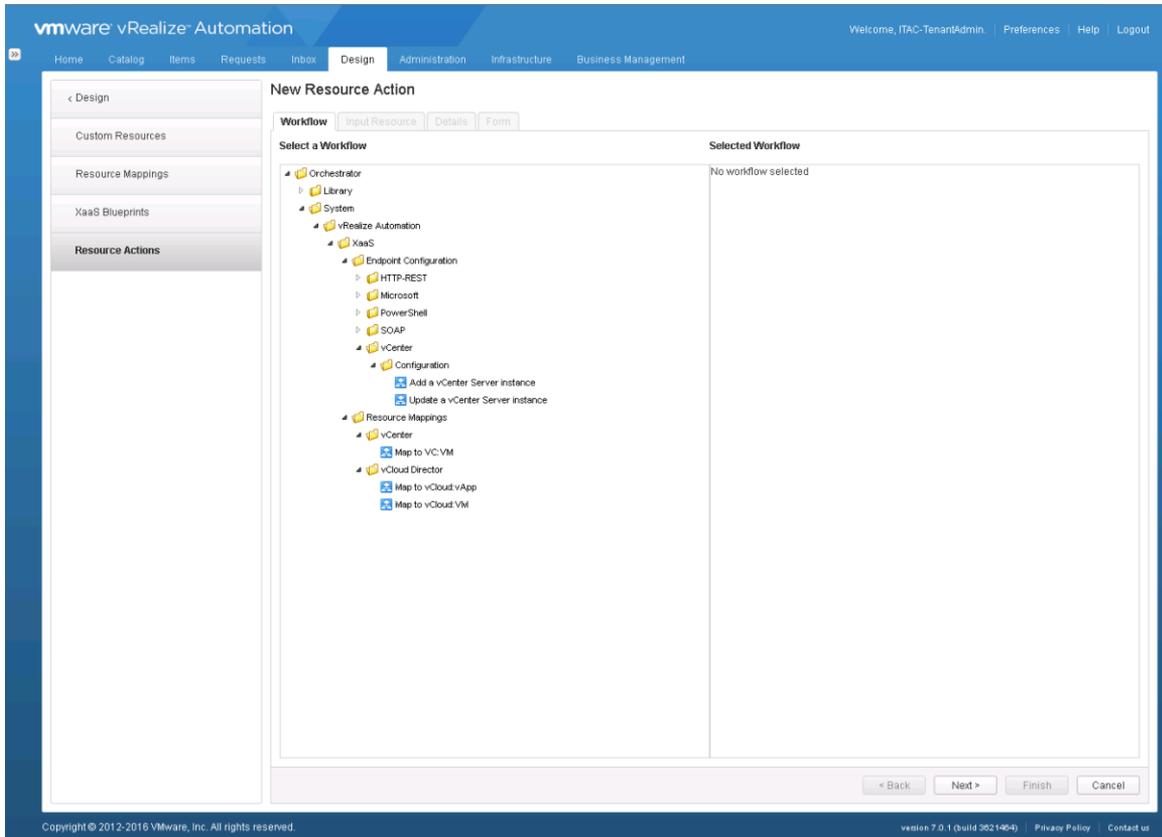


- e Click the **Start** button.
- f Click the **Refresh** button to receive an updated message about the status of the vRealize Orchestrator data collection.
- g Verify that the Status shows the message Data collection succeeded with the updated time.



- 9 (Optional) Verify the vRealize Orchestrator workflow navigation in the vRealize Automation Rainpole portal.
  - a Click the **Design** tab.
  - b Click **XaaS > Resource Actions**.

- c On the **Resource Actions** page, click **New**.
- d In the **Select a Workflow** pane, expand the **Orchestrator** node, and verify that you can view the vRealize Orchestrator folders and workflows.



- 10 (Optional) Verify that the load balancer works for vRealize Orchestrator by accessing the load balancer URL after you stop the vRealize Orchestrator service on the vra01vro01a.rainpole.local appliance.

- a Open a Web browser and go to **https://vra01vro01a.rainpole.local:8283/vco-controlcenter/**.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	vro_appliance_A_root_pwd

- c On the **Home** page, under **Manage**, click **Startup Options**.
- d Click **Stop** to stop the Orchestrator server service on the appliance.
- e Open a Web browser, go to the vRealize Orchestrator load balancer URL **https://vra01vro01.rainpole.local:8281/vco/** and verify that the URL is accessible.
- f Go back to **https://vra01vro01a.rainpole.local:8283/vco-controlcenter/**.

- g On the **Home** page, under **Manage**, click **Startup Options**, and click **Start** to start the Orchestrator server service.
- h Repeat the steps for the other vRealize Orchestrator appliance at <https://vra01vro01b.rainpole.local:8283/vco-controlcenter/>.

## Verify the Status of the Distributed Execution Managers and vSphere Proxy Agents in vRealize Automation

After you perform software maintenance, verify that status the Distributed Execution Manager (DEM) and IaaS vSphere Proxy Agents components

After you patch, update, restore, failover, or failback vRealize Automation, verify that the Distributed Execution Manager (DEM) Orchestrators and Workers are online, and that the IaaS vSphere Proxy Agents that connect vRealize Automation to the compute pods are online.

### 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 Verify the status of the DEM nodes.

- a On the **Infrastructure** tab, click **Monitoring > DEM > Status**.
- b Verify that the status of the DEM-Orchestrator and DEM-Worker virtual machines is **Online**.

vRealize Automation Node	Virtual Machine
iaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local
iaaS Manager Service and DEM Orchestrator	vra01ims01b.rainpole.local
vRealize Automation DEM Worker	vra01dem01.rainpole.local
vRealize Automation DEM Worker	vra01dem02.rainpole.local

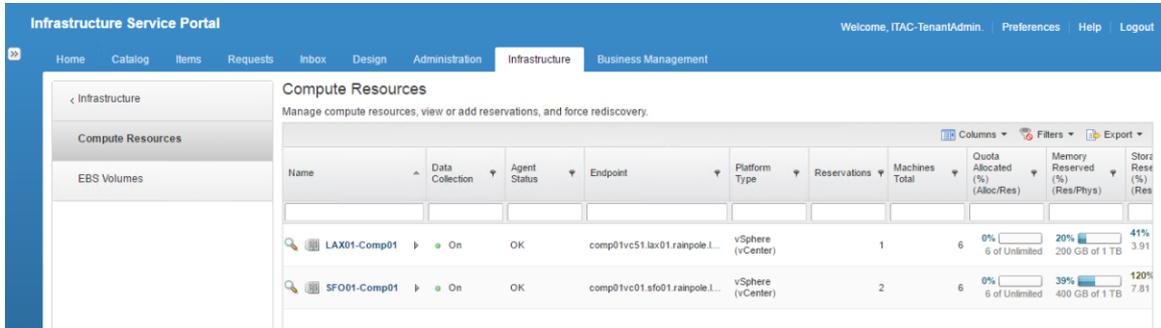
The screenshot shows the VMware vRealize Automation interface. The top navigation bar includes 'Infrastructure' and 'Business Management'. The left sidebar has 'DEM Status' selected. The main content area displays 'DEM Status' with a summary of workflow counts (Total: 0, Executing: 0, Pending: 0) and two tables.

Name	Status	Workflows Executing	Machine	Role	Last Pinged	Last Completed Workflow	Skills
DEM-WORKER-01	Online	0	vra01dem01	Worker	5/20/2016 8:25 AM UTC-07:00	5/20/2016 8:11 AM UTC-07:00	
DEM-WORKER-02	Online	0	vra01dem01	Worker	5/20/2016 8:25 AM UTC-07:00	5/20/2016 8:16 AM UTC-07:00	
DEM-WORKER-03	Online	0	vra01dem01	Worker	5/20/2016 8:25 AM UTC-07:00	5/20/2016 8:21 AM UTC-07:00	
DEM-WORKER-04	Online	0	vra01dem02	Worker	5/20/2016 8:25 AM UTC-07:00	5/20/2016 7:41 AM UTC-07:00	
DEM-WORKER-05	Online	0	vra01dem02	Worker	5/20/2016 8:25 AM UTC-07:00	5/20/2016 7:21 AM UTC-07:00	
DEM-WORKER-06	Online	0	vra01dem02	Worker	5/20/2016 8:25 AM UTC-07:00	5/20/2016 6:11 AM UTC-07:00	
vra01ims01a.rainpole.local DEO	Online (Active)		vra01ims01a	Orchestrator	5/20/2016 8:25 AM UTC-07:00		
vra01ims01b.rainpole.local DEO	Online		vra01ims01b	Orchestrator	5/20/2016 8:25 AM UTC-07:00		

Name	Last Run	Last Successful Run	Next Run	Description
ReclaimDestroyedStaticIPAddresses	5/20/2016 8:21 AM UTC-07:00	5/20/2016 8:21 AM UTC-07:00	5/20/2016 8:26 AM UTC-07:00	
LaunchEndpointDataCollection	5/20/2016 4:51 AM UTC-07:00	5/20/2016 4:51 AM UTC-07:00	5/20/2016 8:51 AM UTC-07:00	
CollectMachinesUsage	5/20/2016 4:51 AM UTC-07:00	5/20/2016 4:51 AM UTC-07:00	5/20/2016 8:51 AM UTC-07:00	
vSphereTBMCostImport	5/19/2016 5:01 PM UTC-07:00	5/19/2016 5:01 PM UTC-07:00	5/20/2016 5:01 PM UTC-07:00	
SendAlertEmail	5/19/2016 7:00 PM UTC-07:00	5/19/2016 7:00 PM UTC-07:00	5/20/2016 7:00 PM UTC-07:00	
CollectEndpointUsage	5/19/2016 8:00 PM UTC-07:00	5/19/2016 8:00 PM UTC-07:00	5/20/2016 8:00 PM UTC-07:00	
DataRollover	5/19/2016 8:00 PM UTC-07:00	5/19/2016 8:00 PM UTC-07:00	5/20/2016 8:00 PM UTC-07:00	
EndpointMetrics	5/19/2016 9:00 PM UTC-07:00	5/19/2016 9:00 PM UTC-07:00	5/20/2016 9:00 PM UTC-07:00	
BlueprintMetrics	5/19/2016 9:00 PM UTC-07:00	5/19/2016 9:00 PM UTC-07:00	5/20/2016 9:00 PM UTC-07:00	
ReservationMetrics	5/19/2016 9:00 PM UTC-07:00	5/19/2016 9:00 PM UTC-07:00	5/20/2016 9:00 PM UTC-07:00	

- 3 Verify that the vSphere Proxy Agents are working properly.
  - a On the **Infrastructure** tab, click **Compute Resources > Compute Resources**.
  - b Verify that the Agent Status for the compute instance is OK.



- 4 If the Agent Status for the compute instance is Down, restart the vRealize Automation services on the vSphere Proxy Agent VMs.
  - a Open a Remote Desktop Protocol (RDP) connection to the virtual machine.

Region	Host Name
Region A	vra01ias01.sfo01.rainpole.local
	vra01ias02.sfo01.rainpole.local
Region B	vra01ias51.lax01.rainpole.local
	vra01ias52.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	Administrator
Password	local_administrator_pwd

- c From the Windows **Start** menu, click **Administrative Tools**, and click **Services**.
    - d In the Services dialog box, restart the following vRealize Automation services.
      - VMware vCloud Automation Center Management Agent
      - VMware vCloud Automation Center Agent
    - e If an agent is down after you restart the services, restart the agent VM.
    - f If the other vSphere Proxy Agent VM is down, repeat the step for it.

## Verify the Status of vRealize Automation Integration with Active Directory

Verify that vRealize Automation is connected to the Active Directory domain after patch, update, restore, failover or failback.

You verify the following configuration as a part of the Active Directory integration with vRealize Automation:

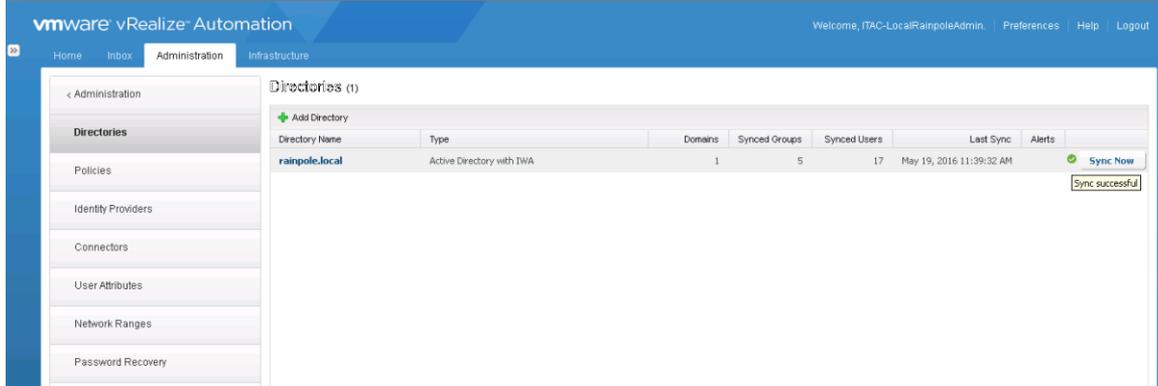
- Active Directory synchronization status
- Identity Providers status
- Connectors status

### Procedure

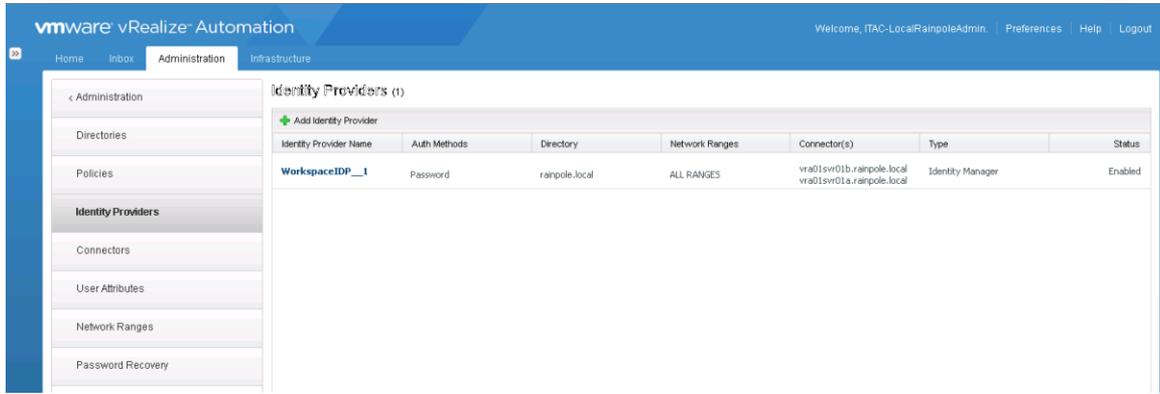
- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	Rainpole.local

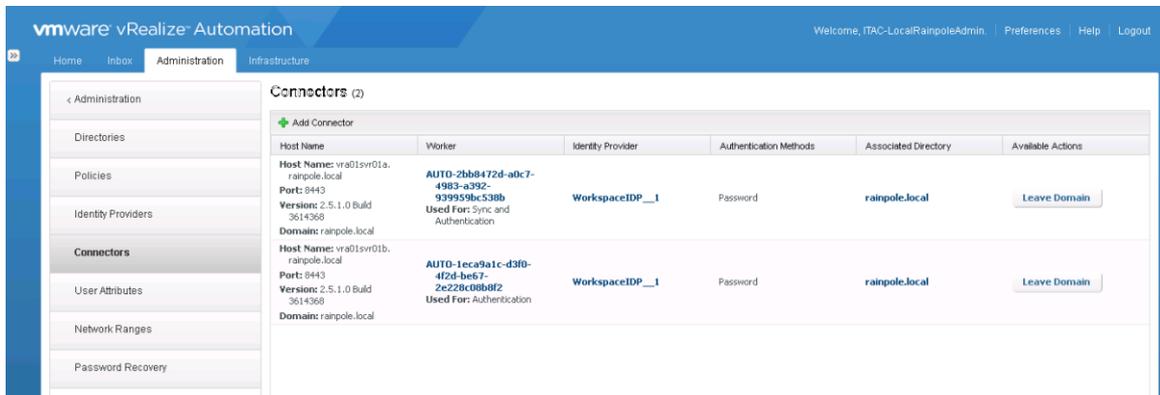
- 2 On the **Administration** tab, click the **Directories Management** tab and click **Directories**.
- 3 On the **Directories** page, hover over the green check mark to verify that the synchronization with the Active Directory is successful.



- 4 Click **Identity Providers** and verify that the Status column for the identity provider WorkspaceIDP\_\_1 shows Enabled.



- 5 Click **Connectors** and verify that for the each appliance-specific connector the Associated Directory column shows the rainpole.local domain.



## Verify the Version, Service Status and Configuration of the vRealize Business VMs

After you perform software maintenance in the Software-Defined Data Center, verify that both the vRealize Business Server and Data Collector are operational.

After a patch, update, restore, failover, or failback is performed, make sure that the version, service status and the configuration are intact.

**Table 2-3. vRealize Business Virtual Appliances Details**

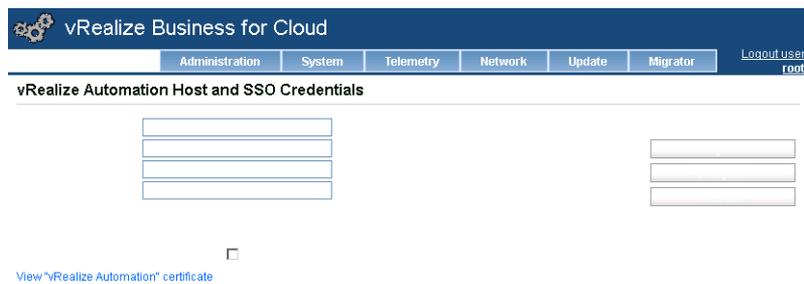
Region	vRealize Appliance	Virtual Appliance Management Interface (VAMI) URL	IP Address	FQDN
Region A	vRealize Business Server	https://vra01bus01.rainpole.local:5480	192.168.11.66	vra01bus01.rainpole.local
	vRealize Business Data Collector	https://vra01buc01.sfo01.rainpole.local:5480	192.168.31.54	vra01buc01.sfo01.rainpole.local
Region B	vRealize Business Data Collector	https://vra01buc51.lax01.rainpole.local:5480	192.168.32.54	vra01buc51.lax01.rainpole.local

## Procedure

- 1 Verify the authentication of the vRealize Business Server and the Data Collector virtual appliances.
  - a Open a Web browser and go to **https://vra01bus01.rainpole.local:5480**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vrb_server_root_password

- c Log in to the vRealize Business Data Collectors vra01buc01.sfo01.rainpole.local and vra01buc51.lax01.rainpole.local to verify the authentication.
- 2 Verify the Single Sign-On status of the vRealize Business Server.
  - a In the management console of the vRealize Business Server, click the **vRealize Automation** tab.
  - b Verify that the SSO Status is Connected to vRealize Automation.



- 3 If you have performed a patch or update, verify the version of the vRealize Business Server.
  - a In the management console of the vRealize Business Server, click the **Update** tab and click **Status**.
  - b Verify that the Appliance Version is correct.



- 4 If you have performed a patch or update, verify the version of the vRealize Business Data Collectors.
  - a In the management console of the vRealize Business Collector `vra01buc01.sfo01.rainpole.local`, click the **Update** tab and click **Status**.
  - b Verify that the Appliance Version is correct.



- c Repeat the step for the vRealize Business Collector `vra01buc51.lax01.rainpole.local` to verify the appliance version.
- 5 Verify the service status of the vRealize Business Server and the Data Collector in Region A.
  - a Open an SSH connection to `vra01bus01.rainpole.local`.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<code>vrb_server_root_password</code>

- c Run the following command to see the summary of all processes and their status.

```
monit summary
```

```

login as: root
VMware "vRealize Business for Cloud" Appliance
root@vra01bus01.rainpole.local's password:
Last login: Wed Feb  8 06:51:02 2017 from 172.18.11.237
vra01bus01:~ # monit summary
The Monit daemon 5.14 uptime: 19h 13m

Filesystem 'rootfs'           Accessible
Process 'vami-lighttp'        Running
Process 'config-service'     Running
Process 'postgres'           Running
Process 'mongo'               Running
Process 'facts-repo'          Running
Process 'bifrost-client'      Running
Process 'pricing-api'         Running
Process 'itbm-server'         Running
Process 'journal-service'     Running
Process 'itbm-data-collector' Running
System 'vra01bus01.rainpole.local' Running
vra01bus01:~ # █

```

- d Verify that the status of Filesystem processes and the System is as described in the following table.

Component	Status
Filesystem 'rootfs'	Accessible
Process 'vami-lighttp'	Running
Process 'config-service'	Running
Process 'postgres'	Running
Process 'mongo'	Running
Process 'facts-repo'	Running
Process 'bifrost-client'	Running
Process 'pricing-api'	Running
Process 'itbm-server'	Running
Process 'journal-service'	Running
Process 'itbm-data-collector'	Running
System 'vra01bus01.rainpole.local'	Running

- e Run the following command to see the detailed status of the appliance components.

```
monit status
```

- f Verify that the status of all processes is Running and the monitoring status is shown as Monitored.

```
vra01buc01:~ # monit status
The Monit daemon 5.14 uptime: 6d 17h 54m

Filesystem 'rootfs'
  status           Accessible
  monitoring status Monitored
  permission       660
  uid              0
  gid              6
  filesystem flags 0x1000
  block size       4.0 kB
  space total      43.1 GB (of which 5.1% is reserved for root user)
  space free for non superuser 34.4 GB [79.9%]
  space free total 36.6 GB [85.0%]
  inodes total     2875392
  inodes free      2834858 [98.6%]
  data collected   Tue, 24 May 2016 09:37:56

Process 'vami-lighttp'
  status           Running
  monitoring status Monitored
  pid              2139
  parent pid       1
  uid              0
  effective uid    0
  gid              0
  uptime           6d 17h 51m
  children         0
  memory           3.4 MB
  memory total     3.4 MB
  memory percent   0.0%
  memory percent total 0.0%
  cpu percent      0.0%
  cpu percent total 0.0%
  port response time 0.004s to [localhost]:5480/ type TCPSSL/IP protocol HTTP
  data collected   Tue, 24 May 2016 09:37:56

Process 'postgres'
  status           Running
  monitoring status Monitored
  pid              1772
  parent pid       1
  uid              1000
  effective uid    1000
  gid              100
  uptime           6d 17h 52m
  children         68
  memory           47.3 MB
```

- g Repeat the step for the other vRealize Business Data Collector vra01buc01.sfo01.rainpole.local. For the second data collector, the process itbm-server appears as Not monitored.

