Operational Verification

26 SEP 2017
VMware Validated Design 4.1
VMware Validated Design for Software-Defined Data Center 4.1

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About VMware Validated Design Operational Verification

The VMware Validated Design Operational Verification document provides step-by-step instructions for verifying that the management components in the Software-Defined Data Center (SDDC) that are 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 SDDC, verifying whether these components are running without any faults ensures continuous operation of the environment. You should verify the operation of the SDDC using this guide after patching, updating, upgrading, restoring and recovering the SDDC management components.

Intended Audience

The *VMware Validated Design Operational Verification* document is intended for cloud architects, infrastructure administrators, cloud administrators and cloud operators who are familiar with and want to use VMware software to manage an SDDC that meets the requirements for capacity, scalability, backup and restore, and extensibility for disaster recovery support.

Required Software

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

Validate vSphere

1

After you perform any type of maintenance in your environment, in each region, you should perform validation steps to verify the operational status of the Platform Services Controller and vCenter Server Appliance instances, ESXi hosts and vSphere Update Manager Download Service virtual machine.

A maintenance operation could be restore, patch, upgrade, failover or failback.

Procedure

1 Verify the Platform Services Controller Instances

   Validate the operational status of the Platform Services Controllers in Region A and Region B after you perform a software maintenance operation in the SDDC.

2 Verify the vCenter Server Instances

   Validate the operational status of the vCenter Server instances in Region A and Region B after you perform a software maintenance operation in the SDDC.

3 Verify the ESXi Hosts

   Validate the operational status of each ESXi hosts in region A and region B after you perform a software maintenance operation in the SDDC.

4 Verify the Status of the vSphere Update Manager Download Service

   Validate the operational status of vSphere Update Manager Download Service in Region A and Region B after you perform a software maintenance in the SDDC.

Verify the Platform Services Controller Instances

Validate the operational status of the Platform Services Controllers in Region A and Region B after you perform a software maintenance operation in the SDDC.

Perform the following verification tasks against each Platform Services Controller instance:

- Health Status
- Version
- Authentication (Active Directory connectivity and identity sources)
- Certificate
- Services

Table 1-1. URLs and FQDNs of the Platform Services Controller Instances

Setting	Cluster	Region A	Region B
FQDN	Management	sfo01m01psc01.sfo01.rainpole.local	lax01m01psc01.lax01.rainpole.local
	Shared edge and compute	sfo01w01psc01.sfo01.rainpole.local	lax01w01psc01.lax01.rainpole.local
VAMI	Management	https://sfo01m01psc01.sfo01.rainpole.local:5480	https://lax01m01psc01.lax01.rainpole.local:5480
	Shared edge and compute	https://sfo01w01psc01.sfo01.rainpole.local:5480	https://lax01w01psc01.lax01.rainpole.local:5480
Administration UI	Management	https://sfo01m01psc01.sfo01.rainpole.local/psc	https://lax01m01psc01.lax01.rainpole.local/psc
	Shared edge and compute	https://sfo01w01psc01.sfo01.rainpole.local/psc	https://lax01w01psc01.lax01.rainpole.local/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://sfo01m01psc01.sfo01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtpsc_root_password*

2 Verify the Health Status and the Single Sign-On status for this Platform Services Controller.

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

   b On the **Summary** page, under **Health Status**, verify the following states.

Setting	Value
Overall Health	Good
CPU	Good
Memory	Good

   c On the **Summary** page, under **Single Sign-On**, verify the following state.

Setting	Value
Status	Running

3 Verify the version of the Platform Services Controller.

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

b On the **Update** page, under **Current version details**, verify the following details are correct.

Setting	Value
Vendor	VMware, Inc.
Appliance Name	VMware vCenter Server Appliance
Update Version	*vcenter_appliance_version*
Description	VMware Platform Services Controller

4 Log in to the Platform Services Controller administration interface.

a Open a Web browser and go to **`https://sfo01m01psc01.sfo01.rainpole.local/psc`**.

b Log in using the following credentials.

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

5 Verify the connection status between the Active Directory and the Platform Services Controller.

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

b On the **Manage** page, under **Active Directory**, verify that following details are correct.

Setting	Value
Domain	SFO01.RAINPOLE.LOCAL
Organizational Unit	-

6 Verify the identity sources for the Platform Services Controller.

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

b On the **Identity Sources** page, verify the following identity sources are listed.

Type	Domain
-	vsphere.local
Local OS	localos
Active Directory (Integrated Windows Authentication)	rainpole.local (default)

7 Verify the certificate of the Platform Services Controller.

a In the **Navigator**, click **Certificate Store**.

b On the **Certificate Store** page, select **__MACHINE_CERT** from**Store**.

c Select **__MACHINE_CERT** from the list, click **Show Details** and verify that the following details are correct.

Setting	Value
Issued By	*certificate_authority*
Status	The certificate is valid
Signature Algorithm	SHA256withRSA

8 Verify that all Platform Services Controller services are available and running.

a Open an SSH connection to the virtual machine **`sfo01m01psc01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtpsc_root_password*

c Run the following command and verify the status of services.

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

d Verify the output as follows:

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

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

Verify the vCenter Server Instances

Validate the operational status of the vCenter Server instances in Region A and Region B after you perform a software maintenance operation in the SDDC.

Perform the following verification tasks against each vCenter Server instance:

- Health Status
- Version
- Services
- Platform Services Controller connectivity

- vSphere vMotion
- vSAN Health
- Proactive Test on vSAN
- Certificate

Start with the Management vCenter Server in Region A.

Table 1-2. URLs and FQDNs of thevCenter Server Instances

Setting	Cluster	Region A	Region B
FQDN	Management	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
	Shared edge and compute	sfo01w01vc01.sfo01.rainpole.local	lax01w01vc01.lax01.rainpole.local
VAMI	Management	https://sfo01m01vc01.sfo01.rainpole.local:5480	https://lax01m01vc01.lax01.rainpole.local:5480
	Shared edge and compute	https://sfo01w01vc01.sfo01.rainpole.local:5480	https://lax01w01vc01.lax01.rainpole.local:5480
vSphere Web Client	Management	https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client	https://lax01m01vc01.lax01.rainpole.local/vsphere-client
	Shared edge and compute	https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client	https://lax01w01vc01.lax01.rainpole.local/vsphere-client

Procedure

1 Log in to the management interface of the vCenter Server Appliance.

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local:5480`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtvc_root_password*

2 Verify the Health Status for this vCenter Server.

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

b On the **Summary** page, under **Health Status**, verify the following states.

Setting	Value
Overall Health	Good
CPU	Good
Memory	Good
Database	Good

3 Verify the version of the vCenter Server instance.

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

b On the **Update** page, under **Current version details**, verify that the following details are correct.

Setting	Value
Vendor	VMware, Inc.
Appliance Name	VMware vCenter Server Appliance
Update Version	*vcenter_appliance_version*
Description	vCenter Server with an external Platform Services Controller

4 Verify that all vCenter Server services are available and running.

a Open an SSH connection to the virtual machine **`sfo01m01vc01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtvc_root_password*

c Run the following command and verify the status of services.

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

d Verify the output as follows.

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

5 Verify the connection between the vCenter Server instances and the Platform Services Controller pairs by using the vSphere Web Client.

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

b Log in using the following credentials.

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

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 vSphere vMotion functionality.

a In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01-mgmt01** inventory tree.

b Right-click the **sfo01m01esx01.sfo01.rainpole.local** host and select **Maintenance Mode > Enter Maintenance Mode**.

c On the **Confirm Maintenance Mode** dialog, accept the default options and click **OK**.

d On the **Warning** dialog, click **OK**.

e Verify that the VMs from the host are migrated to the another host in the cluster and the host is placed in maintenance mode.

f Right-click the **sfo01m01esx01.sfo01.rainpole.local** host and select **Maintenance Mode > Exit Maintenance Mode**.

g Repeat the steps for the each host in the cluster and then for other clusters in the environment.

7 Verify the health of vSAN.

a In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc** tree and select the **sfo01-m01-mgmt01** cluster.

b Click the **Monitor** tab, click **vSAN** and select **Health.**

c Verify the status of vSAN Health.

Expected Result	Test Name
Warning	Hardware compatibility
Warning	Online health
Passed	Network
Passed	Physical disk
Passed	Data
Passed	Cluster
Passed	Limits
Passed	Performance service
Passed	vSAN Build Recommendation

8 Perform a proactive test on vSAN.

a Click the **Monitor** tab for the sfo01-m01-mgmt01 cluster and click the **vSAN** tab.

b Click **Proactive Tests** and select **VM creation test**.

c Click the **Run Test Now** icon and click **Yes** in the **Run VM creation test** dialog box to confirm running the task.

d After the test completes, verify that the **Last Run Results** has a status of `Passed`.

9 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.

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

Verify the ESXi Hosts

Validate the operational status of each ESXi hosts in region A and region B after you perform a software maintenance operation in the SDDC.

Verify the following settings against each ESXi host:

- Version and state
- NTP
- License
- Services
- Security
- Active Directory configuration
- Hardware

Table 1-3. ESXi Host Instances

Cluster	Region A	Region B
Management cluster	sfo01m01esx01.sfo01.rainpole.local	lax01m01esx01.lax01.rainpole.local
	sfo01m01esx02.sfo01.rainpole.local	lax01m01esx02.lax01.rainpole.local
	sfo01m01esx03.sfo01.rainpole.local	lax01m01esx03.lax01.rainpole.local
	sfo01m01esx04.sfo01.rainpole.local	lax01m01esx04.lax01.rainpole.local
Shared edge and compute cluster	sfo01w01esx01.sfo01.rainpole.local	lax01w01esx01.lax01.rainpole.local
	sfo01w01esx02.sfo01.rainpole.local	lax01w01esx02.lax01.rainpole.local
	sfo01w01esx03.sfo01.rainpole.local	lax01w01esx03.lax01.rainpole.local
	sfo01w01esx04.sfo01.rainpole.local	lax01w01esx04.lax01.rainpole.local

Procedure

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

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

b Log in using the following credentials.

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

2 Navigate to the ESXi host.

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

b In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01-mgmt01** inventory tree.

c Click the **sfo01m01esx01.sfo01.rainpole.local** host.

3 On the **Summary** tab, verify the state, version, and build number of the ESXi host.

Setting	Value
Hypervisor	*esx_version*
State	Connected

4 On the **Configure** tab, under **System**, click **Time configuration** and verify the NTP status.

Setting	Value
NTP Client	Enabled
NTP Service Status	Running
NTP Servers	ntp.sfo01.rainpole.local, ntp.lax01.rainpole.local

5 On the **Configure** tab, under **System**, click **Licensing** and verify that the license is valid.

6 Verify the status of services.

a On the **Configure** tab, under **System**, click **Security Profile**.

b On the **Security Profile** page, under **Services**, click the **Deamon** column to sort in ascending order.

c Verify the status of the following services.

