

Site Protection and Recovery

VMware Validated Design 4.0

VMware Validated Design for Software-Defined Data Center 4.0



vmware®

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

<https://docs.vmware.com/>

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

docfeedback@vmware.com

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

Copyright © 2016–2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

	About VMware Validated Design Site Protection and Recovery	5
1	Failover and Failback Checklist for the SDDC Management Applications	6
2	Prerequisites for SDDC Failover or Failback	8
3	Failover of the SDDC Management Applications	9
	Configure Failover of Management Applications	10
	Configure Failover of vRealize Operations Manager	10
	Configure Failover of the Cloud Management Platform	27
	Test the Failover of Management Applications	46
	Test the Failover of vRealize Operations Manager	46
	Test the Failover of the Cloud Management Platform	49
	Perform Planned Migration of Management Applications	52
	Initiate a Planned Migration of vRealize Operations Manager	52
	Initiate a Planned Migration of the Cloud Management Platform	54
	Perform Disaster Recovery of Management Applications	56
	Reconfigure the NSX Instance for the Management Cluster in Region B	56
	Recover the Control VM of the Universal Distributed Logical Router in Region B	59
	Reconfigure the Universal Distributed Logical Router and NSX Edges for Dynamic Routing in Region B	60
	Verify Establishment of BGP for the Universal Distributed Logical Router in Region B	63
	Enable Network Connectivity for the NSX Load Balancer in Region B	63
	Initiate Disaster Recovery of vRealize Operations Manager in Region B	64
	Initiate Disaster Recovery of the Cloud Management Platform in Region B	65
	Post-Failover Configuration of Management Applications	66
	Configure the NSX Controllers and the UDLR Control VM to Forward Events to vRealize Log Insight in Region B	67
	Update the vRealize Log Insight Logging Address after Failover	71
	Reconfigure the NSX Instance for the Management Cluster in Region A after Failover	72
4	Failback of the SDDC Management Applications	76
	Test the Failback of Management Applications	76
	Test the Failback of vRealize Operations Manager	77
	Test the Failback of the Cloud Management Platform	80
	Perform Failback as Planned Migration of Management Applications	83
	Initiate Failback as Planned Migration of vRealize Operations Manager	83
	Initiate Failback as Planned Migration of the Cloud Management Platform	86

- Perform Failback as Disaster Recovery of Management Applications 88
 - Reconfigure the NSX Instance for the Management Cluster in Region A 89
 - Recover the Control VM of the Universal Distributed Logical Router in Region A 91
 - Reconfigure the Universal Distributed Logical Router and NSX Edges for Dynamic Routing in Region A 92
 - Verify the Establishment of BGP for the Universal Distributed Logical Router in Region A 95
 - Enable Network Connectivity for the NSX Load Balancer in Region A 98
 - Initiate Disaster Recovery of vRealize Operations Manager in Region A 98
 - Initiate Disaster Recovery of the Cloud Management Platform in Region A 99
- Post-Failback Configuration of Management Applications 101
 - Configure the NSX Controllers and the UDLR Control VM to Forward Events to vRealize Log Insight in Region A 101
 - Update the vRealize Log Insight Logging Address after Failback 106
 - Reconfigure the NSX Instance for the Management Cluster in Region B after Failback 107

5 Reprotect of the SDDC Management Applications 111

- Prerequisites for Performing Reprotect 111
- Reprotect vRealize Operations Manager 112
- Reprotect the Cloud Management Platform 113

About VMware Validated Design Site Protection and Recovery

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

You 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, vRealize Orchestrator and vRealize Business, and of the vRealize Operations Manager analytics cluster.

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

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

Failover and Failback Checklist for the SDDC Management Applications

1

Use a checklist to verify that you have satisfied all the requirements to initiate disaster recovery and planned migration of the SDDC management applications.

Table 1-1. Checklist for Failover and Failback

Checklist	Tasks
Activation and Assessment	<p>Verify that the disaster failover or failback is really required.</p> <p>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.</p> <p>Also, consider business continuity events such as planned building maintenance or the possibility of a hurricane.</p>
Approval	<p>Submit required documentation for approval to the following roles:</p> <ul style="list-style-type: none">■ IT management■ Business users■ CTO
Activation Logistics	<ul style="list-style-type: none">■ Ensure that all required facilities and personnel are available to start and complete 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.<ul style="list-style-type: none">■ Are the NSX Edges available?■ Are the IP addresses for VXLAN backed networks correct?■ Is load balancer on the NSX Edge configured according to the design?■ Is the firewall on the NSX Edge correctly configured according to the design?

