Backup and Restore

20 NOV 2018
VMware Validated Design 4.3
VMware Validated Design for Software-Defined Data Center 4.3

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 Backup and Restore

1

The VMware Validated Design Backup and Restore document provides guidance on the use of a vSphere Storage API - Data Protection (VADP) solution for performing backup and restore of the management components in the Software-Defined Data Center (SDDC).

After you deploy the VMware Validated Design for Software-Defined Data Center, backing up management components ensures that you can keep your environment operational in the event of data loss or failure. You implement scheduled backups to prepare for:

- A critical failure of any management component
- An upgrade of any management component
- Updating the certificate of any management component

Intended Audience

VMware Validated Design Backup and Restore is intended for cloud architects, infrastructure administrators, cloud administrators, and cloud operators who are familiar with and want to use VMware software to deploy and 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 Backup and Restore* document is compliant and validated with certain product versions. See *VMware Validated Design Release Notes* for more information about supported product versions

Component Backup Jobs for Data Protection 2

You can configure backup for each SDDC management component separately. For this scenario, there is no requirement to back up the entire SDDC, and this design does not imply such an operation. Some products can perform internal configuration backups. Use those products in addition to the whole VM component backups as appropriate.

Backup Jobs in Region A

Create a single backup job for the components of a management application according to the node configuration of the application in Region A.

Table 2-1. VM Backup Jobs in Region A

Product	Image VM Backup Jobs	Application VM Backups
ESXi	Backup is not applicable	-
Platform Services Controller	Part of the vCenter Server backup job	-

vCenter Server	■ Management Job
	  ■ sfo01m01vc01.sfo01.rainpole.local
	  ■ sfo01m01psc01.sfo01.rainpole.local
	■ Compute Job
	  ■ sfo01w01vc01.sfo01.rainpole.local
	  ■ sfo01w01psc01.sfo01.rainpole.local
		-

NSX for vSphere	Backup is not applicable	-

Table 2-1. VM Backup Jobs in Region A (Continued)

Product	Image VM Backup Jobs	Application VM Backups
vRealize Automation	■ vra01mssql01.rainpole.local ■ vrb01svr01.rainpole.local ■ sfo01vrbc01.sfo01.rainpole.local ■ vra01svr01a.rainpole.local ■ vra01svr01b.rainpole.local ■ vra01svr01c.rainpole.local ■ 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	vra01mssql01.rainpole.local
vRealize Log Insight	■ sfo01vrli01a.sfo01.rainpole.local ■ sfo01vrli01b.sfo01.rainpole.local ■ sfo01vrli01c.sfo01.rainpole.local	-
vRealize Operations Manager	■ vrops01svr01a.rainpole.local ■ vrops01svr01b.rainpole.local ■ vrops01svr01c.rainpole.local ■ sfo01vropsc01a.sfo01.rainpole.local ■ sfo01vropsc01b.sfo01.rainpole.local	-
vRealize Business Server vRealize Business Data Collector	Part of the vRealize Automation backup job	-
vSphere Update Manager Download Service (UMDS)	■ sfo01umds01.sfo01.rainpole.local	-
vRealize Suite Lifecycle Manager	vrslcm01svr01a.rainpole.local	-

Backup Jobs in Region B

Create a single backup job for the components of a management application according to the node configuration of the application in Region B.

Note The backup jobs in Region B are not applicable to a single-region SDDC implementation.

Table 2-2. VM Backup Jobs in Region B

Product	Image VM Backup Jobs	Application VM Backups
ESXi	Backup is not applicable	None
Platform Services Controller	Part of the vCenter Server backup job	

Table 2-2. VM Backup Jobs in Region B (Continued)

Product	Image VM Backup Jobs	Application VM Backups
vCenter Server	■ Management Job ■ lax01m01vc01.lax01.rainpole.local ■ lax01m01psc01.lax01.rainpole.local ■ Compute Job ■ lax01w01vc01.lax01.rainpole.local ■ lax01w01psc01.lax01.rainpole.local	
NSX for vSphere	Backup is not applicable	
vRealize Automation	■ lax01ias01a.lax01.rainpole.local ■ lax01ias01b.lax01.rainpole.local ■ lax01vrbc01.lax01.rainpole.local	
vRealize Log Insight	■ lax01vrli01a.lax01.rainpole.local ■ lax01vrli01b.lax01.rainpole.local ■ lax01vrli01c.lax01.rainpole.local	
vRealize Operations Manager	■ lax01vropsc01a.lax01.rainpole.local ■ lax01vropsc01b.lax01.rainpole.local	
vRealize Business Data Collector	Part of the vRealize Automation backup job	
vSphere Update Manager Download Service (UMDS)	■ lax01umds01.lax01.rainpole.local	

Prerequisites for Backing Up the Software-Defined Data Center 3

Before implementing a backup strategy for the Software-Defined Data Center, ensure that your environment meets certain requirements.

This chapter includes the following topics:

Prerequisites for Backing Up Virtual Infrastructure Layer

Before backing up the Virtual Infrastructure Layer, follow these guidelines.

Verify that the following prerequisites are met before you back up vCenter Server and Platform Services Controller nodes:

- Use a host name that is resolvable in DNS and a static IP address for all nodes.
- All nodes must be powered on and accessible during backup.
- Ensure there are no configuration issues on source and target sites before performing a backup operation.

