Backup and Restore

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 Web site at:

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

VMware Validated Design Backup and Restore provides step-by-step instructions about using vSphere Data Protection for backup and restore of the management components in the software-defined data center (SDDC).

Maintaining Operational Infrastructure

After you deploy the SDDC stack using VMware Validated Design, backing up management products ensures that you can keep your environment operational. If a failure occurs, you can restore the failed component from a backup.

Intended Audience

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

Required Software

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

Verifying the SDDC Operational State

After you restore management components of the SDDC, verify they are operating according to design objectives. For more information, see the *VMware Validated Design Operational Verification* documentation.

Backup and Restore 2

The VMware Validated Design supports business continuity by using vSphere Data Protection for backup and restore.

To ensure that all component VMs of a single product are backed up synchronously with each other, a single VM folder for each product needs to be created within vCenter and then a backup policy should be set for each folder.

Stagger the start times of each backup policy by 15 minutes to ensure that the backups are completed in a serial fashion and prevent from resource contention for datastore snapshot limits.

This chapter includes the following topics:

Region A Backup and Restore

Back up the management components of the SDDC in Region A so that you can restore the SDDC state if a hardware failure occurs. You can create backup copies by using either vSphere Data Protection or the built-in backup mechanism of some of the products.

Use backup jobs in vSphere Data Protection for the following components:

- vCenter Server
- Platform Services Controller
- vRealize Operations Manager
- vRealize Log Insight
- Cloud Management Platform
- vSphere Update Manager Download Service

For the networking components of the SDDC, use the following backup mechanisms:

- Use NSX to back up NSX Manager and NSX security configurations.
- Export a configuration of vSphere Distributed Switch as a backup.

Procedure

1 Backing Up and Restoring vCenter Server in Region A on page 8

Schedule regular backup jobs of the vCenter Server instances and the connected Platform Services Controllers in Region A, and perform restore in cases of corrupt appliance instances.

2 Backing Up and Restoring vRealize Operations Manager in Region A on page 14

Back up and restore the virtual appliances for the vRealize Operations Manager nodes in the analytics cluster and the remote collector cluster in Region A. Restore vRealize Operations Manager according to the dependencies between the nodes.

3 Backing Up and Restoring vRealize Log Insight in Region A on page 17

Back up and restore the virtual appliances for the vRealize Log Insight nodes in Region A. Restore vRealize Log Insight according to the dependencies between the nodes.

4 Backing Up and Restoring Cloud Management Platform in Region A on page 20

Backup the Linux virtual appliances and the Windows virtual machines of Cloud Management Platform using image-level backup. Use application-level backup for the Microsoft SQL Server instance that hosts the databases for the IaaS components and vRealize Orchestrator.

5 Backing Up and Restoring the NSX Instances in Region A on page 25

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

6 Backing Up and Restoring vSphere Update Manager Download Service in Region A on page 33

Back up and restore the virtual appliance for the vSphere Update Manager Download Service in Region A.

Backing Up and Restoring vCenter Server in Region A

Schedule regular backup jobs of the vCenter Server instances and the connected Platform Services Controllers in Region A, and perform restore in cases of corrupt appliance instances.

Note Backing up the embedded PostgreSQL database is not required for this validated design. If you plan to add such an additional layer of recoverability, see VMware Knowledge Base article 2091961.

1 Create Scheduled Backup Jobs for the vCenter Server Instances in Region A on page 9

Create a scheduled job for full image backup of vCenter Server and the connected external Platform Services Controller. Schedule backups for both the Management vCenter Server and Compute vCenter Server.

2 Restore the Management vCenter Server in Region A on page 10

If the Management vCenter Server stops responding or becomes corrupt as a result of a failure in the environment, to restore the Management vCenter Server, perform a direct-to-host emergency restore. 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.

3 Restore the Compute vCenter Server in Region A on page 12

Restore the Compute vCenter Server or the connected Platform Services Controller if a major hardware failure occurs.

Create Scheduled Backup Jobs for the vCenter Server Instances in Region A

Create a scheduled job for full image backup of vCenter Server and the connected external Platform Services Controller. Schedule backups for both the Management vCenter Server and Compute vCenter Server.

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 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 a 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, fully 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 vCenter Server and the Platform Services Controller, and click **Next**.

Object	VM name
Management Platform Services Controller	sfo01m01psc01
Management vCenter Server	sfo01m01vc01
Compute Platform Services Controller	sfo01w01psc01
Compute vCenter Server	sfo01w01vc01

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 **`Management and Compute vCenter Server Backups`** as a name for the backup job 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**.

Restore the Management vCenter Server in Region A

If the Management vCenter Server stops responding or becomes corrupt as a result of a failure in the environment, to restore the Management vCenter Server, perform a direct-to-host emergency restore. 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 have created. You cannot use a regular restore in this case because both the Management vCenter Server and the associated Platform Services Controller must be available.

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 write 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
Username	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 starts 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 starts 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, 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.

Restore the Compute vCenter Server in Region A

Restore the Compute vCenter Server or the connected Platform Services Controller if a major hardware failure occurs.

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 Shut down the Platform Services Controller and vCenter Server virtual appliances.

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

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

c Navigate to each vCenter object below, right click the VM, select **Power > Shut Down Guest OS** and click **Yes** in the Confirm Guest Shut Down dialog box.

#	vCenter Server Component	VM Name
1	Compute Platform Services Controller	sfo01w01psc01
2	Compute vCenter Server	sfo01w01vc01

3 Restore the latest vCenter Server and Platform Services Controller backup from vSphere Data Protection.

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 and select the **sfo01w01psc01** virtual appliance from the list of VMs.

You see the list of the backups for the appliance.

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

e From the list of VMs, select the **sfo01w01vc01** virtual appliance and select the latest backup.

f Click **Restore** on the toolbar.