Description	Status
NTP Daemon	`Running`
ESXi Shell	`Running`
SSH	`Running`
Load-Based Teaming Daemon	`Running`
Active Directory Service	`Running`
VMware vCenter Agent	`Running`
Direct Console UI	`Running`
Syslog Server	`Running`
vSphere High Availability Agent	`Running`
SNMP Server	`Stopped`
CIM Server	`Stopped`
PC/SC Smart Card Daemon	`Stopped`
X.Org Server	`Stopped`

7 On the **Security Profile** page, under **Lockdown Mode**, verify that the **Lockdown Mode** is set to `Enabled (Normal)`.

Verifies that the ESXi hosts have security hardening applied.

8 On the **Security Profile** page, under **Host Image Profile Acceptance Level**, verify that the **Acceptance Level** is set to `Partner Supported`.

9 Verify the authentication services.

a On the **Configure** tab, under **System**, click **Authentication Services**.

b Under **Directory Services Configuration**, ensure that the **Directory Service Type** is set to `Active Directory`.

c Under **Domain Settings**, verify the following details.

Setting	Value
Domain	SFO01.RAINPOLE.LOCAL
Trusted Domain Controllers	rainpole.local lax01.rainpole.local

10 Verify the status of system sensors to ensure there are no hardware failures.

   a Click the **Monitor** tab and click the **Hardware Status** tab.

   b On the **Sensors** page, click the **Expand All** icon and ensure that all of the hardware sensors on the ESXi host in the **Status** column have a status `Normal`.

11 Repeat the steps for all the remaining ESXi hosts across all vCenter Server instances.

Verify the Status of the vSphere Update Manager Download Service

Validate the operational status of vSphere Update Manager Download Service in Region A and Region B after you perform a software maintenance in the SDDC.

Perform the following verification tasks against each vSphere Update Manager Download Service (UMDS) virtual machine:

- Version
- Service Status
- Cron Job
- vCenter Configuration

Table 1-4. PropertyVerification for UMDS

Setting	Region A	Region B
Management vCenter Server FQDN	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
Compute vCenter Server FQDN	sfo01w01vc01.sfo01.rainpole.local	lax01w01vc01.lax01.rainpole.local
UMDS FQDN	sfo01umds01.sfo.rainpole.local	lax01umds01.lax01.rainpole.local
UMDS URL	http://sfo01umds01.sfo01.rainpole.local	http://lax01umds01.lax01.rainpole.local

Procedure

1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.

   a Open an SSH connection to **`sfo01umds01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User Name	svc-umds
Password	*svc-umds_password*

2 Verify the version of ngnix and postgresql.

a Run the following commands and verify the correct version is returned.

```
nginx –v
psql –V
```

3 Verify the status of the nginx and postgresql services.

a Run the following commands and verify that the services are running.

```
service nginx status
service postgresql status
```

4 Verify the cron job.

a Run the following commands.

```
cd /etc/cron.daily/
sudo ./umds-download
```

5 Verify the vCenter Server configuration with the UMDS service.

a From the **Home** menu, select **Update Manager**.

b In the **Navigator**, under **Servers** select **sfo01m01vc01.sfo01.rainpole.local**.

c On the **sfo01m01vc01.sfo01.rainpole.local** page, click the **Manage** tab.

d On the **Settings** tab, click **Download Settings**.

e Under **Download sources**, verify that the **Download source** is configured with `http://sfo01umds01.sfo01.rainpole.local` .

f Repeat the steps for each vCenter server.

Validate the Cloud Management Platform

2

After you perform any type of maintenance in your environment, you should perform validation steps to verify the operational status of the Cloud Management Platform (vRealize Automation and vRealize Business for Cloud components) and make sure they work as expected.

Procedure

1 Verify the Power Status and IP Address of All Cloud Management Platform VMs

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

2 Verify the Version and Service Status of the vRealize Automation Virtual Appliances

Validate the operational status of the vRealize Automation instances after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

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

Validate the operational status of the vRealize Automation IaaS Web Server and the IaaS Manager Service nodes after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

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

Validate the operational status of the vRealize Automation Windows nodes after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

5 Verify the Service Status and Authentication Configuration of vRealize Orchestrator

Validate the operational status of vRealize Orchestrator running on the vRealize Automation appliances after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

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

Validate the operational status of the vRealize Automation IaaS Distributed Execution Manager (DEM) and IaaS vSphere Proxy Agents components after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

7 Verify the vRealize Automation Integration with Active Directory

Verify that vRealize Automation is connected to the Active Directory domain after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

8 Verify the Version and Service Status of the vRealize Business VMs

Validate the operational status of the vRealize Business for Cloud instances after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

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

Verify the Cloud Management Platform load balancer after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

Verify the Power Status and IP Address of All Cloud Management Platform VMs

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

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	`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`
Region B	`https://lax01m01vc01.lax01.rainpole.local/vsphere-client`

b Log in using the following credentials.

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

2 Verify that all virtual machines of vRealize Automation and vRealize Business for Cloud are powered on, and have FQDNs and IP addresses assigned according to the design.

a From the **Home** menu, select **VMs and Templates**.

b In the **Navigator**, click **sfo01m01vc01.sfo01.rainpole.local** and click the **VMs** tab .

c On the **Virtual Machines** page, right click the table header and click **Show/Hide Columns**.

d Select **IP Address** and click **OK**.

e Click the **Name** column to sort in ascending order.

f Select the following folder names, click the **VMs** tab and verify that the virtual machines are configured in the following way.

Table 2-1. VMs of the Cloud Management Platform inRegion A

vCenter Server	Folder Name	VM Name	IP Address
sfo01m01vc01.sfo01.rainpole.local	sfo01-m01fd-vra	vra01dem01a.rainpole.local	192.168.11.60
		vra01dem01b.rainpole.local	192.168.11.61
		vra01ims01a.rainpole.local	192.168.11.57
		vra01ims01b.rainpole.local	192.168.11.58
		vra01iws01a.rainpole.local	192.168.11.54
		vra01iws01b.rainpole.local	192.168.11.55
		vra01mssql01.rainpole.local	192.168.11.62
		vra01svr01a.rainpole.local	192.168.11.51
		vra01svr01b.rainpole.local	192.168.11.52
		vrb01svr01.rainpole.local	192.168.11.66
	sfo01-m01fd-vraias	sfo01ias01a.rainpole.local	192.168.31.52
		sfo01ias01b.rainpole.local	192.168.31.53
		sfo01vrbc01.rainpole.local	192.168.31.54

Table 2-2. VMs in the Cloud Management Platform inRegion B

vCenter Server	Folder Name	VM Name	IP Address
lax01m01vc01.lax01.rainpole.local	lax01-m01fd-vraias	lax01ias01a.rainpole.local	192.168.32.52
		lax01ias01b.rainpole.local	192.168.32.53
		lax01vrbc01.rainpole.local	192.168.32.54

Verify the Version and Service Status ofthevRealize Automation Virtual Appliances

Validate the operational status of the vRealize Automation instances after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

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

Perform the following verification tasks against each vRealize Automation instance:

- Version
- vCenter Single Sign-On status
- Licenses

- Database status
- Messaging status
- Cluster status
- Services

	vRealize Appliance A	vRealize Appliance B
FQDN	vra01svr01a.rainpole.local	vra01svr01b.rainpole.local
VAMI	https://vra01svr01a.rainpole.local:5480	https://vra01svr01b.rainpole.local:5480

Procedure

1 Log in to the management interface of the vRealize Automation Appliance.

   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*

2 Click the **Update** tab and under **Update Status** verify the Appliance Version.

Settings	Value
Vendor	VMware, Inc.
Appliance Name	VMware vRealize Appliance
Appliance Version	*vrealize_automation_appliance_version*

3 Click the **vRA Settings** tab, click **SSO**, and under **SSO Info**, verify that the status is `Configured – working connected`.

4 On the **vRA Settings** tab, click **Licensing** and for each license key verify that the **Expires** setting is `never`.

5 On the **vRA Settings** tab, click **Database**, and verify that the **Connection Status** shows `CONNECTED` and verify the Status of vRealize Automation Appliances.

Database node host	Mode	Status
vra01svr01a.rainpole.local	MASTER	Up
vra01svr01b.rainpole.local	REPLICA	Up

6 On the **vRA Settings** tab, click **Messaging** and verify the following details.

Setting	Value
Host	localhost
Port	5671

Setting	Value
Connection Status	CONNECTED
RabbitMQ Process	Running

7 On the **vRA Settings** tab, click **Cluster** and under **Distributed Deployment Information** verify that the status shows `Current node in cluster mode`.

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

9 Repeat the procedure for the other vRealize Appliance instance to verify their version and configuration status.

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

Validate the operational status of the vRealize Automation IaaS Web Server and the IaaS Manager Service nodes after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

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
- VM provisioning service (VMPS) of the IaaS Manager Service nodes

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

IaaS Nodes	FQDN	URL
IaaS Web Server Virtual IP (VIP)	vra01iws01.rainpole.local	https://vra01iws01.rainpole.local/WAPI/api/status
IaaS Web Server A	vra01iws01a.rainpole.local	https://vra01iws01a.rainpole.local/WAPI/api/status
IaaS Web Server B	vra01iws01b.rainpole.local	https://vra01iws01b.rainpole.local/WAPI/api/status
IaaS Manager Service Virtual IP (VIP)	vra01ims01.rainpole.local	https://vra01ims01.rainpole.local/VMPS
IaaS Manager Service A	vra01ims01a.rainpole.local	https://vra01ims01a.rainpole.local/VMPS
IaaS Manager Service B	vra01ims01b.rainpole.local	https://vra01ims01b.rainpole.local/VMPS

Procedure

1 Verify the Web Services API at the VIP address of the IaaS Web Server Nodes.

   a Open a Web browser and go to **`https://vra01iws01.rainpole.local/WAPI/api/status`**.

   b In the XML response verify the following.

```
<ServiceInitializationStatus>REGISTERED</ServiceInitializationStatus>
```

   c Repeat the steps for the individual IaaS Web Server nodes.

Node	URL
IaaS Web Server A	https://vra01iws01a.rainpole.local/WAPI/api/status
IaaS Web Server B	https://vra01iws01b.rainpole.local/WAPI/api/status

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 Open a Remote Desktop Protocol (RDP) connection to the virtual machine **`vra01iws01a.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	Administrator
Password	*local_administrator_pwd*

   c Open a command prompt and run the following command to stop the World Wide Web Publishing Services.

```
net stop w3svc
```

   d Open a Web browser and go to IaaS Web Server VIP address **`https://vra01iws01.rainpole.local/WAPI/api/status`** and verify that the service registry status page loads.

   e Back in the command prompt, run the following command to start the World Wide Web Publishing Services.

```
net start w3svc
```

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

3 Verify the VM provisioning service (VMPS) of the IaaS Manager Service nodes.

   a Open a Web browser and go to **`https://vra01ims01.rainpole.local/VMPS`**.

   b Verify that the **ProvisionService Service** page is returned.

   c Repeat the steps for vra01ims01a.rainpole.local.