Prerequisites for Backing Up Operations Management Layer

Before backing up the Operations Management Layer, follow these guidelines.

vRealize Operations Manager Backup Prerequisites

Verify that the following prerequisites are met before you back up vRealize Operations Manager nodes:

- Do not quiesce the file system.
- Use a host name that is resolvable in DNS and a static IP address for all nodes.
- All nodes must be powered on and accessible during backup.
- Back up the entire VM. You must back up all VMDK files that are part of the virtual appliance.

- Do not stop the cluster while performing the backup.

vRealize Log Insight Backup Prerequisites

Verify that the following prerequisites are met before you back up vRealize Log Insight nodes:

- Ensure no configuration problems on source and target sites exist before performing the backup and restore operations.
- Disable quiesced snapshots, as vRealize Log Insight does not support them.
- Use static IP addresses for all nodes in a vRealize Log Insight cluster.
- Use an FQDN for all nodes in the vRealize Log Insight cluster.

Prerequisites for Backing Up Cloud Management Layer

Before backing up the Cloud Management Layer, follow these guidelines.

vRealize Business Backup Prerequisites

Verify that the following prerequisites are met before you back up a vRealize Business node:

- vRealize Business is running and vRealize Automation is registered with it.
- Ensure that you can view the **Business Management** tab in your vRealize Automation deployment.
- vRealize Business is calculating the correct cost of the virtual machines.
- Verify that the VMs provisioned for vRealize Automation and vRealize Orchestrator are visible in vRealize Business and that vRealize Business can calculate the cost of the VMs.

vRealize Automation Backup Prerequisites

Verify that the following prerequisites are met before you back up vRealize Automation nodes:

- When backing up a complete system, back up all instances of the vRealize Automation appliance and databases simultaneously.
- Minimize the number of active transactions before you begin a backup. Schedule your regular backup during a time of low system load.
- Ensure that you back up all databases at the same time.
- Back up the vRealize Automation appliance and the IaaS components before you update certificates.

Prerequisites for Restoring the Software-Defined Data Center

4

Before restoring the SDDC, follow these guidelines.

Prerequisites

- If you have taken any snapshots, you must remove the snapshots before you restore any virtual machines.
- Make sure that restored nodes are in a powered-off state.
- Restore the nodes in a specific order and apply manual configuration changes where applicable.
- You can restore the virtual machines to the same host, to a different host on the same data center, or to a different host on a target data center, depending on the backup tool used.

Backup and Restore Procedure by Solution

5

You back up and restore the management components in the SDDC using two methods - a solution compatible with vSphere Storage API for Data Protection (VADP) for image-based backup of all components and a solution for file-based backup of NSX components using NSX Manager. This VMware Validated Design operational guide uses vSphere Data Protection as a reference backup solution. You can select a different VADP compatible solution for image-based backup.

- Backup and Restore Procedures Using vSphere Data Protection

  Use the following procedures to perform a backup using vSphere Data Protection, so that you can restore the working state of the system in an event of failure.

- Backup and Restore Procedures of NSX Components Using NSX Manager

  You back up certain components of NSX for the management cluster and for the shared edge and compute cluster to restore the operational state of the system in an event of failure.

Backup and Restore Procedures Using vSphere Data Protection

Use the following procedures to perform a backup using vSphere Data Protection, so that you can restore the working state of the system in an event of failure.

- Create a Scheduled Backup Job by Using vSphere Data Protection

  Create full virtual machine image backup jobs to back up vCenter Server instances, Platform Services Controller instances, vRealize Operations Manager, vRealize Log Insight, Cloud Management Platform, and vSphere Update Manager Download Service in Region A and Region B.

- Create a Scheduled Application Backup Job for Microsoft SQL Server

  You install the backup agent on the Microsoft SQL Server for Cloud Management Platform and create a scheduled job for application backup in vSphere Data Protection.

- Perform a Restore Job Using vSphere Data Protection

  When a major hardware failure occurs, restore the virtual appliance nodes of vCenter Server, Platform Services Controller, vRealize Operations Manager, vRealize Log Insight, Cloud Management Platform applications, vSphere Update Manager Download Service and vRealize Suite Lifecycle Manager by using the backups that are created as a result from the scheduled backup job for the nodes.

- Perform an Emergency Restore of vCenter Server

  If the Management vCenter Server stops responding or becomes corrupt as a result of a failure, you perform a direct-to-host emergency restore to return the Management vCenter Server to an operational state. vSphere Data Protection restores the VM that contains the vCenter Server or Platform Services Controller directly on the ESXi host that is running the vSphere Data Protection appliance.

Create a Scheduled Backup Job by Using vSphere Data Protection

Create full virtual machine image backup jobs to back up vCenter Server instances, Platform Services Controller instances, vRealize Operations Manager, vRealize Log Insight, Cloud Management Platform, and vSphere Update Manager Download Service in Region A and Region B.

To ensure that VMware vSphere Data Protection does not perform a quiesced backup, you must disable quiescing on the vRealize Operations Manager and vRealize Log Insight appliances. For additional information on how to disable quiescing, see *vRealize Operations Manager Preparations for Backing Up* section in the *vRealize Suite 2017 Backup and Restore* documentation.

For solutions that support non-quiesced backups disabling quiescing is not necessary.

Procedure

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

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

vCenter Server	URL
Management vCenter Server in Region A	https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client

b Log in using the following credentials.