The Restore backup wizard opens.

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

h On the Set Restore Options page, select **Restore to original location** and click **Next**.

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

j Click **OK** to close the Info dialog.

4 Verify that the restore is successful.

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

b Locate the following logs:

```
Restore of client named sfo01w01psc01 completed.
Restore of client named sfo01w01vc01 completed.
```

5 After restore job is completed, power on the Compute Platform Services Controller virtual machine.

a Navigate to the virtual machine of Platform Services Controller **sfo01w01psc01**.

b Right-click the **sfo01w01psc01** appliance object and select **Power > Power On**.

6 Wait until the appliance is up and verify the status of the Platform Services Controller services.

a Log in to the Compute Platform Services Controller Appliance shell as the root user.

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

7 After Compute Platform Services Controller is up and running, power on the Compute vCenter Server virtual machine.

   a Navigate to the virtual machine of Compute vCenter Server **sfo01w01vc01**.

   b Right-click the **sfo01w01vc01** appliance object and select **Power > Power On**.

8 Wait until the appliance is up and verify the status of the Compute vCenter Server services.

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

   b Run the `service-control --status --all` command to verify that all the vCenter Server 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
   ```

What to do next

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

Backing Up and Restoring vRealize Operations Manager in Region A

Back up and restore the virtual appliances for the vRealize Operations Manager nodes in the analytics cluster and the remote collector cluster in Region A. Restore vRealize Operations Manager according to the dependencies between the nodes.

Procedure

1 Create a Scheduled Backup Job for vRealize Operations Manager in Region A on page 14

Create a scheduled job for full image backup of the vRealize Operations Manager nodes in Region A.

2 Restore vRealize Operations Manager in Region A on page 15

When a major hardware failure occurs, restore the vRealize Operations Manager nodes by using the backups that are created as a result from the scheduled backup job for the nodes.

Create a Scheduled Backup Job for vRealize Operations Manager in Region A

Create a scheduled job for full image backup of the vRealize Operations Manager nodes in Region A.

Procedure

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

   a Open a Web browser and go to **`https://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, fully 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 vRealize Operations Manager and click **Next**.

Virtual Appliance Name	Role
vrops01svr01a	Master node
vrops01svr01b	Master replica node
vrops01svr01c	Data node
sfo01vropsc01a	Remote collector 1
sfo01vropsc01b	Remote collector 2

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 **`vRealize Operations Manager Backups`** as a name for the backup job 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**.

Restore vRealize Operations Manager in Region A

When a major hardware failure occurs, restore the vRealize Operations Manager nodes 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 **`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 vRealize Operations Manager virtual appliances.

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

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

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

#	vRealize Operations Manager Component	VM Name
1	Remote collector 1	sfo01vropsc01a
2	Remote collector 2	sfo01vropsc01b
3	Data node	vrops01svr01c
4	Master replica node	vrops01svr01b
5	Master node	vrops01svr01a

3 Restore the latest vRealize Operations Manager VMs backup 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 appliance of the vRealize Operations Manager.

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 vRealize Operations Manager.

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.

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 vrops_vm_name completed.
```

5 Power on the nodes of vRealize Operations Manager in the following order:

Appliance Name	Order
vrops01svr01a	1
vrops01svr01b	2
vrops01svr01c	3

Appliance Name	Order
sfo01vropsc01a	4
sfo01vropsc01b	4

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 vRealize Operations Manager is operational. See *Validate vRealize Operations Manager* in the *VMware Validated Design Operational Verification* documentation.

Backing Up and Restoring vRealize Log Insight in Region A

Back up and restore the virtual appliances for the vRealize Log Insight nodes in Region A. Restore vRealize Log Insight according to the dependencies between the nodes.

Procedure

1 Create a Scheduled Backup Job for vRealize Log Insight in Region A on page 17

Create a scheduled job for full image backup of the vRealize Log Insight nodes in Region A.

2 Restore vRealize Log Insight in Region A on page 18

When a major hardware failure occurs, restore the vRealize Log Insight nodes by using the backups that are created as a result from the scheduled backup job for the nodes.

Create a Scheduled Backup Job for vRealize Log Insight in Region A

Create a scheduled job for full image backup of the vRealize Log Insight nodes in Region A.

Procedure

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

a Open a Web browser and go to `https://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 open the Create a 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, fully 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 vRealize Log Insight, and click **Next**.

Virtual Appliance Name	Role
sfo01vrli01a	Master node
sfo01vrli01b	Worker node 1
sfo01vrli01c	Worker node 2

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 **`vRealize Log Insight Backups`** as a name for the backup job 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**.

Restore vRealize Log Insight in Region A

When a major hardware failure occurs, restore the vRealize Log Insight nodes 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 **`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 vRealize Log Insight virtual appliances.

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

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

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

#	vRealize Log Insight Component	VM Name
1	Worker node 1	sfo01vrli01b
2	Worker node 2	sfo01vrli01c
3	Master node	sfo01vrli01a

3 Restore the latest vRealize Log Insight VMs backup 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 appliance of vRealize Log Insight.

   You see the list of backups of 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 vRealize Log Insight.

   g Click **Restore** on the toolbar.

   The Restore backup wizard opens showing the selected backups.

   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.