Table 1-1. Checklist for Failover and Failback (Continued)

Checklist	Tasks
Communication, Initiation and Failover/Failback Validation	<ul style="list-style-type: none"> ■ In the case of a planned migration, <ul style="list-style-type: none"> ■ Notify the users of the outage. ■ At the scheduled time initiate the failover or failback process. ■ In the case of a disaster recovery failover/failback, notify all stakeholders and initiate the failover or failback process ■ Test the application availability after the completion of failover or failback. ■ Notify all stakeholders of completed failover or failback.
Post Failover/Failback Configuration	<p>In the case of disaster recovery failover/failback, perform the following configuration:</p> <ul style="list-style-type: none"> ■ Update the backup jobs to include the applications that are now running in Region B. ■ 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. For example, note which items worked and which did not work, and identify places for improvement that you can incorporate back in the recovery plan.

Prerequisites for SDDC Failover or Failback

2

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

Table 2-1. Failover or Failback Prerequisites

Prerequisite	Value
Compute	The compute in the recovery region must mirror the compute in the protected region.
Storage	<ul style="list-style-type: none">■ The storage configuration and capacity in the recovery region must mirror the storage configuration and capacity in the protected region.■ Shared datastore space on the management pod with enough capacity must be available for all VMs of vRealize Automation and vRealize Operations Manager.
External Services	<p>Provide the following services in the recovery region. See <i>External Service Dependencies</i> from the <i>Planning and Preparation</i> documentation.</p> <ul style="list-style-type: none">■ Active Directory■ DNS■ NTP■ SMTP■ Syslog
Virtual Infrastructure	<ul style="list-style-type: none">■ ESXi, vCenter Server and NSX for vSphere mirrored in the protected region■ Site Recovery Manager and vSphere Replication deployed in both regions and paired■ NSX Edge devices for North-South Routing deployed and configured in both regions■ Universal distributed logical router deployed and configured■ NSX Load Balancer deployed and configured in both regions

Failover of the SDDC Management Applications

3

Configure and perform failover of the management applications in the SDDC from the protected region, Region A, to the recovery region, Region B.

You fail over the following management components:

- Analytics cluster of vRealize Operations Manager
- Primary components of vRealize Automation, vRealize Orchestrator, and vRealize Business

The remote collector nodes of vRealize Operations Manager are not failed over. You deploy a separate pair of remote collectors in each region in an application isolated network. The vSphere Proxy Agents of vRealize Automation and the vRealize Business data collector are not failed over. You deploy a separate pair of agents and collector in each region in an application isolated network.

1 [Configure Failover of Management Applications](#)

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

2 [Test the Failover of Management Applications](#)

Test the recovery plan for the management applications in the SDDC to eliminate potential problems during a future failover.

3 [Perform Planned Migration of Management Applications](#)

After you have successfully configured and tested failover of the management applications, start the migration process from Region A to Region B.

4 [Perform Disaster Recovery of Management Applications](#)

Prepare networking in Region B and perform failover of vRealize Automation, vRealize Orchestrator, vRealize Business, and vRealize Operations Manager to Region B if Region A becomes unavailable in the event of a disaster or if you plan a graceful migration.

5 [Post-Failover Configuration of Management Applications](#)

After failover of the cloud management platform and vRealize Operations Manager, you must perform certain tasks to ensure that applications perform as expected.

Configure Failover of Management Applications

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

- [Configure Failover of vRealize Operations Manager](#)
Prepare vRealize Operations Manager for failover by replicating the virtual machines of the analytics cluster and creating a recovery plan for them in Site Recovery Manager.
- [Configure Failover of the Cloud Management Platform](#)
Prepare vRealize Automation, vRealize Orchestrator, and vRealize Business for failover. Replicate the virtual machines of the primary vRealize Automation components, vRealize Orchestrator, and of vRealize Business Server. Create a recovery plan for them in Site Recovery Manager.

Configure Failover of vRealize Operations Manager

Prepare vRealize Operations Manager for failover by replicating the virtual machines of the analytics cluster and creating a recovery plan for them in Site Recovery Manager.