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

Verify the Version and Service Status of vRealize Automation Windows Nodes

Validate the operational status of the vRealize Automation Windows nodes after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

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, vRealize Automation Proxy Agents and Microsoft SQL Server, for each of them verify the version and the service status of its components.

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

Table 2-3. Program Names and Services to Verify on the Windows Nodes of vRealize Automation in Region A

Role	FQDN	Program Names for Version Check	Services for Availability Check
IaaS Web Server	vra01iws01a.rainpole.local	■ VMware vCloud Automation Center Management Agent ■ VMware vCloud Automation Center Server ■ VMware vCloud Automation Center WAPI	VMware vCloud Automation Center Management Agent
IaaS Web Server	vra01iws01b.rainpole.local	■ VMware vCloud Automation Center Management Agent ■ VMware vCloud Automation Center Server ■ VMware vCloud Automation Center WAPI	VMware vCloud Automation Center Management Agent
IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local	■ VMware vCloud Automation Center DEM-Orchestrator - vra01ims01a.rainpole.local DEO ■ VMware vCloud Automation Center Management Agent ■ VMware vCloud Automation Center Server	■ VMware DEM-Orchestrator - vra01ims01a.rainpole.local DEO ■ VMware vCloud Automation Center Management Agent ■ VMware vCloud Automation Center Service

Table 2-3. Program Names and Services to Verify on the Windows Nodes of vRealize Automation in Region A (Continued)

Role	FQDN	Program Names for Version Check	Services for Availability Check
IaaS Manager Service and DEM Orchestrator	vra01ims01b.rainpole.local	■ VMware vCloud Automation Center DEM-Orchestrator - vra01ims01b.rainpole.local DEO ■ VMware vCloud Automation Center Management Agent ■ VMware vCloud Automation Center Server	■ VMware DEM-Orchestrator - vra01ims01b.rainpole.local DEO ■ VMware vCloud Automation Center Management Agent ■ VMware vCloud Automation Center Service
vRealize Automation DEM Worker	vra01dem01a.rainpole.local	■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-01 ■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-02 ■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-03 ■ VMware vCloud Automation Center Management Agent	■ VMware DEM-Worker - DEM-WORKER-01 ■ VMware DEM-Worker - DEM-WORKER-02 ■ VMware DEM-Worker - DEM-WORKER-03 ■ VMware vCloud Automation Center Management Agent
vRealize Automation DEM Worker	vra01dem01b.rainpole.local	■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-04 ■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-05 ■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-06 ■ VMware vCloud Automation Center Management Agent	■ VMware DEM-Worker - DEM-WORKER-04 ■ VMware DEM-Worker - DEM-WORKER-05 ■ VMware DEM-Worker - DEM-WORKER-06 ■ VMware vCloud Automation Center Management Agent
Microsoft SQL Server	vra01mssql01.rainpole.local	-	SQL Server (MSSQLSERVER)
vRealize Automation Proxy Agent	sfo01ias01a.sfo01.rainpole.local	■ VMware vCloud Automation Center Agents - vSphere-Agent-01 ■ VMware vCloud Automation Center Management Agent	■ VMware vCloud Automation Center Agent - vSphere-Agent-01 ■ VMware vCloud Automation Center Management Agent
vRealize Automation Proxy Agent	sfo01ias01b.sfo01.rainpole.local	■ VMware vCloud Automation Center Agents - vSphere-Agent-02 ■ VMware vCloud Automation Center Management Agent	■ VMware vCloud Automation Center Agent - vSphere-Agent-02 ■ VMware vCloud Automation Center Management Agent

Table 2-4. Program Names and Services to Verify on the Windows Nodes of vRealize Automation in Region B

Role	FQDN	Program Names for Version Check	Services for Availability Check
vRealize Automation Proxy Agent	lax01ias01a.lax01.rainpole.local	■ VMware vCloud Automation Center Agents - vSphere-Agent-51 ■ VMware vCloud Automation Center Management Agent	■ VMware vCloud Automation Center Agent - vSphere-Agent-51 ■ VMware vCloud Automation Center Management Agent
vRealize Automation Proxy Agent	lax01ias01b.lax01.rainpole.local	■ VMware vCloud Automation Center Agents - vSphere-Agent-52 ■ VMware vCloud Automation Center Management Agent	■ VMware vCloud Automation Center Agent - vSphere-Agent-52 ■ VMware vCloud Automation Center Management Agent

Procedure

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

   a Open a Remote Desktop Protocol (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 From the Windows **Start** menu, select **Control Panel > Programs and Features** and 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 From the Windows **Start** menu, select **Administrative Tools > Services** and verify the status and configuration of the VMware vCloud Automation Center Management Agent service.

Setting	Value
Name	VMware vCloud Automation Center Management Agent
Status	`Running`
Startup Type	Automatic
Logon As	RAINPOLE/svc-vra

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

Verify theServiceStatusand Authentication Configurationof vRealize Orchestrator

Validate the operational status of vRealize Orchestrator running on the vRealize Automation appliances after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

After you patch, update, restore, failover, or failback the vRealize Automation appliances, verify the service status and authentication configuration of vRealize Orchestrator.

Perform the following verification tasks against vRealize Orchestrator:

- Service Status
- Configuration
- Authentication

Procedure

1. Log in to the vRealize Orchestrator Control Center.
   a. Open a Web browser and go to **`https://vra01svr01a.rainpole.local:8283/vco-controlcenter`**.
   b. Log in using the following credentials.

Setting	Value
User name	svc-vra
Password	*svc_vra_password*
Domain	rainpole.local

2. On the **Home** page, under **Manage**, click **Startup Options** and verify that Current Status is `RUNNING`.
3. Under **Manage**, click **Validate Configuration** and verify that each system component configuration has a green check mark.
4. Verify that the authentication configuration is correct.
   a. 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`.
5. Repeat the steps for the **`vra01svr01b`** vRealize Automation appliance.

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

Validate the operational status of the vRealize Automation IaaS Distributed Execution Manager (DEM) and IaaS vSphere Proxy Agents components after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

After you patch, update, restore, failover, or failback vRealize Automation, verify that the IaaS 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	*itac-tenantadmin_password*
Domain	Rainpole.local

2 Click the **Infrastructure** tab, click **Monitoring > DEM Status** and verify that the status of the DEM-Orchestrator and DEM-Worker instances is as follows.

Name	Status	Virtual Machine	Role
DEM-WORKER-01	`Online`	vra01dem01a	Worker
DEM-WORKER-02	`Online`	vra01dem01a	Worker
DEM-WORKER-03	`Online`	vra01dem01a	Worker
DEM-WORKER-04	`Online`	vra01dem01b	Worker
DEM-WORKER-05	`Online`	vra01dem01b	Worker
DEM-WORKER-06	`Online`	vra01dem01b	Worker
vra01ims01a.rainpole.local DEO	`Online (Active)`	vra01ims01a	Orchestrator
vra01ims01b.rainpole.local DEO	`Online`	vra01ims01b	Orchestrator

3 Click **Compute Resources > Compute Resources** and verify that the Agent Status for the each 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 A	Region B
sfo01ias01a.sfo01.rainpole.local	lax01ias01a.lax01.rainpole.local
sfo01ias01b.sfo01.rainpole.local	lax01ias01b.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 vSphere Proxy Agent VM.

   f If another vSphere Proxy Agent VM is down, repeat these steps.

Verify thevRealize Automation Integration with Active Directory

Verify that vRealize Automation is connected to the Active Directory domain after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

After you patch, update, restore, failover, or failback the vRealize Automation appliances, 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	*itac-tenantadmin_password*
Domain	Rainpole.local

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

3 Click **Identity Providers** and verify the status of each provider is the following.

Identity Provider Name	Connector(s)	Type	Status
System Identity Provider	-	Built-in	Enabled
WorkspaceIDP__1	vra01svr01b.rainpole.local vra01svr01a.rainpole.local	Identity Manager	Enabled

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

Verify the Version and Service Status of the vRealize Business VMs

Validate the operational status of the vRealize Business for Cloud instances after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

After you patch, update, restore, failover, or failback the vRealize Business for Cloud appliances, verify the version, the service status and the configuration of each. Perform the following verification tasks against each vRealize Business instance:

- Version
- vCenter Single Sign-On
- Services
- Connection with Data Collectors
- Connection with vRealize Automation

Table 2-5. vRealize Business for Cloud Instances in Region A

	vRealize Business for Cloud Server	vRealize Business for Cloud Data Collector
FQDN	vrb01svr01.rainpole.local	sfo01vrbc01.sfo01.rainpole.local
VAMI	https://vrb01svr01.rainpole.local:5480	https://sfo01vrbc01.sfo01.rainpole.local:5480
Data Collector UI	-	sfo01vrbc01.sfo01.rainpole.local:9443/dc-ui

Table 2-6. vRealize Business for Cloud Instances in Region B

	vRealize Business for Cloud Data Collector
FQDN	lax01vrbc01.lax01.rainpole.local
VAMI	https://lax01vrbc01.lax01.rainpole.local:5480
Data Collector UI	lax01vrbc01.lax01.rainpole.local/dc-ui

Procedure

1 Log in to the management interface of the vRealize Business for Cloud virtual appliance.

   a Open a Web browser and go to **`https://vrb01svr01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

2 Click the **Registration** tab, click **vRA** and verify that the SSO Status is `Connected to vRealize Automation`.

   Only perform this step on the vRealize Business for Cloud Server.