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 vrli_vm_name completed.
   ```

5 Power on the nodes of vRealize Log Insight in the following order:

Appliance Name	Order
sfo01vrli01a	1
sfo01vrli01b	2
sfo01vrli01c	2

   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 vRealize Log Insight is operational. See *Validate vRealize Log Insight* in the *VMware Validated Design Operational Verification* documentation.

Backing Up and Restoring Cloud Management Platform in Region A

Backup the Linux virtual appliances and the Windows virtual machines of Cloud Management Platform using image-level backup. Use application-level backup for the Microsoft SQL Server instance that hosts the databases for the IaaS components and vRealize Orchestrator.

Create a Scheduled Backup Job for Cloud Management Platform in Region A

Create a scheduled job for full image backup of the Cloud Management Platform linux appliances and windows virtual machines in Region A.

Procedure

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

   a Open a Web browser and go to `https://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 open the Create a 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, fully 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 machines of the Cloud Management Platform components and click **Next**.

vRealize Automation Component	VM Name
vRealize Automation Appliance	vra01svr01a.rainpole.local
vRealize Automation Appliance	vra01svr01b.rainpole.local
IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local
IaaS Manager Service and DEM Orchestrator	vra01ims01b.rainpole.local
IaaS Web Server	vra01iws01a.rainpole.local
IaaS Web Server	vra01iws01b.rainpole.local
Microsoft SQL Server	vra01mssql01.rainpole.local
vSphere Proxy Agent	sfo01ias01a.sfo01.rainpole.local

vRealize Automation Component	VM Name
vSphere Proxy Agent	sfo01ias01b.sfo01.rainpole.local
vRealize Automation DEM Worker	vra01dem01a.rainpole.local
vRealize Automation DEM Worker	vra01dem01b.rainpole.local
vRealize Business Server	vrb01svr01.rainpole.local
vRealize Business Data Collector	sfo01vrbc01.sfo01.rainpole.local

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 **`Cloud Management Platform Backups`** as a name for the backup job 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 Job for Application Backups of Microsoft SQL Server in Region A

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`** to connect to the Management vCenter Server.

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 click the **Microsoft SQL Server 64 bit** link in the **Downloads** pane.

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, 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 Keep **for 3 days** 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**.

Restore Cloud Management Platform in Region A

Restore the Cloud Management Platform nodes by using a backup that is 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 **`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 Cloud Management Platform virtual machines.

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

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

c Navigate to each virtual machine of Cloud Management Platform in the following order, right-click the appliance object, and select **Power > Shut Down Guest OS** and click **Yes** in the Confirm Guest Shut Down dialog box.

#	Cloud Management Platform Component	VM Name
1	vSphere Proxy Agent	sfo01ias01a.sfo01.rainpole.local
2	vSphere Proxy Agent	sfo01ias01b.sfo01.rainpole.local
3	vRealize Automation DEM Worker	vra01dem01a.rainpole.local
4	vRealize Automation DEM Worker	vra01dem01b.rainpole.local
5	IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local
6	IaaS Manager Service and DEM Orchestrator	vra01ims01b.rainpole.local
7	IaaS Web Server	vra01iws01a.rainpole.local
8	IaaS Web Server	vra01iws01b.rainpole.local
9	vRealize Automation Appliance	vra01svr01a.rainpole.local
10	vRealize Automation Appliance	vra01svr01b.rainpole.local
11	vRealize Business Server	vrb01svr01.rainpole.local
12	vRealize Business Data Collector	sfo01vrbc01.sfo01.rainpole.local
13	Microsoft SQL Server	vra01mssql01.rainpole.local

3 Restore the latest Cloud Management Platform backups 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 virtual machine of Cloud Management Platform.

You see the list of the backups of the virtual machine.

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

f Select the latest backups of the other virtual machines of Cloud Management Platform.

g After you select the virtual machines, click the **vra01mssql01.rainpole.local** application entry and select the check box for the latest backup.

h Click **Restore** on the toolbar.

The Restore backup wizard opens showing the selected backups.

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

j On the Set Restore Options page, select **Restore to original location** for each virtual machine and click **Next**.

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

l Click **OK** to close the Info dialog.

4 Verify that the restore is successful.

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

b Locate the logs.