## 6 Verify the service status of the vRealize Business Data Collector in Region B.

- a Open an SSH connection to vra01buc51.lax01.rainpole.local.  
b Log in using the following credentials.

Setting	Value
User name	root
Password	vrb_server_root_password

- c Run the following command to see the summary of all processes and their status.

```
monit summary
```

- d Verify that the status of Filesystem, Process and the System processes is as described in the following table.

Component	Status
Filesystem 'rootfs'	Accessible
Process 'vami-lighttp'	Running
Process 'config-service'	Running
Process 'itbm-data-collector'	Running
System 'vra01buc51.lax01.rainpole.local'	Running

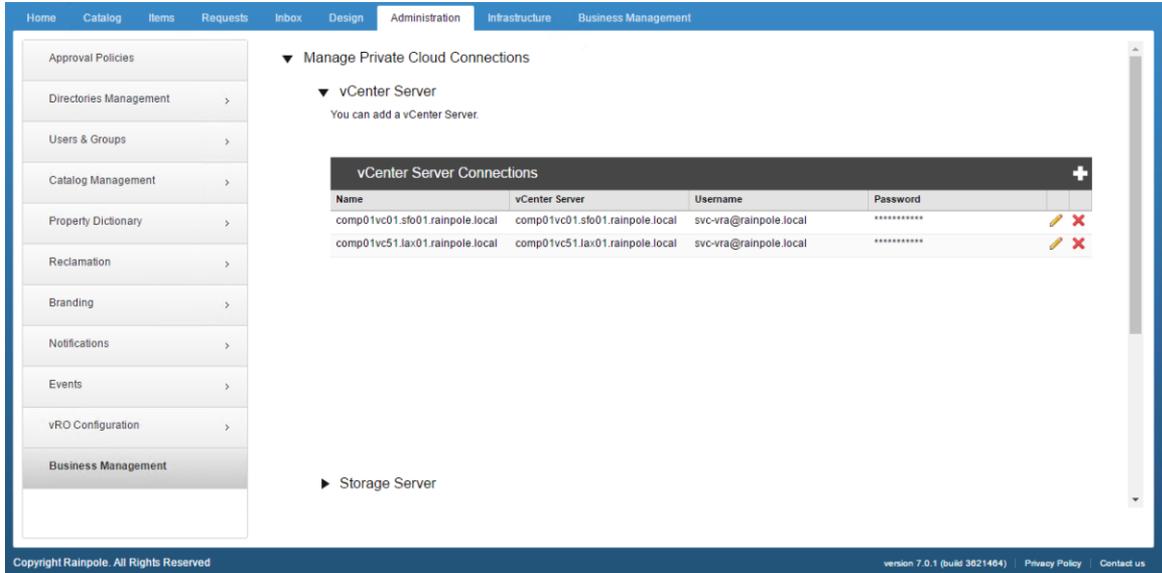
- e Run the following command to see the detailed status of the appliance components.

```
monit status
```

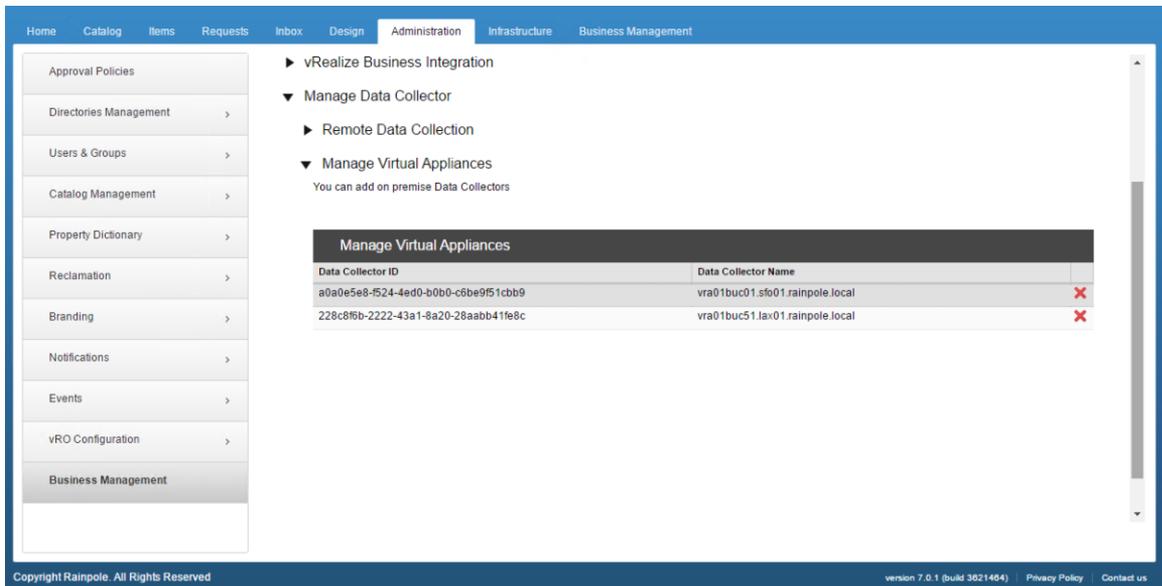
- f Verify that the status of all processes is Running and the monitoring status is shown as Monitored.
- 7 Verify the connection between vRealize Business and the Compute vCenter Server.
- a Open a Web browser and go to **<https://vra01svr01.rainpole.local/vcac/org/rainpole>**.
- b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	Rainpole.local

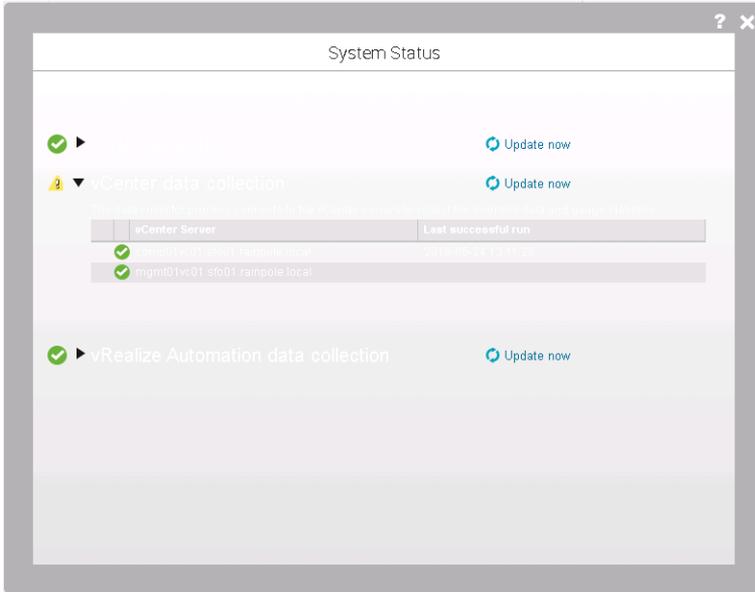
- c Click the **Administration** tab and click **Business Management**.
- d Click **Manage Private Cloud Connections > vCenter Server**, and verify that the Compute vCenter Server is listed in the vCenter Server Connections table.



- 8 Verify the connection between the vRealize Business Server and the vRealize Business Data Collector.
  - a On the **Business Management** page, click **Manage Data Collector > Manage Virtual Appliances**.
  - b Verify that the vra01buc01.sfo01.rainpole.local and vra01buc51.lax01.rainpole.local appliances are listed in the **Manage Virtual Appliances** table.

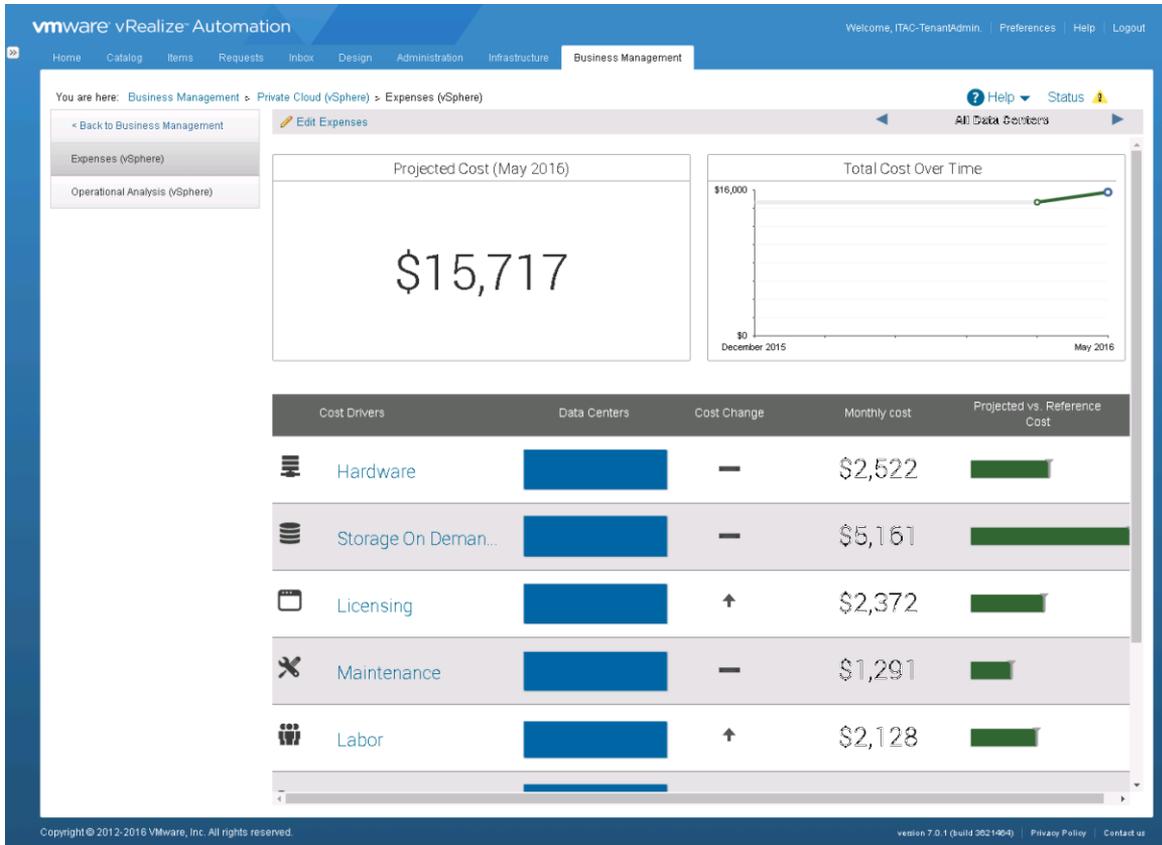


- 9 Verify that vRealize Business collects information from all vCenter Server instances.
  - a On the **Business Management** page, click the **Status** link.
  - b Under **vCenter data collection**, click **Update now**.
  - c Verify that a green sign appears next to all vCenter Server Instances in the table.



10 Verify that the expenses for vSphere are correct.

- a Click the **Business Management** tab, click **Private Cloud (vSphere) > Expenses (vSphere)**.
- b Verify that all the cost details are intact.



11 Verify the reports of vCenter server inventory items.

- a On the **Business Management** tab, click **Data Sets > vCenter Server > Servers** and verify that the data for the ESXi servers is intact.

Server Name	Total Monthly Cost	Infrastructure Type	vCenter Server Alias	Data Center Name	Deleted
comp01esx01.sfo01.rainpole.local	\$3,285.17	Esx Host	comp01vc01.sfo01.rainpole.local	SFO01	No
comp01esx02.sfo01.rainpole.local	\$1,325.17	Esx Host	comp01vc01.sfo01.rainpole.local	SFO01	No
comp01esx03.sfo01.rainpole.local	\$2,305.17	Esx Host	comp01vc01.sfo01.rainpole.local	SFO01	No
comp01esx04.sfo01.rainpole.local	\$2,185.17	Esx Host	comp01vc01.sfo01.rainpole.local	SFO01	No

- b Verify that the data for the Datastores, vSAN Data Stores, Virtual Machines, and Clusters is valid.

# Request a Single-Machine Blueprint from the Service Catalog of vRealize Automation

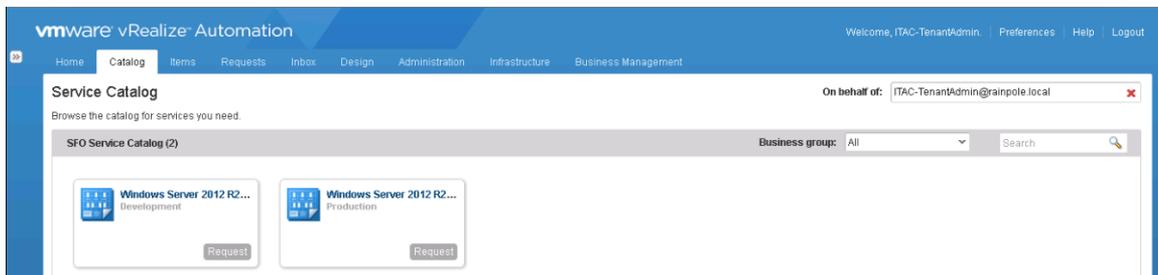
Request a single-machine blueprint item from the service catalog to verify that vRealize Automation provisions items to the cloud environment.

## Procedure

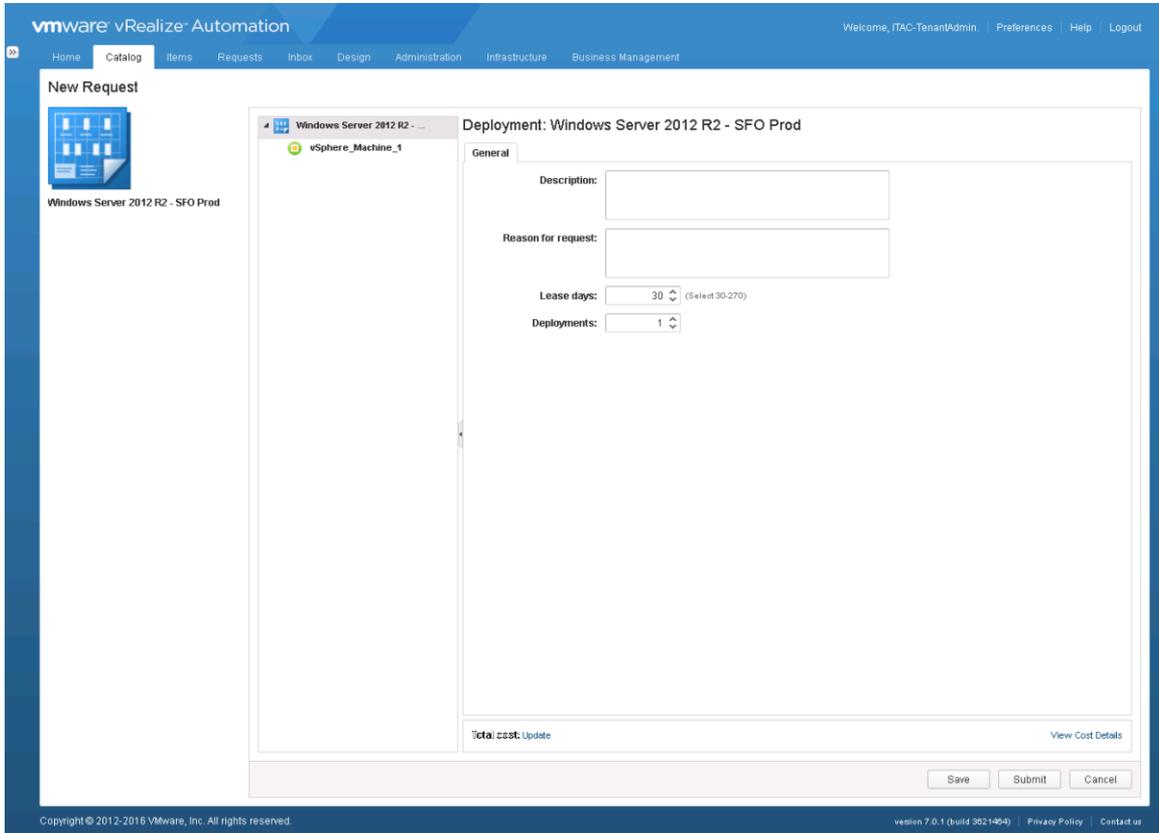
- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	Rainpole.local

- 2 Click the **Catalog** tab and verify that all entitled blueprints are available in the SFO Service Catalog.
  - Windows Server 2012 R2 - SFO Prod
  - Windows Server 2012 R2 - SFO Dev
  - Windows Server 2012 R2 With SQL2012 - SFO Prod
  - Windows Server 2012 R2 With SQL2012 - SFO Dev
  - Redhat Enterprise Linux 6 - SFO Prod
  - Redhat Enterprise Linux 6 - SFO Dev



- 3 Locate the Windows Server 2012 R2 - SFO Prod single-machine blueprint, click **Request**, and on the **New Request** page, click **Submit** to request a VM provisioning.



- In the vRealize Automation portal, click the **Requests** tab and verify that the Status for the Windows Server 2012 R2 - SFO Prodsingle-machine blueprint provisioning is Successful.

The screenshot shows the 'Requests' tab in the VMware vRealize Automation portal. The table displays a list of requests with the following columns: Request, Item, Description, Cost, Lease Cost, Status, Submitter, Submitted, and Last Updated. The status of the requests is as follows:

Request	Item	Description	Cost	Lease Cost	Status	Submitter	Submitted	Last Updated
15	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Successful	ITAC-TenantAdmin@rainpole	5/20/16, 2:00 PM	5/20/16, 2:04 PM
14	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Successful	ITAC-TenantAdmin@rainpole	5/18/16, 3:40 PM	5/18/16, 3:44 PM
13	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Successful	ITAC-TenantAdmin@rainpole	5/18/16, 3:14 PM	5/18/16, 3:18 PM
12	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Failed	ITAC-TenantAdmin@rainpole	5/18/16, 2:04 PM	5/18/16, 2:05 PM
11	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Failed	ITAC-TenantAdmin@rainpole	5/18/16, 11:25 AM	5/18/16, 11:27 AM
10	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Failed	ITAC-TenantAdmin@rainpole	5/18/16, 8:33 AM	5/18/16, 8:35 AM
9	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Failed	ITAC-TenantAdmin@rainpole	5/18/16, 8:30 AM	5/18/16, 8:32 AM
8	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Successful	ITAC-TenantAdmin@rainpole	5/13/16, 11:12 AM	5/13/16, 11:17 AM
7	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Successful	ITAC-TenantAdmin@rainpole	5/13/16, 8:56 AM	5/13/16, 7:00 AM
6	Windows Server 2012 R	Windows Server 2012 R	Not Applicable	Not Applicable	Failed	ITAC-TenantAdmin@rainpole	5/13/16, 8:54 AM	5/13/16, 8:54 AM
5	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Successful	ITAC-TenantAdmin@rainpole	5/13/16, 12:40 AM	5/13/16, 12:44 AM
4	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Failed	ITAC-TenantAdmin@rainpole	5/5/16, 3:53 AM	5/5/16, 8:57 AM
3	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Successful	ITAC-TenantAdmin@rainpole	5/4/16, 9:52 AM	5/4/16, 9:55 AM
2	Windows Server 2012 R	Windows Server 2012 R	\$0.00 / day	\$0.00	Failed	ITAC-TenantAdmin@rainpole	5/4/16, 9:50 AM	5/4/16, 9:50 AM
1	Windows Server 2012 R	Windows Server 2012 R	Not Applicable	Not Applicable	Failed	ITAC-TenantAdmin@rainpole	5/4/16, 9:32 AM	5/4/16, 9:32 AM

- Repeat the steps to provision a VM using Windows Server 2012 R2 - LAX Prod single-machine blueprint in region B.

## Verify the Cloud Management Platform Load Balancing

If you have performed an update, restore, failover or failback of the vRealize Automation, vRealize Orchestrator and vRealize Business VMs, verify the load balancing of the cluster.

The NSX Edge services gateway on which you perform the verification is determined by the type of maintenance operation and its location.

- If you perform an update, patch or restore of the Cloud Management Platform, you verify load balancing of the SFOMGMT-LB01 or LAXMGMT-LB01 NSX Edge Services Gateways respectively of the regions where operation occurred.
- If you perform a failover to Region B, you verify load balancing of the LAXMGMT-LB01 NSX Edge services gateway.
- If you perform a failback to Region A, you verify load balancing of the SFOMGMT-LB01 NSX Edge services gateway.

### Prerequisites

Connectivity status of the OneArmLB interface of the NSX Edge services gateway must be Connected.

### Procedure

- 1 Log in to the Management vCenter Server in Region A by using the vSphere Web Client.
  - a Open a Web browser and go to the following URL.

Region	Operation Type	Management vCenter Server URL
Region A	Update, patch, failback or restore	<a href="https://mgmt01vc01.sfo01.rainpole.local/vsphere-client">https://mgmt01vc01.sfo01.rainpole.local/vsphere-client</a>
Region B	Failover	<a href="https://mgmt01vc51.lax01.rainpole.local/vsphere-client">https://mgmt01vc51.lax01.rainpole.local/vsphere-client</a>

- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Verify the pool configuration by examining the pool statistics that reflect the status of the components behind the load balancer.
  - a From the **Home** menu, select **Networking & Security**.
  - b On the **NSX Home** page, click **NSX Edges** and select the IP address of the NSX Manager from the **NSX Manager** drop-down menu at the top of the NSX Edges page.

Operation Type	NSX Manager
Update, patch, failback or restore	172.16.11.65
Failover	172.17.11.65

- c On the **NSX Edges** page, double-click the NSX edge.

