Site Protection and Recovery

30 OCT 2018
VMware Validated Design 4.3
VMware Validated Design for Software-Defined Data Center 4.3

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Copyright © 2016–2018 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

About VMware Validated Design Site Protection and Recovery

VMware Validated Design Site Protection and Recovery provides step-by-step instructions for performing disaster recovery of VMware management components in the software-defined data center (SDDC).

Use VMware Site Recovery Manager and VMware vSphere Replication to perform site protection and recovery of the Cloud Management Platform that consists of vRealize Automation with embedded vRealize Orchestrator, vRealize Business, vRealize Operations Manager analytics cluster, and vRealize Suite Lifecycle Manager.

VMware Validated Design Site Protection and Recovery covers both failover to the recovery region and failback to the protected region.

Intended Audience

The *VMware Validated Design Site Protection and Recovery* 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 disaster recovery.

Required VMware Software

The *VMware Validated Design Site Protection and Recovery* documentation 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 failover or failback components of the Cloud Management Platform, vRealize Operations Manager or vRealize Suite Lifecycle Manager, verify whether they are operating according to design objectives.

For more information, see the *VMware Validated Design Operational Verification* documentation.

Failover and Failback Checklist for the SDDC Management Applications

1

Use the following checklist to verify that you have fulfilled all the requirements to initiate disaster recovery or planned migration of the SDDC management applications and complete the configuration of these applications.

Table 1-1. Checklist for Failover and Failback in a Validated SDDC

Checklist	Tasks
Activation and Assessment	■ Verify that the disaster failover or failback is required: ■ For example, an application failure might not be a cause to perform a failover or failback, while an extended region outage is a valid cause. ■ Plan for business continuity events such as scheduled building maintenance or the probability of a natural disaster.

Approval	■ Submit the required documentation for approval to the following roles:
	  ■ IT management staff
	  ■ CTO
	  ■ Business users
	  ■ Other stakeholders

Activation Logistics	■ Verify that all the required facilities and personnel are available for the complete duration of the disaster recovery process.
	■ Verify that Site Recovery Manager is available in the recovery region.
	■ Verify the replication status of the applications.
	■ Verify the state of the NSX Edge in the recovery region:
	  ■ Verify that the NSX Edges are available.
	  ■ Verify that the IP addresses for VXLAN backed networks are correct.
	  ■ Verify that the load balancer on the NSX Edge is correctly configured according to the design.
	  ■ Verify that the firewall on the NSX Edge is correctly configured according to the design.

Table 1-1. Checklist for Failover and Failback in a Validated SDDC (Continued)

Checklist	Tasks

Communication, Initiation, and Failover or Failback Validation	■ In case of a planned migration:
	  ■ Notify all stakeholders for the planned outage and the expected duration of the maintenance window.
	  ■ At the scheduled time, initiate the failover or failback process.
	■ In case of a disaster recovery failover or failback:
	  ■ Before initiating a failover or a failback, notify all stakeholders for the event.
	■ After completing a failover or a failback:
	  ■ Test applications availability.
	  ■ Notify all stakeholders for the completed event.

Multiple Availability Zones	In case your environment consists of multiple Availability Zones, perform the following additional configurations for disaster recovery failback. ■ In case of disaster recovery failback in which Region B remains unavailable, the witness vSAN appliance is no longer available, which might impact storage policies. Update the force provisioning setting of the storage policy to Yes (sets FTT=0 for all newly provisioned VMs) to allow for recovery of the vRealize components. Revert the storage policy once the recovery is complete. ■ In case of a planned migration in which Region A and Region B are still operational, you do not need to update the storage policy as the witness vSAN appliance remains available.
Configuration After Failover or Failback	In case of disaster recovery failover or failback, perform the following additional configuration: ■ Update the backup jobs to include the applications that are now running in Region B. For information about the configured backup jobs, see the *VMware Validated Design Backup and Restore* documentation. ■ Configure the NSX Controllers and the UDLR Control VM to forward events to vRealize Log Insight in the recovery region. ■ Redirect the log data from the failed over or failed back applications to vRealize Log Insight in the recovery region. ■ Complete a post-recovery assessment: ■ Note which items worked and which did not work, and identify improvements that you can include in the recovery plan.

Prerequisites for SDDC Failover or Failback 2

For a faultless failover or failback to the recovery region, verify that your environment fulfills the requirements for a failover or a failback capable SDDC configuration.

Table 2-1. Failover or Failback Prerequisites

Prerequisite	Value
Compute	The compute infrastructure in the recovery region must mirror the compute infrastructure in the protected region.
Storage	■ The storage configuration and capacity in the recovery region must mirror the storage configuration and capacity in the protected region. ■ Datastore space on the management pod with sufficient capacity must be available for all the virtual machines of vRealize Automation, vRealize Operations Manager, and vRealize Suite Lifecycle Manager.
External services	Provide the following services in the recovery region. See *External Service Dependencies* from the *Planning and Preparation* documentation. ■ Active Directory ■ DNS ■ NTP ■ SMTP ■ Syslog
Virtual infrastructure	■ Verify that ESXi, vCenter Server, and NSX for vSphere are mirrored in the protected region. ■ Verify that Site Recovery Manager and vSphere Replication are deployed in both regions and paired. ■ Verify that the NSX load balancer is deployed and configured in both regions. ■ Verify that NSX Edge devices for North-South routing are deployed and configured in both regions. ■ Verify that UDLR is deployed and configured.

Failover of the SDDC Management Applications

3

Configure and perform a failover of the management applications in the SDDC from the protected region, Region A, to the recovery region, Region B. Failing over these applications maintains the operational state of the SDDC.

You fail over the following management applications:

- vRealize Suite Lifecycle Manager
- Analytics cluster of vRealize Operations Manager
  - The remote collector nodes of vRealize Operations Manager do not fail over. Deploy a separate pair of remote collectors in each region in the application virtual network that is dedicated to the region.
- Primary components of vRealize Automation with embedded vRealize Orchestrator and vRealize Business
  - vSphere Proxy Agents of vRealize Automation and the vRealize Business data collector do not fail over. Deploy a separate pair of agents and a data collector in each region in an application isolated network.

Table 3-1. Support for Failover of the SDDC Management Applications

Management Component	Supports Failover
vRealize Suite Lifecycle Manager	Yes
vRealize Operations Manager analytics nodes	Yes
vRealize Operations Manager remote collectors	No
vSphere proxy agents	No
vRealize Business data collectors	No
vRealize Automation appliance	Yes
vRealize Business server	Yes
Microsoft SQL server	Yes
IaaS Components	Yes

1 Configure Failover of the SDDC Management Applications

   Prepare the management applications in the SDDC for failover or planned migration. Replicate application-specific VMs by using vSphere Replication and create recovery plans for them by using Site Recovery Manager.

2 Test Failover of the SDDC Management Applications

   You can identify potential problems during a future failover by testing the recovery plan for the management applications in the SDDC.

3 Perform Planned Migration of the SDDC Management Applications

   After you have successfully configured and tested failover of the management applications, you can initiate a migration process from Region A to Region B. The planned migration of the SDDC management components keeps the SDDC operational, for example, when upgrading the hardware or changing the network configuration in Region A.

4 Perform Disaster Recovery of the SDDC Management Applications

   Prepare networking in Region B and perform a failover of vRealize Automation, vRealize Orchestrator, vRealize Business, vRealize Operations Manager, and vRealize Suite Lifecycle Manager to Region B if Region A becomes unavailable.

Configure Failover of the SDDC Management Applications

Prepare the management applications in the SDDC for failover or planned migration. Replicate application-specific VMs by using vSphere Replication and create recovery plans for them by using Site Recovery Manager.

- Configure Failover of the Operations Management Applications

  You replicate the vRealize Suite Lifecycle Manager VM and prepare vRealize Operations Manager for a failover by replicating the VMs of the analytics cluster and create a recovery plan for them in Site Recovery Manager.

- Configure Failover of the Cloud Management Platform

  Prepare vRealize Automation, and vRealize Business for failover. Replicate the virtual machines of the primary vRealize Automation components, and of vRealize Business Server. Create a recovery plan for these application components in Site Recovery Manager.

Configure Failover of the Operations Management Applications

You replicate the vRealize Suite Lifecycle Manager VM and prepare vRealize Operations Manager for a failover by replicating the VMs of the analytics cluster and create a recovery plan for them in Site Recovery Manager.

Procedure

1 Replicate the vRealize Operations Manager Analytics VMs

Configure the replication of the virtual machines that participate in the analytics cluster of the vRealize Operations Manager to support failover of vRealize Operations Manager to Region B. Replica virtual machines become active upon failover. After you configure the replication, you create a protection group to protect the replicated virtual machines together.

2 Replicate the vRealize Suite Lifecycle Manager Appliance in Region A

To support a failover to Region B, you configure the replication of the vRealize Suite Lifecycle Manager virtual appliance. The replica virtual machine becomes active upon failover. After you configure the replication, you create a protection group to protect the replicated virtual machine.

3 Create a Protection Group for the Operations Management Applications

After you configure the replication for the analytics virtual machines of vRealize Operations Manager and vRealize Suite Lifecycle Manager, you create a protection group and include the virtual machines in the protection group. Site Recovery Manager protects the virtual machines together.

4 Create a Recovery Plan for the Operations Management Applications

After you create a protection group for the virtual machines of the vRealize Operations Manager analytics cluster and vRealize Suite Lifecycle Manager, create a recovery plan. You then use this plan to configure dependencies between the virtual machines.

5 Customize the Recovery Plan for the Operations Management Applications

After you create the recovery plan, configure the startup priority and the startup and shutdown options for the virtual machines of the analytics cluster and vRealize Suite Lifecycle Manager. The master node of vRealize Operations Manager must start first after failover.

6 Create an Anti-Affinity Rule for vRealize Operations Manager in Region B

Anti-affinity rules do not persist across regions during recovery using Site Recovery Manager. You must create the anti-affinity rules for the analytics virtual machines in Region B so that the rules still apply after a failover of vRealize Operations Manager.

Replicate the vRealize Operations Manager Analytics VMs

Configure the replication of the virtual machines that participate in the analytics cluster of the vRealize Operations Manager to support failover of vRealize Operations Manager to Region B. Replica virtual machines become active upon failover. After you configure the replication, you create a protection group to protect the replicated virtual machines together.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **VMs and Templates**.

3 Navigate to the **sfo01-m01fd-vrops** VM folder.

Object	Value
vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Data center	sfo01-m01dc
Folder	sfo01-m01fd-vrops

4 On the **sfo01-m01fd-vrops** page, click the **VMs** tab, click **Virtual Machines**, and select the virtual machines of the analytics cluster.

Name	Role
vrops01svr01a	Master node
vrops01svr01b	Master replica node
vrops01svr01c	Data node 1

5 Right-click the selected VMs and select **All vSphere Replication Actions > Configure Replication**.

6 In the dialog box for configuring replication for all objects, click **Yes**.

   The **Configure Replication for 3 Virtual Machines** wizard opens.

7 On the **Validation** page of the Configuration Replication dialog box, wait until the validation completes and click **Next**.

8 On the **Replication type** page, select **Replicate to a vCenter Server** and click **Next**.

9 On the **Target site** page, select the **lax01m01vc01.lax01.rainpole.local** vCenter Server and click **Next**.

10 On the **Replication server** page, select **Auto-assign vSphere Replication server** and click **Next**.

11 On the **Target location** page, set the location on the vSAN datastore in Region B to store replicated VM files.

   a Click the **Edit for all** link.

   b In the **Select Target Location** dialog box, from the datastore list in the upper part of the dialog box, select the **lax01-m01-vsan01** datastore as the datastore for replicated files.

   c In the **Select a target location** pane, select the **lax01-m01-vsan01** root folder underneath and click **OK**.

   vSphere Replication creates a folder in the root datastore folder for each vRealize Operations Manager VM.

   d Back on the **Target location** page, click **Next**.

12 On the **Replication options** page, select only the **Enable network compression for VR data** check box and click **Next**.

Important

- Do not enable guest OS quiescing because some of the vRealize Operations Manager databases do not support quiescing. Quiescing might result in a cluster failure because virtual disks remain in a frozen state for too long.
- Compression requires extra resources. Do not enable it if the hosts are over-utilized.

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

Setting		Value
Recovery Point Objective (RPO)		15 minutes
Point in time instances	Enable	Selected
	Keep 3 instances per day for the last 1 days.	

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

15 (Optional) Monitor the replication progress.

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

   b Click the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server object and click the **Monitor** tab.

   c Click the **vSphere Replication** tab and select **Outgoing Replications** to see details about the replication of the analytics nodes of vRealize Operations Manager from this site.

Replicate the vRealize Suite Lifecycle Manager Appliance in Region A

To support a failover to Region B, you configure the replication of the vRealize Suite Lifecycle Manager virtual appliance. The replica virtual machine becomes active upon failover. After you configure the replication, you create a protection group to protect the replicated virtual machine.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, click **VMs and Templates**.

3 Navigate to the **sfo01-m01fd-mgmt** VM folder.

Object	Value
vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Data center	sfo01-m01dc
Folder	sfo01-m01fd-mgmt

4 Right-click **vrslcm01svr01a**, and select **All vSphere Replication Actions > Configure Replication**.

5 On the **Replication type** page, select **Replicate to a vCenter Server** and click **Next**.

6 On the **Target site** page, select the **lax01m01vc01.lax01.rainpole.local** vCenter Server and click **Next**.

7 On the **Replication server** page, select **Auto-assign vSphere Replication server** and click **Next**.

8 On the **Target location** page, set the location on the vSAN datastore in Region B to store replicated virtual machine files.

   a Click the **Edit** link.

   b In the **Select Target Location** dialog box, from the datastore list in the upper part of the dialog box, select **lax01-m01-vsan01** as the datastore for replicated files.

   c In the **Select a target location** pane, select **lax01-m01-vsan01** to select the root folder of the datastore and click **OK**.

      vSphere Replication creates a folder in the root datastore folder the virtual machine.

   d On the **Target location** page, click **Next**.

9 On the **Replication options** page, under **Network Compresion** only select the **Enable network compression for VR data** check box and click **Next**.

10 On the **Recovery settings** page, enter the following settings and click **Next**.

Setting		Value
Recovery Point Objective (RPO)		15 minutes
Point in time instances	Enable	Selected
	Keep **3** instances per day for the last **1** days.	

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

Replication configuration for the virtual machines from the operations management platform starts.

12 (Optional) Monitor the replication progress.

a From the **Home** menu of the vSphere Web Client, select **Hosts and Clusters**.

b Click the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server object and click the **Monitor** tab.

c Click the **vSphere Replication** tab and select **Outgoing Replications** to see details for the replication of the virtual machines of the operations management layer from this site.

Create a Protection Group for the Operations ManagementApplications

After you configure the replication for the analytics virtual machines of vRealize Operations Manager and vRealize Suite Lifecycle Manager, you create a protection group and include the virtual machines in the protection group. Site Recovery Manager protects the virtual machines together.

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and select the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 If the **Log In Site** dialog box appears, reauthenticate by using the **`svc-srm@rainpole.local`** user name and the ***`svc-srm_password`*** password.

Reauthentication is required if the network connection between Region A and Region B has been interrupted after the last successful authentication.

5 On the **Related Objects** tab, click the **Protection Groups** tab and click **Create Protection Group**.

The **Create Protection Group** wizard appears.

6 On the **Name and location** page, configure the following settings and click **Next**.

Setting	Value
Name	SDDC Operations Management PG
Description	Protection Group for vRealize Operations Manager Cluster and vRealize Suite Lifecycle Manager
Site pair	sfo01m01vc01.sfo01.rainpole.local - lax01m01vc01.lax01.rainpole.local

7 On the **Protection group type** page, configure the following settings and click **Next**.

Setting	Value
Direction of protection	sfo01m01vc01.sfo01.rainpole.local -> lax01m01vc01.lax01.rainpole.local
Protection group type	Individual VMs

8 On the **Virtual machines** page, select the vRealize Operations Manager analytics cluster virtual machines and vRealize Suite Lifecycle Manager appliance from the list of replicated virtual machines and click **Next**.