Procedure

- 1 [Replicate the VMs of vRealize Operations Manager](#)
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.
- 2 [Create a Protection Group for vRealize Operations Manager](#)
After you configure a replication solution for the analytics virtual machines of vRealize Operations Manager, include the virtual machines in a protection group so that Site Recovery Manager protects them together.
- 3 [Create a Recovery Plan for vRealize Operations Manager](#)
After you create a protection group for the virtual machines of the vRealize Operations Manager analytics cluster, create a recovery plan. You use this plan to run commands on Site Recovery Manager and the analytics virtual machines, and configure dependencies between the virtual machines.
- 4 [Customize the Recovery Plan for vRealize Operations Manager](#)
After you create the recovery plan for the vRealize Operations Manager failover, configure the startup priority and the startup and shutdown options for the virtual machines of the analytics cluster.
- 5 [Duplicate the Anti-Affinity Rules for vRealize Operations Manager in Region B](#)
VM anti-affinity rules are not retained during a Site Recovery Manager assisted recovery. You must duplicate the anti-affinity rules for the analytics virtual machines in Region B so that the rules apply after failover of vRealize Operations Manager.

Replicate the VMs of vRealize Operations Manager

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.

Procedure

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

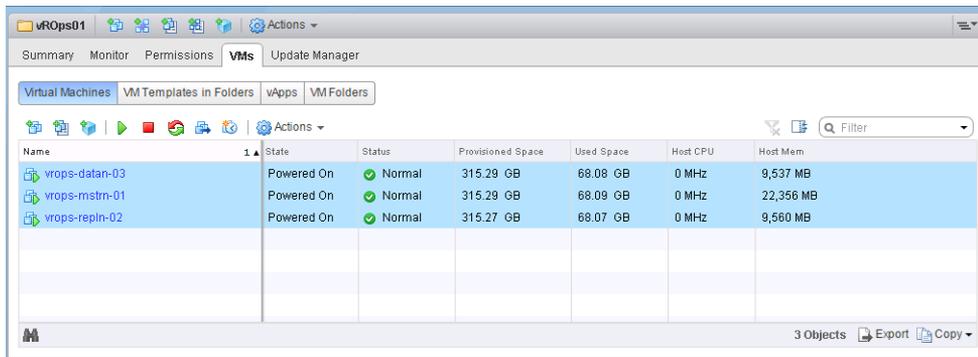
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **VMs and Templates**.
- 3 Navigate to the vROps01 VM folder.

Object	Value
vCenter Server	mgmt01vc01.sfo01.rainpole.local
Data center	SFO01
Folder	vROps01

- 4 On the **vROps01** page, click the **VMs** tab, click **Virtual Machines** and select the virtual machines of the analytics cluster.

Name	Role
vrops-mstrn-01	Master node
vrops-repln-02	Master replica node
vrops-datan-03	Data node 1



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

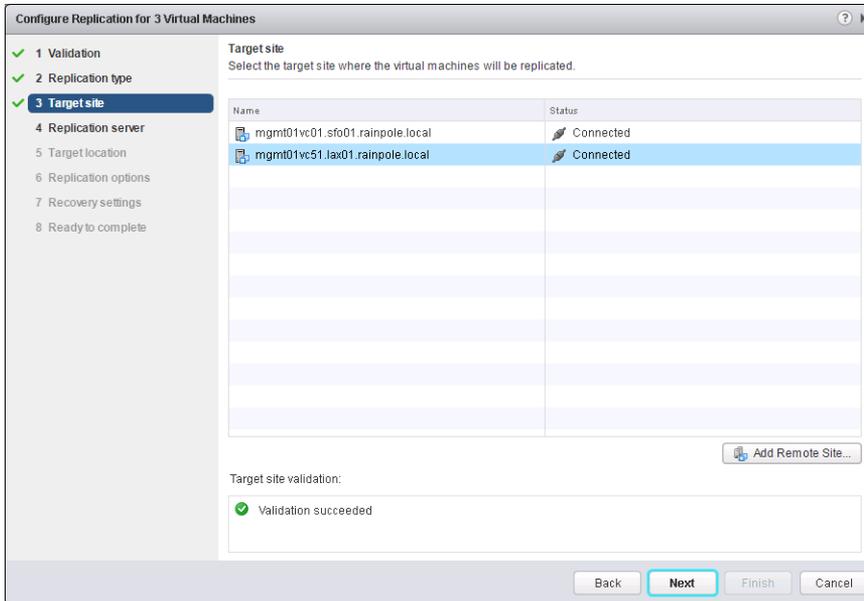
6 Click **Yes** in the dialog box about performing replication for all objects.