3 Click the **Update** tab, click **Status** and verify the following details are correct.

Setting	Value
Vendor	VMware, Inc.
Appliance Name	vRealize Business for Cloud
Appliance Version	*vrealize_automation_appliance_version*

4 Verify the service status of the vRealize Business for Cloud Server.

a Open an SSH connection to **vrb01svr01.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
```

Service Name	Status	Type
vrb01svr01	OK	System
vami-lighttp	OK	Process
vrbc-xenon-services	OK	Process
postgres	OK	Process
mongo	OK	Process
facts-repo	OK	Process
pricing-api	OK	Process
itbm-server	OK	Process
itbm-data-collector	OK	Process
rootfs	OK	Filesystem

5 Verify the service status of the vRealize Business for Cloud Data Collectors.

a Open an SSH connection to **sfo01vrbc01.sfo01.rainpole.local**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_collector_root_password*

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

```
monit summary
```

Service Name	Status	Type
sfo01vrbc01.sfo01.rainpole.l...	OK	System
vami-lighttp	OK	Process
vrbc-xenon-services	OK	Process
itbm-data-collector	OK	Process
rootfs	OK	Filesystem

d Repeat the steps for **`lax01vrbc01.lax01.rainpole.local`**.

For one of the data collectors, the process `itbm-data-collector` appears as `Not monitored`.

6 Verify the connection between vRealize Business for Cloud Data Collector and Compute vCenter Server.

a Open a Web browser and go to **`https://sfo01vrbc01.sfo01.rainpole.local:9443/dc-ui`**.

b Log in using the following credentials.

Setting	Value
Username	root
Password	*vrb_server_root_password*

c Click **Manage Private Cloud Connections > vCenter Server**, and verify that the `sfo01w01vc01.sfo01.rainpole.local` is listed in the vCenter Server Connections table.

d Repeat the steps for **`lax01vrbc01.lax01.rainpole.local`**

7 Log in to the vRealize Automation Rainpole portal.

a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	*itac-tenantadmin_password*
Domain	Rainpole.local

8 Verify the connection between the vRealize Business Server and the vRealize Business Data Collectors.

   a Click the **Administration** tab and click **Business Management**.

   b On the **Business Management** page, expand **Manage Data Collector > Manage Virtual Appliances**.

   c Verify that the `sfo01vrbc01.sfo01.rainpole.local` and `lax01vrbc01.lax01.rainpole.local` appliances are listed in the **Manage Virtual Appliances** table.

9 Verify that vRealize Business for Cloud collects information from all vCenter Server instances.

   a Click **Business Management**.

   b On the **Business Management** page, click the **Status** link.

   c On the **System Status** page, under **vCenter data collection**, click **Update now**.

   d Verify that a green sign appears next to all vCenter Server Instances in the table.

10 Verify the reports of vCenter server inventory items.

   a Click **Business Management**.

   b In the **Navigator**, select **Reports**.

   c On the **Reports** page, under Infrastructure - vCenter select vCenter List and verify that all vCenter Server and ESXi hosts are listed as follows:

Table 2-7.

Server Name	vCenter Server Alias	Data Center Name
sfo01w01esx01.sfo01.rainpole.local	sfo01w01vc01.sfo01.rainpole.local	sfo01-w01dc
sfo01w01esx02.sfo01.rainpole.local		
sfo01w01esx03.sfo01.rainpole.local		
sfo01w01esx04.sfo01.rainpole.local		
lax01w01esx01.lax01.rainpole.local	lax01w01vc01.lax01.rainpole.local	lax01-w01dc
lax01w01esx02.lax01.rainpole.local		
lax01w01esx03.lax01.rainpole.local		
lax01w01esx04.lax01.rainpole.local		

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	*itac-tenantadmin_password*
Domain	Rainpole.local

2 Click the **Catalog** tab, click **LAX Service Catalog** and verify that all entitled LAX blueprints are available.

Table 2-8. LAX Service Catalog

Name	Business Group
Redhat Enterprise Linux 6 - LAX Dev	Development
Redhat Enterprise Linux 6 - LAX Prod	Production
Windows Server 2012 R2 - LAX Dev	Development
Windows Server 2012 R2 - LAX Prod	Production
Windows Server 2012 R2 with SQL2012 - LAX Dev	Development
Windows Server 2012 R2 with SQL2012 - LAX Prod	Production

3 Click **SFO Service Catalog** and verify that all entitled SFO blueprints are available.

Table 2-9. SFO Service Catalog

Name	Business Group
Redhat Enterprise Linux 6 - SFO Dev	Development
Redhat Enterprise Linux 6 - SFO Prod	Production
Windows Server 2012 R2 - SFO Dev	Development
Windows Server 2012 R2 - SFO Prod	Production
Windows Server 2012 R2 with SQL2012 - SFO Dev	Development
Windows Server 2012 R2 with SQL2012 - SFO Prod	Production

4 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.

5 Click the **Requests** tab and verify that the Status for the `Windows Server 2012 R2 – SFO Prod` single-machine blueprint provisioning is `Successful`.

6 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

Verify the Cloud Management Platform load balancer after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

After you patch, update, restore, failover, or failback the vRealize Automation and vRealize Business for Cloud 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 **`sfo01m01lb01`** or **`lax01m01lb01`** NSX Edge services gateway respectively of the regions where operation occurred.
- If you perform a failover(DR) to Region B, you verify load balancing of the **`lax01m01lb01`** NSX Edge services gateway.
- If you perform a failback(DR) to Region A, you verify load balancing of the **`sfo01m01lb01`** NSX Edge services gateway.

Procedure

1 Log in to the Management vCenter Server 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	https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client
Region B	Failover	https://lax01m01vc01.lax01.rainpole.local/vsphere-client

   b Log in using the following credentials.

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

2 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 In the **Navigator**, 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	sfo01m01lb01
Failover	lax01m01lb01

d On the **Load Balancer** page, click **Pools** and click **Show Pool Statistics**.

e In the **Pool and Member Status** table that drops down, select the following vRealize Automation pools, and verify that the status of the pool is `UP` and the status of all members is `UP`, except for `vra01ims01b`.

Pool Name	Member Name	IP address	Status
vra-svr-443	vra01svr01a	192.168.11.51	UP
	vra01svr01b	192.168.11.52	UP
vra-iws-443	vra01iws01a	192.168.11.54	UP
	vra01iws01b	192.168.11.55	UP
vra-ims-443	vra01ims01a	192.168.11.57	UP
	vra01ims01b	192.168.11.58	DOWN
vra-vro-8283	vra01svr01a	192.168.11.51	UP
	vra01svr01b	192.168.11.52	UP
vra-svr-8444	vra01svr01a	192.168.11.51	UP
	vra01svr01b	192.168.11.52	UP

Validate NSX for vSphere

3

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

   Validate the operational status of the deployed NSX Manager instances after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

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.

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

Validate the operational status of the deployed NSX Manager instances after you perform a software maintenance operation in the Software-Defined Data Center (SDDC).

After you patch, update, restore, failover, or failback the NSX instances in the SDDC, or after you have restored the NSX virtual appliances, verify the version, the service status and configuration of each NSX Manager appliance. Perform the following verification tasks against each vRealize Automation instance:

- Version
- Services
- Configuration
- Certificate
- Lookup Service URL
- Connectivity to vCenter Server

Table 3-1. NSX Manager Instances

Cluster	Region A	Region B
Management cluster	sfo01m01nsx01.sfo01.rainpole.local	lax01m01nsx01.lax01.rainpole.local
Shared edge and compute cluster	sfo01w01nsx01.sfo01.rainpole.local	lax01w01nsx01.lax01.rainpole.local

Procedure

1 Log in to the Management NSX Manager appliance user interface.

   a Open a Web browser and go to **`https://sfo01m01nsx01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 On the **Home** page, click the **View Summary** and verify the NSX Manager Virtual Appliance version.

3 On the **Summary** tab verify the status of the following services.

Components	Name	Status
Common components	vPostgres	Running
	RabbitMQ	Running
System-level components	SSH Service	Running
NSX Management Components	NSX Universal Synchronization Service	Running
	NSX Management Service	Running

4 On the **Home** page, click the **Manage Appliance Settings** and verify the value that is assigned during initial setup for the following settings.

Setting category	Setting	Value
Time Settings	NTP Server	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
Syslog Server	Syslog Server	sfo01vrli01.sfo01.rainpole.local
	Port	514
	Protocol	UDP

5 On the **Manage** tab, under **Settings**, click **SSL Certificates**, and verify that the certificate is valid.

6 On the **Manage** tab, under **Settings** click **NSX Management Service**, and verify the following settings under **Lookup Service URL**.

Setting	Value
Lookup Service	https://sfo01psc01.sfo01.rainpole.local:443/lookupservice/sdk
SSO Administrator User Name	administrator@vsphere.local
Status	Connected

7 On the **NSX Management Service** page verify the following settings under **vCenter Server**.

Setting	Value
vCenter Server	sfo01m01vc01.sfo01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Status	Connected

8 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 failback 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 ■ Restore	`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`
Region B	■ Failover ■ Update ■ Patch ■ Restore	`https://lax01m01vc01.lax01.rainpole.local/vsphere-client`

b Log in using the following credentials.

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

2 Select **Home > Networking & Security** and in the **Navigator** pane click **Installation**.

3 On the **Management** tab, select an NSX Manager, and verify the connectivity status and the version of each controller node.

Table 3-2. NSX Controller Instances to Verify inRegion A

NSX Controller location	Operation Type	NSX Manager	Controller Node
NSX Controller instances for the management cluster	■ Failback ■ Update ■ Patch ■ Restore	172.16.11.65	■ 172.16.11.118 ■ 172.16.11.119 ■ 172.16.11.120
NSX Controller instances for the shared edge and compute cluster	■ Update ■ Patch ■ Restore	172.16.11.66	■ 172.16.31.118 ■ 172.16.31.119 ■ 172.16.31.120

Table 3-3. NSX Controller Instances to Verify inRegion B

NSX Controller location	Operation Type	NSX Manager	Controller Node
NSX Controller instances for the management cluster	■ Failover ■ Update ■ Patch ■ Restore	172.17.11.65	■ 172.17.11.118 ■ 172.17.11.119 ■ 172.17.11.120
NSX Controller instances for the shared edge and compute cluster	■ Failover ■ Update ■ Patch ■ Restore	172.17.11.66	■ 172.17.31.118 ■ 172.17.31.119 ■ 172.17.31.120

Controller Node	Expected Value
Status	`Connected`
Peers	*Green icons*
Software Version	Updated to the version applied during maintenance

4 Repeat the step for the NSX Controller instances on the other NSX Manager instances.

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`.

5 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 the **172.16.11.65** NSX Manager.

c Expand the **sfo01-m01-mgmt01** cluster and verify that the following settings are configured.

Table 3-4. Hosts to Verify NSX VIBs on in Region A

Cluster	NSX Manager	Hosts Cluster	Hosts
NSX Controller instances for the management cluster	172.16.11.65	sfo01-m01-mgmt01	■ sfo01m01esx01.sfo01.rainpole.local ■ sfo01m01esx02.sfo01.rainpole.local ■ sfo01m01esx03.sfo01.rainpole.local ■ sfo01m01esx04.sfo01.rainpole.local