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

2 On the vSphere Web Client **Home** page, click the **VDP** icon.

3 On the **Welcome to vSphere Data Protection** page, select **sfo01m01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

4 Click the **Backup** tab.

5 From the **Backup job actions** menu, select **New** to run the **Create new backup job** wizard.

6 On the **Job Type** page, select **Guest Images** and click **Next**.

7 On the **Data Type** page, select **Full Image**, leave the **Fall back to the non-quiesced backup if quiescence fails** check box selected, and click **Next**.

8 On the **Backup Sources** page, expand the **Virtual Machines** tree.

Object	Value
vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Data center	sfo01-m01dc
Cluster	sfo01-m01-mgmt01

9 Select the virtual appliances for the specific product and click **Next**.

Order	Product	Virtual Appliance in Region A	Virtual Appliance in Region B	Backup Job Name
1	vCenter Server and Platform Services Controller	■ sfo01m01psc01 ■ sfo01m01vc01 ■ sfo01w01psc01 ■ sfo01w01vc01	■ lax01m01psc01 ■ lax01m01vc01 ■ lax01w01psc01 ■ lax01w01vc01	Management and Compute vCenter Server Backups
2	vRealize Suite Lifecycle Manager	vrslcm01svr01a	-	vRealize Suite Lifecycle Manager Backups
3	vRealize Operations Manager	■ vrops01svr01a ■ vrops01svr01b ■ vrops01svr01c ■ sfo01vropsc01a ■ sfo01vropsc01b	■ lax01vropsc01a ■ lax01vropsc01b	vRealize Operations Manager Backups
4	vRealize Log Insight	■ sfo01vrli01a ■ sfo01vrli01b ■ sfo01vrli01c	■ lax01vrli01a ■ lax01vrli01b ■ lax01vrli01c	vRealize Log Insight Backups
5	Cloud Management Platform	■ vra01svr01a ■ vra01svr01b ■ vra01svr01c ■ vra01ims01a ■ vra01ims01b ■ vra01iws01a ■ vra01iws01b ■ vra01mssql01 ■ sfo01ias01a ■ sfo01ias01b ■ vra01dem01a ■ vra01dem01b ■ vrb01svr01 ■ sfo01vrbc01	■ lax01ias01a ■ lax01ias01b ■ lax01vrbc01	Cloud Management Platform Backups
6	vSphere Update Manager Download Service	sfo01umds01	lax01umds01	vSphere Update Manager Download Service Backups

10 On the **Schedule** page, set **Backup Schedule** to **Daily** and click **Next**.

11 On the **Retention Policy** page, select **Keep for 3 days** and click **Next**.

12 On the **Job Name** page, enter the component backup job name from Step 9 and click **Next**.

13 On the **Ready to Complete** page, review the summary information for the backup job and click **Finish**.

14 In the dialog box that shows a confirmation that the job is created, click **OK**.

Create a Scheduled Application Backup Job for Microsoft SQL Server

You install the backup agent on the Microsoft SQL Server for Cloud Management Platform and create a scheduled job for application backup in vSphere Data Protection.

Procedure

1 Download the backup agent on the Microsoft SQL Server machine.

a Open a Remote Desktop Protocol (RDP) connection to the virtual machine vra01mssql01.rainpole.local.

b Log in using the following credentials.

Setting	Value
User name	*Windows administrator user*
Password	*windows_administrator_password*

c Open a web browser and go to the vSphere Web Client URL **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

d Log in using the following credentials.

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

e On the vSphere Web Client **Home** page, click the **VDP** icon.

f On the **Welcome to vSphere Data Protection** page, select **sfo01m01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

g Click the **Configuration** tab and in the **Downloads** pane click the **Microsoft SQL Server 64 bit** link.

The Web browser starts downloading the installer of the vSphere Data Protection backup agent.

2 Install the backup agent on the Microsoft SQL Server machine.

   a After the `VMwareVDPSQL-windows-x86_64_version.msi` file is saved, double-click it to start the installation.

      The **VMware VDP for SQL Server Setup** wizard opens.

   b On the **Welcome to the VMware VDP for SQL Server Setup Wizard** page, click **Next**.

   c On the **End-User License Agreement** page, accept the end-user license agreement and click **Next**.

   d On the **VMware VDP for SQL Server Setup** page, click **Next** to accept the default installation location for the backup agent.

   e On the **Appliance Registration Information** page, enter **`sfo01m01vdp01.sfo01.rainpole.local`** in the **VDP Appliance** text box and click **Next**.

   f On the **Ready to install VMware VDP for SQL Server** page, click **Install**.

   g After the installation is complete, on the **Completed the VMware VDP for SQL Server Setup Wizard** page, click **Finish**.

3 Create a scheduled backup job for the Microsoft SQL server.

   a On the vSphere Web Client **Home** page, click the **VDP** icon.

   b On the **Welcome to vSphere Data Protection** page, select **sfo01m01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

   c Click the **Backup** tab, and from the **Backup job actions** menu, select **New** to open the **Create a new backup job** wizard.

   d On the **Job Type** page, select **Applications** and click **Next**.

   e On the **Data Type** page, select **Full Server** and click **Next**.

   f On the **Backup Sources** page, expand Microsoft SQL Server, select **vra01mssql01.rainpole.local**, and click **Next**.

   g On the **Backup Options** page, leave all default values and click **Next**.

   h On the **Schedule** page, set **Backup Schedule** to **Daily** and click **Next**.

   i On the **Retention Policy** page, select **Keepfor3days** and click **Next**.

   j On the **Job Name** page, enter **`Cloud Management Platform MSSQL Server Backups`** as a name for the backup job and click **Next**.

   k On the **Ready to Complete** page, review the summary information for the backup job and click **Finish**.

   l In the dialog box that shows a confirmation that the job is created, click **OK**.