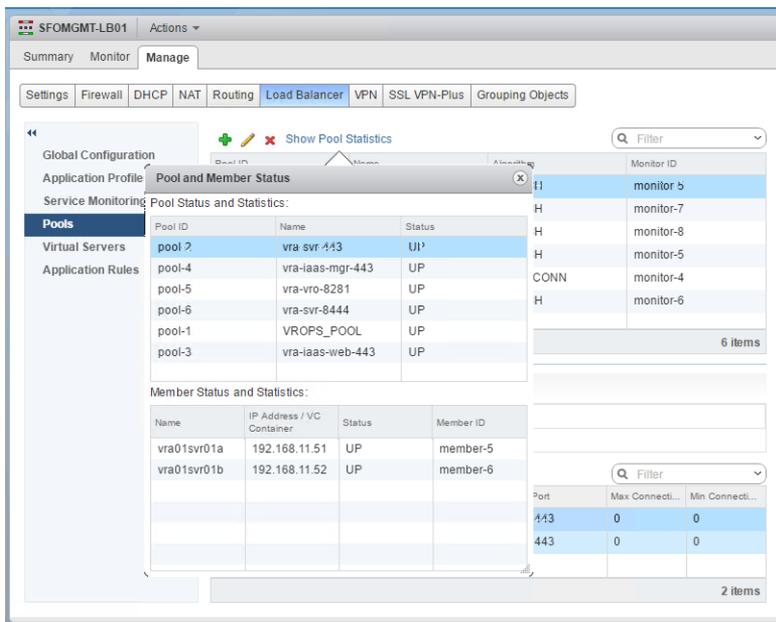
Operation Type	NSX Edge Services Gateway
Update, patch, failback or restore	SFOMGMT-LB01
Failover	LAXMGMT-LB01

- d On the **Manage** tab, click the **Load Balancer** tab.

- e Select **Pools** and click **Show Pool Statistics**.

- f In the **Pool and Member Status** dialog box, select the following vRealize Automation pools, and verify that the status of the pool is UP and the status of all members, except for vra01ims01b, is UP

Pool Name	Member Name	IP address	Status
vra-svr-443	vra01svr01a	192.168.11.51	UP
	vra01svr01b	192.168.11.52	UP
vra-iaas-web-443	vra01iws01a	192.168.11.54	UP
	vra01iws01b	192.168.11.55	UP
vra-iaas-mgr-443	vra01ims01a	192.168.11.57	UP
	vra01ims01b	192.168.11.58	DOWN
vra-vro-8281	vra01vro01a	192.168.11.63	UP
	vra01vro01b	192.168.11.64	UP
vra-svr-8444	vra01svr01a	192.168.11.51	UP
	vra01svr01b	192.168.11.52	UP



# Validate NSX for vSphere

After a maintenance like an update, upgrade, restore or recover, validate the NSX components and make sure they work as expected.

You validate the following NSX components:

- NSX Manager instances for the management cluster and for the shared edge and compute cluster
- NSX Controller nodes for the management cluster and for the shared edge and compute cluster
- NSX vSphere Installation Bundles (VIBs) installed on each host

## Procedure

### 1 [Verify the Version, Service Status and Configuration of the NSX Manager Appliances](#)

When you perform maintenance in your environment, verify that the deployed NSX Manager instances are operational.

### 2 [Verify the Status of NSX Controller Instances and Host Components](#)

After you perform a maintenance in your environment, verify that the deployed NSX Controller instances are operational.

### 3 [\(Optional\) Test VXLAN Connectivity of the Hosts in the Management Cluster](#)

Optionally, after you verify that the NSX components are operational, perform a ping test to check whether two hosts on the VXLAN transport network for the management cluster can reach each other.

### 4 [\(Optional\) Test VXLAN Connectivity of the Hosts in the Shared Edge and Compute Cluster](#)

Optionally, after you verify that the NSX components are operational, perform a ping test to check whether two hosts on the VXLAN transport network for the shared edge and compute cluster can reach each other.

### 5 [Verify the Status of NSX Firewall, Service Composer, and Distributed Switches](#)

After you perform software maintenance in your environment, verify that the NSX firewall, service composer, and distributed switches configurations are intact.

### 6 [Verify the Status of the NSX Edge Devices for North-South Routing](#)

After you perform software maintenance in your environment, verify that the configured NSX Edges are intact.

## 7 Verify the Status of the Universal Distributed Logical Router

After you perform software maintenance in your environment, verify that the configured NSX Edges are intact.

## 8 Verify the Status of the NSX Load Balancer

After you perform software maintenance in your environment, verify that the configured SFOMGMT-LB01 and LAXMGMT-LB01 load balancer NSX Edges are intact.

# Verify the Version, Service Status and Configuration of the NSX Manager Appliances

When you perform maintenance in your environment, verify that the deployed NSX Manager instances are operational.

After you patch, update or upgrade the NSX instances in the SDDC, or after you have restored the NSX appliances, verify the version, the service status and configuration of each NSX Manager appliance.

You verify that the host names and static IP addresses of the NSX Manager appliances remain properly configured after the maintenance.

**Table 3-1. FQDNs, IP Addresses, and Configuration of the NSX Manager Appliances**

Region	Cluster	FQDN	IP Address	Default Gateway	DNS Server and Search Domain
Region A	Management cluster	mgmt01nsxm01.sfo01.rainpole.local	172.16.11.65	172.16.11.1	172.16.11.5 sfo01.rainpole.local
	Shared edge and compute cluster	comp01nsxm01.sfo01.rainpole.local	172.16.11.66		
Region B	Management cluster	mgmt01nsxm51.lax01.rainpole.local	172.17.11.65	172.17.11.1	172.17.11.5 lax01.rainpole.local
	Shared edge and compute cluster	comp01nsxm51.lax01.rainpole.local	172.17.11.66		

You also verify that each NSX Manager instance synchronizes its time from the region-specific NTP server, sends its logs to the region-specific vRealize Log Insight instance, and is connected to the vCenter Server instance.

**Table 3-2. Time Synchronization and Syslog Settings of the NSX Manager Appliances**

Region	Cluster	NTP Server	Syslog Server
Region A	Management cluster	ntp.sfo01.rainpole.local	vrli-cluster-01.sfo01.rainpole.local
	Shared edge and compute cluster	ntp.lax01.rainpole.local	
Region B	Management cluster	ntp.lax01.rainpole.local	vrli-cluster-51.lax01.rainpole.local
	Shared edge and compute cluster	ntp.sfo01.rainpole.local	

**Table 3-3. vCenter Server Connection Settings of the NSX Manager Appliances**

Region	Cluster	vCenter Server FQDN	Lookup Service
Region A	Management cluster	mgmt01vc01.sfo01.rainpole.local	https://sfo01psc01.sfo01.rainpole.local: 443/lookupservice/sdk
	Shared edge and compute cluster	comp01vc01.sfo01.rainpole.local	
Region B	Management cluster	mgmt01vc51.lax01.rainpole.local	https://lax01psc51.lax01.rainpole.local: 443/lookupservice/sdk
	Shared edge and compute cluster	comp01vc51.lax01.rainpole.local	

**Procedure**

- 1 Log in to the Management NSX Manager appliance user interface.
  - a Open a Web browser and go to **https://mgmt01nsxm01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

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

- 2 In the NSX Manager appliance user interface, click **View Summary**.
- 3 If you have performed an update or upgrade, on the **Summary** tab, verify that the version of the NSX Manager is updated under NSX Manager Virtual Appliance.
- 4 Verify that the Status of the following services is Running.
  - vPostgres
  - RabbitMQ
  - NSX Universal Synchronization Service
  - NSX Management Service
  - SSH Service

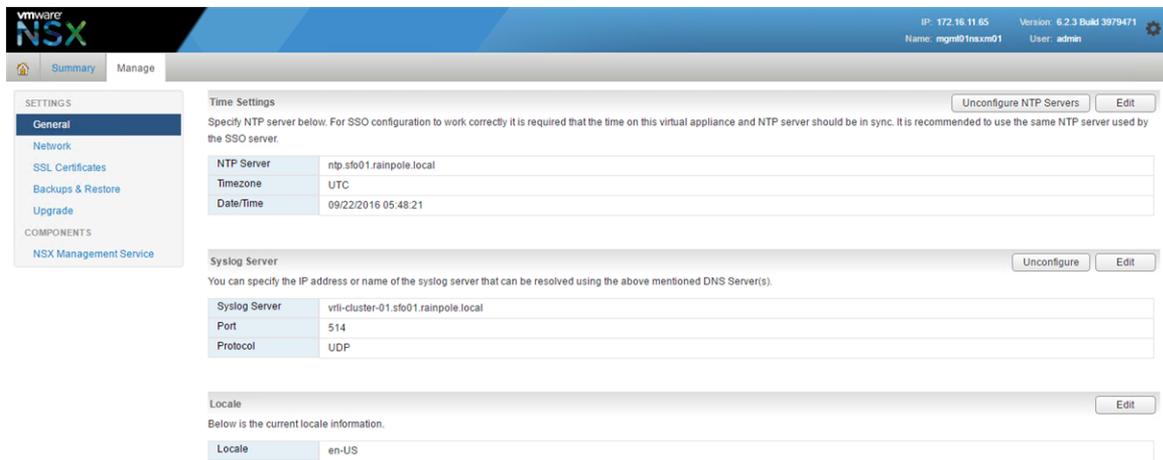
The screenshot displays the NSX Manager Summary page. At the top, it shows the IP address (172.16.11.65), version (6.2.3 Build 3979471), and user (admin). Below this, there are tabs for Summary and Manage. The main content area is divided into several sections:

- NSX Manager Virtual Appliance:** Displays DNS Name (mgmt01nsxm01.sfo01.rainpole.local), IP Address (172.16.11.65), Version (6.2.3 Build 3979471), Uptime (71 days, 11 hours, 24 minutes), and Current Time (Thursday, 22 September 2016 05:46:22 AM UTC).
- System-level components:** A table showing the status of vPostgres and RabbitMQ, both running.
- NSX Management Components:** A table showing the status of NSX Universal Synchronization Service and NSX Management Service, both running.
- Resource Usage:** Horizontal bar charts for CPU (Used: 276 MHz, Free: 2023 MHz, Capacity: 2299 MHz), MEMORY (Used: 9330 MB, Free: 6695 MB, Capacity: 16025 MB), and STORAGE (Used: 25G, Free: 61G, Capacity: 86G).

5 Verify the configuration of the NSX Manager virtual appliance.

- a In the NSX Manager appliance user interface, click the **Manage** tab.
- b Click **General** on the left side, and verify that the following settings have the value that is assigned during initial setup.

Setting Category	Setting	Expected Value
Time Settings	NTP Server	■ ntp.sfo01.rainpole.local
		■ ntp.lax01.rainpole.local
Syslog Server	Syslog Server	vrl-cluster-01.sfo01.rainpole.local
	Port	514
	Protocol	UDP



- c Click **Network** on the left side, and verify that the **General network settings** and **DNS Servers** are intact.

Setting Category	Setting	Expected Value
General network settings	Host name	mgmt01nsxm01
	Domain Name	sfo01.rainpole.local
	IPv4 Address	172.16.11.65
	IPv4 Netmask	255.255.255.0
	IPv4 Default Gateway	172.16.11.1
DNS Servers	Primary Server	172.16.11.5
	Search Domains	sfo01.rainpole.local

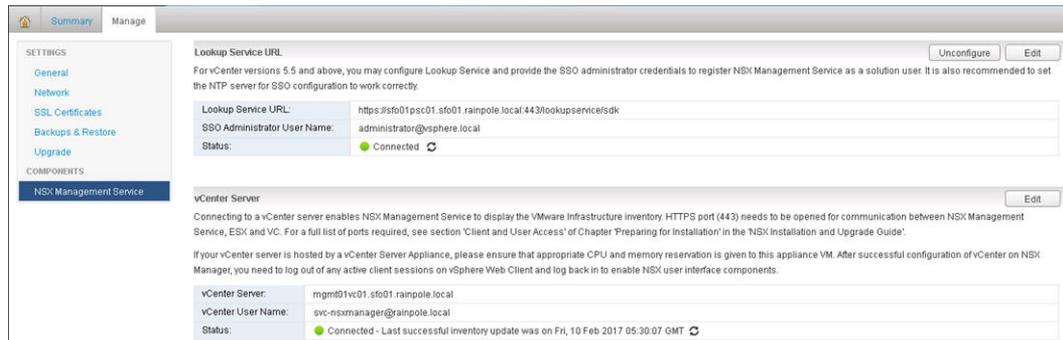
The screenshot shows the VMware NSX Management Service interface. The left sidebar has 'Network' selected under 'SETTINGS'. The main content area displays 'General network settings' and 'DNS Servers' sections. The 'General network settings' section includes fields for Host name, Domain Name, IPv4 Information (Address, Netmask, Default Gateway), and IPv6 Information. The 'DNS Servers' section includes fields for IPv4 DNS Servers (Primary Server, Secondary Server), IPv6 DNS Servers (Primary Server, Secondary Server), and Search Domains.

- d Click **SSL Certificates** on the left side, and verify that the attributes of the issuer certificate match the certificate of the Microsoft certificate authority in the domain.

The screenshot shows the VMware NSX Management Service interface. The left sidebar has 'SSL Certificates' selected under 'SETTINGS'. The main content area displays the 'SSL Certificates' section, which includes a list of certificates and a 'Generate CSR' button. The 'SSL Certificate Details' section is expanded, showing details for the selected certificate, including Issuer, Issued To, Valid from, Valid until, Certificate Type, Algorithm Type, Key Length, and Version.

- e Click **Backups & Restore** on the left side, and verify that the FTP Server Settings match the settings that are provided by your system administrator and that the Schedule is set to an hourly backup frequency.
- f Click **NSX Management Service** on the left side, and verify the Lookup Service and vCenter Server configurations.

Setting Category	Setting	Value
Lookup Service	Lookup Service	https://sfo01psc01.sfo01.rainpole.local:443/lookupservice/sdk
	SSO Administrator User Name	administrator@vsphere.local
	Status	Connected
vCenter Server	vCenter Server	mgmt01vc01.sfo01.rainpole.local
	vCenter User Name	svc-nsxmanager@rainpole.local
	Status	Connected



- 6 Repeat the steps for the remaining NSX Manager appliances.

## Verify the Status of NSX Controller Instances and Host Components

After you perform a maintenance in your environment, verify that the deployed NSX Controller instances are operational.

After you patch, update or upgrade, restore the NSX instances, or after failover or fallback during disaster recovery of the management applications, verify the following configuration:

- Software version and connectivity status of the NSX Controller instances
- Software version of vSphere Installation Bundles (VIBs) on the ESXi hosts

**Procedure**

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

a Open a Web browser and go to the following URL.

Region	Operation Type	Management vCenter Server URL
Region A	Failback, update, patch, or restore	<a href="https://mgmt01vc01.sfo01.rainpole.local/vsphere-client">https://mgmt01vc01.sfo01.rainpole.local/vsphere-client</a>
Region B	Failover, update, patch, or restore	<a href="https://mgmt01vc51.lax01.rainpole.local/vsphere-client">https://mgmt01vc51.lax01.rainpole.local/vsphere-client</a>

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 In the **Navigator** pane, click **Networking & Security** and click **Installation**.

### 3 Verify the connectivity status and the software version of the NSX Controller instances.

- a On the **Management** tab, under NSX Controller Nodes locate each NSX Controller instance.

Region	Operation Type	NSX Manager	NSX Controller Location	IP Addresses
Region A	Failback, update, patch, or restore	172.16.11.65	NSX Controller instances for the management cluster	<ul style="list-style-type: none"> <li>■ 172.16.11.118</li> <li>■ 172.16.11.119</li> <li>■ 172.16.11.120</li> </ul>
Region B	Failover, update, patch, or restore	172.17.11.65	NSX Controller instances for the management cluster	<ul style="list-style-type: none"> <li>■ 172.17.11.118</li> <li>■ 172.17.11.119</li> <li>■ 172.17.11.120</li> </ul>
Region A	Update, patch, or restore	172.16.11.66	NSX Controller instances for the shared edge and compute cluster	<ul style="list-style-type: none"> <li>■ 172.16.31.118</li> <li>■ 172.16.31.119</li> <li>■ 172.16.31.120</li> </ul>
Region B	Failover, update, patch, or restore	172.17.11.66	NSX Controller instances for the shared edge and compute cluster	<ul style="list-style-type: none"> <li>■ 172.17.31.118</li> <li>■ 172.17.31.119</li> <li>■ 172.17.31.120</li> </ul>

- b Verify the connectivity status and the version of each NSX Controller instance.

NSX Controller Option	Expected Value
Status	Connected
Peers	Green icons
Software Version	Updated to the version applied during maintenance

**Note** Each controller in the primary NSX Manager has an inherited controller instance in the secondary NSX Manager. Verify that the status of those instances is Connected.

- c Repeat the steps for the remaining NSX Controller instances.

The screenshot shows the NSX Management console interface. The 'Management' tab is active, displaying 'NSX Managers' and 'NSX Controller nodes' sections.

**NSX Managers Table:**

NSX Manager	Role	IP Address	vCenter	Version
172.16.11.66	Primary	172.16.11.66	comp01vc01.sio01.rainpole.local	6.2.4.4292b76
172.16.11.65	Primary	172.16.11.65	mgmt01vc01.sto01.rainpole.local	6.2.4.4292526
172.17.11.65	Secondary	172.17.11.65	mgmt01vc51.lax01.rainpole.local	6.2.4.4292526
172.17.11.66	Secondary	172.17.11.66	comp01vc51.lax01.rainpole.local	6.2.4.4292526

**NSX Controller nodes Table:**

Name	Controller Node	NSX Manager	Managed By	Status	Peers	Software Version
nsx-controller-mgmt-03	172.16.11.120 controller-14	172.16.11.65	172.16.11.65	Connected	Green icons	6.2.47844
nsx-controller-mgmt-02	172.16.11.119 controller-13	172.16.11.65	172.16.11.65	Connected	Green icons	6.2.47844
nsx-controller-mgmt-01	172.16.11.118 controller-12	172.16.11.65	172.16.11.65	Connected	Green icons	6.2.47844
comp-NSX-A-01	172.16.21.118 controller-27	172.16.11.66	172.16.11.66	Connected	Green icons	6.2.47844

- 4 Verify the status of the NSX VIBs on the management and shared edge and compute clusters.
  - a On the **Installation** page, click the **Host Preparation** tab.
  - b From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager.
  - c Expand the **SFO01-Mgmt01** cluster and verify that the following settings are configured.

**Table 3-4.**

Object	Setting	Expected Value
SFO01-Mgmt01 cluster	VXLAN	Configured
Hosts in the cluster	Installation Status	Updated to the version applied during maintenance
	Firewall	Enabled

Clusters & Hosts	Installation Status	Firewall	VXLAN
SI:O01 Mgmt01	✓ 6.2.4.4292526	✓ Enabled	✓ Configured
mgmt01esx01.sfo01.rainpole.local	✓ 6.2.4.4292526	✓ Enabled	
mgmt01esx03.sfo01.rainpole.local	✓ 6.2.4.4292526	✓ Enabled	
mgmt01esx04.sfo01.rainpole.local	✓ 6.2.4.4292526	✓ Enabled	
mgmt01esx02.sfo01.rainpole.local	✓ 6.2.4.4292526	✓ Enabled	

- d Repeat the steps for the remaining NSX Manager instances.

Region	NSX Manager	NSX Manager IP Address	Hosts Cluster Name
Region A	NSX Manager for the shared edge and compute cluster	172.16.11.66	SFO01-Comp01
Region B	NSX Controller instances for the management cluster	172.17.11.65	LAX01-Mgmt01
Region B	NSX Manager for the shared edge and compute cluster	172.17.11.66	LAX01-Comp01

- 5 (Optional) Confirm that the NSX VIBs on the hosts are updated.
  - a Open an SSH connection to a host in each cluster with user name **root** and password **esxi\_root\_user\_password**.

Cluster	Host
SFO01-Mgmt01	mgmt01esx01.sfo01.rainpole.local
SFO01-Comp01	comp01esx01.sfo01.rainpole.local
LAX01-Mgmt01	mgmt01esx51.lax01.rainpole.local
LAX01-Comp01	comp01esx51.sfo01.rainpole.local

- b Run the following console command.

```
esxcli software vib list | grep esx
```

- c Make sure that the following VIBs have been updated to the expected version.
  - `esx-vsip`
  - `esx-vxlan`
- d Verify that the User World Agent (UWA) in the ESXi host is running.

```
/etc/init.d/netcpad status
```

- e Repeat the steps for a host in each of the other clusters in the SDDC.

## (Optional) Test VXLAN Connectivity of the Hosts in the Management Cluster

Optionally, after you verify that the NSX components are operational, perform a ping test to check whether two hosts on the VXLAN transport network for the management cluster can reach each other.

You create a logical switch on the VXLAN network in Region A and use that switch for the ping between the hosts in both regions.

**Table 3-5. Test Parameters for VXLAN Host Connectivity**

NSX Manager	IP Address	Source Host	Destination Host
NSX Manager for the management cluster in Region A	172.16.11.65	mgmt01esx04.sfo01.rainpole.local	mgmt01esx01.sfo01.rainpole.local
NSX Manager for the management cluster in Region B	172.17.11.65	mgmt01esx54.lax01.rainpole.local	mgmt01esx51.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://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 Create a logical switch to test the logical network.
  - a In the **Navigator** pane, click **Networking & Security** and click **Logical Switches**.
  - b On the **Logical Switches** page, select **172.16.11.65** from the **NSX Manager** drop-down menu.

- c Click the **New Logical Switch** icon.
- d In the **New Logical Switch** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	mgmt01-logical-switch
Transport Zone	Mgmt Transport Zone
Replication mode	Hybrid
Enable IP Discovery	Selected
Enable MAC Learning	Deselected

**New Logical Switch**

Name: \* mgmt01-logical-switch

Description:

Transport Zone: \* Mgmt Transport Zone Change Remove

Replication mode:

Multicast  
*Multicast on Physical network used for VXLAN control plane.*

Unicast  
*VXLAN control plane handled by NSX Controller Cluster.*

Hybrid  
*Optimized Unicast mode. Offloads local traffic replication to physical network.*

Enable IP Discovery

Enable MAC Learning

OK Cancel

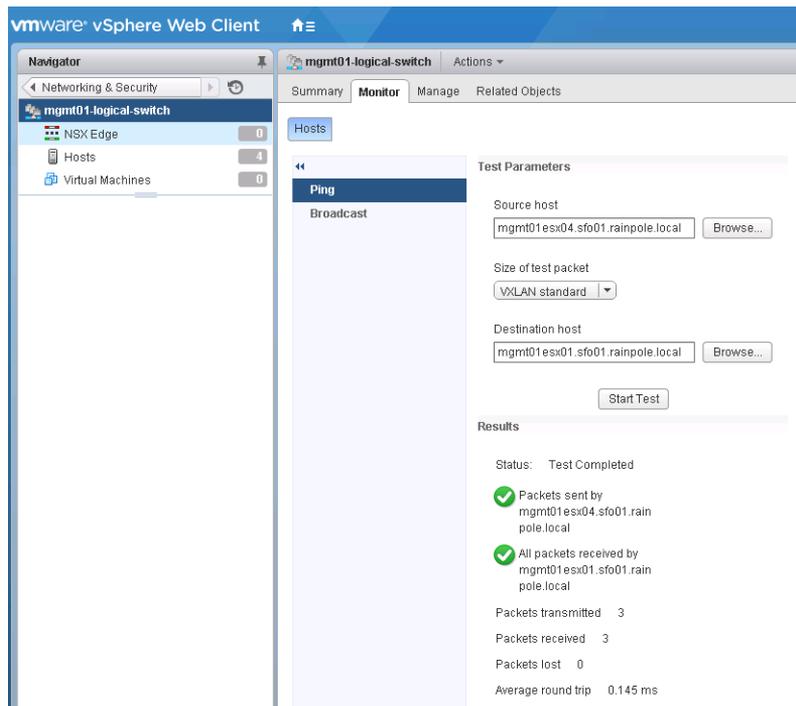
- 3 Use the ping monitor to test connectivity in Region A.
  - a On the **Logical Switches** page, double-click **mgmt01-logical-switch**.
  - b On the **mgmt01-logical-switch** page, click the **Monitor** tab and click **Ping**.