NSX Manager for the shared edge and compute cluster	172.16.11.66	sfo01-w01-comp01	■ sfo01w01esx01.sfo01.rainpole.local ■ sfo01w01esx02.sfo01.rainpole.local ■ sfo01w01esx03.sfo01.rainpole.local ■ sfo01w01esx04.sfo01.rainpole.local

Table 3-5. Hosts to Verify NSX VIBs on in Region B

Cluster	NSX Manager	Hosts Cluster	Hosts
NSX Controller instances for the management cluster	172.17.11.65	lax01-m01-mgmt01	■ lax01m01esx01.lax01.rainpole.local ■ lax01m01esx02.lax01.rainpole.local ■ lax01m01esx03.lax01.rainpole.local ■ lax01m01esx04.lax01.rainpole.local
NSX Manager for the shared edge and compute cluster	172.17.11.66	lax01-w01-comp01	■ lax01w01esx01.lax01.rainpole.local ■ lax01w01esx02.lax01.rainpole.local ■ lax01w01esx03.lax01.rainpole.local ■ lax01w01esx04.lax01.rainpole.local

Object	Setting	Expected Value
sfo01-m01-mgmt01 cluster	Installation Status	*nsx_version*
	Firewall	Enabled
	VXLAN	Configured
Hosts in the cluster	Installation Status	*nsx_version*
	Firewall	Enabled

d Repeat the steps for the remaining NSX Manager instances.

6 (Optional) Confirm that the NSX VIBs on the hosts are updated.

a Open an SSH connection to a host in a cluster with user name **root** and password ***esxi_root_user_password***.

Cluster	Host
sfo01-m01-mgmt01	sfo01m01esx01.sfo01.rainpole.local
sfo01-w01-mgmt01	sfo01w01esx01.sfo01.rainpole.local
lax01-m01-mgmt01	lax01m01esx01.lax01.rainpole.local
lax01-w01-mgmt01	lax01w01esx01.lax01.rainpole.local

b Run the following console command.

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

c In the command output, make sure that the `esx-nsxv` VIB has been updated to the expected version.

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 3-6. Test Parameters for VXLAN Host Connectivity

NSX Manager	IP Address	Source Host	Destination Host
Region A - Management Cluster	172.16.11.65	sfo01m01esx04.sfo01.rainpole.local	sfo01m01esx01.sfo01.rainpole.local
Region B - Management Cluster	172.17.11.65	lax01m01esx04.lax01.rainpole.local	lax01m01esx01.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://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

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

2 Create a 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 Universal Transport Zone
Replication mode	Hybrid
Enable IP Discovery	Selected
Enable MAC Learning	Deselected

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	sfo01m01esx04.sfo01.rainpole.local
Destination host	sfo01m01esx01.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	lax01m01esx04.lax01.rainpole.local
Destination host	lax01m01esx01.lax01.rainpole.local
Size of test packet	VXLAN standard

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

5 After completing VXLAN connectivity tests, remove the mgmt01-logical-switch logical switch.

   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 Select **mgmt01-logical-switch** from the **Logical Switches** list and click **Remove.**

(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 3-7. Test Parameters for VXLAN Host Connectivity

NSX Manager	IP Address	Source Host	Destination Host
Region A - Shared edge and compute cluster	172.16.11.66	sfo01w01esx04.sfo01.rainpole.local	sfo01w01esx01.sfo01.rainpole.local
Region B - Shared edge and compute cluster	172.17.11.66	lax01w01esx04.lax01.rainpole.local	lax01w01esx01.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://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 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 Universal Transport Zone
Replication mode	Hybrid
Enable IP Discovery	Selected
Enable MAC Learning	Deselected

3 Use the ping monitor to test connectivity in Region A.

   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	sfo01w01esx04.sfo01.rainpole.local
Destination host	sfo01w01esx01.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 **172.17.11.66** from the **NSX Manager** drop-down menu.

c Double-click **comp01-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	lax01w01esx04.lax01.rainpole.local
Destination host	lax01w01esx01.lax01.rainpole.local
Size of test packet	VXLAN standard

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

5 After completing VXLAN connectivity tests, remove the comp01-logical-switch logical switch.

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

b On the **Logical Switches** page, select **172.17.11.66** from the **NSX Manager** drop-down menu.

c Select **comp01-logical-switch** from the **Logical Switches** list and click **Remove**.

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 running after you perform maintenance in the SDDC.

2 Verify the Status of vRealize Operations Manager Cluster Nodes and Remote Collectors

Verify the operational status of the analytics and remote collector nodes of vRealize Operations Manager after you perform software maintenance in the SDDC.

3 Verify the vRealize Operations Manager Load Balancing

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

4 Verify the Solution Adapters in vRealize Operations Manager

After you perform a planned maintenance in your environment, verify that the adapters for collecting statistical data from the management components are operational. vRealize Operations Manager must continue collecting information about the health of the SDDC management components.

5 Verification List of vRealize Operations Manager Solutions

Verify the collection status of the solutions that provide statistics about the operation of the SDDC management components to vRealize Operations Manager.

Verify the Power Status of All vRealize Operations Manager VMs

All virtual machines of vRealize Operations Manager must be running after you perform maintenance in the SDDC.

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	`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`
Region B	`https://lax01m01vc01.lax01.rainpole.local/vsphere-client`

b Log in using the following credentials.

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

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

3 In the **Navigator**, navigate to the following folders on vCenter Server and verify the following configuration.

- The state of all virtual machines is `Powered On`.
- The status of all virtual machines is `Normal` indicating that there are no issues in virtual machine setup.

Region	vCenter Server	Folder Name	Name
Region A	sfo01m01vc01.sfo01.rainpole.local	sfo01-m01fd-vrops	vrops01svr01a
			vrops01svr01b
			vrops01svr01c
		sfo01-m01fd-vropsrc	sfo01vropsc01a
			sfo01vropsc01b
Region B	lax01m01vc01.lax01.rainpole.local	lax01-m01fd-vropsrc	lax01vropsc01a
			lax01vropsc01b

Verify the Status of vRealize Operations Manager Cluster Nodes and Remote Collectors

Verify the operational status of the analytics and remote collector nodes of vRealize Operations Manager after you perform software maintenance in the SDDC.

After you patch, update, restore, failover, or failback the vRealize Operations Manager nodes, verify the version and the service status of each node. Perform the verification tasks against each of the following vRealize Operations Manager parameters:

- vRealize Operations Manager health
- Version

- Node Status
- Self Heath
- Alerts
- Authentication sources
- Certificates
- Licensing

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 Verify that the cluster is online, and all data nodes are running and are joined to the cluster.

   a On the main navigation bar, click **Administration**.

   b In the left pane of vRealize Operations Manager, select **Management > Cluster Management**.

   c Verify the cluster status and high availability mode.

Setting	Value
Cluster Status	Online
High Availability	Enabled

3 On the **Cluster Management** page, in the review table under **Nodes in the vRealize Operations Manager Cluster**, verify that following configuration for each node.

Setting	Value
Version	*correct version of vRealize Operations Manager*
State	Running
Status	Online

4 Verify the cluster health of vRealize Operations Manager.

   a On the main navigation bar, click **Dashboards**.

   b In the left pane of vRealize Operations Manager, select **Self Health**.

   c Verify that the status of all objects of the cluster is `Green`.

5 Check that there are no critical alerts for the cluster objects of vRealize Operations Manager.

   a From the **All Dashboards** menu, select **vRealize Operations > Self Services Communications**.

   b Verify that there are no critical alerts for the objects of the analytics cluster.

6 Verify that the authentication sources are valid and synchronization is successful.

   a On the main navigation bar, click **Administration**.

   b In the left pane of vRealize Operations Manager, select **Access > Authentication Sources**.

   c On the **Authentication Sources** page, verify the following settings.

Source Display Name	Source Type	Auto Synchronization	Last synchronized
LAX01.RAINPOLE.LOCAL	Active Directory	True	recent_sync_date
RAINPOLE.LOCAL	Active Directory	True	recent_sync_date
SFO01.RAINPOLE.LOCAL	Active Directory	True	recent_sync_date

7 In the left pane of vRealize Operations Manager, select **Management > Certificates** and verify that the certificates are intact.

8 In the left pane of vRealize Operations Manager, select **Management > Licensing** and verify that the license key is valid and has not expired..

Verify the vRealize Operations Manager Load Balancing

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

You determine the NSX Edge services gateway on which to perform the verification by type and target of maintenance operation.

Maintenance Operation Type	Region	NSX Manager	NSX Load Balancer
Update, patch or restore	Region A	172.16.11.65	sfo01m01lb01
	Region B	172.17.11.65	lax01m01lb01
Failover	Region B	172.17.11.65	lax01m01lb01
Failback	Region A	172.16.11.65	sfo01m01lb01

Prerequisites

Verify that the connectivity status of the OneArmLB interface of the NSX Edge services gateway is `Connected`.

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	https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client
Region B	Failover, update, patch, or restore	https://lax01m01vc01.lax01.rainpole.local/vsphere-client

b Log in using the following credentials.

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

2 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 for the management cluster from the **NSX Manager** drop-down menu.

Region	Operation Type	NSX Manager for the Management Cluster
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 device.

Region	Operation Type	NSX Edge device
Region A	Failback, update, patch, or restore	sfo01m01lb01
Region B	Failover, update, patch, or restore	lax01m01lb01

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-svr-443** pool.

g Verify that the status of the **vrops-svr-443** pool is `UP` and the status of all members is `UP`.

3 In a Web browser, go to **`https://vrops01svr01.rainpole.local`** to verify that the cluster is accessible at the public Virtual Server IP (VIP) address over HTTPS.

4 In a Web browser, go to **`http://vrops01svr01.rainpole.local`** to verify that HTTP requests are auto-redirected to HTTPS.

Verify the Solution Adapters in vRealize Operations Manager

After you perform a planned maintenance in your environment, verify that the adapters for collecting statistical data from the management components are operational. vRealize Operations Manager must continue collecting information about the health of the SDDC management components.

Perform the following verification tasks against each solution in vRealize Operations Manager:

- Version
- Collection status

Verify the operation of the adapters that are collecting statistics for the following components. See Verification List of vRealize Operations Manager Solutions. You can start with the vSphere solution first.