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, 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 **mgmt01vc51.lax01.rainpole.local** vCenter Server in Region B and click **Next**.

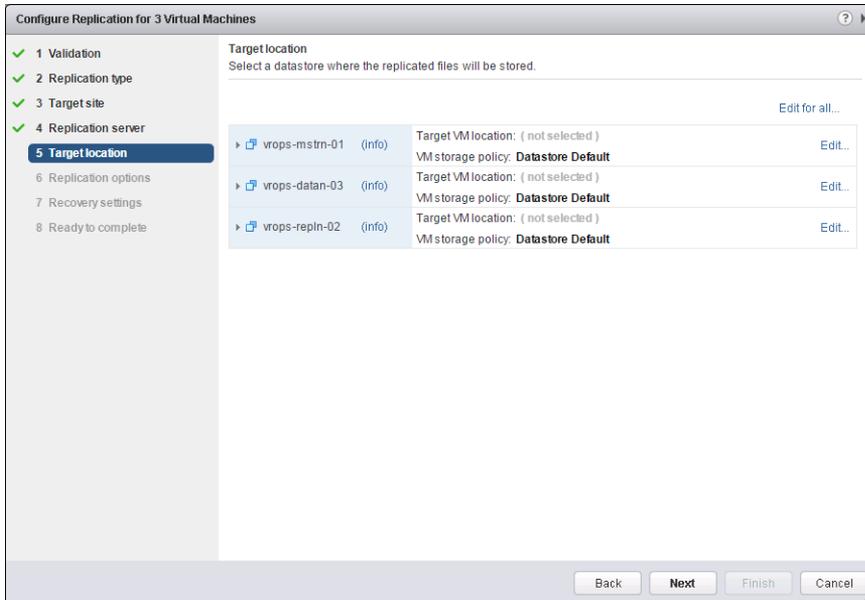


10 On the **Replication server** page, select **Auto-assign vSphere Replication server** and click **Next**.

If the environment contains several replications servers, selecting this option makes use of any of these replication servers.

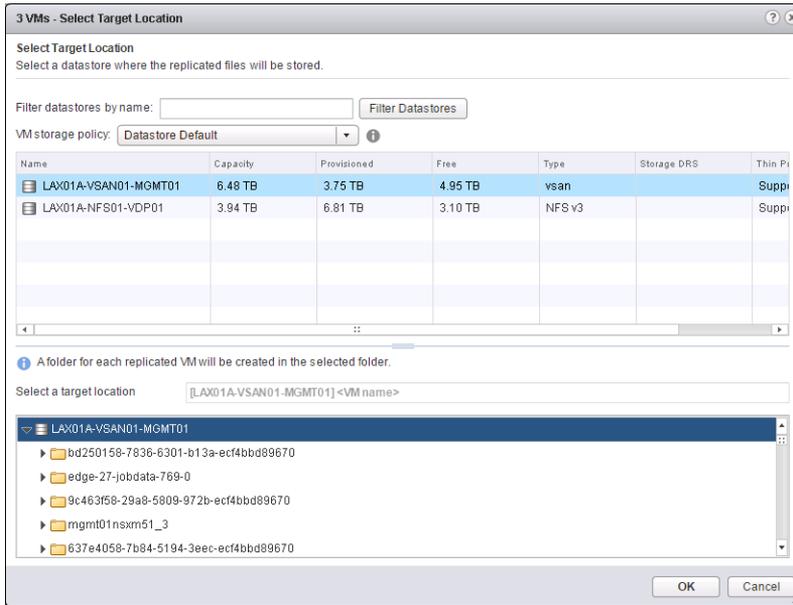
11 On the **Target location** page, set the location on the vSAN datastore in Region B to store replicated VM files.