Perform a Restore Job Using vSphere Data Protection

When a major hardware failure occurs, restore the virtual appliance nodes of vCenter Server, Platform Services Controller, vRealize Operations Manager, vRealize Log Insight, Cloud Management Platform applications, vSphere Update Manager Download Service and vRealize Suite Lifecycle Manager by using the backups that are created as a result from the scheduled backup job for the nodes.

Procedure

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

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

vCenter Server	URL
Management vCenter Server in Region A	https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client

b Log in using the following credentials.

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

2 Shut down all the virtual appliances of the product which you are restoring.

a Click **Home > Hosts and Clusters**.

b In the **Navigator** pane expand the following inventory tree.

Region A inventory tree	Region B
sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc **>** sfo01-m01-mgmt01	lax01m01vc01.lax01.rainpole.local **>** lax01-m01dc **>** lax01-m01-mgmt01

c Navigate to each appliance in the specified order, right-click the appliance object, select **Power > Shut Down Guest OS**, and in the **Confirm Guest Shut Down** dialog box, click **Yes**.

Order	Product	Virtual Appliance in Region A	Virtual Appliance in Region B
1	vCenter Server and Platform Services Controller	■ sfo01w01vc01 ■ sfo01w01psc01	■ lax01w01vc01 ■ lax01w01psc01
	vRealize Suite Lifecycle Manager	vrslcm01svr01a	-
2	vRealize Operations Manager	■ sfo01vropsc01a ■ sfo01vropsc01b ■ vrops01svr01a ■ vrops01svr01b ■ vrops01svr01c	■ lax01vropsc01a ■ lax01vropsc01b
3	vRealize Log Insight	■ sfo01vrli01b ■ sfo01vrli01c ■ sfo01vrli01a	■ lax01vrli01b ■ lax01vrli01c ■ lax01vrli01a
4	Cloud Management Platform	■ sfo01ias01a ■ sfo01ias01b ■ vra01dem01a ■ vra01dem01b ■ vra01ims01a ■ vra01ims01b ■ vra01iws01a ■ vra01iws01b ■ vra01svr01a ■ vra01svr01b ■ vra01svr01c ■ vrb01svr01 ■ sfo01vrbc01 ■ vra01mssql01	■ lax01ias01a ■ lax01ias01b ■ lax01vrbc01
	vSphere Update Manager Download Service	■ sfo01umds01	■ lax01umds01

3 Restore the latest VMs backup of the specific product from the vSphere Data Protection server.

   a On the vSphere Web Client **Home** page, click the **VDP** icon.

   b On the **Welcome to vSphere Data Protection** page, select **sfo01m01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

   c Click the **Restore** tab.

   d Select a node of the specific product.

   You see the list of the backups for the appliance.

   e Select the check box for the latest appliance backup and click the back arrow to return to the list of backups.

   f Select the latest backups of the other appliances of the product.

   g Click **Restore** on the toolbar.

   The **Restore backup** wizard opens.

   h On the **Select Backup** page, click **Next**.

   i On the **Set Restore Options** page, select **Restore to original location** for each appliance, and click **Next**.

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

   k Click **OK** to close the **Info** dialog box.

4 Verify that the restore is successful.

   a On the **vSphere Data Protection** page, click the **Configuration** tab and click **Log**.

   b Locate the following logs:

```
Restore of client named product_vm_name completed.
```

5 Power on the virtual appliance nodes of specific product in the following order:

Product	Virtual Appliance in Region A	Virtual Appliance in Region B
vCenter Server and Platform Services Controller	■ sfo01w01psc01 ■ sfo01w01vc01	■ lax01w01psc01 ■ lax01w01vc01
vRealize Suite Lifecycle Manager	vrslcm01svr01a	-
vRealize Operations Manager	■ vrops01svr01a ■ vrops01svr01b ■ vrops01svr01c ■ sfo01vropsc01a ■ sfo01vropsc01b	■ lax01vropsc01a ■ lax01vropsc01b
vRealize Log Insight	■ sfo01vrli01a ■ sfo01vrli01b ■ sfo01vrli01c	■ lax01vrli01a ■ lax01vrli01b ■ lax01vrli01c

Product	Virtual Appliance in Region A	Virtual Appliance in Region B
Cloud Management Platform	■ vra01mssql01 ■ vra01svr01a ■ vra01svr01b ■ vra01svr01c ■ vra01iws01a ■ vra01iws01b ■ vra01ims01a ■ vra01ims01b ■ sfo01ias01a ■ sfo01ias01b ■ vra01dem01a ■ vra01dem01b ■ vrb01svr01 ■ sfo01vrbc01	■ lax01ias01a ■ lax01ias01b ■ lax01vrbc01
vSphere Update Manager Download Service	■ sfo01umds01	■ lax01umds01

a Navigate to each of the appliance, right-click the appliance object, and select **Power > Power On**.

b Wait until the current appliance is up and running before powering on the next appliance.

What to do next

Verify that all restored virtual machines are operational. See *VMware Validated Design Operations Verification* documentation for product specific verification procedures.