- c Under **Test Parameters**, enter the parameters for the ping and click **Start Test**.

You use VXLAN standard packet size that is 1550 bytes without fragmentation. In this case, NSX checks connectivity and verifies that the infrastructure is prepared for VXLAN traffic.

Ping Test Parameter	Value
Source host	mgmt01esx04.sfo01.rainpole.local
Destination host	mgmt01esx01.sfo01.rainpole.local
Size of test packet	VXLAN standard

- d After the ping is complete, verify that the **Results** pane displays no error messages.



#### 4 Test the connectivity in Region B.

- a In the **Navigator** pane, click **Networking & Security** and click **Logical Switches**.
- b On the **Logical Switches** page, select **172.17.11.65** from the **NSX Manager** drop-down menu.
- c Double-click **mgmt01-logical-switch**, click the **Monitor** tab and click **Ping**.
- d Under **Test Parameters**, enter the parameters for the ping and click **Start Test**.

Ping Test Parameter	Value
Source host	mgmt01esx54.lax01.rainpole.local
Destination host	mgmt01esx51.lax01.rainpole.local
Size of test packet	VXLAN standard

- e After the ping is complete, verify that the **Results** pane displays no error messages.

## (Optional) Test VXLAN Connectivity of the Hosts in the Shared Edge and Compute Cluster

Optionally, after you verify that the NSX components are operational, perform a ping test to check whether two hosts on the VXLAN transport network for the shared edge and compute cluster can reach each other.

You create a logical switch on the VXLAN network in Region A and use that switch for the ping between the hosts in both regions.

**Table 3-6. Test Parameters for VXLAN Host Connectivity**

NSX Manager	IP Address	Source Host	Destination Host
NSX Manager for the shared edge and compute cluster in Region A	172.16.11.66	comp01esx04.sfo01.rainpole.local	comp01esx01.sfo01.rainpole.local
NSX Manager for the shared edge and compute cluster in Region B	172.17.11.66	comp01esx52.lax01.rainpole.local	comp01esx51.lax01.rainpole.local

### Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://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 Create a logical switch to test the logical network.
  - a In the **Navigator** pane, click **Networking & Security** and click **Logical Switches**.
  - b On the **Logical Switches** page, select **172.16.11.66** from the **NSX Manager** drop-down menu.

- c Click the **New Logical Switch** icon.
- d In the **New Logical Switch** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	comp01-logical-switch
Transport Zone	Comp Transport Zone
Replication mode	Hybrid
Enable IP Discovery	Selected
Enable MAC Learning	Deselected

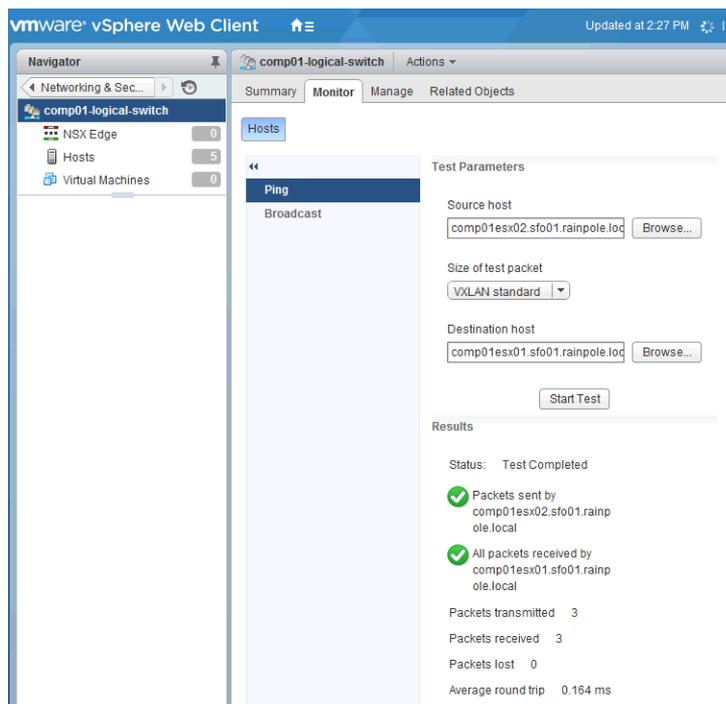
- 3 Use the ping monitor to test connectivity.
  - a On the **Logical Switches** page, double-click **comp01-logical-switch**.
  - b On the **comp01-logical-switch** page, click the **Monitor** tab and click **Ping**.

- c Under Test Parameters, enter the parameters for the ping and click **Start Test**.

You use VXLAN standard packet size that is 1550 bytes without fragmentation. In this case, NSX checks connectivity and verifies that the infrastructure is prepared for VXLAN traffic.

Ping Test Parameter	Value
Source host	comp01esx04.sfo01.rainpole.local
Destination host	comp01esx01.sfo01.rainpole.local
Size of test packet	VXLAN standard

- d After the ping is complete, verify that the **Results** pane displays no error messages.



#### 4 Test the connectivity in Region B.

- In the **Navigator** pane, click **Networking & Security** and click **Logical Switches**.
- On the **Logical Switches** page, select **172.17.11.66** from the **NSX Manager** drop-down menu.
- Double-click **comp01-logical-switch**, click the **Monitor** tab, and click **Ping**.
- Under **Test Parameters**, enter the parameters for the ping and click **Start Test**.

Ping Test Parameter	Value
Source host	comp01esx52.lax01.rainpole.local
Destination host	comp01esx51.lax01.rainpole.local
Size of test packet	VXLAN standard

- After the ping is complete, verify that the **Results** pane displays no error messages.

## Verify the Status of NSX Firewall, Service Composer, and Distributed Switches

After you perform software maintenance in your environment, verify that the NSX firewall, service composer, and distributed switches configurations are intact.

After you patch, update or upgrade the NSX instances, or after you have restored the NSX appliances, verify the NSX firewall, service composer, and distributed switches configuration of each NSX Manager appliance.

**Table 3-7. NSX Manager Instances**

Region	NSX Manager Instance	IP Address
Region A	NSX Manager for the management cluster	172.16.11.65
	NSX Manager for the shared edge and compute cluster	172.16.11.66
Region B	NSX Manager for the management cluster	172.17.11.65
	NSX Manager for the shared edge and compute cluster	172.17.11.66

### 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 Verify the status of the NSX firewall.
  - a In the **Navigator** pane, click **Networking & Security**.
  - b Under **Networking & Security**, click **Firewall**.
  - c Select **172.16.11.65** from the **NSX Manager** drop-down menu.
  - d Verify that the Firewall configurations are intact.
  - e Repeat the step for the remaining NSX Manager instances.
- 3 Verify the status of the service composer.
  - a In the **Navigator** pane, click **Networking & Security**.
  - b Under **Networking & Security**, click **Service Composer**.
  - c Select **172.16.11.65** from the **NSX Manager** drop-down menu.

- d Verify that the Security Groups, Security Policies and Canvas settings are intact.
  - e Repeat the step for the remaining NSX Manager instances.
- 4 Verify the status of the distributed switches and configured port groups for both regions.
- a In the **Navigator** pane, click **Home** and click **Networking**.
  - b Verify that the following distributed switches and port groups are present.

vCenter Server	Distributed Switch	Port Group
mgmt01vc01.sfo01.rainpole.local	vDS-Mgmt	<ul style="list-style-type: none"> <li>■ vDS-Mgmt-Management</li> <li>■ vDS-Mgmt-vMotion</li> <li>■ vDS-Mgmt-VSAN</li> <li>■ vDS-Mgmt-NFS</li> <li>■ vDS-Mgmt-VR</li> <li>■ vDS-Mgmt-Uplink01</li> <li>■ vDS-Mgmt-Uplink02</li> <li>■ vDS-Mgmt-Ext-Management</li> </ul>
comp01vc01.sfo01.rainpole.local	vDS-Comp	<ul style="list-style-type: none"> <li>■ vDS-Comp-Management</li> <li>■ vDS-Comp-vMotion</li> <li>■ vDS-Comp-NFS</li> </ul>
mgmt01vc51.lax01.rainpole.local	vDS-Mgmt	<ul style="list-style-type: none"> <li>vDS-Mgmt-Management</li> <li>vDS-Mgmt-vMotion</li> <li>vDS-Mgmt-VSAN</li> <li>vDS-Mgmt-NFS</li> <li>vDS-Mgmt-VR</li> <li>vDS-Mgmt-Uplink01</li> <li>vDS-Mgmt-Uplink02</li> <li>vDS-Mgmt-Ext-Management</li> </ul>
comp01vc51.lax01.rainpole.local	vDS-Comp	<ul style="list-style-type: none"> <li>vDS-Comp-Management</li> <li>vDS-Comp-vMotion</li> <li>vDS-Comp-NFS</li> </ul>

- c Right-click the **vDS-Mgmt** distributed switch and select **Settings > Edit Settings**.

- d Verify the following values under the **General** and **Advanced** sections.

Setting	Value
Number of uplinks	2
Network I/O Control	Enabled
MTU	9000

- e Under the vDS-Mgmt distributed switch, right-click a port group and click **Edit settings** to verify the following values under **General** and VLAN sections.

■ Region A Configuration

Distributed Switch	Port Group Name	Port Binding	VLAN Type	VLAN ID
vDS-Mgmt	vDS-Mgmt-Management	Ephemeral binding	VLAN	1611
	vDS-Mgmt-vMotion	Static binding	VLAN	1612
	vDS-Mgmt-VSAN	Static binding	VLAN	1613
	vDS-Mgmt-NFS	Static binding	VLAN	1615
	vDS-Mgmt-VR	Static binding	VLAN	1616
	vDS-Mgmt-Uplink01	Static binding	VLAN	2711
	vDS-Mgmt-Uplink02	Static binding	VLAN	2712
	vDS-Mgmt-Ext-Management	Static binding	VLAN	130
vDS-Comp	vDS-Comp-Management	Static binding	VLAN	1621
	vDS-Comp-vMotion	Static binding	VLAN	1622
	vDS-Comp-NFS	Static binding	VLAN	1625

■ Region B Configuration

Distributed Switch	Port Group Name	Port Binding	VLAN Type	VLAN ID
vDS-Mgmt	vDS-Mgmt-Management	Ephemeral binding	VLAN	1711
	vDS-Mgmt-vMotion	Static binding	VLAN	1712
	vDS-Mgmt-VSAN	Static binding	VLAN	1713
	vDS-Mgmt-NFS	Static binding	VLAN	1715
	vDS-Mgmt-VR	Static binding	VLAN	1716
	vDS-Mgmt-Uplink01	Static binding	VLAN	2714
	vDS-Mgmt-Uplink02	Static binding	VLAN	2715
	vDS-Mgmt-Ext-Management	Static binding	VLAN	150

Distributed Switch	Port Group Name	Port Binding	VLAN Type	VLAN ID
vDS-Comp	vDS-Comp-Management	Static binding	VLAN	1731
	vDS-Comp-vMotion	Static binding	VLAN	1732
	vDS-Comp-NFS	Static binding	VLAN	1734

## Verify the Status of the NSX Edge Devices for North-South Routing

After you perform software maintenance in your environment, verify that the configured NSX Edges are intact.

After you patch, update or upgrade the NSX instances in the SDDC, or after you have restored the NSX instances, verify the configuration of each NSX edge appliances are intact.

**Table 3-8. IP Addresses and NSX edges of the NSX Manager Appliances**

Region	NSX Manager Instance	IP Address	NSX Edge Name
Region A	NSX Manager for the management cluster	172.16.11.65	SFOMGMT-ESG01
			SFOMGMT-ESG02
	NSX Manager for the shared edge and compute cluster	172.16.11.66	SFOCOMP-ESG01
			SFOCOMP-ESG02
Region B	NSX Manager for the management cluster	172.17.11.65	LAXMGMT-ESG01
			LAXMGMT-ESG02
	NSX Manager for the shared edge and compute cluster	172.17.11.66	LAXCOMP-ESG01
			LAXCOMP-ESG02

### 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 Verify that the edge interface settings are intact.
  - a In the **Navigator** pane, click **Networking & Security**, and click **NSX Edges**.
  - b Select **172.16.11.65** from the **NSX Manager** drop-down menu.
  - c Double-click the **SFOMGMT-ESG01** NSX Edge device.

- d Click the **Manage** tab, click **Settings**, and select **Interfaces**.
- e Select the **Uplink01** interface and click the **Edit** icon.
- f Verify that the following interface settings are intact.

- **Region A Configuration**

Setting	SFOMGMT-ESG01	SFOMGMT-ESG02	SFOCOMP-ESG01	SFOCOMP-ESG02
Name	Uplink01	Uplink01	Uplink01	Uplink01
Type	Uplink	Uplink	Uplink	Uplink
Connected To	vDS-Mgmt-Uplink01	vDS-Mgmt-Uplink01	vDS-Comp-Uplink01	vDS-Comp-Uplink01
Connectivity Status	Connected	Connected	Connected	Connected
Primary IP Address	172.27.11.2	172.27.11.3	172.16.35.2	172.16.35.3
Subnet Prefix Length	24	24	24	24
MTU	9000	9000	9000	9000
Send ICMP Redirect	Selected	Selected	Selected	Selected

- **Region B Configuration**

Setting	LAXMGMT-ESG01	LAXMGMT-ESG02	LAXCOMP-ESG01	LAXCOMP-ESG02
Name	Uplink01	Uplink01	Uplink01	Uplink01
Type	Uplink	Uplink	Uplink	Uplink
Connected To	vDS-Mgmt-Uplink01	vDS-Mgmt-Uplink01	vDS-Comp-Uplink01	vDS-Comp-Uplink01
Connectivity Status	Connected	Connected	Connected	Connected
Primary IP Address	172.27.14.2	172.27.14.3	172.17.35.2	172.17.35.3
Subnet Prefix Length	24	24	24	24
MTU	9000	9000	9000	9000
Send ICMP Redirect	Selected	Selected	Selected	Selected

- g Select the **Uplink02** interface and click the **Edit** icon.

## h Verify that the following interface settings are intact.

## ■ Region A Configuration

Setting	SFOMGMT-ESG01	SFOMGMT-ESG02	SFOCOMP-ESG01	SFOCOMP-ESG02
Name	Uplink02	Uplink02	Uplink02	Uplink02
Type	Uplink	Uplink	Uplink	Uplink
Connected To	vDS-Mgmt-Uplink02	vDS-Mgmt-Uplink02	vDS-Comp-Uplink02	vDS-Comp-Uplink02
Connectivity Status	Connected	Connected	Connected	Connected
Primary IP Address	172.27.12.3	172.27.12.2	172.27.13.3	172.27.13.2
Subnet Prefix Length	24	24	24	24
MTU	9000	9000	9000	9000
Send ICMP Redirect	Selected	Selected	Selected	Selected

## ■ Region B Configuration

Setting	LAXMGMT-ESG01	LAXMGMT-ESG02	LAXCOMP-ESG01	LAXCOMP-ESG02
Name	Uplink02	Uplink02	Uplink02	Uplink02
Type	Uplink	Uplink	Uplink	Uplink
Connected To	vDS-Mgmt-Uplink02	vDS-Mgmt-Uplink02	vDS-Comp-Uplink02	vDS-Comp-Uplink02
Connectivity Status	Connected	Connected	Connected	Connected
Primary IP Address	172.27.15.3	172.27.15.2	172.27.21.3	172.27.21.2
Subnet Prefix Length	24	24	24	24
MTU	9000	9000	9000	9000
Send ICMP Redirect	Selected	Selected	Selected	Selected

- i Select the **UDLR** interface and click the **Edit** icon.
- j Verify that the following interface settings are intact.

- **Region A Configuration**

Setting	SFOMGMT-ESG01	SFOMGMT-ESG02	SFOCOMP-ESG01	SFOCOMP-ESG02
Name	UDLR	UDLR	UDLR	UDLR
Type	Internal	Internal	Internal	Internal
Connected To	Universal Transit Network	Universal Transit Network	Universal Transit Network	Universal Transit Network
Connectivity Status	Connected	Connected	Connected	Connected
Primary IP Address	192.168.10.1	192.168.10.2	192.168.100.1	192.168.100.2
Subnet Prefix Length	24	24	24	24
MTU	9000	9000	9000	9000
Send ICMP Redirect	Selected	Selected	Selected	Selected

- **Region B Configuration**

Setting	LAXMGMT-ESG02	LAXMGMT-ESG02	LAXCOMP-ESG02	LAXCOMP-ESG02
Name	UDLR	UDLR	UDLR	UDLR
Type	Internal	Internal	Internal	Internal
Connected To	Universal Transit Network	Universal Transit Network	Universal Transit Network	Universal Transit Network
Connectivity Status	Connected	Connected	Connected	Connected
Primary IP Address	192.168.10.51	192.168.10.52	192.168.100.51	192.168.100.52
Subnet Prefix Length	24	24	24	24
MTU	9000	9000	9000	9000
Send ICMP Redirect	Selected	Selected	Selected	Selected

- 3 Verify the firewall settings of the edges.
  - a Click the **Manage** tab and click **Firewall**.
  - b Verify that the **Firewall** is disabled.
- 4 Verify the Routing settings of the edges.
  - a Click the **Manage** tab, click **Routing** and click **Global Configuration**.
  - b Verify that the following Global Configuration settings are intact.

Setting	Value
ECMP	Enabled
Router ID	Uplink01

- c On the **Routing** tab, click **BGP**.

- d Verify that the following BGP Configuration settings are intact.

Setting	SFOMGMT-ESG01 and SFOMGMT- ESG02	SFOCOMP-ESG01 and SFOCOMP- ESG02	LAXMGMT-ESG01 and LAXMGMT- ESG02	LAXCOMP-ESG01 and LAXCOMP- ESG02
Status	Enabled	Enabled	Enabled	Enabled
Local AS	65003	65000	65003	65000
Graceful Restart	Enabled	Enabled	Enabled	Enabled

- e Verify that the following Neighbors settings are intact.

NSX Edge Device	Setting	First Top of Rack Switch Value	Second Top of RackSwitch Value	UDLR Value
SFOMGMT-ESG01 SFOMGMT- ESG02	IP Address	172.27.11.1	172.27.12.1	192.168.10.4
	Remote AS	65001	65001	65003
	Weight	60	60	60
	Keep Alive Time	4	4	1
	Hold Down Time	12	12	3
SFOCOMP-ESG01SFOCOMP- ESG02	IP Address	172.16.35.1	172.27.13.1	192.168.100.4
	Remote AS	65001	65001	65000
	Weight	60	60	60
	Keep Alive Time	4	4	1
	Hold Down Time	12	12	3
LAXMGMT-ESG01LAXMGMT-ESG02	IP Address	172.27.14.1	172.27.15.1	192.168.10.4
	Remote AS	65002	65002	65003
	Weight	60	60	60
	Keep Alive Time	4	4	1
	Hold Down Time	12	12	3
LAXCOMP-ESG01LAXCOMP-ESG02	IP Address	172.17.35.1	172.27.21.1	192.168.100.4
	Remote AS	65002	65002	65000
	Weight	60	60	60
	Keep Alive Time	4	4	1
	Hold Down Time	12	12	3

- f On the **Routing** tab, click **Route Redistribution**.

- g Verify that the following Route Redistribution Status settings are intact.

Setting	Value
OSPF	Deselected
BGP	Selected

- h Verify that the following Route Redistribution table settings are intact.

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

- 5 Repeat this verification procedure for the remaining NSX Edge devices.

#### What to do next

Verify that the NSX Edge devices are successfully peering, and that BGP routing has been established by following the instructions in *Verify Peering of Upstream Switches and Establishment of BGP in Region A* from *VMware Validated Design Deployment Guide for Region A*. Perform verification for the following pairs of NSX Edge devices.

- 1 SFOMGMT-ESG01 and SFOMGMT-ESG02
- 2 SFOCOMP-ESG01 and SFOCOMP-ESG02
- 3 LAXMGMT-ESG01 and LAXMGMT-ESG02
- 4 LAXCOMP-ESG01 and LAXCOMP-ESG02

## Verify the Status of the Universal Distributed Logical Router

After you perform software maintenance in your environment, verify that the configured NSX Edges are intact.

After you patch, update or upgrade the NSX instances in the SDDC, or after you have restored the NSX instances, verify that the Universal Distributed Logical Router (UDLR) configurations are intact.

**Table 3-9. IP Addresses and UDLR of the NSX Manager Appliances**

NSX Manager Instance	IP Address	UDLR Device	Device Name
NSX Manager for the management cluster	172.16.11.65	UDLR01 (Management cluster)	UDLR01
NSX Manager for the shared edge and compute cluster	172.16.11.66	UDLR01 (Shared edge and compute cluster)	UDLR01

## 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 Verify that the UDLR interface settings are intact.
  - a In the **Navigator** pane, click **Networking & Security**, and click **NSX Edges**.
  - b Select **172.16.11.65** from the **NSX Manager** drop-down menu.
  - c Double-click the **UDLR01** NSX Edge device.
  - d Click the **Manage** tab, click **Settings**, and select **Interfaces**.
  - e Select the **Uplink** interface and click the **Edit** icon.
  - f Verify that the following interface settings are intact.