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



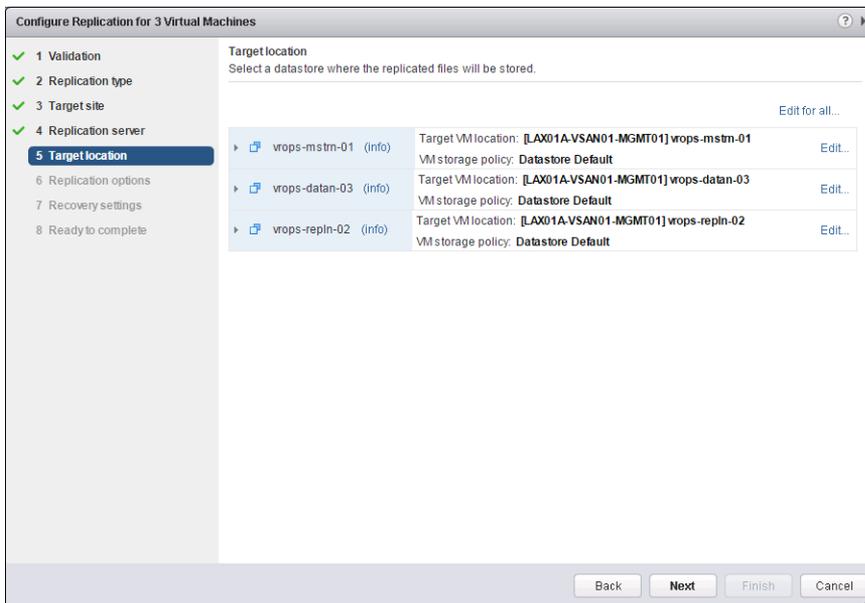
b In the **Select Target Location** dialog box, select the **LAX01A-VSAN01-MGMT01** datastore from the datastore list in the upper part of the dialog box.

- c In the **Select a target location** pane, select the **LAX01-VSAN01-MGMT01** root folder underneath, and click **OK**.



vSphere Replication will create a folder in the root datastore folder for the vRealize Operations Manager VMs.

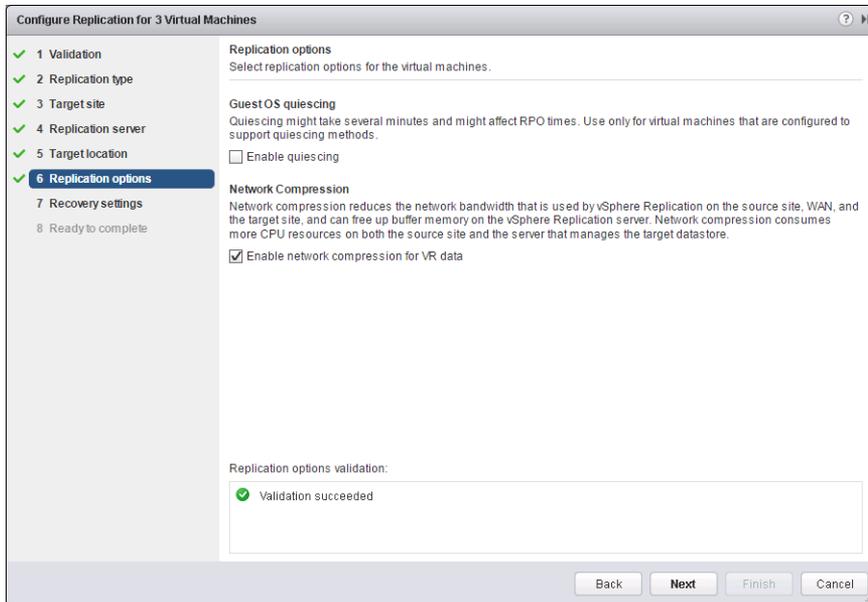
- d Back on the **Target Location** page, click **Next**.