```
Restore of client named vra_vm_name completed.
```

5 Power on the nodes of Cloud Management Platform in the following order:

Cloud Management Platform Component	VM Name	Order
Microsoft SQL Server	vra01mssql01.rainpole.local	1
vRealize Automation Appliance	vra01svr01a.rainpole.local	2
vRealize Automation Appliance	vra01svr01b.rainpole.local	2
IaaS Web Server	vra01iws01a.rainpole.local	3
IaaS Web Server	vra01iws01b.rainpole.local	4
IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local	5
IaaS Manager Service and DEM Orchestrator	vra01ims01b.rainpole.local	6
vSphere Proxy Agent	sfo01ias01a.sfo01.rainpole.local	7
vSphere Proxy Agent	sfo01ias01b.sfo01.rainpole.local	7
vRealize Automation DEM Worker	vra01dem01a.rainpole.local	7
vRealize Automation DEM Worker	vra01dem01b.rainpole.local	7
vRealize Business Server	vrb01svr01.rainpole.local	8
vRealize Business Data Collector	sfo01vrbc01.sfo01.rainpole.local	9

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 vRealize Automation is operational. See *Validate the Cloud Management Platform* in the *VMware Validated Design Operational Verification* documentation.

Backing Up and Restoring the NSX Instances in Region A

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

The following components support backup 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 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.

Backing up NSX Manager regularly enables you to restore the working state of your system in the event of 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.

Procedure

1 Back Up NSX Manager in Region A on page 26

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

2 Restore NSX Manager in Region A on page 27

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

3 Export the NSX Firewall Configuration in Region A on page 29

Export all firewall rules in an NSX Manager to an XML file. You can use that configuration file to import and load firewall rules on another NSX instance in Region A, or to recover the rule configuration in case of misconfiguration.

4 Import the NSX Firewall Configuration in Region A on page 30

You can import a firewall configuration XML file exported from NSX Manager, and then load the configuration in the firewall table. The imported configuration overwrites the existing rules.

5 Export a Service Composer Configuration in Region A on page 30

You can export a Service Composer configuration of security policies and save the configuration file to your computer. You can use the saved configuration as a backup for situations where you accidentally delete a policy configuration, or to replicate to another NSX Manager environment.

6 Import a Security Policies Configuration in Region A on page 31

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

7 Export Configurations of the Distributed Switches in Region A on page 32

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

8 Restore the Configuration of a Distributed Switch in Region A on page 33

Use the restore option to reset the configuration of one of the distributed switches in Region A to the settings in a configuration file.

Back Up NSX Manager in Region A

You can 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 out to a remote location that NSX Manager can access through FTP or SFTP. Backed up 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 up data only on the same NSX Manager version as the version on which the backup was taken.

Prerequisites

- Provide a space on 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.
- Contact your system administrator to obtain a user name and password for access to the FTP server.

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**.

Enter the settings from your system administrator. Write down the details about the FTP backup. You need them to restore the NSX Manager from the backup.

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 in Region A

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

Prerequisites

- Verify that you have the FTP backup details written down.
- 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 to be performed must be the same version as the NSX Manager appliance on 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 in Region A

Export all firewall rules in an NSX Manager to an XML file. You can use that configuration file to import and load firewall rules on another NSX instance in Region A, or to recover the rule configuration in case of misconfiguration.

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 pane, click **Firewall**.

4 On the Firewall page, click the **Configuration** tab.

5 On the Configuration page, from the **NSX Manager** drop-down menu, select the IP address of the NSX Manager instance that runs the firewall rules.

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 Click the **General** tab and click the **Export configuration** icon.

7 On the Export configuration dialog box, click **Download** and save the exported firewall configuration file on your computer.

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

What to do next

Import the backed up configuration of rules to restore the firewall rules if they have been deleted or misconfigured.

Import the NSX Firewall Configuration in Region A

You can import a firewall configuration XML file exported from NSX Manager, and then 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 pane, click **Firewall**.

4 On the Firewall page, click the **Saved Configurations** tab.

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

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 **Saved Configurations** tab, click the **Import configuration** icon.

7 In the Import configuration dialog box, locate the firewall configuration XML file by clicking **Browse** button and click **OK** to close the dialog.

   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 that are managed by Service Composer, these rules are overwritten when you load the imported firewall configuration.

8 If your current configuration contains rules that are managed by Service Composer, synchronize the imported rules and have them 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**.

Export a Service Composer Configuration in Region A

You can export a Service Composer configuration of security policies and save the configuration file to your computer. You can use the saved configuration as a backup for situations where you accidentally delete a policy configuration, or to replicate to another NSX Manager environment.

The backed up configuration also 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 pane, 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 from the list that you want to export and click the **Actions > Export Configuration** menu item.

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 security policies and security groups that are being exported. Setting a prefix makes the names of the exported security policies unique.

8 On the Select security policies page, select the security policies that you want to export and click **Next**.

9 On the Ready to complete page, preview the security policies and the associated objects, click **Finish**, and save the exported service composer configuration file on your computer.

You see the security groups on which the policies apply, and the endpoint services, firewall rules and network introspection services that are a part of the policies.

Import a Security Policies Configuration in Region A

Import a saved security policies configuration file to restore a misconfigured policy or to replicate the configuration to a different NSX Manager in Region A. 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 pane, 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 Click the **Import Configuration** icon.

The Import Configuration wizard opens.

7 On the Select configuration file page, browse to the security policies configuration file on your computer, enter a suffix for the names of the imported policies, and click **Next**.

Service Composer verifies that all services referred to in the configuration are available in the destination environment.

8 If any services from the imported policy configuration are not available in the environment, map the missing services to available target services on the Manage Missing Services page that appears.

9 On the Ready to complete page, examine the security policies along with associated objects and click **Finish**.

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

Export Configurations of the Distributed Switches in Region A

You can export vSphere Distributed Switch and distributed port group configurations to a file. The file preserves validated network configurations, enabling transfer of 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** next to Configurations to export and click **OK**.

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

Restore the Configuration of a Distributed Switch in Region A

Use the restore option to reset the configuration of one of the distributed switches in Region A to the settings 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, examine the changes and click **Finish**.

Backing Up and Restoring vSphere Update Manager Download Service in Region A

Back up and restore the virtual appliance for the vSphere Update Manager Download Service in Region A.

Procedure

1 Create a Scheduled Backup Job for vSphere Update Manager Download Service in Region A on page 34

Create a scheduled job for full image backup of the vSphere Update Manager Download Service node in Region A.

2 Restore vSphere Update Manager Download Service in Region A on page 35

When a major hardware failure occurs, restore the vSphere Update Manager Download Service node by using the backups that are created as a result from the scheduled backup job for the node.

Create a Scheduled Backup Job for vSphere Update Manager Download Service in Region A

Create a scheduled job for full image backup of the vSphere Update Manager Download Service node in Region A.

Procedure

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

   a Open a Web browser and go to **`https://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 open the Create a 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, fully 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 appliance **sfo01umds01** of vSphere Update Manager Download Service, and click **Next**.

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 **`vSphere Update Manager Download Service Backups`** as a name for the backup job 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**.

Restore vSphere Update Manager Download Service in Region A

When a major hardware failure occurs, restore the vSphere Update Manager Download Service node by using the backups that are created as a result from the scheduled backup job for the node.

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 Shut down the vSphere Update Manager Download Service virtual appliance.

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

   b In the Navigator pane expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01-mgmt01 > sfo01umds01** tree.

   c Right-click the vSphere Update Manager Download Service appliance object, select **Power > Shut Down Guest OS**, and click **Yes** in the Confirm Guest Shut Down dialog box.

3 Restore the latest vSphere Update Manager Download Service VM backup from the vSphere Data Protection server.

   a On the vSphere Web Client Home page, click the 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 the node appliance of vSphere Update Manager Download Service.

   You see the list of backups of 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 Click **Restore** on the toolbar.

   The Restore backup wizard opens showing the selected backups.

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

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

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

   j Click **OK** to close the Info dialog.

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 sfo01umds01 completed.
```

5 Power on the vSphere Update Manager Download Service node by navigating to the appliance **sfo01umds01**, right-click the appliance object, and select **Power > Power On**.