- vSphere
- vRealize Log Insight
- NSX for vSphere
- vRealize Automation
- vRealize Business
- Storage

Procedure

1. Log in to vRealize Operations Manager by using the operations interface.
   a. Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.
   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2. On the main navigation bar, click **Administration.**
3. In the left pane of vRealize Operations Manager, click **Solutions**.
4. On the **Solutions** page, in the solutions table select the **VMware vSphere** solution.
5. Verify that the software version of the VMware vSphere solution is correct.
6. Under **Configured Adapter Instances**, verify that the Collection State is `Collecting` and the Collection Status is `Data Receiving` for all vCenter Adapter instances.
7. Repeat the procedure to verify the version and adapter collection status of the other solutions.

Verification List of vRealize Operations Manager Solutions

Verify the collection status of the solutions that provide statistics about the operation of the SDDC management components to vRealize Operations Manager.

You access the solutions from the **Administration > Solutions** page in the vRealize Operations Manager operations interface. See Verify the Solution Adapters in vRealize Operations Manager

VMware vSphere Solution

Verify that the vCenter Adapters are collecting statistics from the Management vCenter Server and Compute vCenter Server in Region A and Region B.

Table 4-1. vCenter Adapter Instances

Region	Adapter Type	Adapter Instance Name	vCenter Server
Region A	vCenter Adapter	vCenter Adapter - sfo01m01vc01	sfo01m01vc01.sfo01.rainpole.local
	vCenter Adapter	vCenter Adapter - sfo01w01vc01	sfo01w01vc01.sfo01.rainpole.local
Region B	vCenter Adapter	vCenter Adapter - lax01m01vc01	lax01m01vc01.lax01.rainpole.local
	vCenter Adapter	vCenter Adapter - lax01w01vc01	lax01w01vc01.lax01.rainpole.local

VMware vRealize Log Insight Solution

Verify that the vRealize Log Insight Adapters are collecting statistics from the vRealize Log Insight clusters in Region A and Region B.

Table 4-2. vRealize Log Insight Adapter Instances

Region	Adapter Type	Adapter Instance Name	vRealize Log Insight Cluster
Region A	vRealize Log Insight Adapter	Log Insight Adapter - sfo01vrli01	sfo01vrli01.sfo01.rainpole.local
Region B	vRealize Log Insight Adapter	Log Insight Adapter - lax01vrli01	lax01vrli01.lax01.rainpole.local

Management Pack for NSX-vSphere

Verify that the NSX-vSphere Adapters for NSX infrastructure are collecting statistics from the NSX Manager instances in Region A and Region B.

Table 4-3. NSX-vSphere Adapter Instances

Region	Adapter Type	Adapter Name	NSX Manager Host
Region A	NSX-vSphere Adapter	NSX Adapter - sfo01m01nsx01	sfo01m01nsx01.sfo01.rainpole.local
	NSX-vSphere Adapter	NSX Adapter - sfo01w01nsx01	sfo01w01nsx01.sfo01.rainpole.local

Table 4-3. NSX-vSphere Adapter Instances (Continued)

Region	Adapter Type	Adapter Name	NSX Manager Host
Region B	NSX-vSphere Adapter	NSX Adapter - lax01m01nsx01	lax01m01nsx01.lax01.rainpole.local
	NSX-vSphere Adapter	NSX Adapter - lax01w01nsx01	lax01w01nsx01.lax01.rainpole.local

Verify that the Network Devices Adapter is collecting statistics about the switches and routers in the network over SNMP.

Table 4-4. Network Devices Adapter Instance

Adapter Type	Adapter Name
Network Devices Adapter	Network Devices Adapter

VMware vRealize Automation

Verify that the vRealize Automation Adapter is collecting statistics about the tenant workloads that are provisioned by using the vRealize Automation service catalog.

Table 4-5. vRealize Automation Adapter Instance

Adapter Type	Adapter Instance Type	vRealize Automation
vRealize Automation Adapter	vRealize Automation Adapter - vra01svr01 (Rainpole)	https://vra01svr01.rainpole.local

VMware vRealize Business for Cloud

Verify that the vRBC Adapter is collecting information about the infrastructure performance, cost information, and troubleshooting tips.

Table 4-6. vRealize Business for Cloud Adapter Instance

Adapter Type	Adapter Instance Name	vRealize Business for Cloud server
vRBC Adapter	vRealize Business Adapter - vrb01svr01	vrb01svr01.rainpole.local

Management Pack for Storage Devices

Verify that the Storage Devices adapters are collecting information about the storage topology, and capacity and problems on the storage components.

Table 4-7. Storage Devices Adapter Instances

Region	Adapter Type	Adapter Instance Name	vCenter Server
Region A	Storage Devices	Storage Devices Adapter - sfo01m01vc01	sfo01m01vc01.sfo01.rainpole.local
	Storage Devices	Storage Devices Adapter - sfo01w01vc01	sfo01w01vc01.sfo01.rainpole.local
Region B	Storage Devices	Storage Devices Adapter - lax01m01vc01	lax01m01vc01.lax01.rainpole.local
	Storage Devices	Storage Devices Adapter - lax01w01vc01	lax01w01vc01.lax01.rainpole.local

VMware vSAN

Verify that the vSAN Adapters are collecting information about the vSAN topology, and capacity and problems on the vSAN datastores.

Table 4-8. vSAN Adapter Instances

Region	Adapter Type	Adapter Instance Name	vCenter Server
Region A	vSAN Adapter	vSAN Adapter - sfo01m01vc01	sfo01m01vc01.sfo01.rainpole.local
Region B	vSAN Adapter	vSAN Adapter - lax01m01vc01	lax01m01vc01.lax01.rainpole.local

Validate vRealize Log Insight

5

Validate the operational status of the vRealize Log Insight in Region A and Region B after you perform a software maintenance operation in the Software-Defined Data Center.

After you patch, update, or restore vRealize Log Insight, verify the version and the service status of each node. Perform the following verification tasks against the functional components of vRealize Log Insight:

- Version
- Cluster Status
- Agent Registration
- License
- Integration with vCenter Server and vRealize Operations Manager
- Integration with vRealize Operations Manager
- Authentication
- Messaging
- Archive
- Content packs and dashboards
- Service Status

Procedure

1 Log in to vRealize Log Insight.

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

Region	URL
Region A	https://sfo01vrli01.sfo01.rainpole.local
Region B	https://lax01vrli01.lax01.rainpole.local

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

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

3 Verify the version of the vRealize Log Insight cluster nodes.

a Under **Management** on the left, click **Cluster**.

b In the **Nodes** table, verify that the version of each node is as expected.

Region	FQDN	Role
Region A	sfo01vrli01.sfo01.rainpole.local	Integrated Load Balancer
	sfo01vrli01a.sfo01.rainpole.local	Master
	sfo01vrli01b.sfo01.rainpole.local	Worker
	sfo01vrli01c.sfo01.rainpole.local	Worker
Region B	lax01vrli01.sfo01.rainpole.local	Integrated Load Balancer
	lax01vrli01a.sfo01.rainpole.local	Master
	lax01vrli01b.sfo01.rainpole.local	Worker
	lax01vrli01c.sfo01.rainpole.local	Worker

4 Verify the cluster and integrated load balancer status.

a In the **Nodes** table, verify that the **Status** for each node is `Connected`.

b Under **Integrated Load Balancer**, verify that the **Status** is `Available`.

5 Verify that the agents on the monitored management nodes are active.

a Under **Management** on the left, click **Agents**.

b On the **Agents** page, from the **Agents** drop-down menu, select each of the following agent groups and verify that all registered agents are visible and their Status is `Active`.

Agent Group	FQDNs in Region A	FQDNs in Region B
vAppliances - Agent Group	■ vrops01svr01a.rainpole.local ■ vrops01svr01b.rainpole.local ■ vrops01svr01c.rainpole.local ■ sfo01vropsc01a.sfo01.rainpole.local ■ sfo01vropsc01b.sfo01.rainpole.local ■ vra01svr01a.rainpole.local ■ vra01svr01b.rainpole.local ■ vrb01svr01.rainpole.local ■ sfo01vrbc01.sfo01.rainpole.local	■ lax01vropsc01a.lax01.rainpole.local ■ lax01vropsc01b.lax01.rainpole.local ■ lax01vrbc01.lax01.rainpole.local
vRA7 - Microsoft SQL Server Agent Group	vra01mssql01.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 ■ vra01dem01a.rainpole.local ■ vra01dem01b.rainpole.local ■ sfo01ias01a.sfo01.rainpole.local ■ sfo01ias01b.sfo01.rainpole.local	■ lax01ias01a.lax01.rainpole.local ■ lax01ias01b.lax01.rainpole.local
vRO7 - Agent Group	■ vra01svr01a.rainpole.local ■ vra01svr01b.rainpole.local	-
vRops6 - Agent Group	■ vrops01svr01a.rainpole.local ■ vrops01svr01b.rainpole.local ■ vrops01svr01c.rainpole.local ■ sfo01vropsc01a.sfo01.rainpole.local ■ sfo01vropsc01b.sfo01.rainpole.local	■ lax01vropsc01a.lax01.rainpole.local ■ lax01vropsc01b.lax01.rainpole.local

6 Verify that the license key is intact.

a Under **Management** on the left, click **License**.

b Verify that the license status in the table is `Active`.

7 Verify that the vRealize Log Insight integration with Management vCenter Server and Compute vCenter Server is intact.

   a Under **Integration** on the left, click **vSphere**.

   b Click **Test Connection** for the Management vCenter Server and Compute vCenter Server, and verify that the `Test successful` message appears.

8 Verify that the vRealize Log Insight integration with vRealize Operations Manager is intact.

   a Under **Integration** on the left, click **vRealize Operations**.

   b Click **Test Connection** and verify that the `Test successful` message appears.

9 Verify that the time configuration of vRealize Log Insight is intact.

   a Under **Configuration** on the left, 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, and verify that the `successful` message appears.

10 Verify that the vRealize Log Insight integration with Active Directory is intact.

   a Under **Configuration** on the left, click **Authentication**.

   b Click the **Active Directory** tab.

   c Verify that the Authentication Configuration is intact.

Setting	Expected Value
Enable Active Directory support	Selected
Default Domain	rainpole.local
Domain Controller	dc01rpl.rainpole.local
User Name	svc-vrli
Password	*svc_vrli_password*
Connection Type	Standard
Require SSL	Yes or No according to the instructions from the IT administrator

   d Click **Test connection** to verify that the connection is successful, and verify that the `Succeeded` message appears..

11 Verify that the configuration for the SMTP email server is intact.

   a Under **Configuration** on the left, 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.

12 Verify that the configuration for log archiving is intact.

a Under **Configuration** on the left, click **Archiving**.

b Verify that the archiving configuration is intact.

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

For example, you can expect a location `nfs://192.168.104.251/V2D_vRLI_MgmtA_400GB` for Region A

c Click **Test** to verify that the NFS share is accessible.

13 Verify that the installed content packs are intact.

a Click the configuration drop-down menu icon  and select **Content Packs**.

b Verify that you see the following content packs under **Installed Content Packs**.

- Linux
- 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 dashboards of the content packs are receiving log information.

a In the vRealize Log Insight user interface, click **Dashboards**.

b In the **Navigator**, under **Content Pack Dashboards**, verify that you see the following dashboards.

- Linux
- Microsoft - SQL Server
- VMware - NSX-vSphere
- VMware - Orchestrator - 7.0.1+
- VMware - VSAN
- VMware - vRA 7
- VMware - vRops 6.x
- VMware - vSphere

15 (Optional) Verify the status of the service of the vRealize Log Insight appliance.

a Open an SSH connection to **sfo01vrli01a.sfo01.rainpole.local**.

b Log in using the following credentials.

Setting	Value
Username	root
Password	*vrli_root_password*

c Run the following command.

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

d Verify that the status as follows.