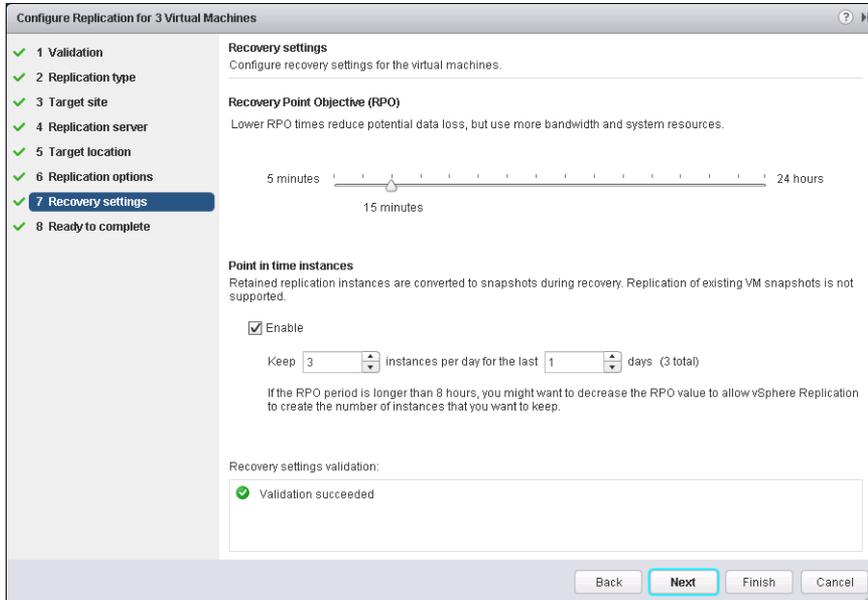
- 12 On the **Replication options** page, select only the **Enable network compression for VR data** check box, and click **Next**.

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 frozen state for too long.
- Compression requires extra resources. Do not enable it if the hosts are over-utilized.



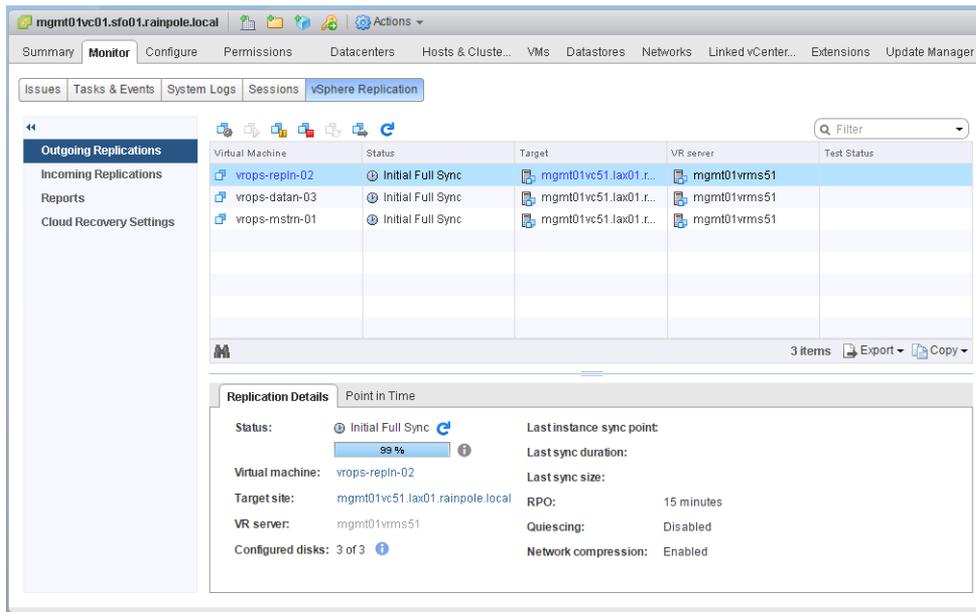
- 13 On the **Recovery settings** page, enter the following settings and click **Next**.
 - a Set the **Recovery Point Objective (RPO)** to **15 minutes**.
 - b Select **Enable** under **Point in time instances** and keep **3** instances per day for the last **1** days.



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

15 (Optional) Monitor the replication progress.

- a In the vSphere Web Client, click **Home > vSphere Replication** and click the **Home** tab.
- b Select the **mgmt01vc01.sfo01.rainpole.local** and click **Monitor** to open the page for replication configuration page for this vCenter Server instance.
- c On the **Monitor** tab, click the **vSphere Replication** tab and select **Outgoing Replications**.