Region B Backup and Restore

Back up the management components of the SDDC in Region B so that you can restore the SDDC state if a hardware failure occurs. You can create backup copies by using either vSphere Data Protection or the built-in backup mechanism of some of the products.

Use backup jobs in vSphere Data Protection for the following components:

- vCenter Server
- Platform Services Controller
- vRealize Operations Manager
- vRealize Log Insight
- Cloud Management Platform
- vSphere Update Manager Download Service

For the networking components of the SDDC, use the following backup mechanisms:

- Use NSX to back up NSX Manager and NSX security configurations.
- Export a configuration of vSphere Distributed Switch as a backup.

Backing Up and Restoring vCenter Server in Region B

Schedule regular backup jobs of the vCenter Server instances and the connected Platform Services Controllers in Region B, and perform restore in cases of corrupt appliance instances.

Note Backing up the embedded PostgreSQL database is not required for this validated design. If you plan to add such an additional layer of recoverability, see VMware Knowledge Base article 2091961.

Create Scheduled Backup Jobs for the vCenter Server Instances in Region B

Create a scheduled job for full image backup of vCenter Server and the connected external Platform Services Controller in Region B. Schedule backups for both the Management vCenter Server and Compute vCenter Server.

Procedure

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

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

b Log in using the following credentials.

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

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

3 On the Welcome to vSphere Data Protection page, select **lax01m01vdp01** 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 a 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, fully expand the **Virtual Machines** tree.

Object	Value
vCenter Server	lax01m01vc01.lax01.rainpole.local
Data center	lax01-m01dc
Cluster	lax01-m01-mgmt01

9 Select the virtual appliances for vCenter Server and the Platform Services Controller and click **Next**.

Object	VM name
Management Platform Services Controller	lax01m01psc01
Management vCenter Server	lax01m01vc01
Compute Platform Services Controller	lax01w01psc01
Compute vCenter Server	lax01w01vc01

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 **`Management and Compute vCenter Server Backups`** as a name for the backup job 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**.

Restore the Management vCenter Server in Region B

If the Management vCenter Server in Region B stops responding or its data is corrupt as a result of a failure in the environment, perform a direct-to-host emergency restore to restore the Management vCenter Server. vSphere Data Protection restores the VM that contains the vCenter Server or Platform Services Controller directly on the ESXi host in Region B 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 have created. You cannot use a regular restore in this case because both the Management vCenter Server and the associated Platform Services Controller must be available.

Procedure

1 Log in to the vSphere Data Protection Configure Utility.

a Open a Web browser and go to **`https://lax01m01vdp01.lax01.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 **lax01m01vdp01** appliance and write 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 In the Host Management pane, click **Disconnect from vCenter Server**.

d Click **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://lax01m01vdp01.lax01.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	lax01m01vc01
Platform Services Controller that is associated with the Management vCenter Server	lax01m01psc01

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
Username	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	lax01m01vc01.restored
Platform Services Controller that is associated with the Management vCenter Server	lax01m01psc01.restored

h From the **Datastore** drop-down menu, select the **lax01-m01-vsan01** datastore and click **Restore**.

i Repeat the step to restore the other appliance.

5 Power on the Platform Services Controller and vCenter Server virtual machines.

a In the vSphere Host Client, navigate to the virtual machine of Platform Services Controller **lax01m01psc01.restored**.

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

6 Wait until the appliance starts 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, navigate to the virtual machine of vCenter Server **lax01m01vc01.restored**.

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

8 Wait until the appliance starts 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, reconnect the ESXi host that is running the vSphere Data Protection appliance.

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

b Log in using the following credentials.

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

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

10 Verify that the Management Platform Services Controller and the Management vCenter Server are up and function flawlessly after restore.

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* documentation.

Restore the Compute vCenter Server in Region B

Restore the Compute vCenter Server or the connected Platform Services Controller if a major hardware failure occurs.

Procedure

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

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

   b Log in using the following credentials.

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

2 Shut down the Platform Services Controller and vCenter Server virtual appliances.

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

   b In the Navigator pane expand the **lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01-mgmt01** tree.

   c Navigate to each vCenter object below, right click the VM, select **Power > Shut Down Guest OS** and click **Yes** in the Confirm Guest Shut Down dialog box.

vCenter Server Component	VM Name
Compute Platform Services Controller	lax01w01psc01
Compute vCenter Server	lax01w01vc01

3 Restore the latest vCenter Server and Platform Services Controller VMs backup from the vSphere Data Protection.

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

   b On the Welcome to vSphere Data Protection page, select **lax01m01vdp01** from the **VDP Appliance** drop-down menu, and click **Connect**.

   c Click the **Restore** tab and select the **lax01w01psc01** virtual appliance.

   You see the list of backups for the appliance.

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

   e From the list of VMs, select the **lax01w01vc01** virtual appliance and select the latest backup.

   f Click **Restore** on the toolbar.

   The Restore backup wizard opens.

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

   h On the Set Restore Options page, select **Restore to original location** and click **Next**.

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

   j Click **OK** to close the Info dialog.

4 Verify that the restore is successful.

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

   b Locate the following logs.

   ```
   Restore of client named lax01w01psc01 completed.

   Restore of client named lax01w01vc01 completed.
   ```

5 After restore job is complete, power on the Compute Platform Services Controller virtual machine.

   a Navigate to the virtual machine of Platform Services Controller **lax01w01psc01**.

   b Right-click the **lax01w01psc01** appliance object and select **Power > Power On**.