```
INFO executor.ProcessExecutor: Finished executing ip –4 addr show eth0, ran for 87 ms
Log Insight is running.
```

Validate vSphere Data Protection

6

After you perform a software maintenance operation, validate the VMware vSphere Data Protection deployment to make sure it works as expected.

Procedure

1 Verify the Appliance Status and Version of vSphere Data Protection

Validate the operational status of the vSphere Data Protection in Region A and Region B.

2 Verify the Configuration and Service Status of vSphere Data Protection

Validate the configuration status of the vSphere Data Protection in Region A and Region B after you perform a software maintenance operation in the Software-Defined Data Center.

Verify the Appliance Status and Version of vSphere Data Protection

Validate the operational status of the vSphere Data Protection in Region A and Region B.

After you patch or update vSphere Data Protection, verify the operational status. Verify each of the following parameters:

- Availability
- Status
- Version
- General configuration

Table 6-1. vSphere Data Protection Instances

Region	FQDN
Region A	sfo01m01vdp01.sfo01.rainpole.local
Region B	lax01m01vdp01.lax01.rainpole.local

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://sfo01m01vc01.sfo01.rainpole.local/vsphere-client
Region B	https://lax01m01vc01.lax01.rainpole.local/vsphere-client

b Log in using the following credentials.

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

2 From the **Home** menu, select **vSphere Data Protection 6.1 (powered by EMC)**.

3 On the **vSphere Data Protection 6.1 (powered by EMC)** page, verify that you can select **sfo01m01vdp01** from the **Switch Appliance** drop-down menu.

4 Select **sfo01m01vdp01** from the **Switch Appliance** drop-down menu, click Connect and verify the connection to the appliance.

5 On the **sfo01m01vdp01** page, click the **Reports** tab and verify the following status.

Setting	Value
Appliance Status	Normal
Integrity check status	Normal

6 On the **sfo01m01vdp01** page, click the **Configuration** tab, and verify the version and configuration of the vSphere Data Protection appliance.

Setting	Region A	Region B
Display name	sfo01m01vdp01	lax01m01vdp01
Product Name	VDP	VDP
IP Address	172.16.11.81	172.17.11.81
Major Version	*vdp_major_version*	*vdp_major_version*
Minor Version	*vdp_minor_version*	*vdp_minor_version*
Status	Normal	Normal
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
VDP backup user	rainpole.local\svc-vdp	rainpole.local\svc-vdp

7 Repeat the steps for the **`lax01m01vdp01`** vSphere Data Protection appliance.

Verify the Configuration and Service Status of vSphere Data Protection

Validate the configuration status of the vSphere Data Protection in Region A and Region B after you perform a software maintenance operation in the Software-Defined Data Center.

After you patch or update vSphere Data Protection, verify the version and the service status. Perform the following verification tasks:

- Configuration
- Connectivity to vCenter Server
- Proxies
- Storage performance
- Service status
- Enterprise Manager Web Status

Table 6-2. vSphere Data Protection Nodes

Setting	Region A	Region B
FQDN	sfo01m01vdp01.sfo01.rainpole.local	lax01m01vdp01.lax01.rainpole.local
URL to configuration interface	https://sfo01m01vdp01.sfo01.rainpole.local:8543/vdp-configure	https://sfo01m01vdp01.sfo01.rainpole.local:8543/vdp-configure

Procedure

1. Log in to the vSphere Data Protection configuration interface.
   a. Open a Web browser and go to **`https://sfo01m01vdp01.sfo01.rainpole.local:8543/vdp-configure`**.
   b. Log in using the following credentials.

Setting	Value
User name	root
Password	*vdp_root_password*

2 Verify the host name and vCenter Server connectivity of the vSphere Data Protection appliance.

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

Setting	Region A	Region B
Hostname	sfo01m01vdp01.sfo01.rainpole.local	lax01m01vdp01.lax01.rainpole.local
Time zone	UTC	UTC
vCenter	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
vCenter SSO	sfo01psc01.sfo01.rainpole.local	lax01psc01.lax01.rainpole.local

b Under **Proxies**, verify that the status of vSphere Data Protection proxy instance is running (`green`).

c Verify the status of all services .

Services	Status
Core	Running
Management	Running
Maintenance	Running
Backup Scheduler	Running
Replication	Running
File Level Restore	Running
Backup Recovery	Running

3 Verify the proxy of the vSphere Data Protection appliance.

a On the **Configuration** tab, under **Proxies**, verify the following parameters.

Setting	Region A	Region B
Name	sfo01m01vdp01	lax01m01vdp01
IP Address	172.16.11.81	172.17.11.81
Datastore	sfo01-m01-vdp01	lax01-m01-vdp01
Status	Running	Running

4 Verify storage performance.

a Click the **Storage** tab.

b Under **Storage summary**, verify that the **Performance Analysis** status is `Passed`.

5 Verify the status of all services of the vSphere Data Protection appliance.

a Open an SSH connection to **sfo01m01vdp01.sfo01.rainpole.local**.

b Log in using the following credentials.

Setting	Values
User Name	root
Password	*vdp_root_password*

c Run the following command.