Component	Virtual Machine
Analytics cluster master node	vrops01svr01a
Analytics cluster master replica node	vrops01svr01b
Analytics cluster data node	vrops01svr01c
vRealize Suite Lifecycle Manager	vrslcm01svr01a

9 On the **Ready to complete** page, review the protection group settings and click **Finish**.

The `SDDC Operations Management PG` protection group appears in the list of protection groups in Site Recovery Manager. You use it to assign a recovery plan for the analytics and vRealize Suite Lifecycle Manager virtual machines.

Create a Recovery Plan for the Operations ManagementApplications

After you create a protection group for the virtual machines of the vRealize Operations Manager analytics cluster and vRealize Suite Lifecycle Manager, create a recovery plan. You then use this plan to configure dependencies between the virtual machines.

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **Create Recovery Plan** icon.

The **Create Recovery Plan** wizard appears.

5 On the **Name and Location** page, configure the following settings and click **Next**.

Setting	Value
Name	SDDC Operations Management RP
Description	Recovery Plan for vRealize Operations Manager Cluster and vRealize Suite Lifecycle Manager
Site pair	sfo01m01vc01.sfo01.rainpole.local - lax01m01vc01.lax01.rainpole.local

6 On the **Recovery Site** page, select **lax01m01vc01.lax01.rainpole.local** as the recovery site and click **Next**.

7 On the **Protection groups** page, select the protection group for the recovery plan and click **Next**.

Setting	Value
Group type	VM protection groups
Protection group	SDDC Operations Management PG

8 On the **Test networks** page, leave the default values and click **Next**.

The default option creates an isolated test network.

9 On the **Ready to complete** page, click **Finish**.

The `SDDC Operations Management RP` recovery plan appears in the list of available recovery plans in Site Recovery Manager.

Customize the Recovery Plan for the Operations ManagementApplications

After you create the recovery plan, configure the startup priority and the startup and shutdown options for the virtual machines of the analytics cluster and vRealize Suite Lifecycle Manager. The master node of vRealize Operations Manager must start first after failover.

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Operations Management RP** recovery plan.

5 Change the startup priority of the virtual machine of the master node.

   a On the recovery plan page, click the **Monitor** tab and click the **Recovery Steps** tab.

   b Under **Power on priority 3** VMs, right-click vrops01svr01a and select **All Priority Actions > 1 > (Highest)**.

   c In the **Change Priority** dialog box, click **Yes** to confirm.

6 Configure startup and shutdown options for the master node.

   a On the **SDDC Operations Management RP** page, right-click **vrops01svr01a** and select **Configure Recovery**.

   b In the **VM Recovery Properties** dialog box, expand **Shutdown Action** and increase the **Shutdown guest OS before power off** timeout to **`10 minutes`**.

   c Expand **Startup Action**, increase the **Wait for VMware tools** timeout to **`10 minutes`**, and click **OK**.

7 Repeat *Step 5* and *Step 6* for the other virtual machines.

Virtual Machine	Startup Priority Order	Update Timeout Values for Shutdown and Startup?
vrops01svr01b	2	No
vrops01svr01c	3	Yes
vrslcm01svr01a	4	No

Create an Anti-Affinity Rule for vRealize Operations Manager in Region B

Anti-affinity rules do not persist across regions during recovery using Site Recovery Manager. You must create the anti-affinity rules for the analytics virtual machines in Region B so that the rules still apply after a failover of vRealize Operations Manager.

Procedure

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

   a Open a Web browser and go to **`https://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 of the vSphere Web Client, select **Hosts and Clusters** and navigate to the lax01m01vc01.lax01.rainpole.local vCenter Server object.

3 Expand the **lax01m01vc01.lax01.rainpole.local > lax01-m01dc** tree and click **lax01-m01-mgmt01**.

4 Click the **Configure** tab, under **Configuration**, select **VM/Host Rules**.

5 In the **VM/Host Rules** list, click **Add** to create an anti-affinity rule.

6 In the **Create VM/Host Rule** dialog box, add an anti-affinity rule for the VMs of the master, master replica, and data nodes, and click **OK**.

Setting	Value
Name	anti-affinity-rule-vropsm
Enable Rule	Selected
Type	Separate Virtual Machines
Members	vrops01svr01a.rainpole.local vrops01svr01b.rainpole.local vrops01svr01c.rainpole.local

Configure Failover of the Cloud Management Platform

Prepare vRealize Automation, and vRealize Business for failover. Replicate the virtual machines of the primary vRealize Automation components, and of vRealize Business Server. Create a recovery plan for these application components in Site Recovery Manager.

Procedure

1 Replicate the Primary VMs of vRealize Automation and vRealize Business

To support failover to Region B, enable the replication of the virtual machines that constitute the primary functionality of the Cloud Management Platform. After you configure the replication, you create a protection group to protect the replicated virtual machines.

2 Create a Protection Group for the Cloud Management Platform

After you configure the replication for the Cloud Management Platform VMs, create and configure a dedicated protection group so that Site Recovery Manager protects them together.

3 Create a Recovery Plan for the Cloud Management Platform

After you create a protection group for the cloud management platform VMs, you create a recovery plan. Use this plan to configure dependencies between the virtual machines.

4 Customize the Recovery Plan for the Cloud Management Platform

After you create the recovery plan for the Cloud Management Platform VMs, configure the startup priority, and the startup and shutdown options for the virtual machines.

5 Create Anti-Affinity Rules for vRealize Automation in Region B

Anti-affinity rules do not persist across regions during recovery using Site Recovery Manager. In Region B, you must create the anti-affinity rules for the components of the Cloud Management Platform that are failed over from Region A so that the rules apply after failover.

6 Create VM Groups to Define the Startup Order of the Cloud Management Platform in Region B

VM groups allow you to define the startup order of virtual machines. The startup order you define ensures that vSphere HA powers on virtual machines in the correct order. In Region B, create the VM groups defining the startup order of the Cloud Management Platform VMs that are failed over from Region A.

Replicate the Primary VMs of vRealize Automation and vRealize Business

To support failover to Region B, enable the replication of the virtual machines that constitute the primary functionality of the Cloud Management Platform. After you configure the replication, you create a protection group to protect the replicated virtual machines.

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, click **VMs and Templates**.

3 Navigate to the **sfo01-m01fd-vra** VM folder.

Object	Value
vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Data center	sfo01-m01dc
Folder	sfo01-m01fd-vra

4 On the **sfo01-m01fd-vra** page, click the **VMs** tab, click **Virtual Machines**, and select the virtual machines of vRealize Automation and vRealize Business Server.

vRealize Automation Component	VM Name
IaaS Manager Service and DEM Orchestrator	vra01ims01a
IaaS Manager Service and DEM Orchestrator	vra01ims01b
IaaS Web Server	vra01iws01a
IaaS Web Server	vra01iws01b
Microsoft SQL Server	vra01mssql01
vRealize Automation Appliance	vra01svr01a
vRealize Automation Appliance	vra01svr01b
vRealize Automation Appliance	vra01svr01c

vRealize Automation Component	VM Name
vRealize Automation DEM Worker	vra01dem01a
vRealize Automation DEM Worker	vra01dem01b
vRealize Business Server	vrb01svr01

5 Right-click the VM selection and select **All vSphere Replication Actions > Configure Replication**.

6 In the dialog box about performing replication for all objects, click **Yes**.

The **Configure Replication for 11 Virtual Machines** wizard opens.

7 On the **Validation** page, wait until the process completes successfully and click **Next**.

8 On the **Replication type** page, select **Replicate to a vCenter Server** and click **Next**.

9 On the **Target site** page, select the **lax01m01vc01.lax01.rainpole.local** vCenter Server and click **Next**.

10 On the **Replication server** page, select **Auto-assign vSphere Replication server** and click **Next**.

11 On the **Target location** page, set the location on the vSAN datastore in Region B to store replicated VM files.

a Click the **Edit for all** link.

b In the **Select Target Location** dialog box, from the datastore list in the upper part of the dialog box, select **lax01-m01-vsan01** as the datastore for replicated files.

c In the **Select a target location** pane, select **lax01-m01-vsan01** to select the root folder of the datastore and click **OK**.

vSphere Replication creates a folder in the root datastore folder for each Cloud Management VM.

d On the **Target Location** page, click **Next**.

12 On the **Replication options** page, select only the **Enable network compression for VR data** check box and click **Next**.

Important

- Do not enable guest OS quiescing because some of the vRealize Automation and vRealize Orchestrator database do not support quiescing. Quiescing might result in a cluster failure because virtual disks remain in a frozen state for too long.
- Compression requires extra resources. Do not enable it if the hosts are over-utilized.

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

Setting		Value
Recovery Point Objective (RPO)		15 minutes
Point in time instances	Enable	Selected
	Keep **3** instances per day for the last **1** days.	

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

Replication configuration for the virtual machines from the cloud management platform starts.

15 (Optional) Monitor the replication progress.

a From the **Home** menu of the vSphere Web Client, select **Hosts and Clusters**.

b Click the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server object and click the **Monitor** tab.

c Click the **vSphere Replication** tab, and select **Outgoing Replications** to see details about the replication of the virtual machines of the Cloud Management Platform from this site.

Create a Protection Group for the Cloud Management Platform

After you configure the replication for the Cloud Management Platform VMs, create and configure a dedicated protection group so that Site Recovery Manager protects them together.

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and select the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 If the **Log In Site** dialog box appears, reauthenticate by using the `svc-srm@rainpole.local` user name and the ***`svc-srm_password`*** password.

Reauthentication is required if the network connection between Region A and Region B has been interrupted after the last successful authentication.

5 On the **Related Objects** tab, click the **Protection Groups** tab and click **Create Protection Group**.

The **Create Protection Group** wizard appears.

6 On the **Name and location** page, configure the following settings and click **Next**.

Setting	Value
Name	SDDC Cloud Management PG
Description	Protection Group for vRealize Automation and vRealize Business
Site pair	sfo01m01vc01.sfo01.rainpole.local - lax01m01vc01.lax01.rainpole.local

7 On the **Protection group type** page, configure the following settings and click **Next**.

Setting	Value
Direction of protection	sfo01m01vc01.sfo01.rainpole.local -> lax01m01vc01.lax01.rainpole.local
Protection group type	Individual VMs (vSphere Replication)

8 On the **Virtual machines** page, select the virtual machines of vRealize Automation and the vRealize Business Server from the list of virtual machines replicated by using vSphere Replication, and click **Next**.

Component	Virtual Machine
vRealize Automation IaaS Managers	vra01ims01a vra01ims01b
vRealize Automation IaaS Web Servers	vra01iws01a vra01iws01b
vRealize Automation Database	vra01mssql01
vRealize Automation Virtual Appliances	vra01svr01a vra01svr01b vra01svr01c
vRealize Automation IaaS DEM Workers	vra01dem01a vra01dem01b
vRealize Business for Cloud Server	vrb01svr01

9 On the **Ready to complete** page, review the protection group settings and click **Finish**.

The `SDDC Cloud Management PG` protection group appears in the list of protection groups for Site Recovery Manager.

Create a Recovery Plan for the Cloud Management Platform

After you create a protection group for the cloud management platform VMs, you create a recovery plan. Use this plan to configure dependencies between the virtual machines.

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **Create Recovery Plan** icon.

The **Create Recovery Plan** wizard appears.

5 On the **Name and location** page, configure the following settings and click **Next**.

Setting	Value
Name	SDDC Cloud Management RP
Description	Recovery Plan for vRealize Automation and vRealize Business
Site pair	sfo01m01vc01.sfo01.rainpole.local - lax01m01vc01.lax01.rainpole.local

6 On the **Recovery Site** page, select **lax01m01vc01.lax01.rainpole.local** as the recovery site and click **Next**.

7 On the **Protection groups** page, select the protection group for the recovery plan and click **Next**.

Setting	Value
Group type	VM protection groups
Protection group	SDDC Cloud Management PG

8 On the **Test networks** page, leave the default values and click **Next**.

The default option automatically creates an isolated test network.

9 On the **Ready to complete** page, click **Finish**.

The `SDDC Cloud Management RP` recovery plan appears in the list of available recovery plans in Site Recovery Manager.

Customize the Recovery Plan for the Cloud Management Platform

After you create the recovery plan for the Cloud Management Platform VMs, configure the startup priority, and the startup and shutdown options for the virtual machines.

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Cloud Management RP** recovery plan.

5 On the **SDDC Cloud Management RP** page, click the **Related Objects** tab and click **Virtual Machines**.

6 Change the priority of the **vra01mssql01** VM.

   a On the **Virtual Machines** tab, right-click **vra01mssql01** and select **All Priority Actions > 1 (Highest)**.

   b In the **Change Priority** dialog box, click **Yes** to confirm.

7 Repeat the previous step to reconfigure the priorities of the following VMs.

VM Name	Priority
vra01svr01a	2
vra01svr01b	2
vra01svr01c	2
vra01iws01a	3
vra01iws01b	3
vra01ims01a	4
vra01ims01b	4
vra01dem01a	5
vra01dem01b	5
vrb01svr01	5

8 Configure dependencies between the virtual machines that have the vRA Server role.

   a Right-click the **vra01svr01b** virtual machine in the recovery plan and select **Configure Recovery**.

   b In the **VM Recovery Properties** dialog box, expand the **VM Dependencies** section and click **Configure**.

   c Select **vra01svr01a** and click **OK**.

   d Click **OK**.

9 Configure dependencies between the virtual machines that have the vRA Replica Server role.

   a Right-click the **vra01svr01c** virtual machine in the recovery plan and select **Configure Recovery**.

   b In the **VM Recovery Properties** dialog box, expand the **VM Dependencies** section and click **Configure**.

c Select **vra01svr01b** and click **OK**.

d Click **OK**.

10 Configure additional startup delay for the primary vRA Server.

a Right-click the **vra01svr01a.rainpole.local** virtual machine in the recovery plan and select **Configure Recovery**.

b In the **VM Recovery Properties** dialog box, expand the **Startup Action** section, select **Additional Delay**, and set **Delay** to 5 minutes.

c Click **OK**.

11 Repeat the step on the vra01iws01a and vra01ims01a virtual machines to configure additional startup delay.

Setting	Value
VM name	vra01iws01a, vra01ims01a
Additional delay	5 minutes

12 Configure dependencies between the virtual machines that have the IaaS Web Server role and additional startup delay for the second IaaS Web Server.

a Right-click the **vra01iws01b** virtual machine in the recovery plan and select **Configure Recovery**.

b In the **VM Recovery Properties** dialog box, expand the **VM Dependencies** section and click **Configure**.

c Select **vra01iws01a** and click **OK**.

d In the **VM Recovery Properties** dialog box, expand the **Startup Action** section, select **Additional Delay**, and set **Delay** to 5 minutes.

e Click **OK**.

13 Repeat the step on the vra01ims01b virtual machine to configure dependencies and additional startup delay after failover for the IaaS Manager Service.

Setting	Value
VM name	vra01ims01b
VM dependencies	vra01ims01a
Additional delay	5 minutes

The Recovery Plan has the following order:

Table 3-2. Recovery Order of the Cloud Management Platform

Priority	VM Name	Dependency	Additional Startup Delay
1	vra01mssql01	-	-
2	vra01svr01a	-	5

Table 3-2. Recovery Order of the Cloud Management Platform (Continued)

Priority	VM Name	Dependency	Additional Startup Delay
2	vra01svr01b	vra01svr01a	-
2	vra01svr01c	vra01svr01b	-
3	vra01iws01a	-	5
3	vra01iws01b	vra01iws01a	5
4	vra01ims01a	-	5
4	vra01ims01b	vra01ims01a	5
5	vra01dem01a	-	-
5	vra01dem01b	-	-
5	vrb01svr01	-	-

Create Anti-Affinity Rules for vRealize Automation in Region B

Anti-affinity rules do not persist across regions during recovery using Site Recovery Manager. In Region B, you must create the anti-affinity rules for the components of the Cloud Management Platform that are failed over from Region A so that the rules apply after failover.