Create a Protection Group for vRealize Operations Manager

After you configure a replication solution for the analytics virtual machines of vRealize Operations Manager, include the virtual machines in a 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://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

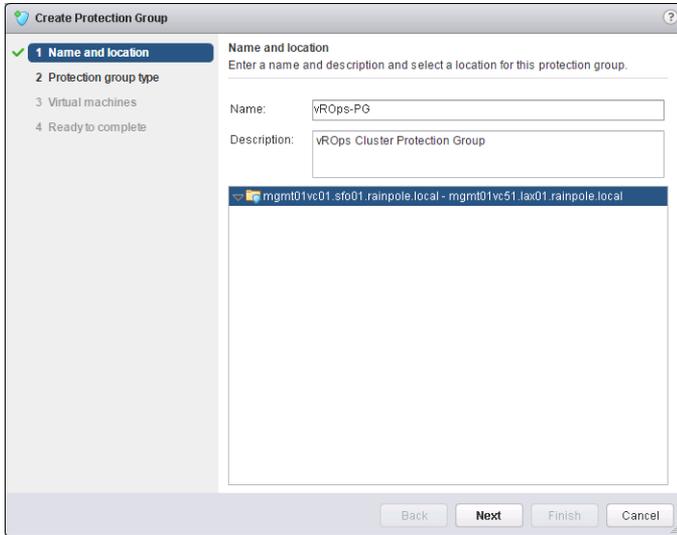
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.
- 3 On the Site Recovery home page, click **Sites** and select the **mgmt01vc01.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.

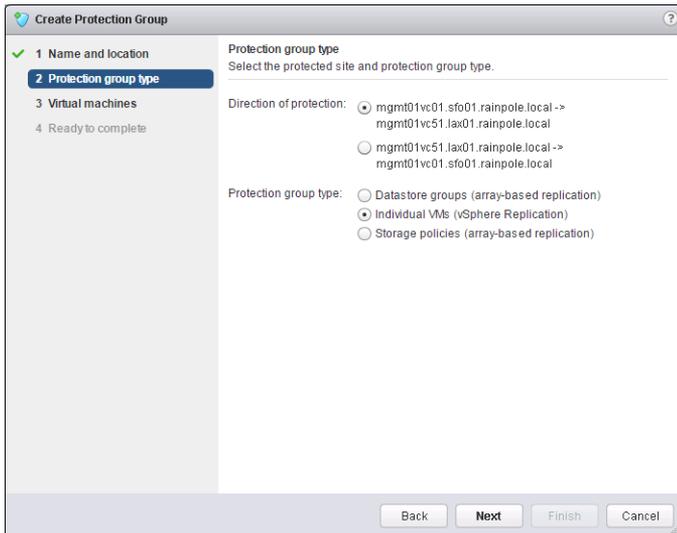
- 5 On the **Related Objects** tab, click the **Protection Groups** tab and click **Create Protection Group**. The **Create Protection Group** wizard appears.
- 6 On the **Name and location** page, configure the following settings and click **Next**.

Setting	Value
Name	vROps-PG
Description	vROps Cluster Protection Group
Site pair	mgmt01vc01.sfo01.rainpole.local - mgmt01vc51.lax01.rainpole.local



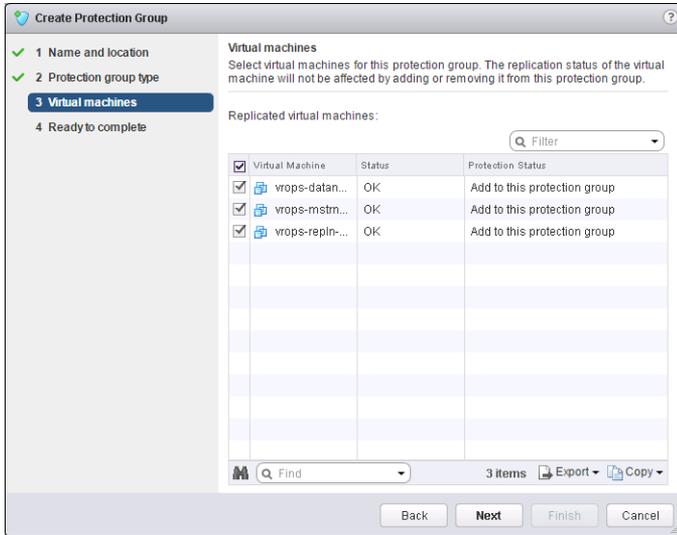
7 On the **Protection group type** page, configure the following settings and click **Next**.