Setting	Value for Management UDLR	Value for Shared Edge and Compute UDLR
Name	Uplink	Uplink
Type	Uplink	Uplink
Connected To	Universal Transit Network	Universal Transit Network
Connectivity Status	Connected	Connected
Primary IP Address	192.168.10.3	192.168.100.3
Subnet Prefix Length	24	24
MTU	9000	9000

- g Select the **Mgmt-xRegion01** interface and click the **Edit** icon.
- h Verify that the following interface settings are intact.

Setting	Value for Management UDLR
Name	Mgmt-xRegion01
Type	Internal
Connected To	Mgmt-xRegion01-VXLAN
Connectivity Status	Connected
Primary IP Address	192.168.11.1
Subnet Prefix Length	24
MTU	9000

- i Select the **Mgmt-RegionA01** interface and click the **Edit** icon.
- j Verify that the following interface settings are intact.

Setting	Value for Management UDLR
Name	Mgmt-RegionA01
Type	Internal
Connected To	Mgmt-RegionA01-VXLAN
Connectivity Status	Connected
Primary IP Address	192.168.31.1
Subnet Prefix Length	24
MTU	9000

### 3 Verify the Routing settings of the UDLR.

- a Click the **Manage** tab, click **Routing** and click **Global Configuration**.
- b Verify that the following Global Configuration settings are intact.

Setting	Value
ECMP	Enabled
Router ID	Uplink

- c On the **Routing** tab, click **BGP**.
- d Verify that the following BGP Configuration settings are intact.

Setting	Value for Management UDLR	Value for Shared Edge and Compute UDLR
Status	Enabled	Enabled
Local AS	65003	65000
Graceful Restart	Enabled	Enabled

- e Verify that the following Neighbors settings are intact.

Setting	Value for Management UDLR01		Value for Shared Edge and Compute UDLR01	
	SFOMGMT-ESG01	SFOMGMT-ESG02	SFOCOMP-ESG01	SFOCOMP-ESG02
Forwarding Address	192.168.10.3	192.168.10.3	192.168.100.3	192.168.100.3
Protocol Address	192.168.10.4	192.168.10.4	192.168.100.4	192.168.100.4
IP Address	192.168.10.1	192.168.10.2	192.168.100.1	192.168.100.2
Remote AS	65003	65003	65000	65000
Weight	60	60	60	60
Keep Alive Time	1	1	1	1
Hold Down Time	3	3	3	3

- f On the **Routing** tab, click **Route Redistribution**.

- g Verify that the following Route Redistribution Status settings are intact.

Setting	Value
OSPF	Deselected
BGP	Selected

- h Verify that the following Route Redistribution table settings are intact.

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

- 4 Verify that the UDLR is successfully peering, and that BGP routing has been established by following the instructions in *Verify Establishment of BGP for the Universal Distributed Logical Router in Region A* from *VMware Validated Design Deployment Guide for Region A*.
- 5 Repeat this verification procedure for UDLR01 in the shared edge and compute clusters in the SDDC and verify that the UDLR is successfully peering, and that BGP routing has been established by following the instructions in *Verify Establishment of BGP for the Universal Distributed Logical Router in the Shared Edge and Compute Cluster in Region A* from *VMware Validated Design Deployment Guide for Region A*.
- 6 Repeat the steps for the remaining NSX Manager appliances.

## Verify the Status of the NSX Load Balancer

After you perform software maintenance in your environment, verify that the configured SFOMGMT-LB01 and LAXMGMT-LB01 load balancer NSX Edges are intact.

The configuration of the two NSX edges is almost identical. The only difference is that the OneArmLB interface of the LAXMGMT-LB01 NSX Edge must be in the disconnected state.

**Table 3-10. NSX Manager Instances and Load Balancer NSX Edges**

Region	NSX Manager Instance	IP Address	Load Balancer
Region A	NSX Manager for the management cluster	172.16.11.65	SFOMGMT-LB01
Region B	NSX Manager for the management cluster	172.17.11.65	LAXMGMT-LB01

## 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 Verify that the settings for the interface of the SFOMGMT-LB01 load balancer are intact.
  - a In the **Navigator**, click **Networking & Security** and click **NSX Edges**.
  - b Select **172.16.11.65** from the **NSX Manager** drop-down menu.
  - c Double-click the **SFOMGMT-LB01** NSX Edge device.
  - d Click the **Manage** tab, click **Settings**, and select **Interfaces**.
  - e Select the **OneArmLB** interface and click the **Edit** icon.
  - f Verify that the following interface settings are intact.

Setting	SFOMGMT-LB01
Name	OneArmLB
Type	Internal
Connected To	Mgmt-xRegion01-VXLAN
Connectivity Status	Connected
Primary IP Address	192.168.11.2
Secondary IP Address	192.168.11.35,192.168.11.59,192.168.11.56,192.168.11.65,192.168.11.53
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- 3 Verify that the SFOMGMT-LB01 load balancer settings are intact.
  - a Click the **Manage** tab, click **Load Balancer**, and select **Global Configuration**.
  - b Verify that Load Balancer Status is Enabled.
  - c Select **Application Profiles**.

- d Select an application profile and click **Edit** for all configured entries to verify that the following settings are intact.

Setting	vRealize-https	VROPS_HTTPS	VROPS_REDIRECT
Type	HTTPS	HTTPS	HTTP
Enable SSL Passthrough	Selected	Selected	N/A
HTTP Redirect URL	N/A	N/A	https://vrops-cluster-01.rainpole.local/vcops-web-ent/login.action
Persistence	Source IP	Source IP	Source IP
Expires in (Seconds)	120	1800	1800
Client Authentication	Ignore	Ignore	N/A

- e Select **Service Monitoring**.

- f Select a Service Monitor and click **Edit** for all configured entries to verify that the following settings are intact.

The following settings are same for all Service Monitors:

- Interval = 3
- Method = GET
- Type = HTTPS

Service Monitor Name	Timeout	Max Retries	Expected	URL	Receive
vra-iaas-mgr-443-monitor	9	3		/VMPSProvision	ProvisionService
vra-iaas-web-443-monitor	9	3		/wapi/api/status/web	REGISTERED
vra-svr-443-monitor	9	3		/vcac/services/api/health	
vra-vro-8281-monitor	9	3	204	/vco/api/healthstatus	RUNNING
VROPS_MONITOR	5	2		/suite-api/api/deployment/node/status	ONLINE

- g Select **Pools** and click **Show Pool Statistics** and verify that the Status of each pool is UP.

- h Select a pool and click **Edit** for all configured entries to verify that the following settings are intact.

The following settings are same for all pools:

- Enable member = Yes
- Weight = 1

Pool Name	Algorithm	Monitors	Members			
			Member Name	IP address	Port	Monitor Port
vra-svr-443	IP-HASH	vra-svr-443-monitor	vra01svr01a	192.168.11.51	443	443
			vra01svr01b	192.168.11.52		
vra-iaas-web-443	IP-HASH	vra-iaas-web-443-monitor	vra01iws01a	192.168.11.54	443	443
			vra01iws01b	192.168.11.55		
vra-iaas-mgr-443	IP-HASH	vra-iaas-mgr-443-monitor	vra01ims01a	192.168.11.57	443	443
			vra01ims01b	192.168.11.58		
vra-vro-8281	IP-HASH	vra-vro-8281-monitor	vra01vro01a	192.168.11.63	8281	8281
			vra01vro01b	192.168.11.64		
vra-svr-8444	IP-HASH	vra-svr-443-monitor	vra01svr01a	192.168.11.51	8444	443
			vra01svr01b	192.168.11.52		
VROPS_POOL	LEASTCONN	VROPS_MONITOR	vrops-mstrn-01	192.168.11.31	443	443
			vrops-repln-02	192.168.11.32		
			vrops-datan-03	192.168.11.33		
			vrops-datan-04	192.168.11.34		

- i Select **Virtual Servers**.
- j Select a virtual server and click **Edit** for all configured entries to verify that the following settings are intact.

Virtual Server Name	Application Profile	IP Address	Protocol	Port	Default Pool
vra-iaas-mgr-443	vRealize-https	192.168.11.59	HTTPS	443	vra-iaas-mgr-443
vra-iaas-web-443	vRealize-https	192.168.11.56	HTTPS	443	vra-iaas-web-443
vra-svr-443	vRealize-https	192.168.11.53	HTTPS	443	vra-svr-443
vra-svr-8444	vRealize-https	192.168.11.53	HTTPS	8444	vra-svr-8444
vra-vro-8281	vRealize-https	192.168.11.65	HTTPS	8281	vra-vro-8281
VROPS_VIRTUAL_SERVER	VROPS_HTTPS	192.168.11.35	HTTPS	443	VROPS_POOL
VROPS_REDIRECT	VROPS_REDIRECT	192.168.11.35	HTTP	80	NONE

- 4 Verify the settings for the LAXMGMT-LB01 NSX Edge.
  - a In the **Navigator**, click **Networking & Security** and click **NSX Edges**.
  - b Select **172.17.11.65** from the **NSX Manager** drop-down menu.
  - c Double-click the **LAXMGMT-LB01** NSX Edge device.
  - d Click the **Manage** tab, click **Settings**, and select **Interfaces**.
  - e Select the **OneArmLB** interface and click the **Edit** icon.
  - f Verify that the following interface settings are intact.

Setting	LAXMGMT-LB01
Name	OneArmLB
Type	Internal
Connected To	Mgmt-xRegion01-VXLAN
Connectivity Status	Disconnected
Primary IP Address	192.168.11.2
Secondary IP Address	192.168.11.35,192.168.11.59,192.168.11.56,192.168.11.65,192.168.11.53
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- g Verify that the LAXMGMT-LB01 load balancer settings are intact by using the values in the previous step.

# Validate vRealize Operations Manager

# 4

After a maintenance like an update, upgrade, restore or recovery, verify that all vRealize Operations Manager nodes are available.

Verify the functionality of vRealize Operations Manager after a planned maintenance.

## Procedure

### 1 [Verify the Power Status of All vRealize Operations Manager VMs](#)

All virtual machines of vRealize Operations Manager must be properly configured and running.

### 2 [Verify the Configuration of vRealize Operations Manager Cluster Nodes and Remote Collectors](#)

After performing planned maintenance in your environment, verify that vRealize Operations Manager Cluster nodes and Remote Collectors are online and performing the data collection.

### 3 [Verify the vRealize Operations Manager Load Balancing](#)

If you perform an update, patch, restore, failover or failback of the vRealize Operations Manager, verify the load balancing of the cluster.

### 4 [Validate vRealize Operations Manager Adapters and Management Packs](#)

After performing maintenance (i.e. patching, updating, upgrading, restoring and disaster recovery) in your environment, validate the configuration of the adapters and management packs in vRealize Operations Manager.

## Verify the Power Status of All vRealize Operations Manager VMs

All virtual machines of vRealize Operations Manager must be properly configured and running.

For more information about the FQDNs and IP address of each VM, see the list of registered DNS Names from *VMware Validated Design Planning and Preparation Guide* for this validated design.

### Prerequisites

Verify that all vRealize Operations Manager VMs are started according to [Startup Order of the Management Virtual Machines](#).

## Procedure

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

a Open a Web browser and go to the following URL.

Region	Management vCenter Server URL
Region A	<a href="https://mgmt01vc01.sfo01.rainpole.local/vsphere-client">https://mgmt01vc01.sfo01.rainpole.local/vsphere-client</a>
Region B	<a href="https://mgmt01vc51.lax01.rainpole.local/vsphere-client">https://mgmt01vc51.lax01.rainpole.local/vsphere-client</a>

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 Verify that all virtual machines of vRealize Operations Manager are powered on and configured properly.

a On the **Home** page, click **VMs and Templates**.

b In the **Navigator**, go to the following folder names of vCenter Server and verify that the virtual machines are configured in the following way.

Region	Folder Name	VM Name	FQDN	IP Address
Region A	vROps01	vrops-mstrn-01	vrops-mstrn-01.rainpole.local	192.168.11.31
		vrops-repln-02	vrops-repln-02.rainpole.local	192.168.11.32
		vrops-datan-03	vrops-datan-03.rainpole.local	192.168.11.33
	vROps01RC	vrops-rmtcol-01	vrops-rmtcol-01.sfo01.rainpole.local	192.168.31.31
		vrops-rmtcol-02	vrops-rmtcol-02.sfo01.rainpole.local	192.168.31.32
		vrops-rmtcol-03	vrops-rmtcol-03.sfo01.rainpole.local	192.168.31.33
Region B	vROps51RC	vrops-rmtcol-51	vrops-rmtcol-51.lax01.rainpole.local	192.168.32.31
		vrops-rmtcol-52	vrops-rmtcol-52.lax01.rainpole.local	192.168.32.32

## Verify the Configuration of vRealize Operations Manager Cluster Nodes and Remote Collectors

After performing planned maintenance in your environment, verify that vRealize Operations Manager Cluster nodes and Remote Collectors are online and performing the data collection.

Verify the following configurations:

- vRealize Operations Manager health
- Self Monitoring dashboard
- Authentication sources
- Certificates

- Licensing

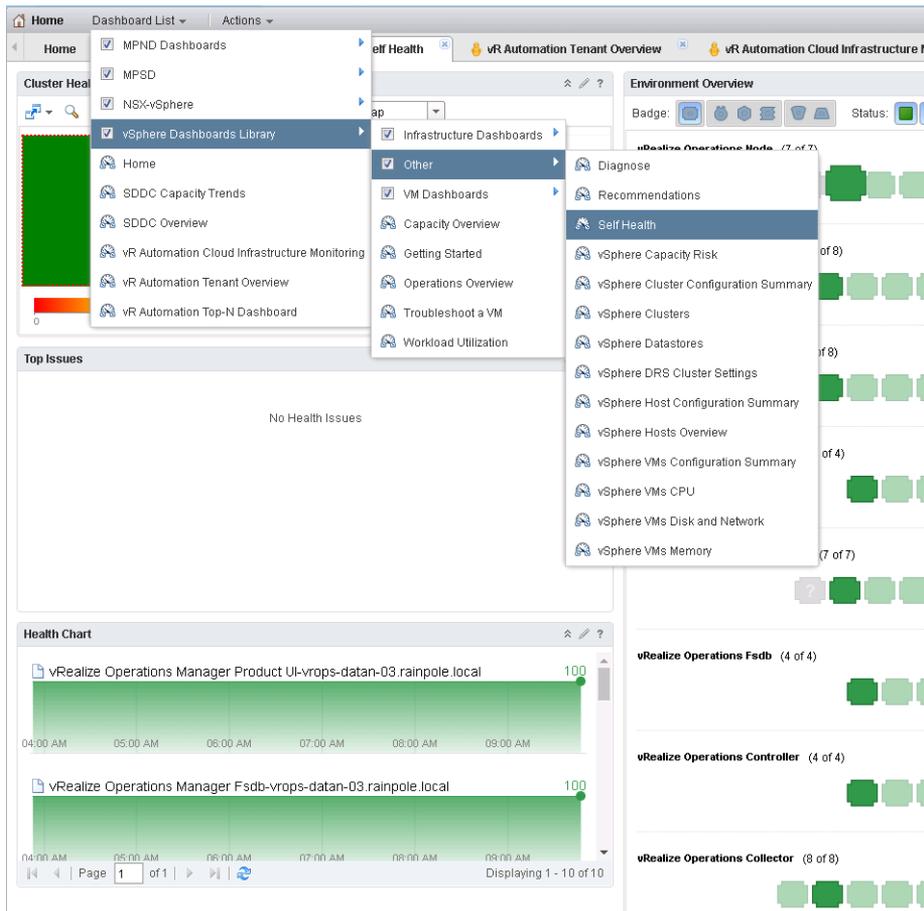
### Procedure

- 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>

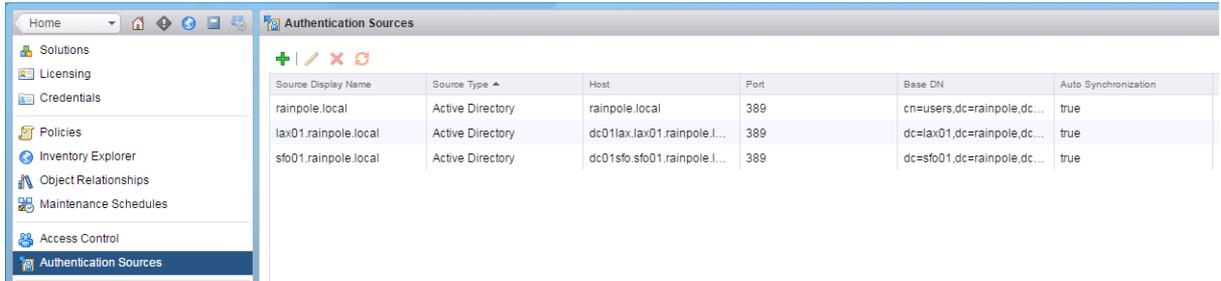
- 2 Verify that the cluster is online, all data nodes are running, and are joined to the cluster.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Cluster Management**.
  - b Verify that the vRealize Operations Manager Cluster Status is OnLine and High Availability mode is Enabled.
- 3 If you have performed an upgrade or update, in the **Nodes in the vRealize Operations Manager Cluster** table, verify that the software version of all vRealize Operations Manager nodes is correct.
- 4 Verify the State and Status of all vRealize Operations Manager nodes.
  - a In the cluster nodes table, verify that the State is Running and Status is OnLine for all nodes.
    - vrops-mstrn-01
    - vrops-repln-02
    - vrops-datan-03
    - vrops-rmtcol-01
    - vrops-rmtcol-02
    - vrops-rmtcol-51
    - vrops-rmtcol-52
  - b In the **Adapter instances** table, verify that Status is Data receiving for all instances.

- 5 Verify the vRealize Operations Manager Cluster Health.
  - a In the left pane of vRealize Operations Manager, click **Home**
  - b On the **Home** page, from the **Dashboard List** drop-down menu, select **vSphere Dashboards Library > Other > Self Health**
  - c Verify that the status of all objects from the cluster is Green.



- 6 Check that there are no critical alerts.
  - a On the **vRealize Operations Clusters** page, click the **Alerts** tab.
  - b Verify that there are no Critical alerts for the vRealize Operations Clusters objects.
- 7 Verify that the authentication sources are valid and synchronization is successful.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Authentication Sources**.
  - b Select the **Active Directory** entry and click the **Synchronize User Groups** icon.

- c In the **Confirmation** dialog box, click **Yes**.
- d Verify that the synchronization is successful and that there are no errors.



- 8 Verify that the CA-Signed certificate is intact.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Certificates**.
  - b Verify that the Certificates are in intact.
- 9 Verify that the License key is intact.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Licensing**.
  - b Verify that the valid License key is intact.

## Verify the vRealize Operations Manager Load Balancing

If you perform an update, patch, restore, failover or failback of the vRealize Operations Manager, verify the load balancing of the cluster.

The NSX Edge services gateway on which you perform the verification is determined by the type of maintenance operation and its location.

- If you perform an update, patch or restore of the vRealize Operations Manager, you verify load balancing of the SFOMGMT-LB01 or LAXMGMT-LB01 NSX Edge services gateways respectively of the regions where operation occurred.
- If you perform a failover to Region B, you verify load balancing of the LAXMGMT-LB01 NSX Edge services gateway.
- If you perform a failback to Region A, you verify load balancing of the SFOMGMT-LB01 NSX Edge services gateway.

### Prerequisites

Connectivity status of the OneArmLB interface of the NSX Edge services gateway must be Connected.

## Procedure

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

- a Open a Web browser and go to the following URL.

Region	Operation Type	Management vCenter Server URL
Region A	Failback, update, patch, or restore	<a href="https://mgmt01vc01.sfo01.rainpole.local/vsphere-client">https://mgmt01vc01.sfo01.rainpole.local/vsphere-client</a>
Region B	Failover, update, patch, or restore	<a href="https://mgmt01vc51.lax01.rainpole.local/vsphere-client">https://mgmt01vc51.lax01.rainpole.local/vsphere-client</a>

- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Verify the pool configuration by examining the pool statistics that reflect the status of the components behind the load balancer.

- a From the **Home** menu, select **Networking & Security**.
- b On the **NSX Home** page, click **NSX Edges** and select the IP address of the NSX Manager from the **NSX Manager** drop-down menu at the top of the NSX Edges page.

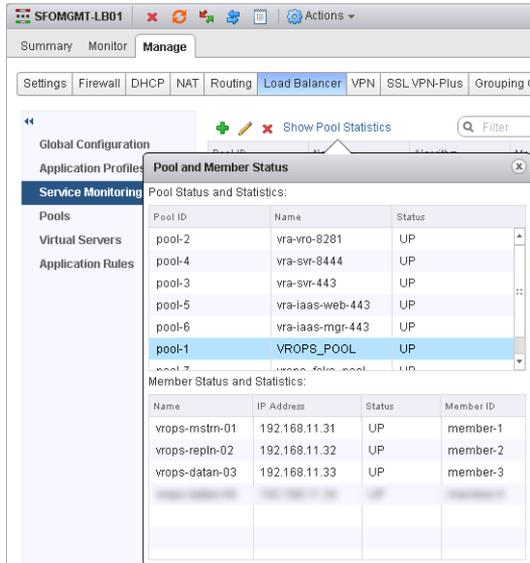
Region	Operation Type	NSX Manager
Region A	Failback, update, patch, or restore	172.16.11.65
Region B	Failover, update, patch, or restore	172.17.11.65

- c On the **NSX Edges** page, double-click the NSX Edge services gateway.

Region	Operation Type	NSX Edge Services Gateway
Region A	Failback, update, patch, or restore	SFOMGMT-LB01
Region B	Failover, update, patch, or restore	LAXMGMT-LB01

- d On the **Manage** tab, click the **Load Balancer** tab.
- e Select **Pools** and click **Show Pool Statistics**.

- f In the **Pool and Member Status** dialog box, select the **VROPS\_POOL** pool.
- g Verify that the status of the **VROPS\_POOL** pool is UP and the status of all members is UP.



- 3 In a Web browser, go to <https://vrops-cluster-01.rainpole.local> to verify that the cluster is accessible at the public Virtual Server IP address over HTTPS.
- 4 In a Web browser, go to <http://vrops-cluster-01.rainpole.local> to verify the auto-redirect requests from HTTP to HTTPS.