6 Wait until the appliance starts and verify the status of the Compute Platform Services Controller services.

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

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

7 After Compute Platform Services Controller is up and running, power on the Compute vCenter Server virtual machine.

   a Navigate to the virtual machine of Compute vCenter Server **lax01w01vc01**.

   b Right-click the **lax01w01vc01** appliance object and select **Power > Power On**.

8 Wait until the appliance starts and verify the status of the Compute vCenter Server services.

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

   b Run the `service-control --status --all` command to verify that all the vCenter Server 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
   ```

What to do next

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

Backing Up and Restoring vRealize Operations Manager in Region B

Back up and restore the virtual appliances for the vRealize Operations Manager nodes in the remote collector cluster in Region B.

Create a Scheduled Backup Job for vRealize Operations Manager in Region B

Create a scheduled job for full image backup of the vRealize Operations Manager remote collector nodes in Region B.

Procedure

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

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

   b Log in using the following credentials.

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 **lax01m01vdp01** 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 a 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, fully expand the Virtual Machines tree.

Object	Value
vCenter Server	lax01m01vc01.lax01.rainpole.local
Data center	lax01-m01dc
Cluster	lax01-m01-mgmt01

9 Select the virtual appliances for vRealize Operations Manager, and click **Next**.

Virtual Appliance Name	Role
lax01vropsc01a	Remote collector 1
lax01vropsc01b	Remote collector 2

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 **`vRealize Operations Manager Backups`** as a name for the backup job, 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**.

Restore vRealize Operations Manager in Region B

Restore the vRealize Operations Manager remote collector nodes in Region B if a major hardware failure occurs by using a backup that is 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 `https://lax01m01vc01.lax01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

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

2 Shut down all vRealize Operations Manager virtual appliances.

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

b In the Navigator pane expand the **lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01-mgmt01** tree.

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

#	vRealize Operations Manager Component	VM Name
1	Remote collector 1	lax01vropsc01a
2	Remote collector 2	lax01vropsc01b

3 Restore the latest vRealize Operations Manager VMs backup from the vSphere Data Protection server.

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

b On the Welcome to vSphere Data Protection page, select **lax01m01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

c Click the **Restore** tab.

d Select a node appliance of vRealize Operations Manager.

You see the list of 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 vRealize Operations Manager.

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** check box for each appliance.

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

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

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 lax01vropsc01a completed.
   Restore of client named lax01vropsc01b completed.
   ```

5 Power on the remote collectors of vRealize Operations Manager.

What to do next

Verify that vRealize Operations Manager is operational. See *Validate vRealize Operations Manager* in the *VMware Validated Design Operational Verification* documentation.

Backing Up and Restoring vRealize Log Insight in Region B

Back up and restore the virtual appliances for the vRealize Log Insight nodes in Region B. Restore vRealize Log Insight according to the dependencies between the nodes.

Create a Scheduled Backup Job for vRealize Log Insight in Region B

Create a scheduled job for full image backup of the vRealize Log Insight nodes in Region B.

Procedure

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

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

   b Log in using the following credentials.

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 **lax01m01vdp01** 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 open the Create a 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, fully expand the **Virtual Machines** tree.

Object	Value
vCenter Server	lax01m01vc01.lax01.rainpole.local
Data center	lax01-m01dc
Cluster	lax01-m01-mgmt01

9 Select the virtual appliances for vRealize Log Insight, and click **Next**.

Virtual Appliance name	Role
lax01vrli01a	Master node
lax01vrli01b	Worker node 1
lax01vrli01c	Worker node 2

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 **`vRealize Log Insight Backups`** as a name for the backup job 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**.

Restore vRealize Log Insight in Region B

Restore the vRealize Log Insight nodes in Region B by using a backup that is 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 **`https://lax01m01vc01.lax01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

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

2 Shut down all vRealize Log Insight virtual appliances.

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

b In the Navigator pane expand the **lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01-mgmt01** tree.

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

#	vRealize Log Insigh Component	VM Name
1	Worker node 1	lax01vrli01b
2	Worker node 2	lax01vrli01c
3	Master node	lax01vrli01a

3 Restore the latest vRealize Log Insight VMs backup 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 **lax01m01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

c Click the **Restore** tab .

d Select a node appliance of vRealize Log Insight.

You see the list of backups of 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 vRealize Log Insight.

g Click **Restore** on the toolbar.

The Restore backup wizard opens showing the selected backups.

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.

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 vrli_vm_name completed.`

5 Power on the nodes of vRealize Log Insight. in the following order:

Appliance Name	Order
lax01vrli01a	1
lax01vrli01b	2
lax01vrli01c	2

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 vRealize Log Insight is operational. See *Validate vRealize Log Insight* in the *VMware Validated Design Operational Verification* documentation.

Backing Up and Restoring Cloud Management Platform in Region B

Backup the Windows virtual machines that host the vSphere Proxy Agents and the vRealize Business Collector for Cloud Management Platform in Region B.

Create a Scheduled Backup Job for Cloud Management Platform in Region B

Create a scheduled job for full image backup of the vSphere Proxy Agents and vRealize Business collector virtual machines in Region B that are part of the Cloud Management Platform.

Procedure

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

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

   b Log in using the following credentials.

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

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

3 On the Welcome to vSphere Data Protection page, select **lax01m01vdp01** 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 open the Create a 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, fully expand the **Virtual Machines** tree.