Table 3-3. Anti-Affinity Rules for the Cloud Management Platform

Name	Type	Members
anti-affinity-rule-vra-svr	Separate Virtual Machines	vra01svr01a, vra01svr01b, vra01svr01c
anti-affinity-rule-vra-dem	Separate Virtual Machines	vra01dem01a, vra01dem01b
anti-affinity-rule-vra-ims	Separate Virtual Machines	vra01ims01a, vra01ims01b
anti-affinity-rule-vra-iws	Separate Virtual Machines	vra01iws01a, vra01iws01b

Procedure

1 Log in to the Management 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 of the vSphere Web Client, select **Hosts and Clusters** and navigate to the **lax01m01vc01.lax01.rainpole.local** vCenter Server object.

3 Expand the **lax01m01vc01.lax01.rainpole.local>lax01-m01dc** tree and click the **lax01-m01-mgmt01** cluster.

4 Click the **Configure** tab, and under **Configuration**, select **VM/Host Rules**.

5 Under **VM/Host Rules**, click **Add** to create a virtual machine anti-affinity rule.

6 In the **Create VM/Host Rule** dialog box, add the first rule for the vRealize Automation Appliances, click **OK**, and click **OK**.

Setting	Value
Name	anti-affinity-rule-vra-svr
Enable rule	Selected
Type	Separate Virtual Machines
Members	vra01svr01a vra01svr01b vra01svr01c

7 Repeat the procedure to configure the remaining anti-affinity rules.

Create VM Groups to Define the Startup Order of the Cloud Management Platform in Region B

VM groups allow you to define the startup order of virtual machines. The startup order you define ensures that vSphere HA powers on virtual machines in the correct order. In Region B, create the VM groups defining the startup order of the Cloud Management Platform VMs that are failed over from Region A.

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 of the vSphere Web Client, select **Host and Clusters** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

3 Create a VM Group for the vRealize Automation IaaS Database.

   a Select the **lax01-m01-mgmt01** cluster and click the **Configure** tab.

   b Click **VM/Host Groups** and on the **VM/Host Groups** page, click the **Add** button.

   c In the **Create VM/Host Group** dialog box, enter **`vRealize Automation IaaS Database`** in the **Name** text box, select **VM Group** from the **Type** drop-down menu, and click the **Add** button.

   d In the **Add VM/Host Group Member** dialog box, select **vra01mssql01**, click **OK**, and click **OK**.

4 Repeat *Step 3* to create the following VM/Host groups.

VM/Host Group Name	VM/Host Group Member
vRealize Automation Virtual Appliances	vra01svr01a
	vra01svr01b
	vra01svr01c
vRealize Automation IaaS Web Servers	vra01iws01a
	vra01iws01b
vRealize Automation IaaS Managers	vra01ims01a
	vra01ims01b
vRealize Automation IaaS DEM Workers	vra01dem01a
	vra01dem01b
vRealize Automation IaaS Proxy Agents	sfo01ias01a
	sfo01ias01b
vRealize Business for Cloud Servers	vrb01svr01
vRealize Business for Cloud Data Collectors	sfo01vrbc01

5 Create a rule to power on the vRealize Automation database before vRealize Automation virtual appliances.

a Select the **lax01-m01-mgmt01** cluster and click the **Configure** tab.

b Click **VM/Host Rules** and on the **VM/Host Rules** page, click the **Add** button.

c In the **Create VM/Host Rule** dialog box, enter `SDDC Cloud Management Platform 01` in the **Name** text box, ensure the **Enable Rule** check box is selected, and select **Virtual Machines to Virtual Machines** from the **Type** drop-down menu.

d Select **vRealize Automation IaaS Database** from the **First restart VMs in VM group** drop-down menu.

e Select **vRealize Automation Virtual Appliances** from the **Then restart VMs in VM group** drop-down menu, and click **OK**.

6 Repeat *Step 5* to create the following VM/Host rules for the correct restart order of the Cloud Management Platform.

VM/Host Rule Name	First Restart VMs in VM Group	Then Restart VMs in VM Group
SDDC Cloud Management Platform 02	vRealize Automation Virtual Appliances	vRealize Automation IaaS Web Servers
SDDC Cloud Management Platform 03	vRealize Automation IaaS Web Servers	vRealize Automation IaaS Managers
SDDC Cloud Management Platform 04	vRealize Automation IaaS Managers	vRealize Automation IaaS DEM Workers
SDDC Cloud Management Platform 05	vRealize Automation IaaS Managers	vRealize Automation IaaS Proxy Agents

VM/Host Rule Name	First Restart VMs in VM Group	Then Restart VMs in VM Group
SDDC Cloud Management Platform 06	vRealize Automation IaaS Managers	vRealize Business for Cloud Servers
SDDC Cloud Management Platform 07	vRealize Business for Cloud Servers	vRealize Business for Cloud Data Collectors

Test Failover of the SDDC Management Applications

You can identify potential problems during a future failover by testing the recovery plan for the management applications in the SDDC.

- Test Failover of the Operations Management Applications

  Validate the configuration by testing the recovery plan for vRealize Operations Manager and vRealize Suite Lifecycle Manager.

- Test Failover of the Cloud Management Platform

  Validate the configuration by testing the recovery plan for vRealize Automation and vRealize Business.

Test Failover of the Operations ManagementApplications

Validate the configuration by testing the recovery plan for vRealize Operations Manager and vRealize Suite Lifecycle Manager.

Site Recovery Manager runs the analytics virtual machines and vRealize Suite Lifecycle Manager on the test network and on a temporary snapshot of replicated data in Region B.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 If the **Log In Site** dialog box appears, re-authenticate by using the **`svc-srm@rainpole.local`** user name and the ***`svc-srm_password`*** password.

   Re-authentication is required if the network connection between Region A and Region B has been interrupted after the last successful authentication.

5 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Operations Management RP** recovery plan.

6 On the **SDDC Operations Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

7 Click the **Test Recovery Plan** icon to run a test recovery.

The **Test** wizard appears.

8 On the **Confirmation options** page, leave the **Replicate recent changes to recovery site** check box selected and click **Next**.

9 On the **Ready to complete** page, click **Finish** to start the test recovery.

Test failover starts. You can follow the progress on the **Recovery Steps** page.

10 After the test recovery is complete, click the **Cleanup Recovery Plan** icon to clean up all the created test VMs.

11 On the **Confirmation options** page of the **Cleanup** wizard, click **Next**.

12 On the **Ready to complete** page, click **Finish** to start the clean-up process.

After the clean-up process finishes, make sure that **Plan status** shows a `Ready` state.

Test Failover of the Cloud Management Platform

Validate the configuration by testing the recovery plan for vRealize Automation and vRealize Business.

Site Recovery Manager runs the vRealize Automation and vRealize Business virtual machines on the test network and on a temporary snapshot of replicated data in Region B.

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 If the **Log In Site** dialog box appears, re-authenticate by using the **`svc-srm@rainpole.local`** user name and the ***`svc-srm_password`*** password.

Re-authentication is required if the network connection between Region A and Region B has been interrupted after the last successful authentication.

5 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Cloud Management RP** recovery plan.

6 On the **SDDC Cloud Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

7 Click the **Test Recovery Plan** icon to run a test recovery.

The **Test** wizard appears.

8 On the **Confirmation options** page, leave the **Replicate recent changes to recovery site** check box selected and click **Next**.

9 On the **Ready to complete** page, click **Finish** to start the test recovery.

Test failover starts. You can follow the progress on the **Recovery Steps** page.

Note Because recovered virtual machines are using the test network, VMware Tools in the vra01svr01a, vra01svr01b, and vra01svr01c virtual machines might not become online within the default timeout. In the recovery plan, increase the startup delay for VMware Tools for these virtual machines to complete the test.

10 After the test recovery is complete, click the **Cleanup Recovery Plan** icon to clean up all the created test VMs.

11 On the **Confirmation options** page of the **Cleanup** wizard, click **Next**.

12 On the **Ready to complete** page, click **Finish** to start the clean-up process.

After the clean-up process finishes, make sure that **Plan status** shows a `Ready` state.

Perform Planned Migration of the SDDC Management Applications

After you have successfully configured and tested failover of the management applications, you can initiate a migration process from Region A to Region B. The planned migration of the SDDC management components keeps the SDDC operational, for example, when upgrading the hardware or changing the network configuration in Region A.

- Initiate a Planned Migration of the Operations Management Applications

  You can run a recovery plan under planned circumstances to migrate the virtual machines of the analytics cluster of vRealize Operations Manager and vRealize Suite Lifecycle Manager from Region A to Region B. You can also run a recovery plan under unplanned circumstances in case Region A suffers an unforeseen event that results in data loss.

- Initiate a Planned Migration of the Cloud Management Platform

  You can run a recovery plan under planned circumstances to migrate the virtual machines of vRealize Automation and vRealize Business from Region A to Region B. You can also run a recovery plan under unplanned circumstances in case Region A suffers an unforeseen event that results in data loss.

Initiate a Planned Migration of the Operations ManagementApplications

You can run a recovery plan under planned circumstances to migrate the virtual machines of the analytics cluster of vRealize Operations Manager and vRealize Suite Lifecycle Manager from Region A to Region B. You can also run a recovery plan under unplanned circumstances in case Region A suffers an unforeseen event that results in data loss.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Operations Management RP** recovery plan.

5 On the **SDDC Operations Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

6 Click the **Run Recovery Plan** icon to run the recovery plan and initiate the failover of the analytics cluster.

   The **Recovery** wizard appears.

7 On the **Confirmation options** page, configure the following settings and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	Selected
Recovery type	Planned migration

8 To initiate the failover of vRealize Operations Manager and vRealize Suite Lifecycle Manager, click **Finish** on the **Ready to complete** page.

What to do next

1 Verify that after failover both vRealize Operations Manager and vRealize Suite Lifecycle Manager are up and operational. See *Verification of vRealize Operations Manager* and *Verification of vRealize Suite Lifecycle Manager* in the *VMware Validated Design Operational Verification* documentation.

2 Prepare vRealize Operations Manager and vRealize Suite Lifecycle Manager for failback by reprotecting the virtual machines of the analytics cluster and vRealize Suite Lifecycle Manager in Site Recovery Manager. See Reprotect the Operations Management Applications.

Initiate a Planned Migration of the Cloud Management Platform

You can run a recovery plan under planned circumstances to migrate the virtual machines of vRealize Automation and vRealize Business from Region A to Region B. You can also run a recovery plan under unplanned circumstances in case Region A suffers an unforeseen event that results in data loss.

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Cloud Management RP** recovery plan.

5 On the **SDDC Cloud Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

6 Click the **Run Recovery Plan** icon to run the recovery plan and initiate the failover of the Cloud Management Platform.

The **Recovery** wizard appears.

7 On the **Confirmation options** page, configure the following settings and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	Selected
Recovery type	Planned migration

8 To initiate the failover of the Cloud Management Platform, on the **Ready to complete** page click **Finish**.

What to do next

1 Verify that vRealize Automation and vRealize Business VMs are up and operational. See *Operational Verification of the Cloud Management Layer* in the *VMware Validated Design Operational Verification* documentation.

2 Prepare vRealize Automation and vRealize Business for failback by reprotecting their VMs in Site Recovery Manager. See Reprotect the Cloud Management Platform.

Perform Disaster Recovery of the SDDC Management Applications

Prepare networking in Region B and perform a failover of vRealize Automation, vRealize Orchestrator, vRealize Business, vRealize Operations Manager, and vRealize Suite Lifecycle Manager to Region B if Region A becomes unavailable.

Procedure

1 Reconfigure the NSX Instance for the Management Cluster in Region B

If Region A becomes unavailable, prepare the network layer in Region B for a failover of the management applications. Change the role of the NSX Manager to primary, deploy the universal controller cluster, and synchronize the universal controller cluster configuration.

2 Recover the Control VM of the Universal Distributed Logical Router in Region B

In the event of a site failure in Region A, dynamic routing in Region B might not be available. Deploy a Control VM for the universal distributed logical router sfo01m01udlr01 in Region B to recover dynamic routing in the environment. You then configure the recovered Control VM to provide dynamic routing for the SDDC management applications that are failed over.

3 Reconfigure the Universal Distributed Logical Router and NSX Edges for Dynamic Routing in Region B

To support dynamic routing in Region B before you start disaster recovery from Region A, configure the universal distributed logical router sfo01m01udlr01 and NSX Edges lax01m01esg01 and lax01m01esg02. This configuration ensures that the management components of the SDDC continue to communicate using optimal routes in a fault-tolerant network.

4 Verify Establishment of BGP for the Universal Distributed Logical Router in Region B

Verify that the UDLR for the management applications is successfully peering, and that BGP routing has been established in Region B. After you perform disaster recovery, they can continue communicating to keep the SDDC operational.

5 Enable Network Connectivity for the NSX Load Balancer in Region B

Enable the network connectivity on lax01m01lb01 load balancer to support high-availability and distribute the network traffic load for vRealize Operations Manager, vRealize Suite Lifecycle Manager, and the Cloud Management Platform after disaster recovery to Region B.

6 Initiate Disaster Recovery of the Operations Management Applications in Region B

In the event of a site failure in Region A, initiate disaster recovery of vRealize Suite Lifecycle Manager and of vRealize Operations Manager to keep the monitoring functionality of the SDDC running.

7 Initiate Disaster Recovery of the Cloud Management Platform in Region B

In the event of a site failure in Region A, initiate disaster recovery of the vRealize Automation and vRealize Business components to keep the workload provisioning functionality of the SDDC available.

8 Post-Failover Configuration of the SDDC Management Applications

After failover of the Cloud Management Platform, vRealize Operations Manager, and vRealize Suite Lifecycle Manager, you must perform additional tasks to ensure that the applications perform as expected.

Reconfigure the NSX Instance for the Management Cluster in Region B

If Region A becomes unavailable, prepare the network layer in Region B for a failover of the management applications. Change the role of the NSX Manager to primary, deploy the universal controller cluster, and synchronize the universal controller cluster configuration.

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 Promote the NSX Manager for the management cluster in Region B to the primary role.

You must first disconnect the NSX Manager for the management cluster in Region B from the Primary NSX Manager in Region A.

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

b In the **Navigator** pane, click **Installation and Upgrade**.

c On the **Management** tab, click **NSX Managers** tab and select the **172.17.11.65** instance.

d Click the **Actions** menu and click **Disconnect from Primary NSX Manager**.

e In the **Disconnect from Primary NSX Manager** dialog box, click **Yes**.

The NSX Manager gets the Transit role.

f On the **NSX Managers** tab, select the **172.17.11.65** instance again.

g Click **Actions** and select **Assign Primary Role**.

h In the **Assign Primary Role** dialog box, click **Yes**.

3 Configure an IP pool for the new universal controller cluster.

a In the **Navigator** pane, click **Groups and Tags**.

b Click the **IP Pools** tab and select the **172.17.11.65** instance.

c On the **IP Pools** tab, click **+ ADD**.

d In the **New IP Pool** dialog box, enter the following settings, and click **Add**.

Setting	Value
Name	lax01-mgmt01-nsxc01
Gateway	172.17.11.253
Prefix Length	24
Primary DNS	172.17.11.5
Secondary DNS	172.17.11.4
DNS Suffix	lax01.rainpole.local
IP Pool Range	172.17.11.118-172.17.11.120

You enter the IP pool range by clicking **+ ADD** below **IP Pool Range**.

4 Deploy the universal controller cluster in Region B.

a In the **Navigator** pane, click **Installation and Upgrade**.

b On the **Management** tab, under **NSX Controller nodes**, click the **Add** icon to deploy three NSX Controller nodes with the same configuration.

c In the **Add Controller** dialog box, enter the following settings and click **Next**.

Setting	Value
NSX Manager	172.17.11.65
Password	*mgmtnsx_controllers_password*
Confirm Password	*mgmtnsx_controllers_password*

You configure a password only during the deployment of the first controller. The other controllers use the same password.

d In the **Add Controller** dialog box, under **Deployment & Connectivity**, enter the following settings and click **Finish**.