## Validate vRealize Operations Manager Adapters and Management Packs

After performing maintenance (i.e. patching, updating, upgrading, restoring and disaster recovery) in your environment, validate the configuration of the adapters and management packs in vRealize Operations Manager.

### Procedure

- 1 [Verify the Version, Status, and Configuration of the VMware vSphere Adapter in vRealize Operations Manager](#)

After you perform a planned maintenance in your environment, verify that the VMware vSphere Adapter is configured and collecting the data from the Management and Compute vCenter Server instances.

- 2 [Verify the Version and Configuration of the vRealize Operations Management Pack for Log Insight](#)

After you perform a planned maintenance in your environment, verify the configuration of the vRealize Log Insight Adapter from the vRealize Operations Manager user interface.

### 3 [Verify the Version, Status, and Configuration of vRealize Operations Manager Management Pack for NSX for vSphere](#)

After you perform a planned maintenance in your environment, verify the configuration of the NSX for vSphere Adapters from the vRealize Operations Manager user interface. Verify also that vRealize Operations Manager receives monitoring data from the NSX Manager instances and from the physical network.

### 4 [Verify the Version, Status, and Configuration of the vRealize Automation Management Pack](#)

After you perform a planned maintenance in your environment, verify the configuration of the vRealize Automation Adapter from the vRealize Operations Manager user interface.

### 5 [Verify the Version, Status, and Configuration of the Management Pack for Storage Devices in vRealize Operations Manager](#)

After you perform a planned maintenance in your environment, verify the configuration of the Storage Devices Adapters. Verify also that the adapter is collecting the data about the storage devices in the SDDC.

## Verify the Version, Status, and Configuration of the VMware vSphere Adapter in vRealize Operations Manager

After you perform a planned maintenance in your environment, verify that the VMware vSphere Adapter is configured and collecting the data from the Management and Compute vCenter Server instances.

**Table 4-1. vCenter Adapter Instances**

Region	Adapter Type	Adapter Name	vCenter Server
Region A	vCenter Adapter	mgmt01vc01-sfo01	mgmt01vc01.sfo01.rainpole.local
	vCenter Adapter	comp01vc01-sfo01	comp01vc01.sfo01.rainpole.local
Region B	vCenter Adapter	mgmt01vc51-lax01	mgmt01vc51.lax01.rainpole.local
	vCenter Adapter	comp01vc51-lax01	comp01vc51.lax01.rainpole.local

### Procedure

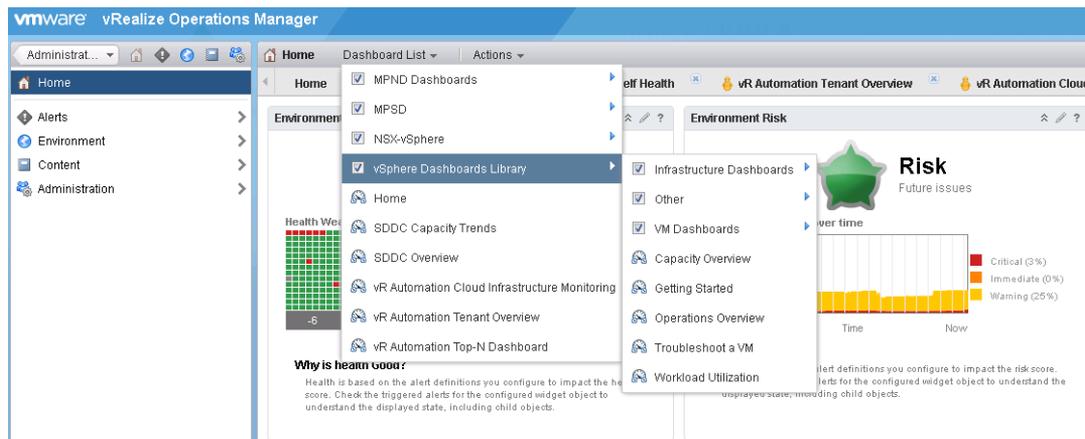
- 1 Log in to vRealize Operations Manager by using the administration console.
  - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
  - b Log in using the following credentials.

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

- 2 Verify that the software version of the VMware vSphere solution is correct.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Solutions**.
  - b From the solution table on the **Solutions** page, select the **VMware vSphere** solution.
  - c Verify that the software version of the VMware vSphere solution is correct.
- 3 Verify that all VMware vSphere adapter instances are configured and collecting the data from the vSphere objects.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Solutions**.
  - b From the solution table on the **Solutions** page, select the **VMware vSphere** solution.
  - c Under **Solution Details**, verify that the Collection State is `Collecting` and the Collection Status is `Data Receiving` for all vCenter Adapter instances.
- 4 Verify collection activity on all vCenter Server objects.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Inventory Explorer**.
  - b On the **Inventory Explorer** page, expand the **Adapter Instances** object in the **Inventory Explorer** pane.
  - c Expand **vCenter Server** object and select each vCenter adapter instance.
  - d On the **List** tab, verify that the Collection State is `Collecting` and the Collection Status is `Data Receiving` for all vCenter Servers objects.

- 5 Verify that all vSphere dashboards are showing up as expected and monitor the state of the vSphere objects.
  - a In the left pane of vRealize Operations Manager, click **Home**.
  - b On the **Home** page, from the **Dashboard List** drop-down menu select **vSphere Dashboards Library > Infrastructure Dashboards**.
  - c Go to each of the vSphere Dashboards and verify that the state of the vSphere vCenter Server components is monitored.

vSphere Dashboards	List of Dashboards
vSphere Dashboards Library	Infrastructure Dashboards
	Other
	VM Dashboards
	Capacity Overview
	Getting Started
	Operations Overview
	Troubleshoot a VM
	Workload Utilization



## Verify the Version and Configuration of the vRealize Operations Management Pack for Log Insight

After you perform a planned maintenance in your environment, verify the configuration of the vRealize Log Insight Adapter from the vRealize Operations Manager user interface.

**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 Verify that the software version of the vRealize Operations Management Pack for Log Insight is correct.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Solutions**.
  - b From the solution table on the **Solutions** page, select the **VMware vRealize Operations Management Pack for Log Insight** solution.
  - c Verify that the software version of the solution is correct.
- 3 Verify that the vRealize Log Insight Adapter instance exists.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Solutions**.
  - b From the solution table on the **Solutions** page, select the **VMware vRealize Operations Management Pack for Log Insight** solution.
  - c Under **Solution Details**, verify that the vRealize Log Insight Adapter instance exists.

## Verify the Version, Status, and Configuration of vRealize Operations Manager Management Pack for NSX for vSphere

After you perform a planned maintenance in your environment, verify the configuration of the NSX for vSphere Adapters from the vRealize Operations Manager user interface. Verify also that vRealize Operations Manager receives monitoring data from the NSX Manager instances and from the physical network.

Verify the following configurations:

- NSX-vSphere Adapter is configured and collecting the data from the management and compute NSX Managers
- Network Devices Adapter is configured and monitoring the switches and routers

**Table 4-2. NSX-vSphere Adapter Instances**

Region	Adapter Type	Adapter Name	NSX Manager Host
Region A	NSX-vSphere Adapter	Mgmt NSX Adapter - SFO01	mgmt01nsxm01.sfo01.rainpole.local
	NSX-vSphere Adapter	Comp NSX Adapter - SFO01	comp01nsxm01.sfo01.rainpole.local

**Table 4-2. NSX-vSphere Adapter Instances (Continued)**

Region	Adapter Type	Adapter Name	NSX Manager Host
Region B	NSX-vSphere Adapter	Mgmt NSX Adapter - LAX01	mgmt01nsxm51.lax01.rainpole.local
	NSX-vSphere Adapter	Comp NSX Adapter - LAX01	comp01nsxm51.lax01.rainpole.local

**Table 4-3. Network Devices Adapter Instance**

Adapter Type	Adapter Name
Network Devices Adapter	Network Devices Adapter

**Procedure**

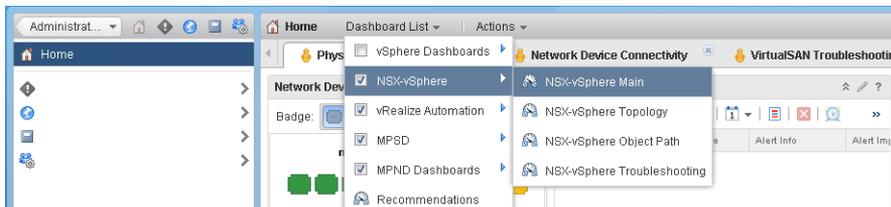
- 1 Log in to vRealize Operations Manager by using the administration console.
  - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
  - b Log in using the following credentials.

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

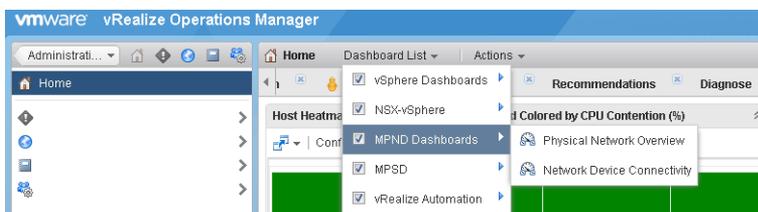
- 2 Verify that the software version of the Management Pack for NSX-vSphere is correct.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Solutions**.
  - b From the solution table on the **Solutions** page, select the **Management Pack for NSX-vSphere** solution.
  - c Verify that the software version of Management Pack for NSX-vSphere solution is correct.
- 3 Verify that all NSX-vSphere Adapter instances are configured and collecting the data from the management and compute NSX Managers.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Solutions**.
  - b On the **Solutions** page, from the solution table, select the **Management Pack for NSX-vSphere** solution.
  - c Under **Solution Details**, verify that the Collection State is **Collecting** and the Collection Status is **Data Receiving** for all NSX-vSphere Adapter instances.

- 4 Verify that Network Devices Adapter instance is configured and collecting the data about the network devices.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Solutions**.
  - b From the solution table on the **Solutions** page, select the **Management Pack for NSX-vSphere** solution.
  - c Under **Solution Details**, verify that the Collection State is **Collecting** and the Collection Status is **Data Receiving** for the Network Devices Adapter instance.
- 5 Verify the collection activity of the NSX-vSphere Environment objects.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Inventory Explorer**.
  - b On the **Inventory Explorer** page, expand the **Adapter Instances** object in the **Inventory Explorer** pane.
  - c Expand the **NSX-vSphere Environment** object and select each NSX-vSphere adapter instance.
  - d On the **List** tab, verify that the Collection State is **Collecting** and the Collection Status is **Data Receiving** for the NSX-vSphere Environment objects.
- 6 Verify collection activity from the Network Devices objects.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Inventory Explorer**.
  - b On the **Inventory Explorer** page, expand the **Adapter Instances** object in the **Inventory Explorer** pane.
  - c Expand the **Network Devices Adapter Instance** object and select Network Devices adapter instance.
  - d On the **List** tab, verify that the Collection State is **Collecting** and the Collection Status is **Data Receiving** for the Network Devices objects.

- 7 Verify that all NSX-vSphere dashboards are showing up as expected and monitor the state of the NSX components and networking in the SDDC.
  - a In the left pane of vRealize Operations Manager, click **Home**.
  - b On the **Home** page, from the **Dashboard List** drop-down menu, select **NSX-vSphere > NSX-vSphere Main**.
  - c Go to each of the NSX-vSphere dashboards and check that the state of the NSX components and networking in the SDDC is monitored.
    - NSX-vSphere Main
    - NSX-vSphere Topology
    - NSX-vSphere Object Path
    - NSX-vSphere Troubleshooting



- 8 Verify that all MPND dashboards are showing up as expected, and monitor physical network and network devices in the SDDC.
  - a In the left pane of vRealize Operations Manager, click **Home**.
  - b On the **Home** page, from the **Dashboard List** drop-down menu, select **MPND-Dashboards > Physical Network Overview**.
  - c Go to each of the MPND-Dashboards and check that the state of the physical network and network devices in the SDDC is monitored.
    - Physical Network Overview
    - Network Device Connectivity



## Verify the Version, Status, and Configuration of the vRealize Automation Management Pack

After you perform a planned maintenance in your environment, verify the configuration of the vRealize Automation Adapter from the vRealize Operations Manager user interface.

## 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.

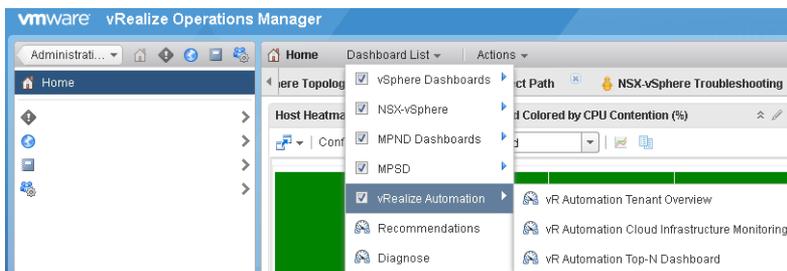
Setting	Value
User name	admin
Password	vrops_admin_password

- 2 Verify that the software version of the vRealize Automation Management Pack is correct.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Solutions**.
  - b From the solution table on the **Solutions** page, select the **vRealize Automation Management Pack** solution.
  - c Verify that the software version of the vRealize Automation Management Pack solution is correct.
- 3 Verify that the vRealize Automation MP instance is configured and collecting the data from vRealize Automation.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Solutions**.
  - b From the solution table on the **Solutions** page, select the **vRealize Automation Management Pack** solution.
  - c Under **Solution Details**, verify that the Collection State is **Collecting** and the Collection Status is **Data Receiving** for the vRealize Automation MP adapter instance.

The screenshot displays the 'Solutions' page in vRealize Operations Manager. At the top, there is a 'Show:' dropdown set to 'All Solutions'. Below this is a table listing various solutions. The 'vRealize Automation Management Pack' solution is highlighted in blue and shows a status of 'Data receiving (1)'. Other solutions listed include 'VMware vSphere', 'VMware vRealize Log Insight', 'Operating Systems / Remote Service Monitoring', 'Management Pack for Storage Devices', and 'Management Pack for NSX-vSphere'. Below the main table, there is a section titled 'vRealize Automation Management Pack Solution Details' which contains a table with the following data:

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
vRealize Automation MP	vRealize Automation Adapter	Credentials-vRA-Adapter	vRealize Operations Manager Coll...	Collecting	Data receiving

- 4 Verify the collection activity of the vRealize Automation objects.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Inventory Explorer**.
  - b In the **Inventory Explorer** pane, select **Adapter Instances > vRealize Automation MP Instance > vRealize Automation Adapter**.
  - c On the **List** tab, verify that the Collection State is **Collecting** and the Collection Status is **Data receiving** for the vRealize Automation objects.
  
- 5 Verify that all vRealize Automation dashboards are showing up as expected and monitor the state of the vRealize Automation components in SDDC.
  - a In the left pane of vRealize Operations Manager, click **Home**.
  - b On the **Home** page, from the **Dashboard List** drop-down menu select **vRealize Automation > vR Automation Tenant Overview**.
  - c Go to each of the vRealize Automation dashboards and check that the state of the vRealize Automation components in the SDDC is monitored.
    - vR Automation Tenant Overview
    - vR Automation Cloud Infrastructure Monitoring
    - vR Automation Top-N Dashboard



## Verify the Version, Status, and Configuration of the Management Pack for Storage Devices in vRealize Operations Manager

After you perform a planned maintenance in your environment, verify the configuration of the Storage Devices Adapters. Verify also that the adapter is collecting the data about the storage devices in the SDDC.

**Table 4-4. Storage Devices Adapter Instances**

Region	Adapter Type	Adapter Name	vCenter Server
Region A	Storage Devices	Storage MP SFO MGMT	mgmt01vc01.sfo01.rainpole.local
	Storage Devices	Storage MP SFO Compute	comp01vc01.sfo01.rainpole.local
Region B	Storage Devices	Storage MP LAX MGMT	mgmt01vc51.lax01.rainpole.local
	Storage Devices	Storage MP LAX Compute	comp01vc51.lax01.rainpole.local

## Procedure

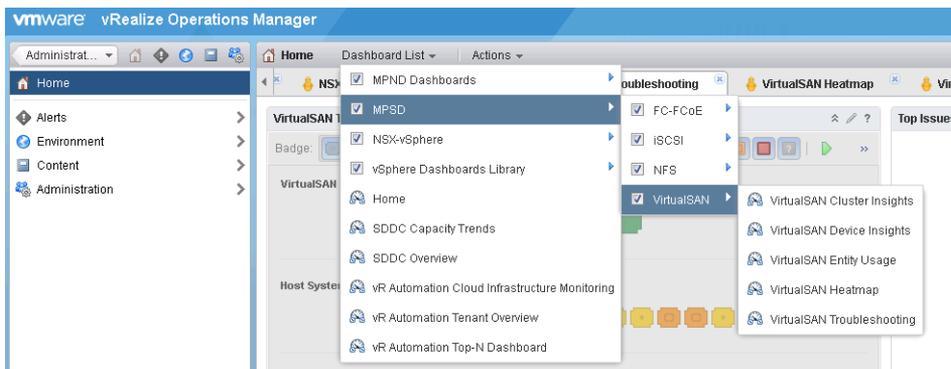
- 1 Log in to vRealize Operations Manager by using the administration console.
  - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
  - b Log in using the following credentials.

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

- 2 Verify that the software version of the Management Pack for Storage Devices is correct.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Solutions**.
  - b From the solution table on the **Solutions** page, select the **Management Pack for Storage Devices** solution.
  - c Verify that the software version of Management Pack for Storage Devices solution is correct.
- 3 Verify that all Storage Devices adapter instances are configured and collecting the data about the storage devices in the SDDC.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Solutions**.
  - b From the solution table on the **Solutions** page, select the **Management Pack for Storage Devices** solution.
  - c Under **Solution Details**, verify that the Collection State is *Collecting* and the Collection Status is *Data Receiving* for all Storage Devices adapter instances.
- 4 Verify the collection activity on the storage devices objects.
  - a In the left pane of vRealize Operations Manager, click **Home** and select **Administration > Inventory Explorer**.
  - b On the **Inventory Explorer** page, expand **Adapter Instances** object in the **Inventory Explorer** pane.
  - c Expand the **Storage Devices Instance** object and select each **Storage Devices** adapter instance.
  - d On the **List** tab, verify that the Collection State is *Collecting* and the Collection Status is *Data Receiving* for the storage devices objects.

- 5 Verify that all the **MPSD** dashboards are showing up as expected and monitor the data about the storage devices in the SDDC.
  - a In the left pane of vRealize Operations Manager, click **Home**.
  - b On the Home page, from the **Dashboard List** drop-down menu select **MPSD > VirtualSAN > VirtualSAN Troubleshooting**.
  - c Go to each of the **MPSD** dashboards and verify that vRealize Operations Manager shows monitoring data about the storage devices in the SDDC.

MPSD Dashboard Category	Dashboards
FC-FCoE	FC-FCoE Components Usage
	FC-FCoE Components Heatmap
	FC-FCoE Troubleshooting
iSCSI	iSCSI Components Heatmap
	iSCSI Components Usage
	iSCSI Troubleshooting
NFS	NFS Components Heatmap
	NFS Components Usage
	NFS Troubleshooting
VirtualSAN	VirtualSAN Cluster Insights
	VirtualSAN Device Insights
	VirtualSAN Entity Usage
	VirtualSAN Heatmap
	VirtualSAN Troubleshooting



# 5

## Validate vRealize Log Insight

After a planned maintenance operation such as an update, upgrade, restore or recovery, verify that all vRealize Log Insight nodes are available and work as expected.

### Verify the Status of the vRealize Log Insight Nodes

After a maintenance operation such as an update, upgrade, restore or recovery, validate the version, service status and configuration of each vRealize Log Insight appliance.

#### Procedure

- 1 Log in to vRealize Log Insight.
  - a Open a Web browser and go to the following URLs.

Region	URL
Region A	<code>https://vrli-cluster-01.sfo01.rainpole.local</code>
Region B	<code>https://vrli-cluster-51.lax01.rainpole.local</code>

- b Log in using the following credentials.

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

- 2 Click the configuration drop-down menu icon  and select **Administration**.

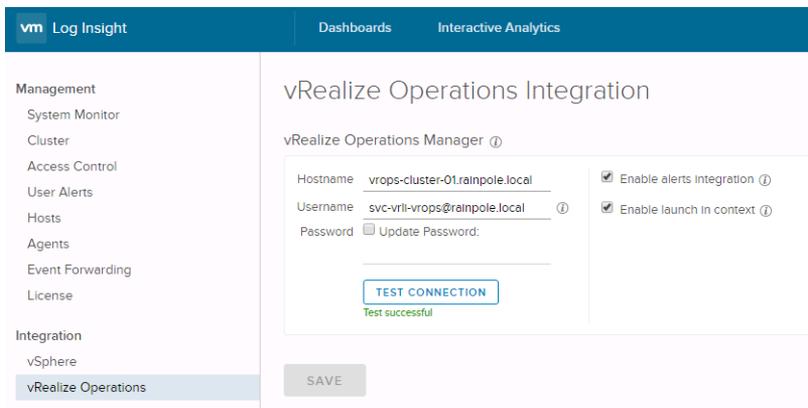
- 3 Verify the software version and the connectivity status of the cluster nodes and Integrated Load Balancer.
  - a Under **Management**, click **Cluster**.
  - b If you have performed a patch or upgrade, verify that the Version of the vRealize Log Insight nodes is as expected.
  - c Verify the Status of cluster nodes and Integrated Load Balancer.

Region	Host Name or IP Address	Role	Expected Status
Region A	vrli-mstr-01.sfo01.rainpole.local (192.168.31.11)	Master	Connected
	vrli-wrkr-01.sfo01.rainpole.local (192.168.31.12)	Worker	
	vrli-wrkr-02.sfo01.rainpole.local (192.168.31.13)	Worker	
	vrli-cluster-01.sfo01.rainpole.local (192.168.31.10)	Integrated Load Balancer	
Region B	vrli-mstr-51.lax01.rainpole.local (192.168.32.11)	Master	Connected
	vrli-wrkr-51.lax01.rainpole.local (192.168.32.12)	Worker	
	vrli-wrkr-52.lax01.rainpole.local (192.168.32.13)	Worker	
	vrli-cluster-51.lax01.rainpole.local (192.168.32.10)	Integrated Load Balancer	

- 4 Verify that the registered agents on the monitored management SDDC nodes are active.
  - a Under **Management**, click **Agents**.
  - b On the **Agents** page, from the **Agents** drop-down menu, select each of the following agent group and verify that all registered agents are visible and their Status is Active.