```
dpnctl status all
```

d Verify that the status of all services as follows.

Note The status of axionfs service should be down.

Service	Status
gsan	up
MCS	up
emt	up
Backup scheduler status	up
axionfs status	down
Maintenance windows scheduler status	enabled
Unattended startup status	enabled
avinstaller status	up

e Verify the status of Enterprise Manager Web application in the vSphere Data Protection appliance by run the following command.

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

6 Repeat the procedure for lax01m01vdp01.lax01.rainpole.local in Region B.

Validate Site Recovery Manager 7

Validate the operational status of the Site Recovery Manager in Region A and Region B after you perform a software maintenance operation in the Software-Defined Data Center.

After you patch or update Site Recovery Manager, verify the version and the service status. Verify the following parameters:

- Version
- Service Status
- Licenses
- Site Pairing
- Mappings
- Protection groups for the Cloud Management Platform and vRealize Operations Manager
- Recovery plans for the Cloud Management Platform and vRealize Operations Manager

Procedure

1 Log in to the Windows virtual machine of Site Recovery Manager by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the virtual machine **`sfo01m01srm01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	*windows_administrator_password*

2 Verify the version of 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 up-to-date.

      - VMware vCenter Site Recovery Manager
      - VMware vCenter Site Recovery Manager Embedded Database

3 Verify the status of the Site Recovery Manager services.

   a From the Windows **Start** menu, select **Administrative Tools > Services**.

   b Verify that the status and startup configuration of the following services.

Name	Status	Startup Type
VMware vCenter Site Recovery Manager Embedded Database	Running	Automatic
VMware vCenter Site Recovery Manager Server	Running	Automatic (Delayed Start)

4 Repeat the step for the lax01m01srm01.lax01.rainpole.local Site Recovery Manager in the other region.

5 In the vSphere Web Client, verify that you have a valid license for Site Recovery Manager.

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

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

   c Log in using the following credentials.

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

   d From the **Home** menu, select **Administration**.

   e In the **Navigator**, under **Administration**, click **Licenses**.

   f On the **Licenses** page, click the **Assets** tab, and click **Solutions**.

   g Verify that the license is valid for the sfo01m01vc01.sfo01.rainpole.local and lax01m01vc01.lax01.rainpole.local assets.

6 In the vSphere Web Client, verify the status of site pairing.

   a From the **Home** menu, select **Site Recovery**.

   b In the **Navigator**, click **Sites**.

c In the **Navigator**, under **Sites**, click the **sfo01m01vc01.sfo01.rainpole.local** site.

d On the **Summary** tab, verify the following details.

Settings	Site	Paired Site
Name	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
Client Connection	Connected	Connected
Server Connection	Connected	Connected
SRM Server	sfo01m01srm01.sfo01.rainpole.local:9086	lax01m01srm01.lax01.rainpole.local:9086
vCenter Server	sfo01m01vc01.sfo01.rainpole.local:443	lax01m01vc01.lax01.rainpole.local:443
SRM Server Build	*srm_build_version*	*update_build_version*
Organization	VMware, Inc.	VMware, Inc.
Logged in as	VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator
VR Compatibility	*vr_version* - Compatible	*vr_version* - Compatible

7 Verify the configuration of network, folder, resource and resource mappings, and the placeholder datastore of the sfo01m01vc01.sfo01.rainpole.local site.

a On the **Sites** page, click the **sfo01m01vc01.sfo01.rainpole.local** site.

b Click the **Manage** tab and verify that the following mappings and configurations for them are intact.

Settings	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.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	■ sfo01-m01fd-vra ■ sfo01-m01fd-vrops	■ lax01-m01fd-vra ■ lax01-m01fd-vrops	Yes
Resource Mappings	sfo01-m01-mgmt01	lax01-m01-mgmt01	Yes
Placeholder Datastores	sfo01-m01-vsan01	-	-

8 Verify the configuration of network, folder, resource and resource mappings, and the placeholder datastore of the lax01m01vc01.lax01.rainpole.local site.

a On the **Sites** page, click the **lax01m01vc01.lax01.rainpole.local** site.

b Click the **Manage** tab and verify that the following mappings and configurations for them are intact.

Settings	lax01m01vc01.lax01.rainpole.local	sfo01m01vc01.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	■ lax01-m01fd-vra ■ lax01-m01fd-vrops	■ sfo01-m01fd-vra ■ sfo01-m01fd-vrops	Yes
Resource Mappings	lax01-m01-mgmt01	sfo01-m01-mgmt01	Yes
Placeholder Datastores	lax01-m01-vsan01	-	-

9 Verify the protection groups for the Cloud Management Platform and vRealize Operations Manager.

a In the **Navigator**, click **Protection Groups**.

b In the **Navigator**, under **Protection Groups**, click the **SDDC Cloud Management PG** protection group and click the **Summary** tab.

c Verify that the **Status** is `OK`.

d Repeat the steps for the **SDDC Operations Management PG** protection group.

10 Verify the recovery plans for the Cloud Management Platform and vRealize Operations Manager.

a In the **Navigator**, click **Recovery Plans**.

b In the **Navigator**, under **Recovery Plans**, click the **SDDC Cloud Management RP** recovery plan and click the **Summary** tab.

c Verify that **Plan Status** is `Ready`.

d Repeat the steps for the **SDDC Operations Management RP** recovery plan.

Validate vSphere Replication

8

Validate the operational status of the vSphere Replication in Region A and Region B after you perform a maintenance operations in the SDDC.

After you patch or update vSphere Replication, perform the following verification tasks:

- Version
- Configuration
- Service status
- Enabled
- Availability
- Target sites
- Replication servers
- Replication

Table 8-1. vSphere Replication Nodes

Setting	Region A	Region B
FQDN	sfo01m01vrms01.sfo01.rainpole.local	lax01m01vrms01.lax01.rainpole.local
VAMI	https://sfo01m01vrms01.sfo01.rainpole.local :5480	https://lax01m01vrms01.lax01.rainpole.local :5480

Procedure

1 Log in to the vSphere Replication appliance management interface.

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

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vr_sfo_root_password*

2 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 following details are correct.

Setting	Value
Vendor	VMware, Inc.
Appliance Name	vSphere Replication Appliance
Appliance Version	*vr_appliance_version*

3 Verify the configuration of the vSphere Replication 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	sfo01m01vrms01.sfo01.rainpole.local	lax01m01vrms01.lax01.rainpole.local
Configuration Mode	Configure using the embedded database	Configure using the embedded database
Lookup Service Address	sfo01psc01.sfo01.rainpole.local	lax01psc01.lax01.rainpole.local
SSO Administrator	svc-vr@rainpole.local	svc-vr@rainpole.local
VRM Host	172.16.11.123	172.17.11.123
VRM Site Name	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
vCenter Server Address	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
vCenter Server Admin Mail	*vcenter_server_admin_email*	*vcenter_server_admin_email*
IP Address for Incoming Storage Traffic	172.16.16.71	172.17.16.71

4 Verify the service status of the vSphere Replication appliance.

a In the appliance management console, click the **VR** tab and click the **Configuration** tab.

b Under **Service Status**, verify that the VRM service is `running`.

5 Repeat the steps for other vSphere Replication appliance lax01m01vrms01.lax01.rainpole.local.

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

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

b Log in using the following credentials.

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

7 Verify that vSphere Replication is enabled for sfo01m01vc01.sfo01.rainpole.local and lax01m01vc01.lax01.rainpole.local.

   a From the **Home** menu, select **vSphere Replication**.

   b On the **vSphere Replication** page, click the **Home** tab.

   c Verify vSphere Replication status for the vCenter Server instances.

vCenter Server	vSphere Replication
sfo01m01vc01.sfo01.rainpole.local	Enabled
lax01m01vc01.lax01.rainpole.local	Enabled

8 Open the vSphere Replication configuration settings on the Management vCenter Server in Region A.

   a On the **Home** tab for vSphere Replication, select the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server and click **Manage**.

   The vCenter Server inventory appears, and the **Configure** tab for sfo01m01vc01.sfo01.rainpole.local opens with the **vSphere Replication** settings selected.

9 On the **sfo01m01vc01.sfo01.rainpole.local** page, under **vSphere Replication** click **About** and verify that the **Availability** status of the vSphere Replication `OK`.

10 Under **vSphere Replication**, click **Target Sites** and verify that the connection status for the lax01m01vc01.lax01.rainpole.local site is `Connected`.

11 Under **vSphere Replication**, click **Replication Servers** and verify that the status of **vSphere Replication (Embedded)** is `Connected`.

   vSphere Replication (Embedded) represents the replication server running on the vSphere Replication appliance.

12 Repeat Step 6 to Step 11 on the lax01m01vc01.lax01.rainpole.local vCenter Server.

13 Open the vSphere Replication monitoring details on the Management vCenter Server in Region A.

   a On the **Home** tab for vSphere Replication, select the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server and click **Monitor**.

   The vCenter Server inventory appears, and the **Monitor** tab for sfo01m01vc01.sfo01.rainpole.local opens with the **vSphere Replication** tab selected.

14 Verify the replication status for the sfo01m01vc01.sfo01.rainpole.local.

   a On the **vSphere Replication** tab, click **Outgoing Replications**.

   b Verify that the replication status is `OK` for vRealize Operations Manager and Cloud Management Platform VMs for replication from sfo01m01vc01.sfo01.rainpole.local to lax01m01vc01.lax01.rainpole.local.

c On the **vSphere Replication** tab, click **Incoming Replications**.

d Verify that the replication status is OK for vRealize Operations Manager and Cloud Management Platform VMs when replication happens from the lax01m01vc01.lax01.rainpole.local to sfo01m01vc01.sfo01.rainpole.local.

15 Open the vSphere Replication monitoring details on the Management vCenter Server in Region B.

a From the **Home** menu of the vSphere Web Client, select **vSphere Replication**.

b On the **vSphere Replication** page, click the **Home** tab.

c Select the **lax01m01vc01.lax01.rainpole.local** vCenter Server and click **Monitor**.

The vCenter Server inventory appears, and the **Monitor** tab for lax01m01vc01.lax01.rainpole.local opens with the **vSphere Replication** tab selected.

16 Verify the replication status for the lax01m01vc01.lax01.rainpole.local site.

a On the **vSphere Replication** tab, click **Outgoing Replications**.

b Verify that the replication status is OK for vRealize Operations Manager and Cloud Management Platform VMs for replication from lax01m01vc01.lax01.rainpole.local to sfo01m01vc01.sfo01.rainpole.local.

c On the **vSphere Replication** tab, click **Incoming Replications**.

d Verify that the replication status is OK for vRealize Operations Manager and Cloud Management Platform VMs when replication happens from the sfo01m01vc01.sfo01.rainpole.local to lax01m01vc01.lax01.rainpole.local.

SDDC Startup and Shutdown

9

When you perform patch, upgrade, recovery, or 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.

- 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.

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

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
vSphere Data Protection **Total Number of VMs (1)**	**vSphere Data Protection** **Total Number of VMs (1)**	**1**
sfo01m01vdp01	lax01m01vdp01	1
vRealize Log Insight **Total Number of VMs (3)**	**vRealize Log Insight** **Total Number of VMs (3)**	**1**
sfo01vrli01c	lax01vrli01c	1
sfo01vrli01b	lax01vrli01b	1
sfo01vrli01a	lax01vrli01a	2
vRealize Operations Manager **Total Number of VMs (5)**	**vRealize Operations Manager** **Total Number of VMs (2)**	**1**
sfo01vropsc01b	lax01vropsc01b	1
sfo01vropsc01a	lax01vropsc01a	1
vrops01svr01c	-	2
vrops01svr01b	-	3

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
vrops01svr01a	-	4
vRealize Business for Cloud **Total Number of VMs (2)**	**Realize Business for Cloud** **Total Number of VMs (2)**	**2**
sfo01vrbc01	lax01vrbc01	1
vrb01svr01	-	2
vRealize Automation **Total Number of VMs (11)**	**vRealize Automation** **Total Number of VMs (2)**	**3**
vra01dem01a	-	1
vra01dem01b	-	1
sfo01ias01b	lax01ias01b	1
sfo01ias01a	lax01ias01a	1
vra01ims01b	-	2
vra01ims01a	-	2
vra01iws01b	-	3
vra01iws01a	-	4
vra01svr01b	-	5
vra01svr01a	-	5
vra01mssql01	-	6
Site Recovery Manager and vSphere Replication **Total Number of VMs (2)**	**Site Recovery Manager and vSphere Replication** **Total Number of VMs (2)**	**4**
sfo01m01vrms01	lax01m01vrms01	1
sfo01m01srm01	lax01m01srm01	2
Update Manager Download Service (UMDS) **Total Number of VMs (1)**	**Update Manager Download Service (UMDS)** **Total Number of VMs (1)**	**4**
sfo01umds01	lax01umds01	1
Core Stack **Total Number of VMs (21)**	**Core Stack** **Total Number of VMs (13)**	**5**
sfo01m01lb01 (0,1)	lax01m01lb01 (0,1)	1
sfo01m01udlr01 (0,1)	-	1
sfo01m01esg01	lax01m01esg01	1
sfo01m01esg02	lax01m01esg02	1
sfo01w01udlr01 (0,1)	-	1
sfo01w01dlr01 (0,1)	lax01w01dlr01 (0,1)	1
sfo01w01esg01	lax01w01esg01	1
sfo01w01esg02	lax01w01esg02	1
sfo01m01nsx01	lax01m01nsx01	2

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
sfo01w01nsx01	lax01w01nsx01	2
sfo01m01nsxc01	-	3
sfo01m01nsxc02	-	3
sfo01m01nsxc03	-	3
sfo01w01nsxc01	-	3
sfo01w01nsxc02	-	3
sfo01w01nsxc03	-	3
sfo01m01vc01	lax01m01vc01	4
sfo01w01vc01	lax01w01vc01	4
sfo01psc01 (0,1)	lax01psc01 (0,1)	5
sfo01w01psc01	lax01w01psc01	6
sfo01m01psc01	lax01m01psc01	6

Note For more information about shutting down and starting up vCenter Server when using a vSAN datastore, see VMware Knowledge Base article 2142676.

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
Core Stack Total Number of VMs (21)	**Core Stack Total Number of VMs (13)**	**1**
sfo01m01psc01	lax01m01psc01	1
sfo01w01psc01	lax01w01psc01	1
sfo01psc01 (0,1)	lax01psc01 (0,1)	2
sfo01m01vc01	lax01m01vc01	3
sfo01w01vc01	lax01w01vc01	3
sfo01m01nsx01	lax01m01nsx01	4
sfo01w01nsx01	lax01w01nsx01	4
sfo01m01nsxc01	-	5
sfo01m01nsxc02	-	5
sfo01m01nsxc03	-	5

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
sfo01w01nsxc01	-	5
sfo01w01nsxc02	-	5
sfo01w01nsxc03	-	5
sfo01m01lb01 (0,1)	lax01m01lb01 (0,1)	6
sfo01m01udlr01 (0,1)	-	6
sfo01m01esg01	lax01m01esg01	6
sfo01m01esg02	lax01m01esg02	6
sfo01w01udlr01 (0,1)	-	6
sfo01w01dlr01 (0,1)	lax01w01dlr01(0,1)	6
sfo01w01esg01	lax01w01esg01	6
sfo01w01esg02	lax01w01esg02	6
Update Manager Download Service (UMDS) Total Number of VMs (1)	**Update Manager Download Service (UMDS) Total Number of VMs (1)**	**2**
sfo01umds01	lax01umds01	1
Site Recovery Manager and vSphere Replication Total Number of VMs (2)	**Site Recovery Manager and vSphere Replication Total Number of VMs (2)**	**2**
sfo01m01vrms01	lax01m01vrms01	1
sfo01m01srm01	lax01m01srm01	1
vRealize Automation Total Number of VMs (11)	**vRealize Automation Total Number of VMs (2)**	**3**
vra01mssql01	-	1
vra01svr01a	-	2
vra01svr01b	-	2
vra01iws01a	-	3
vra01iws01b	-	4
vra01ims01a	-	5
vra01ims01b	-	6
sfo01ias01a	lax01ias01a	7
sfo01ias01b	lax01ias01b	7
vra01dem01a	-	7
vra01dem01b	-	7
vRealize Business for Cloud Total Number of VMs (2)	**vRealize Business for Cloud Total Number of VMs (1)**	**4**
vrb01svr01	-	1
sfo01vrbc01	lax01vrbc01	2
vRealize Operations Manager Total Number of VMs (5)	**vRealize Operations Manager Total Number of VMs (2)**	**5**

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
vrops01svr01a	-	1
vrops01svr01b	-	2
vrops01svr01c	-	3
sfo01vropsc01a	lax01vropsc01a	4
sfo01vropsc01b	lax01vropsc01b	4
vRealize Log Insight Total Number of VMs (3)	**vRealize Log Insight Total Number of VMs (3)**	**5**
sfo01vrli01a	lax01vrli01a	1
sfo01vrli01b	lax01vrli01b	2
sfo01vrli01c	lax01vrli01c	2
vSphere Data Protection Total Number of VMs (1)	**vSphere Data Protection Total Number of VMs (1)**	**5**
sfo01m01vdp01	lax01m01vdp01	1