Object	Value
vCenter Server	lax01m01vc01.lax01.rainpole.local
Data center	lax01-m01dc
Cluster	lax01-m01-mgmt01

9 Select the virtual machines of the vSphere Proxy Agents and vRealize Business Data Collector and click **Next**.

vRealize Automation Component	VM Name
vSphere Proxy Agent	lax01ias01a.lax01.rainpole.local
vSphere Proxy Agent	lax01ias01b.lax01.rainpole.local
vRealize Business Data Collector	lax01vrbc01.lax01.rainpole.local

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 **`vRealize Automation Backups`** as a name for the backup job 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**.

Restore Cloud Management Platform in Region B

Restore the vSphere Proxy Agent nodes and vRealize Business Data Collector node of Cloud Management Platform in Region B by using a backup that is 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 `https://lax01m01vc01.lax01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

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

2 Shut down all Cloud Management Platform virtual machines.

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

b In the Navigator pane expand the **lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01-mgmt01** tree.

c Navigate to each Cloud Management Platform virtual machine in the following order, right-click the appliance object, select **Power > Shut Down Guest OS** and click **Yes** in the Confirm Guest Shut Down dialog box.

#	Cloud Management Platform Component	VM Name
1	vSphere Proxy Agent	lax01ias01a.lax01.rainpole.local
2	vSphere Proxy Agent	lax01ias01b.lax01.rainpole.local
3	vRealize Business Data Collector	lax01vrbc01.lax01.rainpole.local

3 Restore the latest Cloud Management Platform backups 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 **lax01m01vdp01** from the **VDP Appliance** drop-down menu, and click **Connect**.

c Click the **Restore** tab.

d Select a node virtual machine of Cloud Management Platform.

You see the list of the backups of the virtual machine.

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

f Select the latest backups of the other virtual machines of Cloud Management Platform.

g Click **Restore** on the toolbar.

The Restore backup wizard opens showing the selected backups.

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

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

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

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

4 Verify that the restore is successful.

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

b Locate the following logs.

```
Restore of client named vra_vm_name completed.
```

5 Power on the nodes of Cloud Management Platform.

Cloud Management Platform Component	VM Name
vSphere Proxy Agent	lax01ias01a
vSphere Proxy Agent	lax01ias01b
vRealize Business Data Collector	lax01vrbc01

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 vRealize Automation is operational. See *Validate vRealize Automation* in the *VMware Validated Design Operational Verification* documentation.

Backing Up and Restoring the NSX Instances in Region B

You can back up certain components of NSX for the management cluster and for the shared edge and compute cluster in Region B to restore the working state of the system in the event of failure.

The following components support backup and restore in Region B:

- NSX Manager
- NSX Firewall Rules
- NSX Service Composer
- vSphere Distributed Switch

You can schedule regular 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.

Back Up NSX Manager in Region B

In Region B, you can 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 out to a remote location that NSX Manager can access through FTP or SFTP. Backed up 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 up data only on the same NSX Manager version as the version on which the backup was taken.

Prerequisites

- Provide a space on 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.
- Contact your system administrator to obtain a user name and password for access to the FTP server.

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://lax01m01nsx01.lax01.rainpole.local
NSX Manager for the shared edge and compute cluster	https://lax01w01nsx01.lax01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

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

3 On the Backup & 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**.

Enter the settings from your system administrator. Write down the details about the FTP backup. You need them to restore the NSX Manager from the backup.

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	■ **`lax_NSX_Mgmt`** for the NSX Manager for the management cluster ■ **`lax_NSX_Comp`** for the NSX Manager for the shared edge and compute cluster
Pass Phrase	*nsx_backup_pass_phrase*

5 On the Backup & 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 a 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. You simply click the **Redeploy NSX Edge** button on the edge in the vSphere Web Client.

Restore NSX Manager in Region B

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

The new NSX Manager appliance on which the restore is performed must be the same version as the NSX Manager appliance on which the backup was taken.

Prerequisites

- Verify that you have the FTP backup details written down.
- 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 B* and *Deploy and Configure the Shared Edge and Compute Cluster NSX Instance in Region B*.

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://lax01m01nsx01.lax01.rainpole.local
NSX Manager for the shared edge and compute cluster	https://lax01w01nsx01.lax01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 On the main page of the appliance user interface, click **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 of the backup data on the FTP server*
Filename Prefix	■ **`lax_NSX_Mgmt`** for the NSX Manager for the management cluster ■ **`lax_NSX_Comp`** for the NSX Manager for the shared edge and compute cluster
Pass Phrase	*nsx_backup_pass_phrase*

5 In the **Backup 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 in Region B

Export all firewall rules in an NSX Manager to an XML file. You can use that configuration file to import and load firewall rules on another NSX instance in Region B, or to recover the rule configuration in case of misconfiguration.

Procedure

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

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

b Log in using the following credentials.

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

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

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

4 On the Firewall page, click the **Configuration** tab.

5 In the Configuration page, from the **NSX Manager** drop-down menu, select the IP address of the NSX Manager instance that runs the firewall rules.

NSX Manager	IP Address
NSX Manager for the management cluster	172.17.11.65
NSX Manager for the shared edge and compute cluster	172.17.11.66

6 Click the **General** tab and click the **Export configuration** icon.

7 In the Export configuration dialog box, click **Download** and save the exported firewall configuration file on your computer.

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

What to do next

Import the backed up configuration of rules to restore the firewall rules if they have been deleted or misconfigured.

Import the NSX Firewall Configuration in Region B

You can import a firewall configuration XML file exported from NSX Manager, and then load the configuration in the firewall table for Region B. 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://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 **Networking & Security**.

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

4 On the Firewall page, click the **Saved configurations** tab.

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

NSX Manager	IP Address
NSX Manager for the management cluster	172.17.11.65
NSX Manager for the shared edge and compute cluster	172.17.11.66

6 On the **Saved Configurations** tab, click the **Import configuration** icon.

7 In the Import configuration dialog box, locate the firewall configuration XML file by clicking **Browse** button and click **OK** to close the dialog.