Agent Group	Agent Host Names from Region A	Agent Host Names from Region B
vSphere 6.x - vCenter (Linux) Complete	mgmt01vc01.sfo01.rainpole.local comp01vc01.sfo01.rainpole.local mgmt01psc01.sfo01.rainpole.local comp01psc01.sfo01.rainpole.local	mgmt01vc51.lax01.rainpole.local comp01vc51.lax01.rainpole.local mgmt01psc51.lax01.rainpole.local comp01psc51.lax01.rainpole.local
vRA7 - Linux Agent Group	vrA01svr01a.rainpole.local vrA01svr01b.rainpole.local	
vRA7 - Windows Agent Group	vrA01iws01a.rainpole.local vrA01iws01b.rainpole.local vrA01ims01a.rainpole.local vrA01ims01b.rainpole.local vrA01dem01.rainpole.local vrA01dem02.rainpole.local vrA01ias01.sfo01.rainpole.local vrA01ias02.sfo01.rainpole.local	vrA01ias51.lax01.rainpole.local vrA01ias52.lax01.rainpole.local
vRA7 - Microsoft SQL Server Agent Group	vrA01mssql01.rainpole.local	

- 5 Verify that the license key is intact.
  - a Under **Management**, click **License**.
  - b Verify that the license Status in the table is Active.
- 6 Verify that the vRealize Log Insight integration with Management vCenter Server and Compute vCenter Server is intact.
  - a Under **Integration**, click **vSphere**.
  - b Click **Test Connection** for the Management vCenter Server and Compute vCenter Server.
  - c Verify that the Test successful message appears.
- 7 Verify that the vRealize Log Insight integration with vRealize Operations Manager is intact.
  - a Under **Integration**, click **vRealize Operations**.
  - b Click **Test Connection**.
  - c Verify that the Test successful message appears.



- 8 Verify that the time configuration of vRealize Log Insight is intact.
  - a Under **Configuration**, click **Time**.
  - b Verify that the NTP Servers page contains the ntp.sfo01.rainpole.local and ntp.lax01.rainpole.local time servers.
  - c Click **Test** to verify that the connection is successful.

- 9 Verify that the vRealize Log Insight integration with Active Directory is intact.
  - a Under **Configuration**, click **Authentication**.
  - b Verify that the Authentication Configuration is intact.

Setting	Expected 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	As required from the IT administrator

- c Click **Test connection** to verify that the connection is successful.

The screenshot shows the 'Authentication Configuration' page in the vRealize Log Insight interface. The left sidebar contains a navigation menu with categories like Management, Integration, and Configuration. The 'Authentication' option is selected. The main content area displays the following configuration:

- Enable Active Directory support:** A green toggle switch is turned on.
- Default Domain:** rainpole.local
- Domain Controller(s):** Optional comma-separated servers
- Username:** svc-loginsight@rainpole.local
- Password:** A field with a checkbox for 'Update Password'.
- Connection Type:** Standard (selected from a dropdown menu).
- Require SSL:** Checked.

At the bottom of the configuration area, there is a blue button labeled 'TEST CONNECTION'. Below this button, a green message indicates 'Succeeded'. A 'SAVE' button is located at the bottom left of the configuration area.

- 10 Verify that the configuration for the SMTP email server is intact.
  - a Under **Configuration**, click **SMTP**.
  - b Verify that the SMTP Configuration is intact.
  - c Type a valid email address and click **Send Test Email**.
  - d Verify that vRealize Log Insight sends a test email to the address that you provided.

11 Verify that the configuration of log archiving is intact.

- a Under **Configuration**, click **Archiving**.
- b Verify that the Archiving Configuration is intact.

Setting	Expected Value
Enable Data Archiving	Selected
Archive Location	<i>nfs://nfs-server-address/nfs-datastore-name</i>

For example, you can set location `nfs://192.168.104.251/VVD_Demand_MgmtA_1TB` for Region A

- c Click **Test** next to the **Archive Location** text box to verify that the NFS share is accessible.

12 Verify that the configuration of the CA-signed certificate is intact.

- a Under **Configuration**, click **SSL**.
- b Verify that the SSL Configuration contains the certificate signed by the Microsoft CA on the domain controller in the Custom SSL Certificate section.

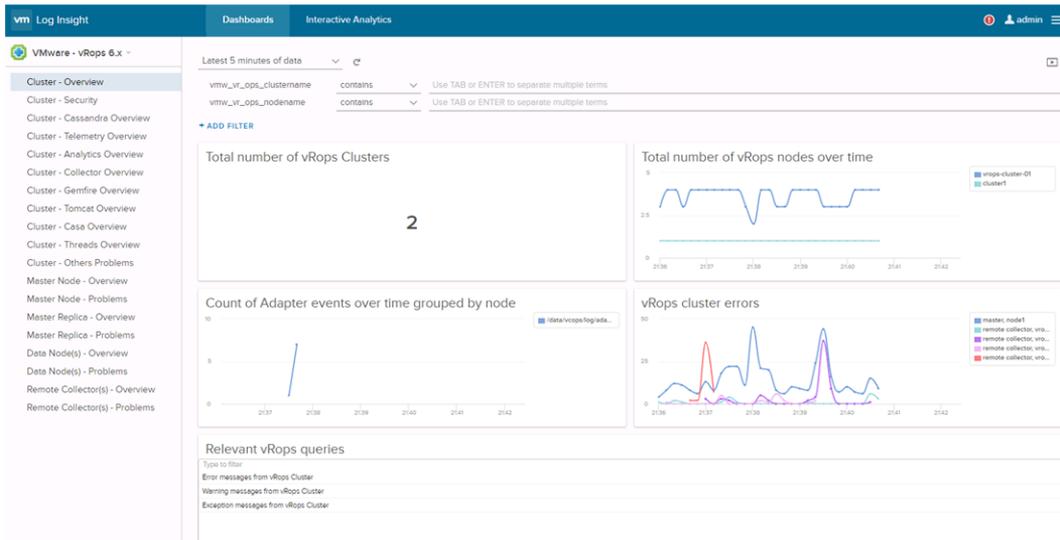
13 Verify that the installed content packs are intact.

- a Click the configuration drop-down menu icon  and select **Content Packs**.
- b Verify that the following Content Packs are listed under **Installed Content Packs**.
  - Microsoft - SQL Server
  - VMware - NSX-vSphere
  - VMware - Orchestrator - 7.0.1+
  - VMware - VSAN
  - VMware - vRA 7
  - VMware - vRops 6.x
  - VMware - vSphere

14 Verify that the Content Pack Dashboards are receiving log information.

- a In the vRealize Log Insight user interface, click **Dashboards**.
- b From the **Content Pack Dashboards** drop-down menu, select **VMware - vRops 6.x**.

- c Verify that the dashboard shows log information about the operation of vRealize Operations Manager.



- d Repeat the step for each of the remaining content packs in the drop-down menu.
- 15 (Optional) Verify the service status and cluster status of vRealize Log Insight from the command line.
- a Open a Secure Shell (SSH) connection to `vrli-mstr-01.sfo01.rainpole.local`.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	<code>vrli_master_root_password</code>

- c Run the following command to validate that the Log Insight service is running.

```
/etc/init.d/loginsight status
```

```
vrli-mstr-01:~ # /etc/init.d/loginsight status
16/05/24 11:18:59 INFO executor.ProcessExecutor: Finished executing ip -4 addr show eth0, ran for 58 ms
Log Insight is running.
vrli-mstr-01:~ # █
```

- d Change the working directory by running the following command.

```
cd /usr/lib/loginsight/application/lib/apache-cassandra-*/bin
```

- e Verify that the cluster status is up by running this command.

```
./nodetool status
```

```
vrli-mstr-01:~ # cd /usr/lib/loginsight/application/lib/apache-cassandra-2.0.17/bin
You have new mail in /var/mail/root
vrli-mstr-01:/usr/lib/loginsight/application/lib/apache-cassandra-2.0.17/bin # ./nodetool status
Note: Ownership information does not include topology; for complete information, specify a keyspace
Datacenter: datacenter1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address          Load          Tokens  Owns    Host ID                               Rack
UN 192.168.31.11    25.45 MB     256     30.6%  e981761b-a351-4598-a360-479d19e15441 rack1
UN 192.168.31.12    25.24 MB     256     35.3%  02c81e72-607d-4c71-9aa0-31dc06c8e28f rack1
UN 192.168.31.13    25.12 MB     256     34.1%  9c3f3643-e58d-4194-9344-785138d050c9 rack1
vrli-mstr-01:/usr/lib/loginsight/application/lib/apache-cassandra-2.0.17/bin # █
```

The output shows a row for each cluster node. The U letter indicates the node is Up. The N letter indicates the node is in Normal state.

- f Repeat the step for each of the remaining vRealize Log Insight nodes.

Region	URL
Region A	■ vrli-wrkr-01.sfo01.rainpole.local
	■ vrli-wrkr-02.sfo01.rainpole.local
Region B	■ vrli-mstr-51.lax01.rainpole.local
	■ vrli-wrkr-51.lax01.rainpole.local
	■ vrli-wrkr-52.lax01.rainpole.local

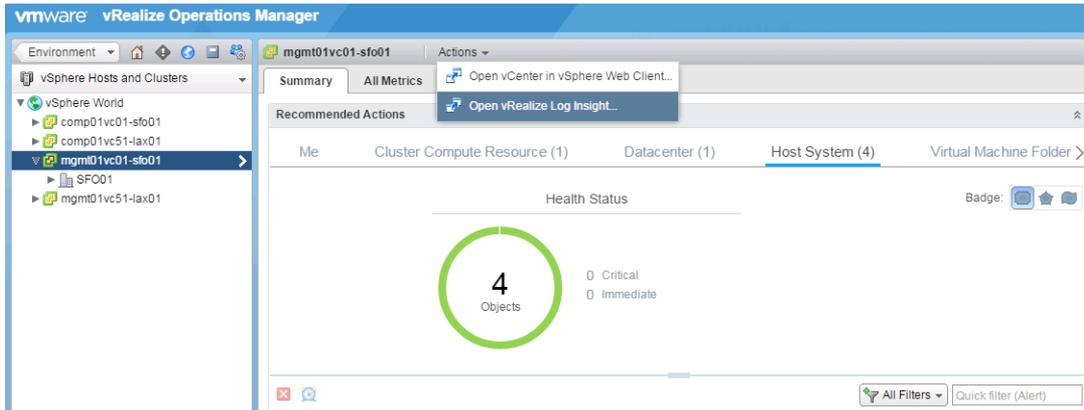
- 16 (Optional) Verify that you can open vRealize Log Insight from vRealize Operations Manager and you can query for selected objects.

- 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

- c In the left pane of vRealize Operations Manager, click **Environment > vSphere Hosts and Clusters**.
- d Expand the **vSphere World** tree and select **mgmt01vc01-sfo01**.

- e Click **Actions** and verify that the user interface shows the Open vRealize Log Insight option.



- f On the left, select **mgmt01vc51-lax01**.
- g Click **Actions** and verify that the user interface shows the **Open vRealize Log Insight** option.

# Validate vSphere Data Protection

# 6

After a maintenance such as an update or upgrade, validate the VMware vSphere Data Protection to make sure it works as expected.

## Procedure

### 1 Verify the Appliance Status and Version of vSphere Data Protection

After an upgrade or update of vSphere Data Protection, verify the version number and appliance status.

### 2 Verify the Configuration and Service Status of vSphere Data Protection

After you patch or update the vSphere Data Protection instances mgmt01vdp01 and mgmt01vdp51, verify the configuration and service status of each of them.

## Verify the Appliance Status and Version of vSphere Data Protection

After an upgrade or update of vSphere Data Protection, verify the version number and appliance status.

## Procedure

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

a Open a Web browser and go to the following URL.

Region	vCenter Server URL
Region A	https://mgmt01vc01.sfo01.rainpole.local/vsphere-client
Region B	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 vCenter server, verify that the vSphere Data Protection **VDP** icon is visible.

3 Click the **VDP** icon to open the Welcome screen of vSphere Data Protection.

- 4 On the vSphere Data Protection **Welcome** screen, verify that the connection to the vSphere Data Protection appliances.

Region	Appliance Name
Region A	mgmt01vdp01
Region B	mgmt01vdp51

- a Verify that the appliance is available in **VDP Appliance** drop-down menu.
  - b Select the appliance from the **VDP Appliance** drop-down menu, click **Connect** and verify that you can connect to the vSphere Data Protection appliance and can see its home page.
  - c Repeat the steps for the other vSphere Data Protection appliance.
- 5 Click the **Reports** tab and verify that the Appliance status and Integrity check status are Normal.
- 6 Click the **Configuration** tab and click **Backup Appliance**.
- a Verify that the display name, IP Address, and vCenter Server values are correct.

Setting	Expected Value in Region A	Expected Value in Region B
Display name	mgmt01vdp01	mgmt01vdp51
IP Address	172.16.11.81	172.17.11.81
vCenter Server	mgmt01vc01.sfo01.rainpole.local	mgmt01vc51.lax01.rainpole.local

- b Verify that the vSphere Data Protection version is correct.

The screenshot shows the vSphere Data Protection 6.1 (powered by EMC) interface. The 'Configuration' tab is selected, and the 'Backup Appliance' sub-tab is active. The 'Backup appliance details' section displays the following information:

- Display name: mgmt01vdp01
- Product name: VDP
- IP Address: 172.18.11.81
- Major Version: 6.1.3.70
- Minor Version: 7.2.80.118\_6.1.3.70
- Status: Normal
- Host: mgmt01esx02.sfo01.rainpole.local
- vCenter server: mgmt01vc01.sfo01.rainpole.local
- VDP backup user: vsphere.localadministrator
- VDP appliance time: 12/08/2016 05:08 PM
- Time zone: GMT +0:00

The 'VDP Appliance storage summary details' section shows a storage bar chart with the following data:

- Capacity: 4.1 TiB
- Space free: 4.1 TiB
- Deduplicated size: 6.4 GiB
- Non-Deduplicated size: Collecting

## Verify the Configuration and Service Status of vSphere Data Protection

After you patch or update the vSphere Data Protection instances mgmt01vdp01 and mgmt01vdp51, verify the configuration and service status of each of them.

## Procedure

1 Log in to the vSphere Data Protection configuration page.

a Open a Web browser and go to the following URL.

Region	VM	URL
Region A	mgmt01vdp01	https://mgmt01vdp01.sfo01.rainpole.local:8543/vdp-configure
Region B	mgmt01vdp51	https://mgmt01vdp51.lax01.rainpole.local:8543/vdp-configure

b Log in using the following credentials.

Setting	Value
User name	root
Password	vdp_root_password

2 On the **Configuration** tab, under **VDP Appliance**, verify the following parameters of vSphere Data Protection.

- Verify that the values of host name, time zone, vCenter and vCenter SSO are compliant with your VMware Validated Design environment.
- Verify that the status of vSphere Data Protection Proxy instance is running.
- Verify that all services like Core, Management, Maintenance, Backup Scheduler, Replication, File Level Restore and Backup Recovery are running.

The screenshot displays the vSphere Data Protection Configuration interface. The top navigation bar includes tabs for Configuration, Storage, Rollback, Upgrade, Emergency Restore, Log Collector, and Avamar Migration. The main content area is divided into two sections: VDP Appliance and Proxies.

**VDP Appliance Settings:**

- Hostname: mgmt01vdp01.sfo01.rainpole.local
- Time zone: UTC
- vCenter: mgmt01vc01.sfo01.rainpole.local
- vCenter SSO: sfo01psc01.sfo01.rainpole.local

**Services Status:**

- Core:  Stop
- Management:  Stop
- Maintenance:  Stop
- Backup Sched...:  Stop
- Replication:  Stop

**Proxies Table:**

Name	IP Address	ESX Host Name	Datastore	Status
mgmt01vdp01	172.18.11.81	mgmt01esx02.sfo01.rainpole.local	SFO01A-NFS01-VDP01	<input checked="" type="checkbox"/>

**Additional Services Status:**

- mgmt01vdp01.sfo01.rainpole.local
- File Level Res...:  Stop
- Backup Recov...:  Stop

The interface also shows a timestamp of 12/08/2016 05:15 AM.

3 Click the **Storage** tab and verify that the storage statistics are intact.

- 4 Log in to the vSphere Data Protection appliance over SSH using root credentials.

Appliance Name	User Name	Password
mgmt01vdp01	root	<i>vdp_root_password</i>
mgmt01vdp51	root	<i>vdp_root_password</i>

- 5 Verify the status of all services of the vSphere Data Protection appliance.
- a Run the following command.

```
dpnctl status all
```

- b Verify that the status of all services are **up/enabled**.

```
root@mgmt01vdp01:~/#: dpnctl status all
Identity added: /home/dpn/.ssh/dpnid (/home/dpn/.ssh/dpnid)
dpnctl: INFO: gsan status: up
dpnctl: INFO: MCS status: up.
dpnctl: INFO: emt status: up.
dpnctl: INFO: Backup scheduler status: up.
dpnctl: INFO: axionfs status: down.
dpnctl: INFO: Maintenance windows scheduler status: enabled.
dpnctl: INFO: Unattended startup status: enabled.
dpnctl: INFO: avinstaller status: up.
dpnctl: INFO: [see log file "/usr/local/avamar/var/log/dpnctl.log"]
root@mgmt01vdp01:~/#: █
```

The status of axionfs service might be down.

- 6 Verify the status of Enterprise Manager Web application in the vSphere Data Protection appliance.
- a Run the following command.

```
emwebapp.sh --test
```

- b Verify that the status of Enterprise Manager Web application service is **up**.

```
root@mgmt01vdp01:~/#: emwebapp.sh --test
INFO: Enterprise Manager web application status: up
root@mgmt01vdp01:~/#: █
```

# Validate Site Recovery Manager

After a maintenance like an update or upgrade, validate the VMware Site Recovery Manager and make sure it works as expected.

## Verify the Version and Service Status of Site Recovery Manager

After you patch or update the Site Recovery Manager instances mgmt01srm01 and mgmt01srm51, verify the version, service status and configuration of each of them.

**Table 7-1. Program Names and Services to Verify on Site Recovery Manager**

Region	VM Name/Host Name	Program Names for Version Check	Services for Availability Check
Region A	mgmt01srm01	<ul style="list-style-type: none"> <li>■ VMware vCenter Site Recovery Manager Server</li> <li>■ VMware vCenter Site Recovery Manager Embedded Database</li> </ul>	<ul style="list-style-type: none"> <li>■ VMware vCenter Site Recovery Manager Server</li> <li>■ VMware vCenter Site Recovery Manager Embedded Database</li> </ul>
Region B	mgmt01srm51	<ul style="list-style-type: none"> <li>■ VMware vCenter Site Recovery Manager Server</li> <li>■ VMware vCenter Site Recovery Manager Embedded Database</li> </ul>	<ul style="list-style-type: none"> <li>■ VMware vCenter Site Recovery Manager Server</li> <li>■ VMware vCenter Site Recovery Manager Embedded Database</li> </ul>

### 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.

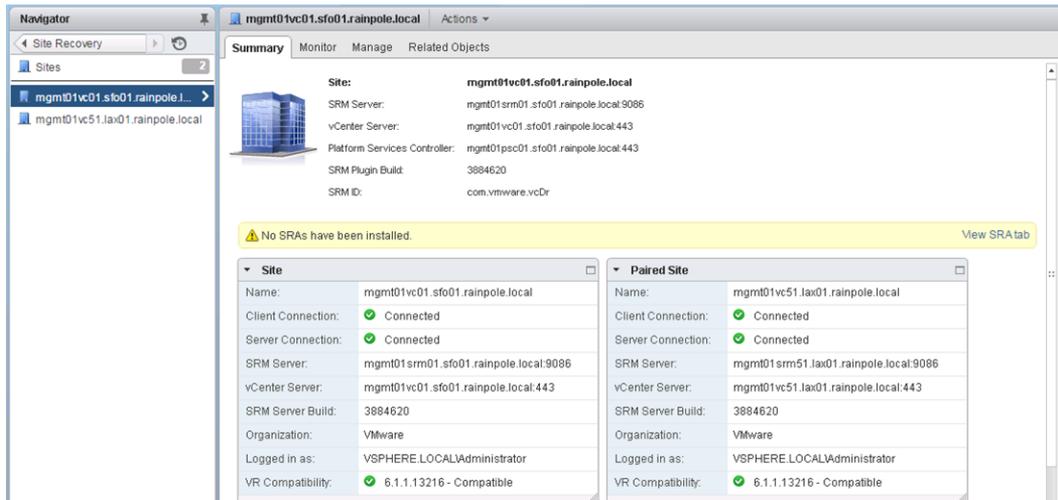
Setting	Value
User name	Windows administrator user
Password	<i>windows_administrator_password</i>

- 2 If you have performed a patch or update, verify the version of VMware Site Recovery Manager.
  - a From the Windows **Start** menu, select **Control Panel > Programs and Features**.
  - b Verify that the version of the following programs is successfully updated.
    - VMware vCenter Site Recovery Manager Server
    - VMware vCenter Site Recovery Manager Embedded Database
- 3 Verify the status of the IaaS Web Server services.
  - a From the Windows **Start** menu, select **Administrative Tools > Services**.
  - b Verify that the status of Site Recovery Manager Server and Site Recovery Manager Embedded Database service is Running.
- 4 Repeat the step for each of the other Windows nodes of Site Recovery Manager to verify the version and services availability.
- 5 Verify that the license is intact in the vSphere Web Client.
  - a Log in to the Management vCenter Server by using the vSphere Web Client.
  - b Open a Web browser and go to **https://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
  - c Log in using the following credentials.
 

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password
  - d Under **Administration**, click **Licensing**.
  - e Click the **Assets** tab, and click **Solutions**.
  - f Verify that the license is intact for the **mgmt01vc01.sfo01.rainpole.local** and **mgmt01vc51.lax01.rainpole.local** assets.
- 6 Verify that the Site Recovery console in the vSphere Web Client shows the updated build version of Site Recovery Manager and that site pairing is intact.
  - 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 Verify that the following settings are intact in summary section.