Setting	Value
Name	■ lax01m01nsxc01 for controller 1 ■ lax01m01nsxc02 for controller 2 ■ lax01m01nsxc03 for controller 3
Data center	lax01-m01dc
Cluster/Resource Pool	lax01-m01-mgmt01
Datastore	lax01-m01-vsan01
Folder	lax01-m01fd-nsx
Connected To	lax01-m01-vds01-management
Select IP Pool	lax01-mgmt01-nsxc01

e After the **Status** of the controller node changes to `Connected`, deploy the remaining two NSX Controller nodes lax01m01nsxc02 and lax01m01nsxc03.

Wait until the current deployment finishes before you start with the next controller.

5 Configure DRS affinity rules for the deployed NSX Controller nodes.

a From the **Home** menu of the vSphere Web Client, select **Hosts and Clusters**.

b Expand the **lax01m01vc01.lax01.rainpole.local>lax01-m01dc** and click the **lax01-m01-mgmt01** cluster.

c Click the **Configure** tab, under **Configuration**, click **VM/Host Rules**, and click **Add**.

d In the **Create VM/Host Rule** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	anti-affinity-rule-nsxc
Enable rule	Selected
Type	Separate Virtual Machines
Members	■ lax01m01nsxc01 ■ lax01m01nsxc02 ■ lax01m01nsxc03

6 Synchronize the state of the newly deployed controllers by using the Update Controller State mechanism on the NSX Manager.

Update Controller State pushes the current VXLAN and universal distributed logical router configuration from NSX Manager to the Controller cluster.

a From the **Home** menu of the vSphere Web Client, select **Networking & Security**.

b In the **Navigator** pane, click **Installation and Upgrade**.

c On the **Management** tab, under **NSX Managers**, select the **172.17.11.65** instance.

d From the **Actions** menu, select **Update Controller State**.

e In the **Update Controller State** dialog box, click **Yes**.

Recover the Control VM of the Universal Distributed Logical Router in Region B

In the event of a site failure in Region A, dynamic routing in Region B might not be available. Deploy a Control VM for the universal distributed logical router sfo01m01udlr01 in Region B to recover dynamic routing in the environment. You then configure the recovered Control VM to provide dynamic routing for the SDDC management applications that are failed over.

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 of the vSphere Web Client, click **Networking & Security**.

3 In the **Navigator** pane, click **NSX Edges**.

4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.

5 Double-click **sfo01m01udlr01**.

6 Redeploy the Control VM of the universal distributed logical router and enable HA.

a Click the **Manage** tab and click **Settings**.

b Select **Configuration**, under **Logical Router Appliances** click the **Add** icon.

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

Setting	Value
Data center	lax01-m01dc
Cluster/Resource Pool	lax01-m01-mgmt01
Datastore	lax01-m01-vsan01

d To deploy another NSX Edge device with the same configuration, click the **Add** icon and repeat this step.

7 Configure high availability for the Control VM.

a On the **Configuration** page for sfo01m01udlr01, click **Change** under **HA Configuration**, configure the following settings, and click **OK**.

Setting	Value
HA Status	Enable
Connected To	lax01-m01-vds01-management
Enable Logging	Selected

b In the **Change HA configuration** dialog box, click **Yes**.

8 Configure the CLI Credentials for the Control VM.

a In the **Navigator** pane, click **NSX Edges**.

b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

c Right-click **sfo01m01udlr01** and select **Change CLI Credentials**.

d In the **Change CLI Credentials** dialog box, configure the following settings and click **OK**.

Setting	Value
User Name	admin
Password	*udlr_admin_password*
Enable SSH access	Selected

Reconfigure the Universal Distributed Logical Router and NSX Edges for Dynamic Routing in Region B

To support dynamic routing in Region B before you start disaster recovery from Region A, configure the universal distributed logical router sfo01m01udlr01 and NSX Edges lax01m01esg01 and lax01m01esg02. This configuration ensures that the management components of the SDDC continue to communicate using optimal routes in a fault-tolerant network.

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 of the vSphere Web Client, select **Networking & Security**.

3 In the **Navigator** pane, click **NSX Edges**.

4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.

5 Verify the routing configuration for the universal distributed logical router.

a Double-click **sfo01m01udlr01**.

b Click the **Manage** tab, click **Routing**, and verify the following settings.

Setting	Value
Global Configuration > Routing Configuration > ECMP	Started
Global Configuration > Dynamic Routing Configuration > Router ID	192.168.10.3

6 On the left side, select **BGP** to verify the protocol settings and configure BGP peering between the UDLR device and the NSX Edge devices for the ECMP-enabled North/South routing in Region A.

a On the **BGP** page, verify the following settings.

Setting	Value
Status	Started
Local AS	65003
Graceful Restart	Started

b Under **Neighbors**, select **192.168.10.50** which represents the connection settings for the lax01m01esg01 neighbor and click the **Edit** icon.

c In the **Edit Neighbor** dialog box, change the **Weight** value to **60**, enter the BGP password that was configured during the initial setup of the UDLR, and click **OK**.

Setting	lax01m01esg01 Value	lax01m01esg02 Value
IP Address	192.168.10.50	192.168.10.51
Forwarding Address	192.168.10.3	192.168.10.3
Protocol Address	192.168.10.4	192.168.10.4
Remote AS	65003	65003
Weight	**60**	**60**
Keep Alive Time	1	1
Hold Down Time	3	3
Password	*BGP_password*	*BGP_password*

d On the **BGP** page, repeat the steps for the **192.168.10.51** neighbor which represents the lax01m01esg02 device.

e Click **Publish Changes**.

7 On the left side, select **Route Redistribution** to verify redistribution status.

Category	Setting	Value
Route Redistribution Status	OSPF	Deselected
	BGP	Selected
Route Redistribution table	Learner	BGP
	From	Connected
	Prefix	Any
	Action	Permit

8 Reconfigure the routing and weight values of lax01m01esg01 and lax01m01esg02 edges.

a In the **Navigator** pane, click **NSX Edges**.

b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

c Double-click **lax01m01esg01** to open its configuration interface.

d Click the **Manage** tab and click the **Routing** tab.

e On the left side, select **BGP**, select the **192.168.10.4** neighbor under **Neighbors**, and click the **Edit** icon.

f In the **Edit Neighbor** dialog box, change the **Weight** value to **60** and click **OK**.

g Click **Publish Changes**.

h Repeat the steps for the lax01m01esg02 edge.

Verify Establishment of BGP for the Universal Distributed Logical Router in Region B

Verify that the UDLR for the management applications is successfully peering, and that BGP routing has been established in Region B. After you perform disaster recovery, they can continue communicating to keep the SDDC operational.

Procedure

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

a Open an SSH connection to sfo01m01udlr01.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*udlr_admin_password*

2 Verify that the UDLR can peer with the ECMP-enabled NSX Edge services gateways.

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

   b In the command output, verify that the BGP state is `Established, up` for 192.168.10.50 (lax01m01esg01) and 192.168.10.51 (lax01m01esg02).

3 Verify that the UDLR receives routes by using BGP and that multiple routes are established to BGP-learned networks.

   a Run the `show ip route` command.

   b In the command output, verify that the routes to the networks are marked with the letter `B` and several routes to each adjacent network exist.

   The letter `B` in front of each route indicates that this route is established over BGP.

Enable Network Connectivity for the NSX Load Balancer in Region B

Enable the network connectivity on lax01m01lb01 load balancer to support high-availability and distribute the network traffic load for vRealize Operations Manager, vRealize Suite Lifecycle Manager, and the Cloud Management Platform after disaster recovery to 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 From the **Home** menu of the vSphere Web Client, select **Networking & Security**.

3 In the **Navigator** pane, click **NSX Edges**.

4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.

5 Double-click the **lax01m01lb01** device.

6 Click the **Manage** tab and click the **Settings** tab.

7 Click **Interfaces**, select the **OneArmLB** vNIC, and click **Edit**.

8 In the **Edit NSX Edge Interface** dialog box, set **Connectivity Status** to **`Connected`** and click **OK**.

Initiate Disaster Recovery ofthe Operations ManagementApplications in Region B

In the event of a site failure in Region A, initiate disaster recovery of vRealize Suite Lifecycle Manager and of vRealize Operations Manager to keep the monitoring functionality of the SDDC running.

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 of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **lax01m01vc01.lax01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Operations Management RP** recovery plan.

5 On the **SDDC Operations Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

6 Click the **Run Recovery Plan** icon to run the recovery plan and initiate the failover of the analytics cluster of vRealize Operations Manager and vRealize Suite Lifecycle Manager.

   The **Recovery** wizard appears.

7 On the **Confirmation options** page of the **Recovery** wizard, configure the following settings and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	Selected
Recovery type	Disaster recovery

8 On the **Ready to complete** page, click **Finish** to initiate the failover of vRealize Operations Manager and vRealize Suite Lifecycle Manager.

Site Recovery Manager runs the recovery plan. After disaster recovery, the **Plan status** of the recovery plan changes to `Disaster recovery complete`.

What to do next

- Verify that vRealize Suite Lifecycle Manager is up and operates correctly after a failover. See *Verification of vRealize Suite Lifecycle Manager* in the *VMware Validated Design Operational Verification* documentation.
- Verify that vRealize Operations Manager is up and operates correctly after a failover. See *Verification of vRealize Operations Manager* in the *VMware Validated Design Operational Verification* documentation.
- Perform the procedures in chapter Post-Failover Configuration of the SDDC Management Applications.
- Prepare vRealize Operations Manager and vRealize Suite Lifecycle Manager for failback by reprotecting the virtual machines of the analytics cluster and the vRealize Suite Lifecycle Manager in Site Recovery Manager. See Reprotect the Operations Management Applications.

Initiate Disaster Recovery of the Cloud Management Platform in Region B

In the event of a site failure in Region A, initiate disaster recovery of the vRealize Automation and vRealize Business components to keep the workload provisioning functionality of the SDDC available.

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 of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **lax01m01vc01.lax01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Cloud Management RP** recovery plan.

5 On the **SDDC Cloud Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

6 Click the **Run Recovery Plan** icon to run the recovery plan and initiate the failover of the cloud management platform.

7 On the **Confirmation options** page of the **Recovery** wizard, configure the following settings and click **Next**.

Confirmation Option	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters	Selected
Recovery type	Disaster recovery

8 On the **Ready to complete** page, click **Finish** to initiate the failover of the cloud management platform.

Site Recovery Manager runs the recovery plan. After disaster recovery, the Plan status of the recovery plan changes to `Disaster recovery complete`.

What to do next

- Verify that vRealize Automation and vRealize Business VMs are up and operational after failover. See *Operational Verification of the Cloud Management Layer* in the *VMware Validated Design Operational Verification* documentation.
- Perform the procedures in chapter Post-Failover Configuration of the SDDC Management Applications.
- Prepare vRealize Automation and vRealize Business for failback by reprotecting their virtual machines in Site Recovery Manager. See Reprotect the Cloud Management Platform.

Post-Failover Configuration of the SDDC Management Applications

After failover of the Cloud Management Platform, vRealize Operations Manager, and vRealize Suite Lifecycle Manager, you must perform additional tasks to ensure that the applications perform as expected.

Procedure

1 Configure the NSX Controllers and UDLR Control VM to Forward Events to vRealize Log Insight in Region B

Configure the NSX Controllers and UDLR Control VM instances for the management cluster to forward log information to vRealize Log Insight in Region B. Use the NSX REST API to configure the NSX Controllers. To enable log forwarding, you can use a REST client, such as the Postman application for Google Chrome.

2 Update the vRealize Log Insight Logging Address After Failover

After you fail over the management applications in the SDDC to Region B, update the address configured on the management applications for vRealize Log Insight. All management applications are still configured to send logs to the vRealize Log Insight instance in Region A.

3 Connect vRealize Operations Manager to vRealize Log Insight in Region B

Reconfigure the vRealize Log Insight Adapter to integrate vRealize Log Insight with vRealize Operations Manager in your environment.

4 Reconfigure the NSX Instance for the Management Cluster in Region A After Failover

After you have successfully completed a failover of the management applications to Region B and you have restored the Region A environment, you must perform additional configurations to avoid conflicts in the network layer. These steps must be performed before you reprotect the SDDC Management Applications from Region B to Region A.

5 Connect vRealize Operations Manager to vRealize Log Insight in Region A

After you have successfully completed a failover of the management applications to Region B and you have restored the Region A environment, to continue log collection from Region A, you reconfigure the vRealize Log Insight Adapter to integrate vRealize Log Insight with vRealize Operations Manager.

Configure the NSX Controllers and UDLR Control VM to Forward Events to vRealize Log Insight in Region B

Configure the NSX Controllers and UDLR Control VM instances for the management cluster to forward log information to vRealize Log Insight in Region B. Use the NSX REST API to configure the NSX Controllers. To enable log forwarding, you can use a REST client, such as the Postman application for Google Chrome.

Procedure

1 Log in to the Windows host that has access to your data center.

2 In a Chrome browser, start the Postman application and log in.

3 Specify the request headers for requests to the NSX Manager.

a On the **Authorization** tab, configure the following authorization settings and click **Update Request**.

Settings	Value
Type	Basic Auth
User name	admin
Password	*lax01m01nsx01_admin_password*

The Authorization:Basic XXX header appears in the **Headers** pane.

b On the **Headers** tab, enter the following header details.

Setting	Value
Key	Content-Type
Value	application/xml

The Content-Type:application/xml header appears in the **Headers** pane.

4 Contact the NSX Manager to retrieve the IDs of the associated NSX Controllers.

a Select **GET** from the drop-down menu that contains the HTTP request methods.

b In the **URL** text box next to the selected method, enter the following URL, and click **Send**.

NSX Manager	URL
NSX Manager for the management cluster	https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller

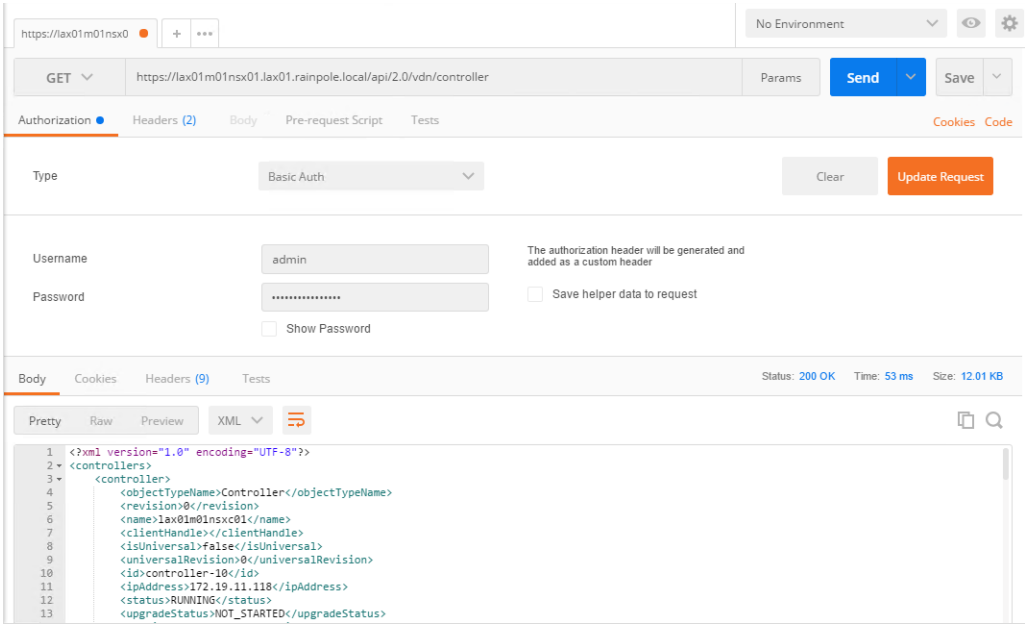
The Postman application sends a query to the NSX Manager about the installed NSX controllers.

c After the NSX Manager sends a response back, click the **Body** tab in the response pane.