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 that are managed by Service Composer, these rules are overwritten when you load the imported firewall configuration.

8 If your current configuration contains rules that are managed by Service Composer, synchronize the imported rules and have them 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**.

Export a Service Composer Configuration in Region B

You can export a Service Composer configuration of security policies in Region B and save the configuration file to your computer. The saved configuration can be used as a backup for situations where you accidentally delete a policy configuration, or to replicate to another NSX Manager environment.

The backed up configuration also 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://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 **Networking & Security**.

3 In the Navigator pane, 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	172.17.11.65
NSX Manager for the shared edge and compute cluster	172.17.11.66

6 Select the security policy from the list that you want to export and click the **Actions > Export Configuration** menu item.

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 security policies and security groups that are being exported. Setting a prefix makes the names of the exported security policies unique.

8 On the Select security policies page, select the security policies that you want to export and click **Next**.

9 On the Ready to complete page, preview the security policies and the associated objects, click **Finish** and save the exported service composer configuration file on your computer.

You see the security groups on which the policies apply, and the endpoint services, firewall rules and network introspection services that are a part of the policies.

Import a Security Policies Configuration in Region B

Import a saved security policies configuration file to restore a misconfigured policy or to replicate the configuration to a different NSX Manager in Region B. 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://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 **Networking & Security**.

3 In the Navigator pane, 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	172.17.11.65
NSX Manager for the shared edge and compute cluster	172.17.11.66

6 Click the **Import Configuration** icon.

The Import Configuration wizard opens.

7 On the Select Configuration File page, browse to the security policies configuration file on your computer, enter a suffix for the names of the imported policies, and click **Next**.

Service Composer verifies that all services referred to in the configuration are available in the destination environment.

8 If any services from the imported policy configuration are not available in the environment, map the missing services to available target services on the Manage Missing Services page that appears.

9 On the Ready to Complete page, examine the security policies along with associated objects and click **Finish**.

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

Export Configurations of the Distributed Switches in Region B

You can export vSphere Distributed Switch and distributed port group configurations in Region B to a file. The file preserves validated network configurations, enabling transfer of 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://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 **Networking**, expand the vCenter Server tree and locate the distributed switch.

vCenter Server	Distributed Switch
lax01m01vc01.lax01.rainpole.local	lax01-m01-vds01
lax01w01vc01.lax01.rainpole.local	lax01-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** next to Configurations to export, and click **OK**.

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

Restore the Configuration of a Distributed Switch in Region B

Use the restore option to reset the configuration of one of the distributed switches in Region B to the settings 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://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 **Networking**, expand the vCenter Server tree and locate the distributed switch.

vCenter Server	Distributed Switch
lax01m01vc01.lax01.rainpole.local	lax01-m01-vds01
lax01w01vc01.lax01.rainpole.local	lax01-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, examine the changes and click **Finish**.

Backing Up and Restoring vSphere Update Manager Download Service in Region B

Back up and restore the virtual appliance for the vSphere Update Manager Download Service in Region B.

Procedure

1 Create a Scheduled Backup Job for vSphere Update Manager Download Service in Region B on page 57

Create a scheduled job for full image backup of the vSphere Update Manager Download Service node in Region B.

2 Restore vSphere Update Manager Download Service in Region B on page 58

When a major hardware failure occurs, restore the vSphere Update Manager Download Service node by using the backups that are created as a result from the scheduled backup job for the node.

Create a Scheduled Backup Job for vSphere Update Manager Download Service in Region B

Create a scheduled job for full image backup of the vSphere Update Manager Download Service node in Region B.

Procedure

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

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

b Log in using the following credentials.

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

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

3 On the Welcome to vSphere Data Protection page, select **lax01m01vdp01** 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 open the Create a 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, fully expand the **Virtual Machines** tree.

Object	Value
vCenter Server	lax01m01vc01.lax01.rainpole.local
Data center	lax01-m01dc
Cluster	lax01-m01-mgmt01

9 Select the virtual appliance **lax01umds01** of vSphere Update Manager Download Service, and click **Next**.

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 **`vSphere Update Manager Download Service Backups`** as a name for the backup job 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**.

Restore vSphere Update Manager Download Service in Region B

When a major hardware failure occurs, restore the vSphere Update Manager Download Service node by using the backups that are created as a result from the scheduled backup job for the node.

Procedure

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

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

   b Log in using the following credentials.

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

2 Shut down the vSphere Update Manager Download Service virtual appliance.

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

   b In the Navigator pane expand the **lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01-mgmt01 > lax01umds01** tree.

   c Right-click the vSphere Update Manager Download Service appliance object, select **Power > Shut Down Guest OS**, and click **Yes** in the Confirm Guest Shut Down dialog box.

3 Restore the latest vSphere Update Manager Download Service VM backup 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 **lax01m01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

   c Click the **Restore** tab.

d Select the node appliance of vSphere Update Manager Download Service.

You see the list of backups of 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 Click **Restore** on the toolbar.

The Restore backup wizard opens showing the selected backups.

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

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

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

j Click **OK** to close the Info dialog.

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 lax01umds01 completed.
```

5 Power on the vSphere Update Manager Download Service node by navigating to the appliance **lax01umds01**, right-click the appliance object, and select **Power > Power On**.

SDDC Startup and Shutdown 3

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.

This chapter includes the following topics:

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
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

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
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
sfo01w01nsx01	lax01w01nsx01	2
sfo01m01nsxc01	-	3
sfo01m01nsxc02	-	3
sfo01m01nsxc03	-	3
sfo01w01nsxc01	-	3
sfo01w01nsxc02	-	3
sfo01w01nsxc03	-	3
sfo01m01vc01	lax01m01vc01	4
sfo01w01vc01	lax01w01vc01	4

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
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
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

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
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**
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