Perform an Emergency Restore of vCenter Server

If the Management vCenter Server stops responding or becomes corrupt as a result of a failure, you perform a direct-to-host emergency restore to return the Management vCenter Server to an operational state. vSphere Data Protection restores the VM that contains the vCenter Server or Platform Services Controller directly on the ESXi host that is running the vSphere Data Protection appliance.

You perform the direct-to-host emergency restore from backups of vCenter Server and Platform Services Controller that vSphere Data Protection has previously saved according to the settings in the backup job you created. You cannot use a regular restore because both the Management vCenter Server and the associated Platform Services Controller must be available.

Note If vCenter Server and Platform Services Controller instances fail at the same time, you must first restore the Platform Services Controller and then the vCenter Server instances.

Procedure

1 Log in to the vSphere Data Protection Configure Utility.

   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_appliance_root_password*

2 Click the **Configuration** tab. In the **Proxies** table, locate the ESXi host that runs the **sfo01m01vdp01** appliance and note down the FQDN of the host.

3 Disconnect the ESXi host that is running the vSphere Data Protection appliance from the Management vCenter Server.

   a On the Windows host that has access to your data center, log in to the ESXi host using the FQDN that you have located in the vSphere Data Protection Configure Utility and the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

   b Navigate to the host object in the **Navigator** pane.

   c Click the **Actions** tab and select **Disconnect from vCenter Server**.

   d Click the **Disconnect** in the **Disconnect from vCenter Server** dialog box.

4 Restore the virtual appliance of the Management vCenter Server or Management Platform Services Controller.

   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_appliance_root_password*

   c Click the **Emergency Restore** tab.

d Expand the virtual appliance node for the Management vCenter Server or Management Platform Services Controller that you must restore, expand the virtual machine, and select the latest backup to restore from.

Role	Virtual Appliance Name
Management vCenter Server	sfo01m01vc01
Platform Services Controller that is associated with the Management vCenter Server	sfo01m01psc01

e Click the **Restore** button.

f In the **Host Credentials** dialog box, enter the credentials for connection to the ESXi host that is running the vSphere Data Protection appliance and click **OK**.

ESXi Host Connection Option	Value
Hostname or IP	Default value
Port number	443
User name	root
Password	*esxi_root_user_password*

g In the **Restore a Backup** dialog box, enter a new name for the restored VM in the **New Name** text box.

Role	Virtual Appliance Name
Management vCenter Server	sfo01m01vc01.restored
Platform Services Controller that is associated with the Management vCenter Server	sfo01m01psc01.restored

h From the **Datastore** drop-down menu, select the **sfo01-m01-vsan01** datastore and click **Restore**.

i Repeat the step to restore the other appliance.

5 Power on the Platform Services Controller virtual machine.

a In the vSphere Host Client connected to the host that runs the vSphere Data Protection appliance, navigate to the virtual machine of Platform Services Controller **sfo01m01psc01.restored**.

b Right-click the virtual machine and select **Power > Power On**.

6 Wait until the appliance turns on and verify the status of the Platform Services Controller services.

a Log in to the Platform Services Controller appliance shell as the `root` user.

b Run the `service-control --status --all` command to verify that all the services are running.

7 Power on the vCenter Server virtual machine.

   a In the vSphere Host Client connected to the host that runs the vSphere Data Protection appliance, navigate to the virtual machine of vCenter Server **sfo01m01vc01.restored**.

   b Right-click the virtual machine and select **Power > Power On**.

8 Wait until the appliance turns on and verify the status of the vCenter Server services.

   a Log in to the vCenter Server Appliance shell as the root user.

   b Run the `service-control --status --all` command to verify that all the services are running.

   c If the services are not running, run the `vcenter-restore` script in the following way.

```
vcenter-restore -u administrator@vsphere.local -p vsphere_admin_password
```

9 After the Management vCenter Server is up and running, use the vSphere Web Client to reconnect the ESXi host that is running the vSphere Data Protection appliance.

   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 Right-click the host and select **Connection > Connect**.

   d On the **Reconnect host** dialog box, click **Yes**.

What to do next

Verify that the Management Platform Services Controller and the Management vCenter Server are operational. See *Validate Platform Services Controller and vCenter Server Instances* in the *VMware Validated Design Operational Verification Guide* documentation.

Backup and Restore Procedures of NSX Components Using NSX Manager

You back up certain components of NSX for the management cluster and for the shared edge and compute cluster to restore the operational state of the system in an event of failure.

The following components support back up and restore:

- NSX Manager
- NSX Firewall Rules
- NSX Service Composer

- vSphere Distributed Switch

All NSX Edge configurations, such as distributed logical routers and services gateways, and controller nodes are backed up as part of the NSX Manager data backup.

If the configuration of the NSX Manager is intact, you can recreate an inaccessible or failed edge appliance VM by redeploying the NSX Edge. To redeploy the NSX Edge, click the **Redeploy NSX Edge** button in the vSphere Web Client.

Backing up NSX Manager regularly enables you to restore the operational state of your system in the event of a catastrophic failure. You can schedule backups for business continuity and operational requirements. Set the backup frequency according to the rate of configuration changes occurring in NSX. You can back up NSX manually or schedule hourly, daily, or weekly automatic backups.

Back up NSX and vCenter Server before and after the following events:

- NSX or vCenter Server upgrade.
- Day 0 deployment and configuration of NSX components.
- Major Day 2 changes.

- Backup NSX Manager

  You back up the NSX Manager data by scheduling a regular backup.