The response body contains a root <controllers> XML element that groups the details about the three controllers that form the controller cluster.

d Within the <controllers> element, locate the <controller> element for each controller and write down the content of the <id> element.

Controller IDs have the `controller-`*id* format where *id* represents the sequence number of the controller in the cluster.



5 For each NSX Controller, send a request to configure vRealize Log Insight as a remote syslog server.

a In the request pane at the top, select **POST** from the drop-down menu that contains the HTTP request methods, and in the **URL** text box, enter the following URL.

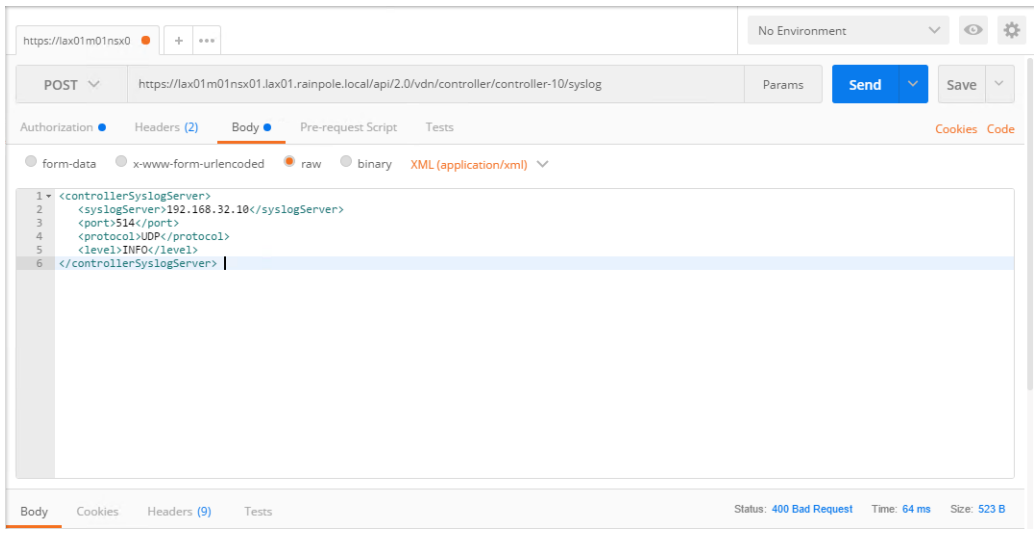
Replace *controller-ID* with the controller IDs you have written down.

NSX Manager	NSX Controller in the Controller Cluster	POST URL
NSX Manager for the management cluster	NSX Controller 1	https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-1**/syslog
	NSX Controller 2	https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-2**/syslog
	NSX Controller 3	https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-3**/syslog

b In the **Request** pane, click the **Body** tab, select **Raw**, and using the drop-down menu, select **XML (Application/XML)**.

c Paste the following request body in the **Body** text box and click **Send**.

```
<controllerSyslogServer>
   <syslogServer>192.168.32.10</syslogServer>
   <port>514</port>
   <protocol>UDP</protocol>
   <level>INFO</level>
</controllerSyslogServer>
```



d Repeat the steps for the other NSX Controllers in the management cluster.

6 Verify the syslog configuration on each NSX Controller.

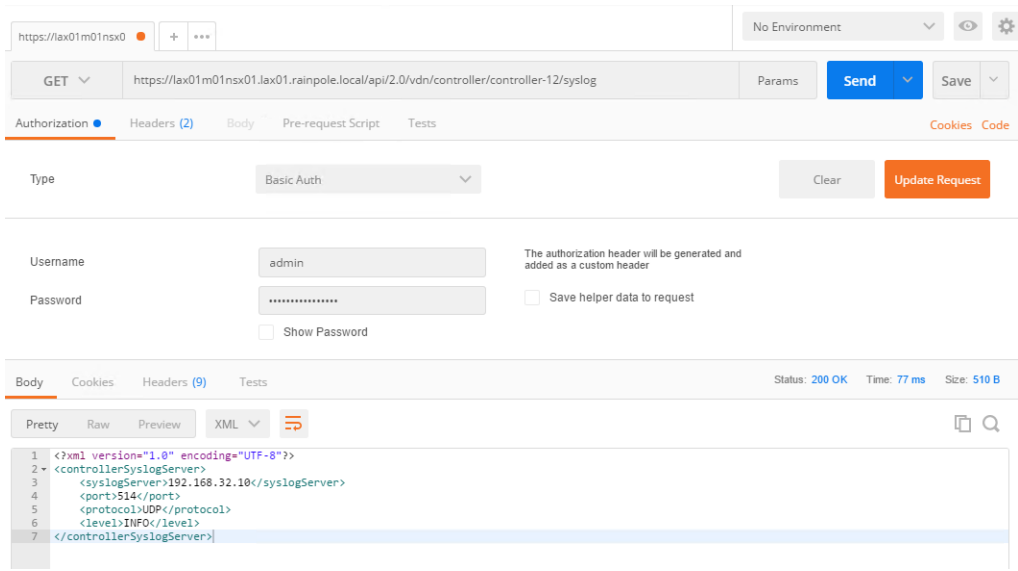
a In the **Request** pane, from the **Method** drop-down menu, select **GET**, in the **URL** text box, enter the controller-specific syslog URL from the previous step, and click the **SEND** button.

b After the NSX Manager sends a response back, click the **Body** tab under **Response**.

The response body contains a root <controllerSyslogServer> element, which represents the settings for the remote syslog server on the NSX Controller.

c Verify that the value of the <syslogServer> element is 192.168.32.10.

d Repeat the steps for the other NSX Controllers to verify the syslog configuration.



7 Log in to the Management 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*

8 Configure the newly deployed Control VM of the UDLR in Region B to forward events to vRealize Log Insight in Region B.

a From the **Home** menu of the vSphere Web Client, click **Networking & Security**.

b In the **Navigator**, click **NSX Edges**.

c Select **172.17.11.65** from the **NSX Manager** drop-down menu.

d Double-click **sfo01m01udlr01** to open its configuration interface.

e On the NSX Edge device page, click the **Manage** tab, click **Settings**, and click **Configuration**.

f In the **Details** pane, click **Change** next to **Syslog servers**.

g In the **Edit Syslog Servers Configuration** dialog box, enter the following settings and click **OK**.

Setting	Value
Syslog Server 1	192.168.32.10
Protocol	UDP

Update the vRealize Log Insight Logging Address After Failover

After you fail over the management applications in the SDDC to Region B, update the address configured on the management applications for vRealize Log Insight. All management applications are still configured to send logs to the vRealize Log Insight instance in Region A.

You update the DNS entry for sfo01vrli01.sfo01.rainpole.local to point to the IP address **192.168.32.10** of lax01vrli01.lax01.rainpole.local in Region B.

Procedure

1 Log in to the DNS server dc51rpl.rainpole.local that resides in Region B.

2 Open the Windows **Start** menu, enter **dns** in the **Search** text box, and press Enter.

The **DNS Manager** dialog box appears.

3 In the **DNS Manager** dialog box, under **Forward Lookup Zones**, select the **sfo01.rainpole.local** domain by expanding the tree and locate the sfo01vrli01 record on the right side.

4 Double-click the **sfo01vrli01** record, change the IP address of the record from 192.168.31.10 to **192.168.32.10** and click **OK**.

Setting	Value
Fully qualified domain name (FQDN)	sfo01vrli01.sfo01.rainpole.local
IP Address	192.168.32.10
Update associated pointer (PTR) record	Selected

Connect vRealize Operations Manager to vRealize Log Insight in Region B

Reconfigure the vRealize Log Insight Adapter to integrate vRealize Log Insight with vRealize Operations Manager in your environment.

Procedure

1 Log in to vRealize Operations Manager by using the administration console.

   a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

3 In the left pane of vRealize Operations Manager, click **Solutions**.

4 On the **Solutions** page, select **VMware vRealize Log Insight**, and click **Configure**.

   The **Manage Solution - VMware vRealize Log Insight** dialog box appears.

5 Under **Instance Settings**, modify the settings for the connection to vRealize Log Insight.

   a Enter the display name, description, and the FQDN of the vRealize Log Insight instance.

Setting	Value
Display Name	Log Insight Adapter - lax01vrli01
Description	vRealize Log Insight for lax01
Log Insight server	lax01vrli01.lax01.rainpole.local

6 Expand the **Advanced Settings** pane and select the collector group for the region from the **Collectors/Groups** drop-down menu.

Setting	Value
Collectors/Groups	lax01-remote-collectors

7 Click **Test Connection** to validate the connection to vRealize Log Insight and in the **Info** dialog box click **OK**.

8 Click **Save Settings** and in the **Info** dialog box click **OK**.

9 In the **Manage Solution - VMware vRealize Log Insight** dialog box, click **Close**.

The vRealize Log Insight Adapter is available on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is `Collecting` and the **Collection Status** is `Data receiving`.

Reconfigure the NSX Instance for the Management Cluster in Region A After Failover

After you have successfully completed a failover of the management applications to Region B and you have restored the Region A environment, you must perform additional configurations to avoid conflicts in the network layer. These steps must be performed before you reprotect the SDDC Management Applications from Region B to Region A.

After the environment in Region A is restored and all management components are operational in Region B, in Region A you demote the NSX Manager to the secondary role, delete the universal controller cluster, disable the load balancer, and perform additional configuration on the NSX Edges.

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 of the vSphere Web Client, select **Networking & Security**.

3 In the **Navigator** pane, click **Installation and Upgrade**.

4 On the **Management** tab, click **NSX Managers**.

   Both NSX Manager instances **172.16.11.65** and **172.17.11.65** are assigned with the primary role.

5 Force the removal of the registered secondary NSX Manager before removing the primary role from the NSX Manager in Region A.

   a Select the **172.16.11.65** instance, and select **Actions > Remove Secondary NSX Manager**.

   b Select the **Perform operation even if the NSX manager is inaccessible** check box and click **Remove**.

6 Demote the original primary site NSX Manager in Region A to the transit role.

   a Select the **172.16.11.65** instance, click **Actions > Remove Primary Role**.

   b Click **Yes** in the confirmation dialog box.

7 Delete the NSX Controllers in the protected site.

   a On the **Management** tab, click **NSX Controller Nodes**.

   b Select the **sfo01m01nsxc01** node and click **Delete**.

   c In the **Delete Controller** dialog box, click **Delete**.

d Repeat the step to delete the remaining two NSX Controller nodes.

e Select **Proceed to Force Delete** option when you delete the last controller.

8 Delete the UDLR edge in the protected site.

a In the **Navigator**, click **NSX Edges**.

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

c Select the **sfo01m01udlr01** and click **Delete**.

d In the **Delete NSX Edge** confirmation dialog box, click **Yes**.

9 Assign the NSX Manager for the management cluster in Region A the secondary role to the NSX Manager in Region B.

a In the **Navigator** pane, click **Installation and Upgrade**.

b On the **Management** tab, click **NSX Managers**, select the primary **172.17.11.65** instance.

c Select **Actions > Add Secondary Manager**.

d In the **Add secondary Manager** dialog box, enter the following settings and click **Add**.

Setting	Value
NSX Manager	172.16.11.65
User Name	admin
Password	*mgmtnsx_admin_password*
Confirm Password	*mgmtnsx_admin_password*

e In the **Thumbprint confirmation** dialog box, click **Accept**.

10 Disable network connectivity for the NSX load balancer in Region A.

a In the **Navigator** pane, click **NSX Edges**.

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

c Double-click the **sfo01m01lb01** device.

d Click the **Manage** tab and click the **Settings** tab.

e Click **Interfaces**, select the **OneArmLB** vNIC, and click **Edit**.

f In the **Edit NSX Edge Interface** dialog box, select **Disconnected** as **Connectivity Status** and click **OK**.

11 Configure the routing on the universal distributed logical router in Region B.

a In the **Navigator**, click **NSX Edges**.

b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

c Double-click **sfo01m01udlr01**.

d Click the **Manage** tab and click **Routing**.

e On the left, select **BGP**.

f Select the following NSX Edge devices, click **Edit**, configure the following settings, and click **OK**.

Setting	sfo01m01esg01 Value	sfo01m01esg02 Value
IP Address	192.168.10.1	192.168.10.2
Forwarding Address	192.168.10.3	192.168.10.3
Protocol Address	192.168.10.4	192.168.10.4
Remote AS	65003	65003
Weight	10	10
Keep Alive Time	1	1
Hold Down Time	3	3
Password	*BGP_password*	*BGP_password*

g Click **Publish Changes**.

h On the left, select **Static Routes**.

i On the **Static Routes** page, click the existing static route (Network: 172.17.11.0/24) and click the **Edit** button.

j In the **Edit Static Route** dialog box, update the following values and click **OK**.

Setting	Value
Network	172.16.11.0/24
Next Hop	192.168.10.1,192.168.10.2
Admin Distance	1

k Click **Publish Changes**.

12 Reconfigure the weight value of the sfo01m01esg01 and sfo01m01esg02 edges.

a In the **Navigator** pane, click **NSX Edges**.

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

c Double-click **sfo01m01esg01**.

d Click the **Manage** tab and click **Routing**.

e On the left, select **BGP**, select the **192.168.10.4** neighbor, and click **Edit**.

f In the **Edit Neighbor** dialog box, change the **Weight** value to **10** and click **OK**.

g Click **Publish Changes**.

h Repeat the step for the sfo01m01esg02 edge.

13 Verify that the NSX Edge devices are successfully peering, and that BGP routing has been established.

a Log in to the sfo01m01esg01 NSX Edge device using a Secure Shell (SSH) client with the following credentials.

Setting	Value
User name	admin
Password	*edge_admin_password*

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

The BGP State displays `Established UP` if you have successfully peered with UDLR.

c Run the `show ip route` command to verify that you are receiving routes using BGP.

d Repeat the step for the sfo01m01esg02 NSX Edge device.

14 Change the DNS entry for sfo01vrli01.sfo01.rainpole.local to point to its original IP address 192.168.31.10.

a Open a Remote Desktop Protocol (RDP) connection and lLog in to the DNS server **`dc01rpl.rainpole.local`** that resides in Region A.

b Log in using the following credentials.

Option	Description
User name	Active Directory administrator
Password	*ad_admin_password*

c Open the Windows **Start** menu, enter **`dns`** in the **Search** text box, and press Enter.

d In the **DNS Manager** dialog box, under **Forward Lookup Zones**, expand the tree and select the **sfo01.rainpole.local** domain.

e Double-click the **sfo01vrli01** record on the right, change the IP address of the record from **192.168.32.10** to **`192.168.31.10`**, and click **OK**.

Setting	Value
Fully qualified domain name (FQDN)	sfo01vrli01.sfo01.rainpole.local
IP Address	192.168.31.10
Update associated pointer (PTR) record	Selected

Connect vRealize Operations Manager to vRealize Log Insight in Region A

After you have successfully completed a failover of the management applications to Region B and you have restored the Region A environment, to continue log collection from Region A, you reconfigure the vRealize Log Insight Adapter to integrate vRealize Log Insight with vRealize Operations Manager.

Procedure

1 Log in to the vRealize Operations Manager master node by using the administration interface.

   a Open a Web browser and go to **`https://vrops01svr01a.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

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

3 In the left pane of vRealize Operations Manager, click **Solutions**.

4 On the **Solutions** page, select **VMware vRealize Log Insight**, and click **Configure**.

   The **Manage Solution - VMware vRealize Log Insight** dialog box appears.

5 Under **Instance Settings**, modify the settings for the connection to vRealize Log Insight.

   a Enter the display name, description, and the FQDN of the vRealize Log Insight instance.

Setting	Value
Display Name	Log Insight Adapter - sfo01vrli01
Description	vRealize Log Insight for sfo01
Log Insight server	sfo01vrli01.sfo01.rainpole.local

6 Expand the **Advanced Settings** pane and select the collector group for the region from the **Collectors/Groups** drop-down menu.

Setting	Value
Collectors/Groups	sfo01-remote-collectors

7 Click **Test Connection** to validate the connection to vRealize Log Insight and in the **Info** dialog box click **OK**.