Settings	Site	Paired Site
Name	mgmt01vc01.sfo01.rainpole.local	mgmt01vc51.lax01.rainpole.local
Client Connection	Connected	Connected
Server Connection	Connected	Connected
SRM Server	mgmt01srm01.sfo01.rainpole.local:9086	mgmt01srm51.lax01.rainpole.local:9086
vCenter Server	mgmt01vc01.sfo01.rainpole.local:443	mgmt01vc51.lax01.rainpole.local:443
SRM Server Build	<i>updated_build_version</i>	<i>update_build_version</i>
Organization	VMware	VMware
Logged in as	VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator
VR Compatibility	Compatible VR version	Compatible VR version



7 Verify that network, folder, resource and resource mappings, and the placeholder datastore configuration of the mgmt01vc01.sfo01.rainpole.local site are intact.

- a Under **Sites**, click the **mgmt01vc01.sfo01.rainpole.local** site.
- b Click the **Manage** tab and verify the following mappings and its configurations are intact.

Settings	mgmt01vc01.sfo01.rainpole.local	mgmt01vc51.lax01.rainpole.local	Reverse Mapping Exists
Network Mappings	Port group whose name contains xRegion01-VXLAN	Port group whose name contains xRegion01-VXLAN	Yes
Folder Mappings	<ul style="list-style-type: none"> <li>■ vRA01</li> <li>■ vRops01</li> </ul>	<ul style="list-style-type: none"> <li>■ vRA51</li> <li>■ vRops51</li> </ul>	Yes
Resource Mappings	SFO01-Mgmt01	LAX01-Mgmt01	Yes
Placeholder Datastores	SFO01A-VSAN01-MGMT01	N/A	N/A

8 Verify that network, folder, resource and resource mappings, and the placeholder datastore configuration of the mgmt01vc51.lax01.rainpole.local site are intact.

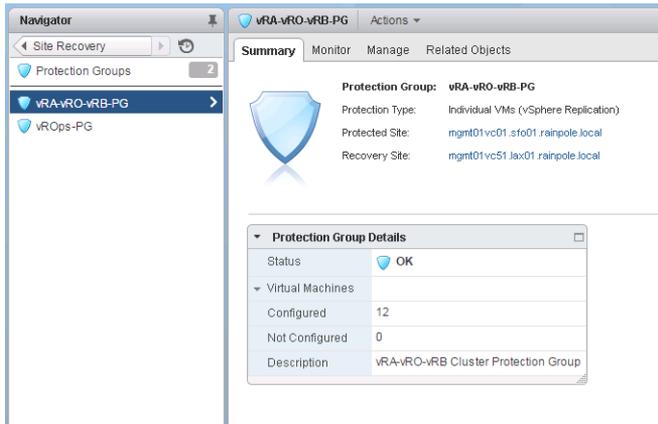
- a Under **Sites**, click the **mgmt01vc51.lax01.rainpole.local** site.
- b Click the **Manager** tab and verify the following mappings and its configurations are intact.

Settings	mgmt01vc51.lax01.rainpole.local	mgmt01vc01.sfo01.rainpole.local	Reverse Mapping Exists
Network Mappings	Port group whose name contains xRegion01-VXLAN	Port group whose name contains xRegion01-VXLAN	Yes
Folder Mappings	<ul style="list-style-type: none"> <li>■ vRA51</li> <li>■ vRops51</li> </ul>	<ul style="list-style-type: none"> <li>■ vRA01</li> <li>■ vRops01</li> </ul>	Yes
Resource Mappings	LAX01-Mgmt01	SFO01-Mgmt01	Yes
Placeholder Datastores	LAX01A-VSAN01-MGMT01	N/A	N/A

9 Verify that the protection group is intact.

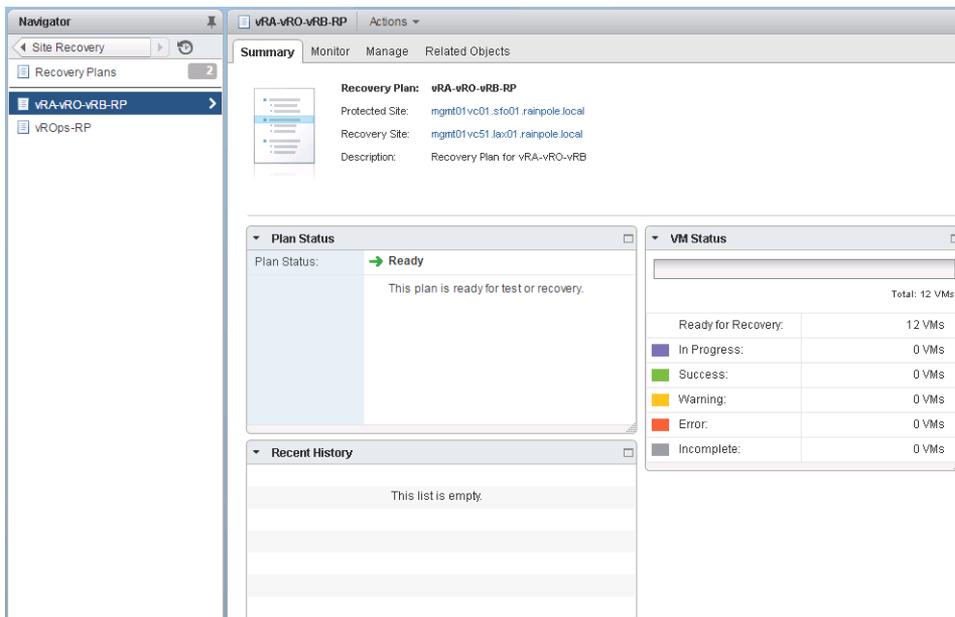
- a From the **Home** menu, select **Site Recovery**.
- b In the **Navigator**, click **Protection Groups**.
- c Under **Protection Groups**, click the **vRA-vRO-vRB-PG** protection group and click the **Summary** tab.

- d Verify that the protection status is **OK** and the replication shows no error or warning message.
- e Repeat the steps for the vROps-PG protection group.



**10** Verify that the recovery plan is intact.

- a From the **Home** menu, select **Site Recovery**.
- b In the **Navigator**, click **Recovery Groups**.
- c Under **Recovery Groups**, click the **vRA-vRO-vRB-RP** recovery plan and click the **Summary** tab.
- d Verify that the plan status is Ready and **VM Status** shows no error or warning message.
- e Repeat the steps for the vROps-RP recovery plan.



# Validate the vSphere Replication



After a maintenance such as an update or upgrade, validate the vSphere Replication to make sure it works as expected.

## Verify the Version and Service Status of vSphere Replication

After you patch or update the vSphere Replication appliances mgmt01vrms01 and mgmt01vrms51, verify the version, the service status and the configuration of each of them.

### Network Parameters for the vSphere Replication Appliances

vSphere Replication	Appliance Management Console URL	IP Address	FQDN
vSphere Replication Appliance A	https://mgmt01vrms01.sfo01.rainpole.local:5480	172.16.11.123	mgmt01vrms01.sfo01.rainpole.local
vSphere Replication Appliance B	https://mgmt01vrms51.lax01.rainpole.local:5480	172.17.11.123	mgmt01vrms51.lax01.rainpole.local

### Procedure

- 1 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	<i>vr_sfo_root_password</i>

- c Verify that authentication is successful.
- 2 If you have performed a patch or update, verify the version of the vSphere Replication appliance.
    - a In the appliance management console, click the **Update** tab and click the **Status** tab.
    - b Verify that the Appliance Version property shows the target appliance version.

- 3 Verify the configuration and service status of the vRealize Automation appliance.
  - a In the appliance management console, click the **VR** tab and click the **Configuration** tab.
  - b Under **Startup Configuration**, verify the following configurations.

Configuration	mgmt01vrms01.sfo01.rainpole.local	mgmt01vrms51.lax01.rainpole.local
Configuration Mode	Configure using the embedded database	Configure using the embedded database
Lookup Service Address	mgmt01psc01.sfo01.rainpole.local	mgmt01psc51.lax01.rainpole.local
SSO Administrator	administrator@vsphere.local	administrator@vsphere.local
VRM Host	172.16.11.123	172.16.11.123
VRM Site Name	mgmt01vc01.sfo01.rainpole.local	mgmt01vc51.lax01.rainpole.local
vCenter Server Address	mgmt01vc01.sfo01.rainpole.local	mgmt01vc51.lax01.rainpole.local
vCenter Server Admin Mail	<i>vcenter_server_admin_email</i>	<i>vcenter_server_admin_email</i>
IP Address for Incoming Storage Traffic	172.16.16.71	172.17.16.71

- c Under **Service Status**, verify that the status shows VRM service is running.

The screenshot shows the vSphere Replication Appliance configuration interface. The 'Startup Configuration' section is active, displaying various configuration fields. The 'Configuration Mode' is set to 'Configure using the embedded database'. The 'LookupService Address' is 'mgmt01psc01.sfo01.rainpole.local'. The 'SSO Administrator' is 'Administrator@vsphere.local'. The 'VRM Host' is '172.16.11.123'. The 'VRM Site Name' is 'mgmt01vc01.sfo01.rainpole.local'. The 'vCenter Server Address' is 'mgmt01vc01.sfo01.rainpole.local'. The 'vCenter Server Port' is '80'. The 'vCenter Server Admin Mail' is 'root@172.16.11.123'. The 'IP Address for Incoming Storage Traffic' is '172.16.16.71'. The 'Service Status' section shows 'VRM service is running' with a 'Restart' button.

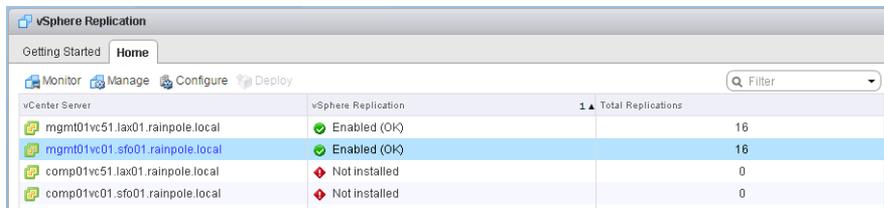
- 4 Repeat the step for other appliance mgmt01vrms51.lax01.rainpole.local to verify the version and configuration status.

- 5 Verify that vSphere Replication status is enabled for mgmt01vc01.sfo01.rainpole.local and mgmt01vc51.lax01.rainpole.local.

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

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- From the **Home** menu, select **vSphere Replication**.
- Under **vSphere Replication**, click **Home**.
- Verify that vSphere Replication status is Enabled for mgmt01vc01.sfo01.rainpole.local and mgmt01vc51.lax01.rainpole.local.



vCenter Server	vSphere Replication	Total Replications
mgmt01vc51.lax01.rainpole.local	Enabled (OK)	16
mgmt01vc01.sfo01.rainpole.local	Enabled (OK)	16
comp01vc51.lax01.rainpole.local	Not installed	0
comp01vc01.sfo01.rainpole.local	Not installed	0

- 6 Verify the Availability status, Version, Build number Target Sites and Replication Servers of the vSphere Replication appliance in vSphere Web Client.

- Under **vSphere Replication**, click the **Home** tab.
- Select **mgmt01vc01.sfo01.rainpole.local** vCenter server and click **Manage**.
- Click the **vSphere Replication** tab, verify that status of Availability is **OK** in About section .
- Also verify that Version and Build number of vSphere Replication are correct.
- Select Target Sites and verify that status of target site is Connected.
- Select **Replication Servers** and verify that status of vSphere Replication (Embedded) is Connected.
- Repeat the procedure for the mgmt01vc51.lax01.rainpole.local vCenter Server .

- 7 Verify the replication status for the mgmt01vc01.sfo01.rainpole.local site.

- From the **Home** menu, select **vSphere Replication**.
- On the **Home** tab, select the **mgmt01vc01.sfo01.rainpole.local** vCenter server and click **Monitor**.
- On the **vSphere Replication** tab, click **Outgoing Replications**.

- d Verify that the replication status is OK for vRealize Operations Manager and Cloud Management Platform VMs when replication happens from the **mgmt01vc01.sfo01.rainpole.local** site to **mgmt01vc51.lax01.rainpole.local** site.
  - e Click the **vSphere Replication** tab and click **Incoming Replications**.
  - f Verify that the replication status is OK for vRealize Operations Manager and Cloud Management Platform VMs when replication happens from the **mgmt01vc51.lax01.rainpole.local** to **mgmt01vc01.sfo01.rainpole.local** site.
- 8 Verify the replication status for the **mgmt01vc51.lax01.rainpole.local** site.
- a From the **Home** menu, select **vSphere Replication**.
  - b On the **Home** tab, select the **mgmt01vc51.lax01.rainpole.local** vCenter server and click **Monitor**.
  - c On the **vSphere Replication** tab, click **Outgoing Replications**.
  - d Verify that the replication status is OK for vRealize Operations Manager and Cloud Management Platform VMs when replication happens from the **mgmt01vc51.lax01.rainpole.local** site to **mgmt01vc01.sfo01.rainpole.local** site.
  - e Click the **vSphere Replication** tab and click **Incoming Replications**.
  - f Verify that the replication status is OK for vRealize Operations Manager and Cloud Management Platform VMs when replication happens from the **mgmt01vc01.sfo01.rainpole.local** to **mgmt01vc51.lax01.rainpole.local** site.

# SDDC Startup and Shutdown

When you restore or configure failover of the SDDC management applications, make sure that you start up and shut down the management virtual machines according to a predefined order.

- **Shutdown Order of the Management Virtual Machines**

Shut down the virtual machines of the SDDC management stack by following a strict order to avoid data loss and faults in the applications when you restore them.

- **Startup Order of the Management Virtual Machines**

Start up the virtual machines of the SDDC management stack by following a strict order to guarantee the faultless operation of and the integration between the applications.

## Shutdown Order of the Management Virtual Machines

Shut down the virtual machines of the SDDC management stack by following a strict order to avoid data loss and faults in the applications when you restore them.

Ensure that the console of the VM and its services are fully shut down before moving to the next VM.

Virtual Machine in Region A	Virtual Machine in Region B	Shutdown Order
<b>vSphere Data Protection</b>	<b>vSphere Data Protection</b>	<b>1</b>
<b>Total Number of VMs (1)</b>	<b>Total Number of VMs (1)</b>	
mgmt01vdp01	mgmt01vdp51	1
<b>vRealize Log Insight</b>	<b>vRealize Log Insight</b>	<b>1</b>
<b>Total Number of VMs (3)</b>	<b>Total Number of VMs (3)</b>	
vrli-wrkr-02	vrli-wrkr-52	1
vrli-wrkr-01	vrli-wrkr-51	1
vrli-mstr-01	vrli-mstr-51	2
<b>vRealize Operations Manager</b>	<b>vRealize Operations Manager</b>	<b>1</b>
<b>Total Number of VMs (5)</b>	<b>Total Number of VMs (2)</b>	
vrops-rmtcol-02	vrops-rmtcol-52	1
vrops-rmtcol-01	vrops-rmtcol-51	1
vrops-datan-03	-	2
vrops-repln-02	-	3

Virtual Machine in Region A	Virtual Machine in Region B	Shutdown Order
vrops-mstrn-01	-	4
<b>vRealize Business</b>	<b>Realize Business</b>	<b>2</b>
<b>Total Number of VMs (2)</b>	<b>Total Number of VMs (2)</b>	
vra01buc01.sfo01.rainpole.local	vra01buc51.lax01.rainpole.local	1
vra01bus01.rainpole.local	-	2
<b>vRealize Automation</b>	<b>vRealize Automation</b>	<b>3</b>
<b>Total Number of VMs (13)</b>	<b>Total Number of VMs (2)</b>	
vra01dem01.rainpole.local	-	1
vra01dem02.rainpole.local	-	1
vra01ias02.sfo01.rainpole.local	vra01ias52.lax01.rainpole.local	1
vra01ias01.sfo01.rainpole.local	vra01ias51.lax01.rainpole.local	1
vra01ims01b.rainpole.local	-	2
vra01ims01a.rainpole.local	-	2
vra01iws01b.rainpole.local	-	3
vra01iws01a.rainpole.local	-	4
vra01svr01b.rainpole.local	-	5
vra01svr01a.rainpole.local	-	5
vra01vro01b.rainpole.local	-	6
vra01vro01a.rainpole.local	-	6
vra01mssql01.rainpole.local	-	7
<b>Site Recovery Manager</b>	<b>Site Recovery Manager</b>	<b>4</b>
<b>Total Number of VMs (2)</b>	<b>Total Number of VMs (2)</b>	
mgmt01vrms01	mgmt01vrms51	1
mgmt01srm01	mgmt01srm51	2
<b>vSphere Update Manager Download Service (UMDS)</b>	<b>vSphere Update Manager Download Service (UMDS)</b>	<b>4</b>
<b>Total Number of VMs (1)</b>	<b>Total Number of VMs (1)</b>	
mgmt01umds01.sfo01.rainpole.local	mgmt01umds51.lax01.rainpole.local	1
<b>Core Stack</b>	<b>Core Stack</b>	<b>5</b>
<b>Total Number of VMs (21)</b>	<b>Total Number of VMs (13)</b>	
SFOMGMT-LB01 (0,1)	LAXMGMT-LB01 (0,1)	1
SFOMGMT-UDLR01 (0,1)	-	1
SFOMGMT-ESG01	LAXMGMT-ESG01	1
SFOMGMT-ESG02	LAXMGMT-ESG02	1
SFOCOMP-UDLR01 (0,1)	-	1
SFOCOMP-DLR01 (0,1)	LAXCOMP-DLR01(0,1)	1

Virtual Machine in Region A	Virtual Machine in Region B	Shutdown Order
SFOCOMP-ESG01	LAXCOMP-ESG01	1
SFOCOMP-ESG02	LAXCOMP-ESG02	1
mgmt01nsxm01	mgmt01nsxm51	2
comp01nsxm01	comp01nsxm51	2
NSX_Controller_0-Mgmt	-	3
NSX_Controller_1-Mgmt	-	3
NSX_Controller_2-Mgmt	-	3
NSX_Controller_0-Comp	-	3
NSX_Controller_1-Comp	-	3
NSX_Controller_2-Comp	-	3
mgmt01vc01	mgmt01vc51	4
comp01vc01	comp01vc51	4
SFO01PSC01	LAX01PSC51	5
comp01psc01	comp01psc51	6
mgmt01psc01	mgmt01psc51	6

## Startup Order of the Management Virtual Machines

Start up the virtual machines of the SDDC management stack by following a strict order to guarantee the faultless operation of and the integration between the applications.

Before you begin, verify that external dependencies for your SDDC, such as Active Directory, DNS, and NTP are available.

Ensure that the console of the VM and its services are all up before moving to the next VM.

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
<b>Core Stack Total Number of VMs (21)</b>	<b>Core Stack Total Number of VMs (13)</b>	<b>1</b>
mgmt01psc01	mgmt01psc51	1
comp01psc01	comp01psc51	1
SFO01PSC01	LAX01PSC51	2
mgmt01vc01	mgmt01vc51	3
comp01vc01	comp01vc51	3
mgmt01nsxm01	mgmt01nsxm51	4
comp01nsxm01	comp01nsxm51	4
NSX_Controller_0-Mgmt	-	5
NSX_Controller_1-Mgmt	-	5
NSX_Controller_2-Mgmt	-	5

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
NSX_Controller_0-Comp	-	5
NSX_Controller_1-Comp	-	5
NSX_Controller_2-Comp	-	5
SFOMGMT-LB01 (0,1)	LAXMGMT-LB01 (0,1)	6
SFOMGMT-UDLR01 (0,1)	-	6
SFOMGMT-ESG01	LAXMGMT-ESG01	6
SFOMGMT-ESG02	LAXMGMT-ESG02	6
SFOCOMP-UDLR01 (0,1)	-	6
SFOCOMP-DLR01 (0,1)	LAXCOMP-DLR01(0,1)	6
SFOCOMP-ESG01	LAXCOMP-ESG01	6
SFOCOMP-ESG02	LAXCOMP-ESG02	6
<b>vSphere Update Manager Download Service (UMDS) Total Number of VMs (1)</b>	<b>vSphere Update Manager Download Service (UMDS) Total Number of VMs (1)</b>	<b>2</b>
mgmt01umds01.sfo01.rainpole.local	mgmt01umds51.lax01.rainpole.local	1
<b>Site Recovery Manager Total Number of VMs (2)</b>	<b>Site Recovery Manager Total Number of VMs (2)</b>	<b>2</b>
mgmt01vrms01	mgmt01vrms51	1
mgmt01srm01	mgmt01srm51	1
<b>vRealize Automation Total Number of VMs (13)</b>	<b>vRealize Automation Total Number of VMs (2)</b>	<b>3</b>
vra01mssql01.rainpole.local	-	1
vra01vro01a.rainpole.local	-	2
vra01vro01b.rainpole.local	-	2
vra01svr01a.rainpole.local	-	3
vra01svr01b.rainpole.local	-	3
vra01iws01a.rainpole.local	-	4
vra01iws01b.rainpole.local	-	5
vra01ims01a.rainpole.local	-	6
vra01ims01b.rainpole.local	-	6
vra01ias01.sfo01.rainpole.local	vra01ias51.lax01.rainpole.local	7
vra01ias02.sfo01.rainpole.local	vra01ias52.lax01.rainpole.local	7
vra01dem01.rainpole.local	-	7
vra01dem02.rainpole.local	-	7
<b>vRealize Business Total Number of VMs (2)</b>	<b>vRealize Business Total Number of VMs (1)</b>	<b>4</b>
vra01bus01.rainpole.local	-	1
vra01buc01.sfo01.rainpole.local	vra01buc51.lax01.rainpole.local	2
<b>vRealize Operations Manager Total Number of VMs (5)</b>	<b>vRealize Operations Manager Total Number of VMs (2)</b>	<b>5</b>

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
vrops-mstrn-01	-	1
vrops-repln-02	-	2
vrops-datan-03	-	3
vrops-rmtcol-01	vrops-rmtcol-51	4
vrops-rmtcol-02	vrops-rmtcol-52	4
<b>vRealize Log Insight Total Number of VMs (3)</b>	<b>vRealize Log Insight Total Number of VMs (3)</b>	<b>5</b>
vrli-mstr-01	vrli-mstr-51	1
vrli-wrkr-01	vrli-wrkr-51	2
vrli-wrkr-02	vrli-wrkr-52	2
<b>vSphere Data Protection Total Number of VMs (1)</b>	<b>vSphere Data Protection Total Number of VMs (1)</b>	<b>5</b>
mgmt01vdp01	mgmt01vdp51	1