- Restore NSX Manager

  When you restore NSX Manager from a backup, you deploy a new NSX Manager appliance to restore the backup to. Restoring to an existing NSX Manager instances is not supported.

- Export the NSX Firewall Configuration

  You export all firewall rules in an NSX Manager to an XML configuration file. You use that configuration file to import and load firewall rules on another NSX instance to recover the rule configuration.

- Import the NSX Firewall Configuration

  You can import a configuration XML file exported from NSX Manage to load the configuration in the firewall table. The imported configuration overwrites the existing rules.

- Export a Service Composer Configuration

  You export a Service Composer configuration of security policies to use as a backup or to replicate the configuration to another NSX Manager environment. The exported configuration includes the security groups to which the security policies are mapped.

- Import a Security Policies Configuration

  You import a saved security policies configuration file to restore a misconfigured policy or to replicate the configuration to a different NSX Manager. The imported configuration also contains the security groups to which the security policies are mapped.

- Export Configurations of the Distributed Switches

  You can export vSphere Distributed Switch and distributed port group configurations to a file. The file preserves validated network configurations and enables you to transfer these configurations to other environments.

- Restore the Configuration of a Distributed Switch

  You use the restore option to reset the configuration of one of the distributed switches in Region A from the settings exported in a configuration file.

Backup NSX Manager

You back up the NSX Manager data by scheduling a regular backup.

You configure backup and restore operations from the NSX Manager virtual appliance UI. You can schedule backups on an hourly, daily, or weekly basis. The backup data is saved to a remote location that NSX Manager can access through FTP or SFTP. Backed data includes System Configuration, Audit Logs, System Events, and Flow Records. Configuration tables are included in every backup. Backup for the NSX Manager certificate is not supported.

You can restore backed data only on the same NSX Manager version as the version on which the backup was taken.

Prerequisites

- An FTP server that is accessible from the NSX Manager for the management cluster and from the NSX Manager for the shared edge and compute cluster.

Procedure

1 Log in to the NSX Manager appliance user interface.

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

NSX Manager	URL
NSX Manager for the management cluster	`https://sfo01m01nsx01.sfo01.rainpole.local`
NSX Manager for the shared edge and compute cluster	`https://sfo01w01nsx01.sfo01.rainpole.local`

  b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 On the main page of the appliance user interface, click **Backup & Restore**.

3 On the **Backups & Restore** page, click **Change** next to **FTP Server Settings** to set a storage location for the backup job.

4 In the **Backup Location** dialog box, configure the following settings for the backup storage on the FTP server and click **OK**.

Backup Location Setting	Value
IP/Host name	*FQDN of the FTP Server*
Transfer protocol	Select the protocol from the drop-down menu
Port	*Server port for FTP or SFTP requests*
User name	*User name on the FTP server*
Password	*Password for the name you specified in User name*
Backup Directory	Absolute path to the location on the FTP server where you want to store the backup
Filename Prefix	■ **`sfo_NSX_Mgmt`** for the NSX Manager for the management cluster ■ **`sfo_NSX_Comp`** for the NSX Manager for the shared edge and compute cluster
Pass Phrase	*nsx_backup_pass_phrase*

5 On the **Backups & Restore** page, click **Change** next to **Scheduling**.

6 In the **Create or Schedule Backup** dialog box, configure the following schedule for the backup and click **Schedule**.

Setting	Value
Backup Frequency	Hourly
Day of week	-
Hour of day	-
Minute	0

All NSX Edge configurations, such as distributed logical routers and services gateways, and controller nodes are backed up as part of NSX Manager data backup. If the configuration of the NSX Manager is intact, you can recreate an inaccessible or failed edge appliance VM by redeploying the NSX Edge. You simply click the **Redeploy NSX Edge button** on the edge in the vSphere Web Client.

Restore NSX Manager

When you restore NSX Manager from a backup, you deploy a new NSX Manager appliance to restore the backup to. Restoring to an existing NSX Manager instances is not supported.

Prerequisites

- Verify that the FTP server storing the backup data is running.
- Deploy a new NSX Manager appliance. See *Deploy and Configure the Management Cluster NSX Instance in Region A* and *Deploy and Configure the Shared Edge and Compute Cluster NSX Instance in Region A*.
- The new NSX Manager appliance on which the restore is performed must be the same version as the NSX Manager appliance from which the backup was taken.

Procedure

1 Log in to the NSX Manager appliance user interface.

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

NSX Manager	URL
NSX Manager for the management cluster	`https://sfo01m01nsx01.sfo01.rainpole.local`
NSX Manager for the shared edge and compute cluster	`https://sfo01w01nsx01.sfo01.rainpole.local`

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 On the main page of the appliance user interface, click **Backup & Restore**.

3 On the **Backups & Restore** page, click **Change** next to **FTP Server Settings** to set a storage location for the backup job.

4 In the **Backup Location** dialog box, configure the following settings for the backup storage on the FTP server and click **OK**.

Backup Location Setting	Value
IP/Host name	*FQDN of the FTP Server*
Transfer protocol	Select the protocol from the drop down menu
Port	*Server port for FTP or SFTP requests*
User name	*User name on the FTP server*
Password	*Password for the name you specified in User name*
Backup Directory	*Absolute path to the location on the FTP server where you want to store the backup*
Filename Prefix	■ **`sfo_NSX_Mgmt`** for the NSX Manager for the management cluster ■ **`sfo_NSX_Comp`** for the NSX Manager for the shared edge and compute cluster
Pass Phrase	*nsx_backup_pass_phrase*

5 In the **Backups History** section on the **Backups & Restore** page, select the latest restore point, and click **Restore**.