8 Click **Save Settings** and in the **Info** dialog box click **OK**.

9 In the **Manage Solution - VMware vRealize Log Insight** dialog box, click **Close**.

The vRealize Log Insight Adapter is available on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is `Collecting` and the **Collection Status** is `Data receiving`.

Failback of the SDDC Management Applications

4

Configure and perform a failback of the management applications in the SDDC from the protected region, Region B, to the recovery region, Region A. Failing back these applications restores the pre-recovery configuration of the SDDC.

You fail back the following management components:

- vRealize Suite Lifecycle Manager
- Analytics cluster of vRealize Operations Manager
  - The remote collector nodes of vRealize Operations Manager do not fail back. Deploy a separate pair of remote collectors in each region in the application virtual network that is dedicated to the region.
- Primary components of vRealize Automation with embedded vReaize Orchestrator and vRealize Business
  - The vSphere Proxy Agents of vRealize Automation and the vRealize Business data collector do not fail back. Deploy a separate pair of agents and collector in each region in an application isolated network.

Table 4-1. Support for Failback of the SDDC Management Components

Management Component	Supports Fail Back
vRealize Suite Lifecycle Manager Appliance	Yes
vRealize Operations Manager analytics nodes	Yes
vRealize Operations Manager remote collectors	No
vSphere Proxy Agents	No
vRealize data collectors	No
vRealize Automation Appliance	Yes
vRealize Business server	Yes
Microsoft SQL Server	Yes
IaaS Components	Yes

Procedure

1 Test Failback of the SDDC Management Applications

You can identify potential problems during a future failback by testing the recovery plan for the management applications in the SDDC.

2 Perform Failback as Planned Migration of the SDDC Management Applications

After you have successfully configured and tested failback of the SDDC management applications and you have restored the infrastructure of Region A, start the migration process from Region B back to Region A.

3 Perform Failback as Disaster Recovery of the SDDC Management Applications

If Region B becomes unavailable in the event of a disaster, you perform a failback as disaster recovery to Region A by preparing the network and NSX components in Region A, updating the vSAN Default Storage policy, and performing failback of the Operations Management Applications and the Cloud Management Platform.

Test Failback of the SDDC Management Applications

You can identify potential problems during a future failback by testing the recovery plan for the management applications in the SDDC.

- Test Failback of the Operations Management Applications

  Validate the configuration by testing the recovery plan for vRealize Operations Manager and vRealize Suite Lifecycle Manager.

- Test Failback of the Cloud Management Platform

  Validate the configuration by testing the recovery plan for vRealize Automation and vRealize Business.

Test Failback of the Operations ManagementApplications

Validate the configuration by testing the recovery plan for vRealize Operations Manager and vRealize Suite Lifecycle Manager.

Site Recovery Manager runs the analytics virtual machines and vRealize Suite Lifecycle Manager on the test network and on a temporary snapshot of replicated data 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://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 of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **lax01m01vc01.lax01.rainpole.local** protected site.

4 If the **Log In Site** dialog box appears, re-authenticate by using the **`svc-srm@rainpole.local`** user name and the ***`svc-srm_password`*** password.

   Re-authentication is required if the network connection between Region A and Region B has been interrupted after the last successful authentication.

5 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Operations Management RP** recovery plan.

6 On the **SDDC Operations Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

7 Click the **Test Recovery Plan** icon to run a test recovery.

   The **Test** wizard appears.

8 On the **Confirmation options** page, leave the **Replicate recent changes to recovery site** check box selected and click **Next**.

9 On the **Ready to complete** page, click **Finish** to start the test recovery.

   Test failback starts. You can follow the progress on the **Recovery Steps** page.

10 After the test recovery is complete, click the **Cleanup Recovery Plan** icon to clean up all the created test VMs.

11 On the **Confirmation options** page of the **Cleanup** wizard, click **Next**.

12 On the **Ready to complete** page, click **Finish** to start the clean-up process.

   After the clean-up process finishes, make sure that **Plan status** shows a `Ready` state.

Test Failback of the Cloud Management Platform

Validate the configuration by testing the recovery plan for vRealize Automation and vRealize Business.

Site Recovery Manager runs vRealize Automation and vRealize Business virtual machines on the test network and on a temporary snapshot of replicated data 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://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 of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **lax01m01vc01.lax01.rainpole.local** protected site.

4 If the **Log In Site** dialog box appears, re-authenticate by using the **`svc-srm@rainpole.local`** user name and the ***`svc-srm_password`*** password.

   Re-authentication is required if the network connection between Region A and Region B has been interrupted after the last successful authentication.

5 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Cloud Management RP** recovery plan.

6 On the **SDDC Cloud Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

7 Click the **Test Recovery Plan** icon to run a test recovery.

   The **Test** wizard appears.

8 On the **Confirmation options** page, leave the **Replicate recent changes to recovery site** check box selected and click **Next**.

9 On the **Ready to complete** page, click **Finish** to start the test recovery.

   Test failback starts. You can follow the progress on the **Recovery Steps** page.

10 After the test recovery is complete, click the **Cleanup Recovery Plan** icon to clean up all the created test VMs.

   Note Because recovered virtual machines are using the test network, VMware Tools in the vra01svr01a, vra01svr01b, and vra01svr01c virtual machines might not become online within the default timeout. Increase the timeout value for these virtual machines to complete the test.

11 On the **Confirmation options** page of the **Cleanup** wizard, click **Next**.

12 On the **Ready to complete** page, click **Finish** to start the clean-up process.

   After the clean-up process finishes, make sure that **Plan status** shows a `Ready` state.

Perform Failback as Planned Migration of the SDDC Management Applications

After you have successfully configured and tested failback of the SDDC management applications and you have restored the infrastructure of Region A, start the migration process from Region B back to Region A.

- Initiate Failback as Planned Migration of the Operations Management Applications

  Run a recovery plan under planned circumstances to migrate the virtual machines of the analytics cluster of vRealize Operations Manager and vRealize Suite Lifecycle Manager from Region B to Region A. You can also run a recovery plan under unplanned circumstances if Region B suffers an unforeseen event that results in data loss.

- Initiate Failback as Planned Migration of the Cloud Management Platform

  You can run a recovery plan under planned circumstances to migrate the virtual machines of vRealize Automation and vRealize Business from Region B to Region A. You can also run a recovery plan under unplanned circumstances if Region B suffers an unforeseen event that might result in data loss.

Initiate Failback as Planned Migration of theOperations ManagementApplications

Run a recovery plan under planned circumstances to migrate the virtual machines of the analytics cluster of vRealize Operations Manager and vRealize Suite Lifecycle Manager from Region B to Region A. You can also run a recovery plan under unplanned circumstances if Region B suffers an unforeseen event that results in data loss.

Procedure

1 Log in to the Management 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 of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **lax01m01vc01.lax01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Operations Management RP** recovery plan.

5 On the **SDDC Operations Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

6 Click the **Run Recovery Plan** icon to run the recovery plan and initiate the failback of the analytics cluster.

The **Recovery** wizard appears.

7 On the **Confirmation options** page, configure the following settings and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery data centers.	Selected
Recovery type	Planned Migration

8 On the **Ready to complete** page, click **Finish** to initiate vRealize Operations Manager failback.

What to do next

- Verify that vRealize Suite Lifecycle Manager is up and operates correctly after a failover. See *Verification of vRealize Suite Lifecycle Manager* in the *VMware Validated Design Operational Verification* documentation.
- Verify that vRealize Operations Manager is up and operates correctly after a failover. See *Verification of vRealize Operations Manager* in the *VMware Validated Design Operational Verification* documentation.
- Prepare vRealize Operations Manager and vRealize Suite Lifecycle Manager for failback by reprotecting the virtual machines of the analytics cluster and the vRealize Suite Lifecycle Manager in Site Recovery Manager. See Reprotect the Operations Management Applications.

Initiate Failback as Planned Migration of the Cloud Management Platform

You can run a recovery plan under planned circumstances to migrate the virtual machines of vRealize Automation and vRealize Business from Region B to Region A. You can also run a recovery plan under unplanned circumstances if Region B suffers an unforeseen event that might result in data loss.

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 of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **lax01m01vc01.lax01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Cloud Management RP** recovery plan.

5 On the **SDDC Cloud Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

6 Click the **Run Recovery Plan** icon to run the recovery plan and initiate the failback of the cloud management platform.

The **Recovery** wizard appears.

7 On the **Confirmation options** page, configure the following settings and click **Next**.

Confirmation Option	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery data centers	Selected
Recovery type	Planned Migration

8 On the **Ready to complete** page, click **Finish** to initiate failback of the cloud management platform.

What to do next

1 Verify that vRealize Automation and vRealize Business VMs are up and operational after failback. See *Validate the Cloud Management Platform* in the *VMware Validated Design Operational Verification* documentation.

2 Prepare vRealize Automation and vRealize Business Server for failover by reprotecting the virtual machines of the vRealize Automation components in Site Recovery Manager. See Reprotect the Cloud Management Platform.

Perform Failback as Disaster Recovery of the SDDC Management Applications

If Region B becomes unavailable in the event of a disaster, you perform a failback as disaster recovery to Region A by preparing the network and NSX components in Region A, updating the vSAN Default Storage policy, and performing failback of the Operations Management Applications and the Cloud Management Platform.

Prerequisites

You perform failback as disaster recovery if the following conditions are met:

- The SDDC Management Applications reside in Region B after a successful failover.
- The SDDC Management Applications are reprotected Region B to Region A. See Reprotect the Operations Management Applications and Reprotect the Cloud Management Platform.

Procedure

1 Reconfigure the NSX Instance for the Management Cluster in Region A

In the event of a site failure, when Region B becomes unavailable, prepare the network layer in Region A for failback of management applications. Change the role of the NSX Manager in Region A to primary, redeploy the universal controller cluster, and synchronize the universal controller cluster configuration.

2 Recover the Control VM of the Universal Distributed Logical Router in Region A

In the case of failback, because of the failure in Region B, dynamic routing in Region A is not available. Deploy a Control VM for the universal dynamic logical router sfo01m01udlr01 in Region A to recover dynamic routing in the environment. You then reconfigure the recovered Control VM to provide dynamic routing for the SDDC management applications that are failed back.

3 Reconfigure the Universal Distributed Logical Router and NSX Edges for Dynamic Routing in Region A

To support dynamic routing in Region A before you start disaster recovery from Region B, you configure the universal distributed logical router sfo01m01udlr01, and NSX Edges sfo01m01esg01 and sfo01m01esg02. This configuration ensures that the management components of the SDDC continue to communicate using optimal routes in a fault-tolerant network.

4 Verify the Establishment of BGP for the Universal Distributed Logical Router in Region A

Verify that the UDLR for the management applications is successfully peering, and that BGP routing has been established in Region A. After you perform failback of disaster recovery, they can continue communicating to keep SDDC operational.

5 Enable Network Connectivity for the NSX Load Balancer in Region A

Enable the network connectivity on sfo01m01lb01 load balancer to support high availability and distribute the network traffic load for vRealize Operations Manager and the Cloud Management Platform after disaster recovery to Region A.

6 Update the vSAN Default Storage Policy of the Management Cluster in Region A

In the event of a site failure in Region B, the witness VM part of Region B is not available. This results in one fault domain being unavailable for the vSAN stretched cluster. To satisfy the provisioning of a VM with Site Recovery Manager, update the vSAN Default Storage Policy for the management cluster.

7 Initiate Disaster Recovery of the Operations Management Applications in Region A

In the event of a site failure in Region B, initiate disaster recovery of vRealize Suite Lifecycle Manager and of vRealize Operations Manager to keep the monitoring functionality of the SDDC running.

8 Initiate Disaster Recovery of the Cloud Management Platform in Region A

In the event of a site failure in Region B, initiate disaster recovery of vRealize Automation and vRealize Business in Region A to fail the Cloud Management Platform back to Region A.

9 Post-Failback Configuration of the SDDC Management Applications

After failback of the Operations Management applications and the Cloud Management Platform, you must perform certain tasks to ensure that applications perform as expected.

Reconfigure the NSX Instance for the Management Cluster in Region A

In the event of a site failure, when Region B becomes unavailable, prepare the network layer in Region A for failback of management applications. Change the role of the NSX Manager in Region A to primary, redeploy the universal controller cluster, and synchronize the universal controller cluster configuration.

Procedure

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

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

b Log in using the following credentials.

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

2 Promote the NSX Manager for the management cluster in Region A to the primary role. You first disconnect the NSX Manager for the Management cluster in Region A from the primary NSX Manager in Region B.

a From the **Home** menu of the vSphere Web Client, click **Networking & Security**.

b In the **Navigator**, click **Installation and Upgrade**.

c On the **Management** tab, click **NSX Managers** tab and select the **172.16.11.65** instance.

d Click the **Actions** menu and click **Disconnect from Primary NSX Manager**.

e In the **Disconnect from Primary NSX Manager** dialog box, click **Yes**.

The NSX Manager gets the **Transit** role.

f On the **NSX Managers** tab, select the **172.16.11.65** instance again.

g Click **Actions** and select **Assign Primary Role**.

h In the **Assign Primary Role** dialog box, click **Yes**.

3 Deploy the universal controller cluster in Region A.

a In the **Navigator** pane, click **Installation and Upgrade**.

b On the **Management** tab, under **NSX Controller nodes**, click the **Add** icon to deploy three NSX Controller nodes with the same configuration.

c In the **Add Controller** dialog box, enter the following settings and click **Next**.

Setting	Value
NSX Manager	172.16.11.65
Password	*mgmtnsx_controllers_password*
Confirm Password	*mgmtnsx_controllers_password*

You configure a password only during the deployment of the first controller. The other controllers use the same password.

d In the **Add Controller** dialog box, under **Deployment & Connectivity**, enter the following settings and click **Finish**.

Setting	Value
Name	■ sfo01m01nsxc01 for controller 1 ■ sfo01m01nsxc02 for controller 2 ■ sfo01m01nsxc03 for controller 3
Data center	sfo01-m01dc
Cluster/Resource Pool	sfo01-m01-mgmt01
Datastore	sfo01-m01-vsan01
Folder	sfo01-m01fd-nsx
Connected To	sfo01-m01-vds01-management
IP Pool	sfo01-mgmt01-nsxc01

e After the **Status** of the controller node changes to `Connected`, deploy the remaining two NSX Controller nodes sfo01m01nsxc02 and sfo01m01nsxc03.

Wait until the current deployment is finished, before you start the next one.

4 Configure DRS affinity rules for the deployed NSX Controller nodes.

a From the **Home** menu of the vSphere Web Client, select **Hosts and Clusters**.

b Expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc** tree and click the **sfo01-m01-mgmt01** cluster.

c Click the **Configure** tab, under **Configuration**, click **VM/Host Rules**, and click **Add**.

d In the sfo01-m01-mgmt01 **- Create VM/Host Rule** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	anti-affinity-rule-nsxc
Enable rule	Selected
Type	Separate Virtual Machines
Members	■ sfo01m01nsxc01 ■ sfo01m01nsxc02 ■ sfo01m01nsxc03

5 Use the `Update Controller State` mechanism on the NSX Manager to synchronize the state of the newly deployed controllers. Update Controller State pushes the current VXLAN and universal distributed logical router configuration from NSX Manager to the controller cluster.

a From the **Home** menu of the vSphere Web Client, select **Networking & Security**.

b In the **Navigator** pane, click **Installation and Upgrade**.

c On the **Management** tab, under **NSX Managers** tab, select the **172.16.11.65** instance.

d Click the **Actions** menu and select **Update Controller State**.

e In the **Update Controller State** dialog box, click **Yes**.

Recover the Control VM of the Universal Distributed Logical Router in Region A

In the case of failback, because of the failure in Region B, dynamic routing in Region A is not available. Deploy a Control VM for the universal dynamic logical router sfo01m01udlr01 in Region A to recover dynamic routing in the environment. You then reconfigure the recovered Control VM to provide dynamic routing for the SDDC management applications that are failed back.

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, click **Networking & Security**.

3 In the **Navigator** pane, click **NSX Edges**.

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

5 Double-click **sfo01m01udlr01**.

6 Redeploy the universal distributed logical router control VM and enable HA.

a Click the **Manage** tab and click **Settings**.

b Select **Configuration** and under **Logical Router Appliances** click the **Add** icon.

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

Setting	Value
Data center	sfo01-m01dc
Cluster/Resource Pool	sfo01-m01-mgmt01
Datastore	sfo01-m01-vsan01

d To deploy another NSX Edge device with the same configuration, click the **Add** icon and repeat the previous step.

7 Configure high availability for the Control VM.

a On the **Configuration** page for sfo01m01udlr01, click **Change** under **HA Configuration**, configure the following settings, and click **OK**.

Setting	Value
HA Status	Enable
Connected To	sfo01-m01-vds01-management
Enable Logging	Selected

b In the **Change HA configuration** dialog box, click **Yes**.

8 Configure the CLI Credentials for the Control VM.

a In the **Navigator**, click **NSX Edges**.

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

c Right-click **sfo01m01udlr01** and select **Change CLI Credentials**.

d In the **Change CLI Credentials** dialog box, configure the following settings and click **OK**.

Setting	Value
User Name	admin
Password	*udlr_admin_password*
Enable SSH access	Selected

Reconfigure the Universal Distributed Logical Router and NSX Edges for Dynamic Routing in Region A

To support dynamic routing in Region A before you start disaster recovery from Region B, you configure the universal distributed logical router sfo01m01udlr01, and NSX Edges sfo01m01esg01 and sfo01m01esg02. This configuration ensures that the management components of the SDDC continue to communicate using optimal routes in a fault-tolerant network.

Procedure

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

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

   b Log in using the following credentials.

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

2 In the **Navigator**, click **Networking & Security** and click **NSX Edges**.

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

4 Verify the routing configuration for the universal distributed logical router.

   a Double-click **sfo01m01udlr01**.

   b Click the **Manage** tab and click **Routing**.

Setting	Value
Global Configuration > Routing Configuration > ECMP	Started
Global Configuration > Dynamic Routing Configuration > Router ID	192.168.10.3

5 On the left side, select **BGP** to verify the protocol settings and configure BGP peering between the UDLR device and the NSX Edge devices for the ECMP-enabled North/South routing in Region A.

   a On the **BGP** page, verify the following settings.

Setting	Value
Status	Started
Local AS	65003
Graceful Restart	Started

   b Under **Neighbors**, select **192.168.10.1** which represents the connection settings for the sfo01m01esg01 neighbor and click the **Edit** icon.

c In the **Edit Neighbor** dialog box, update the **Weight** value to **60** , enter the BGP password that was configured during the initial setup of the UDLR, and click **OK**.

Setting	sfo01m01esg01 Value	sfo01m01esg02 Value
IP Address	192.168.10.1	192.168.10.2
Forwarding Address	192.168.10.3	192.168.10.3
Protocol Address	192.168.10.4	192.168.10.4
Remote AS	65003	65003
Weight	**60**	**60**
Keep Alive Time	1	1
Hold Down Time	3	3
Password	***BGP_password***	***BGP_password***

d On the **BGP** page, repeat the steps for the **192.168.10.2** entry which represents the sfo01m01esg02 neighbor.

e Click **Publish Changes**.

6 On the left side, select **Route Redistribution** to verify redistribution status.

Category	Setting	Value
Route Redistribution Status	OSPF	Deselected
	BGP	Selected
Route Redistribution table	Learner	BGP
	From	Connected
	Prefix	Any
	Action	Permit

7 Reconfigure the routing and weight value of sfo01m01esg01 and sfo01m01esg02 edge devices.

a In the **Navigator**, click **NSX Edges**.

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

c Double-click **sfo01m01esg01** to open its configuration interface.

d Click the **Manage** tab and click the **Routing** tab.

e On the left side, select **BGP**, select the **192.168.10.4** neighbor, and click **Edit**.

f In the **Edit Neighbor** dialog box, change the **Weight** value to **60** and click **OK**.

g Click **Publish Changes**.

h Repeat this step for the sfo01m01esg02 edge.

Verify the Establishment of BGP for the Universal Distributed Logical Router in Region A

Verify that the UDLR for the management applications is successfully peering, and that BGP routing has been established in Region A. After you perform failback of disaster recovery, they can continue communicating to keep SDDC operational.

Procedure

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

   a Open an SSH connection to **`sfo01m01udlr01`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*udlr_admin_password*

2 Verify that the UDLR can peer with the ECMP-enabled NSX Edge services gateways.

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

   b In the command output, verify that the BGP state is `Established, up` for 192.168.10.1 (sfo01m01esg01) and 192.168.10.2 (sfo01m01esg02).

3 Verify that the UDLR receives routes by using BGP and that multiple routes are established to BGP-learned networks.

   a Run the `show ip route` command.

   b In the command output, verify that the routes to the networks are marked with the letter B and several routes to each adjacent network exist.

   The letter B in front of each route indicates that the route is established over BGP.

Enable Network Connectivity for the NSX Load Balancer in Region A

Enable the network connectivity on sfo01m01lb01 load balancer to support high availability and distribute the network traffic load for vRealize Operations Manager and the Cloud Management Platform after disaster recovery to Region A.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

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

5 Double-click the **sfo01m01lb01** device.

6 Click the **Manage** tab and click the **Settings** tab.

7 Click **Interfaces**, select the **OneArmLB** vNIC, and click **Edit**.

8 In the **Edit NSX Edge Interface** dialog box, set **Connectivity Status** to `Connected` and click **OK**.

Update the vSAN Default Storage Policy of the Management Cluster in Region A

In the event of a site failure in Region B, the witness VM part of Region B is not available. This results in one fault domain being unavailable for the vSAN stretched cluster. To satisfy the provisioning of a VM with Site Recovery Manager, update the vSAN Default Storage Policy for the management cluster.

Procedure

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

   a Open a Web browser and go to **`https://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 **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.

4 Expand the **vSAN** menu and click **Health and Performance**.

5 Under **Performance Service is Turned ON**, click **vSAN Default Storage Policy**.

The **vSAN Default Storage Policy** page appears.

6 Click the **Manage** tab, and click **Edit**.

7 In the **Edit VM Storage Policy** dialog box, select **Rule-set 1**, from the drop-down menu for **Force provisioning** select **Yes**, and click **OK**.

The vSAN Default Storage Policy: VM Storage Policy in Use dialog box appears.

8 In the **VM Default Storage Policy: vSAN Storage Policy in Use** dialog box, from the drop-down menu select **Manually later** and click **Yes**.

Initiate Disaster Recovery ofthe Operations ManagementApplications in Region A

In the event of a site failure in Region B, initiate disaster recovery of vRealize Suite Lifecycle Manager and of vRealize Operations Manager to keep the monitoring functionality of the SDDC running.

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Operations Management RP** recovery plan.

5 On the **SDDC Operations Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

6 Click the **Run Recovery Plan** icon to run the recovery plan and initiate the failback of the analytics cluster of vRealize Operations Manager and vRealize Suite Lifecycle Manager.

The **Recovery** wizard appears.

7 On the **Confirmation options** page of the **Recovery** wizard, configure the following settings and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	Selected
Recovery type	Disaster recovery

8 On the **Ready to complete** page, click **Finish** to initiate the failback of vRealize Operations Manager and vRealize Suite Lifecycle Manager.

After disaster recovery, the **Plan status** of the recovery plan changes to `Disaster recovery complete`.

What to do next

1 Verify that vRealize Suite Lifecycle Manager is up and operates correctly after a failback. See *Verification of vRealize Suite Lifecycle Manager* in the *VMware Validated Design Operational Verification* documentation.

2 Verify that vRealize Operations Manager is up and functional after the failback. See *Verification of vRealize Operations Manager* in the *VMware Validated Design Operational Verification* documentation.

3 Perform the procedures in chapter Post-Failback Configuration of the SDDC Management Applications.

4 Prepare vRealize Operations Manager and vRealize Suite Lifecycle Manager for failover by reprotecting the virtual machines of the analytics cluster and the vRealize Suite Lifecycle Manager in Site Recovery Manager. See Reprotect the Operations Management Applications.

Initiate Disaster Recovery of the Cloud Management Platform in Region A

In the event of a site failure in Region B, initiate disaster recovery of vRealize Automation and vRealize Business in Region A to fail the Cloud Management Platform back to Region A.

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.

3 On the Site Recovery home page, click **Sites** and double-click the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Cloud Management RP** recovery plan.

5 On the **SDDC Cloud Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

6 Click the **Run Recovery Plan** icon to run the recovery plan and initiate the failback of the Cloud Management Platform.

7 On the **Confirmation options** page of the **Recovery** wizard, configure the following settings and click **Next**.

Confirmation Option	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters	Selected
Recovery type	Disaster recovery

8 On the **Ready to complete** page, click **Finish** to initiate the failback of the cloud management platform.

After disaster recovery, the status of the recovery plan is `Disaster Recovery Completed`.

What to do next

1 Verify that vRealize Automation and vRealize Business VMs are up and functional after failback. See *Validate the Cloud Management Platform* in the *VMware Validated Operational Verification* document.

2 Perform the procedures in chapter Post-Failback Configuration of the SDDC Management Applications.

3 Prepare vRealize Automation and vRealize Business Server for failover by reprotecting the virtual machines of the vRealize Automation components in Site Recovery Manager. See Reprotect the Cloud Management Platform.

Post-Failback Configuration of the SDDC Management Applications

After failback of the Operations Management applications and the Cloud Management Platform, you must perform certain tasks to ensure that applications perform as expected.

Procedure

1 Revert the vSAN Default Storage Policy of the Management Cluster in Region A

Revert the vSAN Default Storage Policy of the Management Cluster in Region A after failback of the Operations Management Applications and Cloud Management Platform is complete.

2 Configure the NSX Controllers and the UDLR Control VM to Forward Events to vRealize Log Insight in Region A

Configure the NSX Controllers and UDLR Control VM instances for the management cluster to forward log information to vRealize Log Insight in Region A. Use the NSX REST API to configure the NSX Controllers. To enable log forwarding, you can use a REST client, such as the Postman application for Google Chrome.

3 Reconfigure the NSX Instance for the Management Cluster in Region B After Failback

After Region B comes back online, you must perform additional configurations within the network layer to avoid conflicts. These steps must be performed before you reprotect the SDDC Management Applications from Region A to Region B.

Revert the vSAN Default Storage Policy of the Management Cluster in Region A

Revert the vSAN Default Storage Policy of the Management Cluster in Region A after failback of the Operations Management Applications and Cloud Management Platform is complete.

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 **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.

4 Expand the **vSAN** menu and click **Health and Performance**.

5 Under **Performance Service is Turned ON**, click **vSAN Default Storage Policy**.

The **vSAN Default Storage Policy** page appears.

6 Click the **Manage** tab and click **Edit**.

7 In the **Edit VM Storage Policy** dialog box, select **Rule-set 1**, from the drop-down menu for **Force provisioning** select **No**, and click **OK**.

The vSAN Default Storage Policy: VM Storage Policy in Use dialog box appears.

8 In the **VM Default Storage Policy: vSAN Storage Policy in Use** dialog box, from the drop-down menu select **Now** for **Reapply to VMs** and click **Yes**.

During this operation, vSAN performance might be affected as objects are recreated to match the Storage Policy.

Configure the NSX Controllers and the UDLR Control VM to Forward Events to vRealize Log Insight in Region A

Configure the NSX Controllers and UDLR Control VM instances for the management cluster to forward log information to vRealize Log Insight in Region A. Use the NSX REST API to configure the NSX Controllers. To enable log forwarding, you can use a REST client, such as the Postman application for Google Chrome.

Procedure

1 Log in to the Windows host that has access to your data center.

2 In a Chrome browser, start the Postman application and log in.

3 Specify the request headers for requests to the NSX Manager.

a On the **Authorization** tab, configure the following authorization settings and click **Update Request**.

Settings	Value
Type	Basic Auth
User name	admin
Password	*sfo01m01nsx01_admin_password*

The Authorization:Basic XXX header appears in the **Headers** pane.

b On the **Headers** tab, enter the following header details.

Setting	Value
Key	Content-Type
Value	application/xml

The Content-Type:application/xml header appears in the **Headers** pane.

4 Contact the NSX Manager to retrieve the IDs of the associated NSX Controllers.

a Select **GET** from the drop-down menu that contains the HTTP request methods.

b In the **URL** text box next to the selected method, enter the following URL, and click **Send**.

NSX Manager	URL
NSX Manager for the management cluster	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller

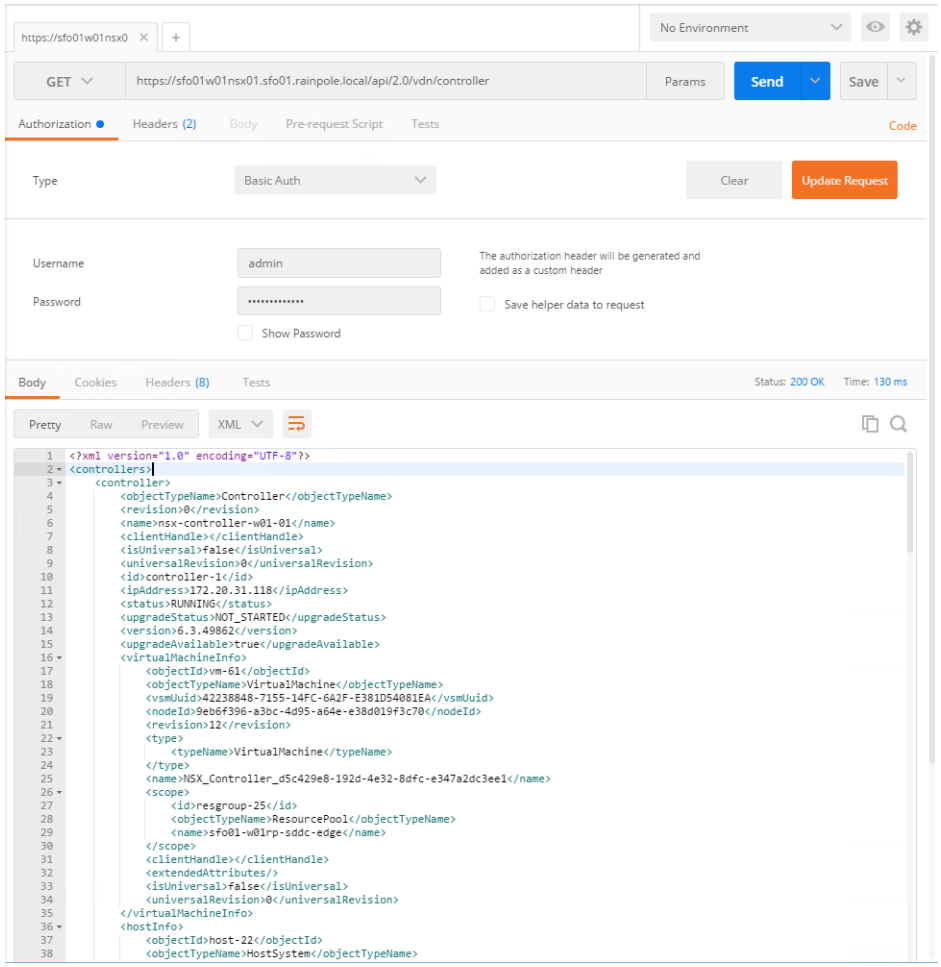
The Postman application sends a query to the NSX Manager about the installed NSX controllers.

c After the NSX Manager sends a response back, click the **Body** tab in the response pane.

The response body contains a root <controllers> XML element that groups the details about the three controllers that form the controller cluster.

d Within the <controllers> element, locate the <controller> element for each controller and write down the content of the <id> element.

Controller IDs have the `controller-`*id* format where *id* represents the sequence number of the controller in the cluster, for example, `controller-1` in the image below.