6 In the **Restore from Backup** dialog box, click **Yes** to confirm the restart of the appliance.

The appliance management will be unavailable for during the restart.

What to do next

Verify that NSX Manager is operational. See *Validate NSX Manager and NSX Controller Instances* in the *VMware Validated Design Operational Verification* documentation.

Export the NSX Firewall Configuration

You export all firewall rules in an NSX Manager to an XML configuration file. You use that configuration file to import and load firewall rules on another NSX instance to recover the rule configuration.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu, select **Networking & Security**.

3 In the **Navigator**, click **Firewall**.

4 On the **Firewall** page, from the **NSX Manager** drop-down menu, select the IP address of the NSX Manager instance.

NSX Manager	URL
NSX Manager for the management cluster	172.16.11.65
NSX Manager for the shared edge and compute cluster	172.16.11.66

5 On the **Firewall** page, from the **More** drop-down menu, select **Export Current Configuration**.

6 On the **Export Current Configuration** dialog box, click **Export** and save the exported firewall configuration file.

7 Repeat the steps to export the firewall configuration of the second NSX Manager.

What to do next

Import the exported rule configuration to restore the firewall rules or import the firewall rule configuration in a new NSX Manager instance.

Import the NSX Firewall Configuration

You can import a configuration XML file exported from NSX Manage to load the configuration in the firewall table. The imported configuration overwrites the existing rules.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu, select **Networking & Security**.

3 In the **Navigator**, click **Firewall Settings**.

4 From the **NSX Manager** drop-down menu, select the IP address of the NSX Manager instance.

NSX Manager	URL
NSX Manager for the management cluster	172.16.11.65
NSX Manager for the shared edge and compute cluster	172.16.11.66

5 On the **Firewall Settings** page, click the **Saved Configurations** tab and click **Import**.

6 On the **Import Configuration** dialog box, click **Choose File**, select the exported firewall configuration XML file, and click **Import**.

   The firewall configuration is imported into **Saved Configurations**.

7 In the **Navigator**, click **Firewall**.

8 On the **Firewall** page, from the **More** drop-down menu, select **Load Saved Configuration**.

9 On the **Load Saved Configuration** dialog box, select the imported configuration file and click **Load**.

   Rules are imported based on rule names. During the import, the firewall ensures that each object referenced in the rule exists in your environment. If an object is not found, the rule is marked as invalid. If a rule references a dynamic security group, the dynamic security group is created in NSX Manager during the import. If your current configuration contains rules managed by Service Composer, these rules are overwritten when you load the imported firewall configuration.

10 If the imported firewall configuration contains rules managed by Service Composer, synchronize the imported rules and reconfigure them to be managed by the Service Composer again.

   a On the **Service Composer** page, click the **Security Policies** tab and select the policy.

   b From the **Actions** menu, select **Synchronize Firewall Config**.

11 Repeat the steps to import the firewall configuration for the second NSX Manager.

Export a Service Composer Configuration

You export a Service Composer configuration of security policies to use as a backup or to replicate the configuration to another NSX Manager environment. The exported configuration includes the security groups to which the security policies are mapped.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu, select **Networking & Security**.

3 In the **Navigator**, click **Service Composer**.

4 Click the **Security Policies** tab.

5 From the **NSX Manager** drop-down menu, select the IP address of the NSX Manager instance that runs the Service Composer.

NSX Manager	IP Address
NSX Manager for the management cluster	172.16.11.65
NSX Manager for the shared edge and compute cluster	172.16.11.66

6 Select the security policy to export and click **More > Export Configuration**.

   The **Export Services Composer Configuration** wizard opens.

7 On the **Name and Description** page, enter name, description, and prefix for the backup, and click **Next**.

   The prefix is added to the exported security policies and security groups. Setting a prefix makes the names of the exported security policies unique.

8 On the **Select Security Policies** page, select the security policies to export and click **Next**.

9 On the **Preview Selection** page, review the security policies and associated objects, click **Finish**, and save the exported service composer configuration file.

10 Repeat the steps for second NSX manager.

Import a Security Policies Configuration

You import a saved security policies configuration file to restore a misconfigured policy or to replicate the configuration to a different NSX Manager. The imported configuration also contains the security groups to which the security policies are mapped.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu, select **Networking & Security**.

3 In the **Navigator**, click **Service Composer**.

4 Click the **Security Policies** tab.

5 From the **NSX Manager** drop-down menu, select the IP address of the NSX Manager instance that runs the Service Composer.

NSX Manager	URL
NSX Manager for the management cluster	172.16.11.65
NSX Manager for the shared edge and compute cluster	172.16.11.66

6 On the **Service Composer** page, select **More > Import Configuration**.

   The **Import Policy Configuration** wizard opens.

7 On the **Import policy Configuration** dialog box, click **Choose File**, navigate to the security policies configuration file, enter a suffix for the names of the imported policies, and click **Apply**.

   The page shows the security groups to which the policies are applied, the endpoint services, firewall rules, and network introspection services which are part of the policies.

8 Repeat the steps for the second NSX Manager.

Export Configurations of the Distributed Switches

You can export vSphere Distributed Switch and distributed port group configurations to a file. The file preserves validated network configurations and enables you to transfer these configurations to other environments.