5 For each NSX Controller, send a request to configure vRealize Log Insight as a remote syslog server.

a In the request pane at the top, select **POST** from the drop-down menu that contains the HTTP request methods, and in the **URL** text box, enter the following URL.

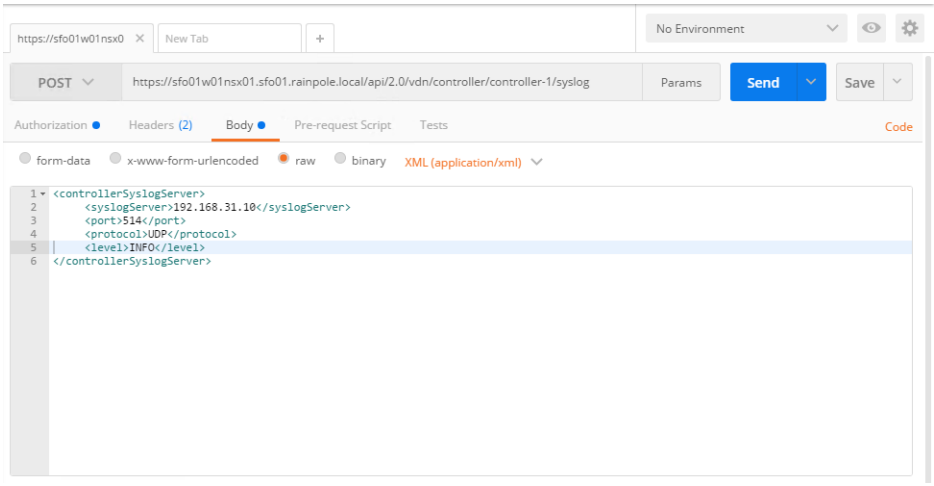
Replace *controller-ID* with the controller IDs you have written down.

NSX Manager	NSX Controller in the Controller Cluster	POST URL
NSX Manager for the management cluster	NSX Controller 1	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-1**/syslog
	NSX Controller 2	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-2**/syslog
	NSX Controller 3	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-3**/syslog

b In the **Request** pane, click the **Body** tab, select **Raw**, and using the drop-down menu, select **XML (Application/XML)**.

c Paste the following request body in the **Body** text box and click **Send**.

```
<controllerSyslogServer>
   <syslogServer>192.168.31.10</syslogServer>
   <port>514</port>
   <protocol>UDP</protocol>
   <level>INFO</level>
</controllerSyslogServer>
```



d Repeat the steps for the other NSX Controllers in the management cluster.

6 Verify the syslog configuration on each NSX Controller.

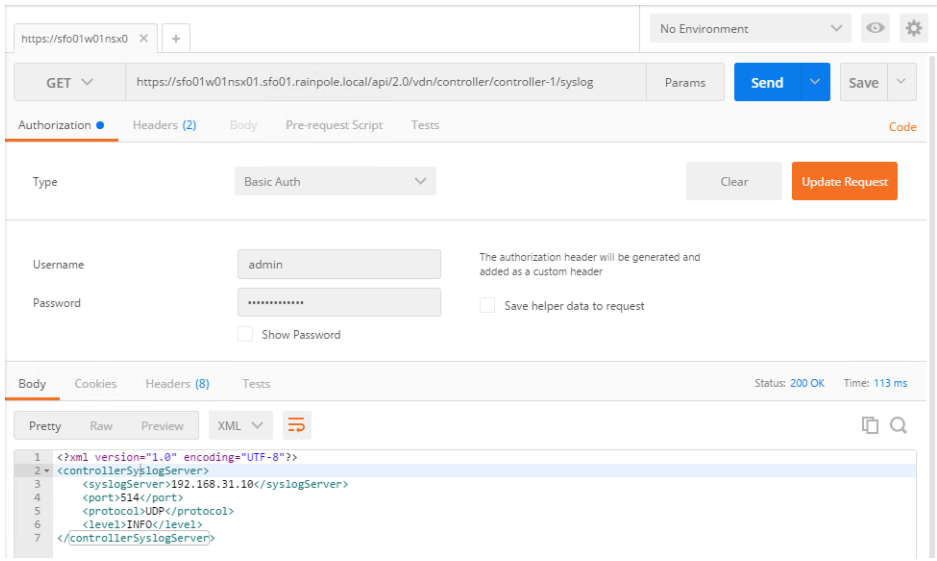
a In the **Request** pane, from the **Method** drop-down menu, select **GET**, in the **URL** text box, enter the controller-specific syslog URL from the previous step, and click the **SEND** button.

b After the NSX Manager sends a response back, click the **Body** tab under **Response**.

The response body contains a root <controllerSyslogServer> element, which represents the settings for the remote syslog server on the NSX Controller.

c Verify that the value of the <syslogServer> element is 192.168.31.10.

d Repeat the steps for the other NSX Controllers to verify the syslog configuration.



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

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

b Log in using the following credentials.

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

8 Configure the newly deployed UDLR Control VM to forward events to vRealize Log Insight in Region A.

a From the **Home** menu of the vSphere Web Client, click **Networking & Security**.

b In the **Navigator**, click **NSX Edges**.

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

d Double-click **sfo01m01udlr01** to open its configuration interface.

e On the NSX Edge device page, click the **Manage** tab, click **Settings**, and click **Configuration**.

f In the **Details** pane, click **Change** next to **Syslog servers**.

g In the **Edit Syslog Servers Configuration** dialog box, enter the following settings and click **OK**.

Setting	Value
Syslog Server 1	192.168.31.10
Protocol	udp

Reconfigure the NSX Instance for the Management Cluster in Region B After Failback

After Region B comes back online, you must perform additional configurations within the network layer to avoid conflicts. These steps must be performed before you reprotect the SDDC Management Applications from Region A to Region B.

You demote the NSX Manager to the secondary role, delete the universal controller cluster, disable the load balancer, and configure BGP on the NSX Edge devices.

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 of the vSphere Web Client, click **Networking & Security**.

3 In the **Navigator** pane, click **Installation and Upgrade** and click the **Management** tab.

Under the **NSX Managers** tab, both NSX Managers **172.17.11.65** and **172.16.11.65** are assigned the primary role.

4 Force the removal of the registered secondary NSX Manager before removing the primary role.

a Select the **172.17.11.65** instance and select **Actions > Remove Secondary Manager** .

b Under **Remove Secondary Manager** dialog box, select the **Perform Operation even if the NSX manager is inaccessible** check box and click **Remove**.

5 Demote the original primary site NSX Manager to the transit role.

a Select the **172.17.11.65** instance, and select **Actions > Remove Primary Role**.

b Click **Yes** in the confirmation dialog box.

6 Delete the NSX Controllers in the primary site.

   a Select the **lax01m01nsxc01** node and click **Delete**.

   b In the **Delete Controller** dialog box, click **Delete**.

   c Repeat the steps to delete the remaining two NSX Controller nodes.

   d When you delete the last controller, select **Forcefully remove the controller** and **Check here to acknowledge the warning**.

7 Delete the UDLR edge in the protected site.

   a In the **Navigator** pane, click **NSX Edges**.

   b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

   c Select **sfo01m01udlr01** and click the **Delete** icon.

   d In the **Delete NSX Edge** dialog box, click **Yes**.

8 Assign the NSX Manager for the management cluster in Region B the secondary role to the already promoted primary NSX Manager in Region A.

   a In the **Navigator** pane, click **Installation and Upgrade**.

   b On the **Management** tab, under **NSX Managers** tab, select the primary **172.16.11.65** instance.

   c Select **Actions > Add Secondary Manager**.

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

Setting	Value
NSX Manager	172.17.11.65
User Name	admin
Password	*mgmtnsx_admin_password*
Confirm Password	*mgmtnsx_admin_password*

   e In the **Trust Certificate** dialog box, click **Yes**.

9 Disable network connectivity for the NSX load balancer in Region B.

   a In the **Navigator** pane, click **NSX Edges**.

   b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

   c Double-click the **lax01m01lb01** device.

   d Click the **Manage** tab and click the **Settings** tab.

   e Click **Interfaces**, select the **OneArmLB** vNIC, and click **Edit**.

   f In the **Edit NSX Edge Interface** dialog box, set **Connectivity Status** to **Disconnected** and click **OK**.

10 Configure the routing for the universal distributed logical router in Region A.

a In the **Navigator** pane, click **NSX Edges**.

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

c Double-click **sfo01m01udlr01** to open the configuration interface.

d Click the **Manage** tab and click **Routing**.

e On the left, select **BGP**.

f Select the following NSX Edge devices, click **Edit**, configure the following settings, and click **OK**.

Setting	lax01m01esg01 Value	lax01m01esg02 Value
IP Address	192.168.10.50	192.168.10.51
Forwarding Address	192.168.10.3	192.168.10.3
Protocol Address	192.168.10.4	192.168.10.4
Remote AS	65003	65003
Weight	10	10
Keep Alive Time	1	1
Hold Down Time	3	3
Password	*BGP_password*	*BGP_password*

g Click **Publish Changes**.

h On the left, select **Static Routes**.

i On the **Static Routes** page, click the existing static route (Network: 172.16.11.0/24) and click the **Edit** button.

j In the **Edit Static Route** dialog box, update the following values and click **OK**.

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

k Click **Publish Changes**.

11 Reconfigure the weight value of lax01m01esg01 and lax01m01esg02.

a In the **Navigator** pane, click **NSX Edges**.

b Select **172.17.11.65** from the **NSX Manager** drop-down menu.

c Double-click **lax01m01esg01**.

d Click the **Manage** tab and click **Routing**.

e On the left, select **BGP**, select the **192.168.10.4** neighbor, and click **Edit**.

f In the **Edit Neighbor** dialog box, change the **Weight** value to **10** and click **OK**.

g Click **Publish Changes**.

h Repeat the step for the lax01m01esg02 edge.

12 Verify that the NSX Edge devices are successfully peering, and that BGP routing has been established.

a Log in to the NSX Edge device by using a Secure Shell (SSH) client.

b Open an SSH connection to lax01m01esg01.

c Log in using the following credentials.

Setting	Value
User name	admin
Password	*edge_admin_password*

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

The **BGP State** displays `Established, UP` if you have successfully peered with UDLR.

e Run the `show ip route` command to verify that you are receiving routes using BGP.

f Repeat this step for the lax01m01esg02 NSX Edge device.

Reprotect of the SDDC Management Applications

5

After a disaster recovery or planned migration, the recovery region becomes the protected region, but the VMs are not protected yet. If the original protected region is operational, you can reverse the direction of protection to protect the new primary region.

During the reprotect operation, after Site Recovery Manager reverses the direction of protection, it forces a synchronization of the storage from the new protected region to the new recovery region. Forcing data synchronization ensures that the recovery region has a current copy of the protected virtual machines running at the protection region. Recovery is possible immediately after the reprotect operation finishes.

- Prerequisites for Performing Reprotect

  To reprotect the virtual machines of the SDDC management applications, your environment must meet certain requirements for the availability of the original protected region and state of recovery plans.

- Reprotect the Operations Management Applications

  Prepare vRealize Operations Manager and vRealize Suite Lifecycle Manager for failback or failover by reprotecting the virtual machines in Site Recovery Manager.

- Reprotect the Cloud Management Platform

  Prepare vRealize Automation and vRealize Business for failback or failover by reprotecting the virtual machines in Site Recovery Manager.

Prerequisites for Performing Reprotect

To reprotect the virtual machines of the SDDC management applications, your environment must meet certain requirements for the availability of the original protected region and state of recovery plans.

Make sure that your environment meets the following requirements before you perform the reprotect operation:

- The original protected region must be available. The vCenter Server instances, ESXi hosts, Site Recovery Manager Server instances, and corresponding databases must all be recoverable.

  To unpair and recreate the pairing of protected and recovery regions, both regions must be available. If you cannot restore the original protected region, you must reinstall Site Recovery Manager on the protected and recovery regions.

- If you performed a planned migration or disaster recovery, ensure that all steps of the recovery plan finish successfully. If errors occur during the recovery, resolve the problems that caused the errors and rerun the recovery plan. When you rerun a recovery plan, the operations that previously succeeded are skipped. For example, successfully recovered virtual machines are not recovered again and continue running without interruption.
- If you performed a disaster recovery operation, you must perform the following tasks before reprotect:
  - After the protected region is repaired, Site Recovery Manager detects the availability of the region and changes the Recovery Plan status to `Recovery Required`. Rerun the recovery plans for the Cloud Management Platform and Operations Management Applications in the `Recovery Required` state so that Site Recovery Manager can perform actions on the original region which failed during disaster recovery.
  - Perform a planned migration when both regions are running again.

    If errors occur during the attempted planned migration, resolve the errors and rerun the planned migration until it succeeds.

Reprotect the Operations ManagementApplications

Prepare vRealize Operations Manager and vRealize Suite Lifecycle Manager for failback or failover by reprotecting the virtual machines in Site Recovery Manager.

Procedure

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

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

Type of Reprotect	URL
Reprotect after failover.	`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`
Reprotect after failback.	`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 of the vSphere Web Client, select **Site Recovery**.

3 Click **Recovery Plans**, right-click the **SDDC Operations Management RP** recovery plan, and select **Reprotect**.

The **Reprotect** wizard appears.

4 On the **Confirmation options** page, select the check box to confirm that you understand the reprotect operation is irreversible, and click **Next**.

5 On the **Ready to complete** page, review the reprotect information and click **Finish**.

6 Select the **SDDC Operations Management RP** recovery plan and click the **Monitor > Recovery Steps** tab to monitor the progress of the reprotect operation.

7 If the status of the SDDC Operations Management RP recovery plan changes to `Reprotect interrupted`, run the **Reprotect** wizard again and select the **Force cleanup** check box on the confirmation page.

8 After the status of the SDDC Operations Management RP recovery plan changes to `Ready`, click **Monitor > History** and click **Export the recovery plans history list**.

   The recovery plan can return to the `Ready` state even if errors occurred during the reprotect operation. View the history report for the reprotect operation and ensure that there are no errors. If errors occurred during reprotect, attempt to fix them and run a test recovery to ensure that the errors are fixed. If you do not fix the errors and you attempt to run a planned migration or disaster recovery later, some virtual machines might fail to recover.

After successful reprotect, Site Recovery Manager performs the following actions:

- Reverses the recovery site and protected site
- Creates placeholder copies of the virtual machines of vRealize Operations Manager and vRealize Suite Lifecycle Manager from the new protected site to the new recovery site

Reprotect the Cloud Management Platform

Prepare vRealize Automation and vRealize Business for failback or failover by reprotecting the virtual machines in Site Recovery Manager.

Procedure

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

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

Type of Reprotect	URL
Reprotect after failover.	`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`
Reprotect after failback.	`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 of the vSphere Web Client, select **Site Recovery**.

3 Click **Recovery Plans**, right-click the **SDDC Cloud Management RP** recovery plan, and select **Reprotect**.

   The **Reprotect** wizard appears.

4 On the **Confirmation options** page, select the check box to confirm that you understand the reprotect operation is irreversible, and click **Next**.

5 On the **Ready to complete** page, review the reprotect information and click **Finish**.

6 Select the **SDDC Cloud Management RP** recovery plan and click the **Monitor > Recovery Steps** tab to monitor the progress of the reprotect operation.

7 If the status of the SDDC Cloud Management RP recovery plan changes to `Reprotect interrupted`, run the **Reprotect** wizard again and select the **Force cleanup** check box on the confirmation page.

8 After the status of the SDDC Cloud Management RP recovery plan changes to `Ready`, click the **Monitor > History** tab and click **Export the recovery plans history list**.

   The recovery plan can return to the `Ready` state even if errors occurred during the reprotect operation. View the history report for the reprotect operation to ensure that there are no errors. If errors occurred during reprotect, attempt to fix them and run a test recovery ensure that the errors are fixed. If you do not fix the errors and you attempt to run a planned migration or disaster recovery later, some virtual machines might fail to recover.

After successful reprotect, Site Recovery Manager performs the following actions:

- Reverses the recovery site and protected site
- Creates placeholder copies of the virtual machines of the Cloud Management Platform from the new protected site to the new recovery site