You can use the exported file to create multiple copies of the distributed switch configuration on an existing deployment, or overwrite the settings of existing distributed switches and port groups.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu, select **Networking**, expand the vCenter Server tree, and locate the distributed switch.

vCenter Server	Distributed Switch
sfo01m01vc01.sfo01.rainpole.local	sfo01-m01-vds01
sfo01w01vc01.sfo01.rainpole.local	sfo01-w01-vds01

3 Right-click the distributed switch and select **Settings > Export Configuration**.

4 In the **Export Configuration** dialog box, select **Distributed switch and all port groups** and click **OK**.

5 After the configuration is generated, click **Yes** to save the configuration file.

6 Repeat the steps for the second distributed switch.

Restore the Configuration of a Distributed Switch

You use the restore option to reset the configuration of one of the distributed switches in Region A from the settings exported in a configuration file.

The restore operation changes the settings on the selected switch back to the settings saved in the configuration file. The operation overwrites the current settings of the distributed switch and its port groups. It does not delete existing port groups that are not a part of the configuration file.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu, select **Networking**, expand the vCenter Server tree, and locate the distributed switch.

vCenter Server	Distributed Switch
sfo01m01vc01.sfo01.rainpole.local	sfo01-m01-vds01
sfo01w01vc01.sfo01.rainpole.local	sfo01-w01-vds01

3 Right-click the distributed switch and select **Settings > Restore Configuration**.

4 In the **Restore Configuration** wizard, browse to the location of the configuration file for the distributed switch.

5 Select the **Restore distributed switch and all port groups** option and click **Next**.

6 On the **Ready to complete** page, review the changes and click **Finish**.

7 Repeat the steps for the second distributed switch.

SDDC Startup and Shutdown

6

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 components.

- 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 components.

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 components.

Before you begin:

- Verify that virtual machines are not running on snapshots.
- Ensure verified backups of all management and tenant virtual machines are available.
- If a data protection solution is running on the management clusters, verify that the solution is properly shutdown following the vendor guidance.
- If the hosts in a vSAN cluster are to be shut down, appropriately shut down the tenant workloads in the shared edge and compute cluster.

Shutting down the ESXi hosts in the vSAN clusters:

- Refer to VMware Knowledge Base article 2142676 for information on preparing and shutting down ESXi hosts in vSAN clusters.

Shutting down the management virtual machines:

- Shut down the virtual machines of the SDDC management stack in the shutdown order provided in the following table.

- Verify that the console of the virtual machine and its services are completely shut down before moving to the next virtual machine.

Note The vCenter Server instances, NSX load balancers for the Platform Services Controllers, the Platform Services Controllers, and the management clusters are the last virtual machines to be shut down.

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
vRealize Suite Lifecycle Manager Total Number of VMs (1)	**vRealize Suite Lifecycle Manager Total Number of VMs (0)**	**1**
vrslcm01svr01a	-	1
vRealize Log Insight Total Number of VMs (3)	**vRealize Log Insight Total Number of VMs (3)**	**2**
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)**	**2**
sfo01vropsc01b	lax01vropsc01b	1
sfo01vropsc01a	lax01vropsc01a	1
vrops01svr01c	-	2
vrops01svr01b	-	3
vrops01svr01a	-	4
vRealize Business for Cloud Total Number of VMs (2)	**Realize Business for Cloud Total Number of VMs (2)**	**3**
sfo01vrbc01	lax01vrbc01	1
vrb01svr01	-	2
vRealize Automation Total Number of VMs (11)	**vRealize Automation Total Number of VMs (2)**	**4**
vra01dem01a	-	1
vra01dem01b	-	1
sfo01ias01b	lax01ias01b	1
sfo01ias01a	lax01ias01a	1
vra01ims01b	-	2
vra01ims01a	-	2
vra01iws01b	-	3
vra01iws01a	-	4
vra01svr01c	-	5
vra01svr01b	-	5

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
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)**	**5**
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)**	**5**
sfo01umds01	lax01umds01	1
Core Stack **Total Number of VMs (26)**	**Core Stack** **Total Number of VMs (16)**	**6**
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
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

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 components.

Before you begin:

- Verify that external dependencies for the SDDC, such as, Active Directory, DNS, NTP, SMTP, and FTP/SFTP are available.

Starting up the ESXi hosts in the vSAN clusters:

- If the vSAN clusters are shut down, refer to VMware Knowledge Base article 2142676 for information on starting up hosts and exiting maintenance mode.

Starting up the management virtual machines:

- Start up the virtual machines in the startup order provided in the following table.
- Verify that the console of the virtual machine and its services are all up before proceeding with the next virtual machine.
- Refer to VMware Knowledge Base article 2142676 for information on verifying the health of the vSAN clusters before starting up tenant workloads.
- If a data protection solution is deployed on the management cluster, verify that the solution is properly started and operational, following the vendor guidance.

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
Core Stack Total Number of VMs (26)	**Core Stack Total Number of VMs (16)**	**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
sfo01w01nsxc01	-	5
sfo01w01nsxc02	-	5
sfo01w01nsxc03	-	5
sfo01m01lb01 (0,1)	lax01m01lb01 (0,1)	6

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
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
vra01svr01c	-	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**
vrops01svr01a	-	1

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
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
vRealize Suite Lifecycle Manager **Total Number of VMs (1)**	**vRealize Suite Lifecycle Manager** **Total Number of VMs (0)**	**6**
vrslcm01svr01a	-	1