Setting	Value
Direction of protection	mgmt01vc01.sfo01.rainpole.local -> mgmt01vc51.lax01.rainpole.local
Protection group type	Individual VMs



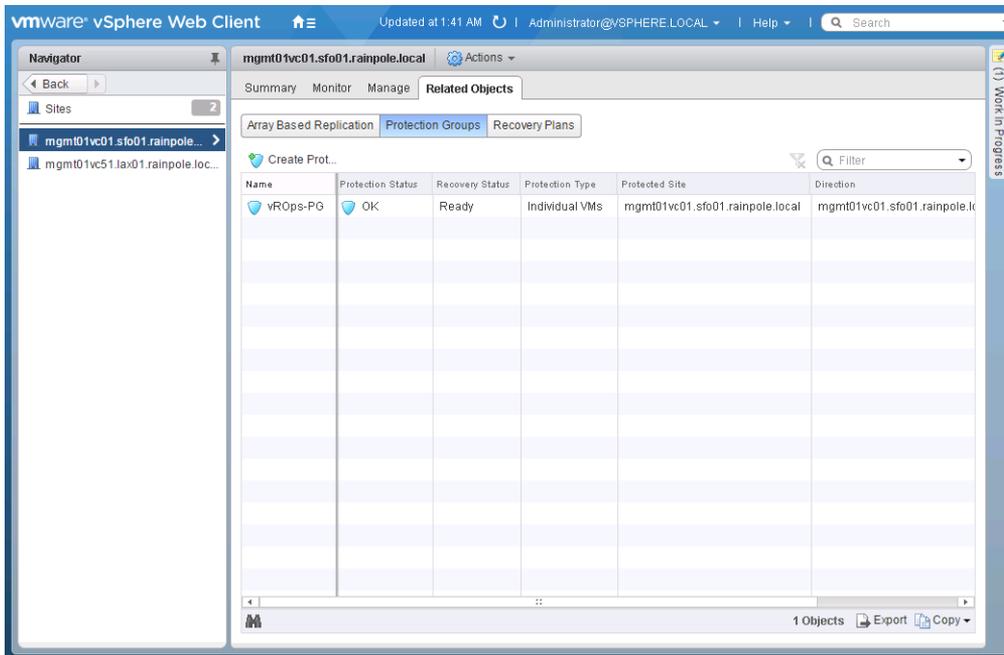
8 On the **Virtual machines** page, select the analytics virtual machines from the list of machines replicated by using vSphere Replication and click **Next**.

- vrops-mstrn-01
- vrops-repln-02
- vrops-datan-03



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

The vROps-PG protection group appears in the list of protection groups for Site Recovery Manager.



Create a Recovery Plan for vRealize Operations Manager

After you create a protection group for the virtual machines of the vRealize Operations Manager analytics cluster, create a recovery plan. You use this plan to run commands on Site Recovery Manager and the analytics virtual machines, and configure dependencies between the virtual machines.

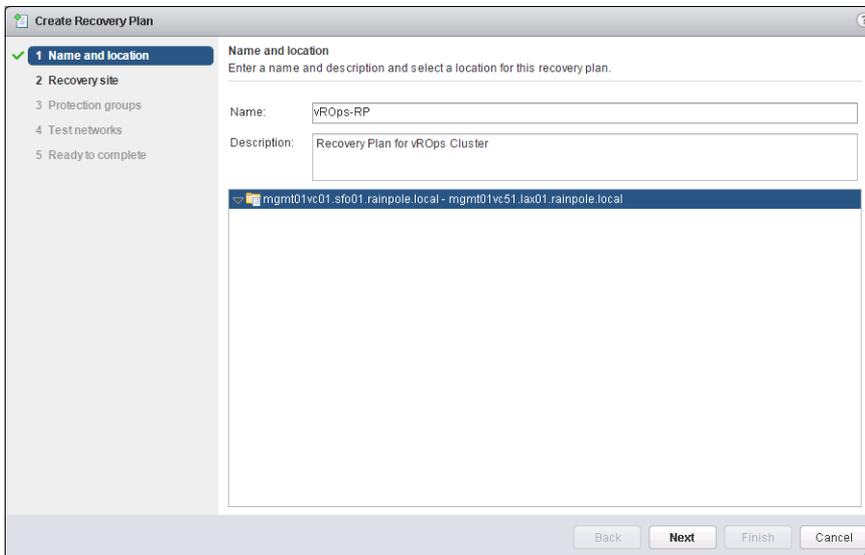
Procedure

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

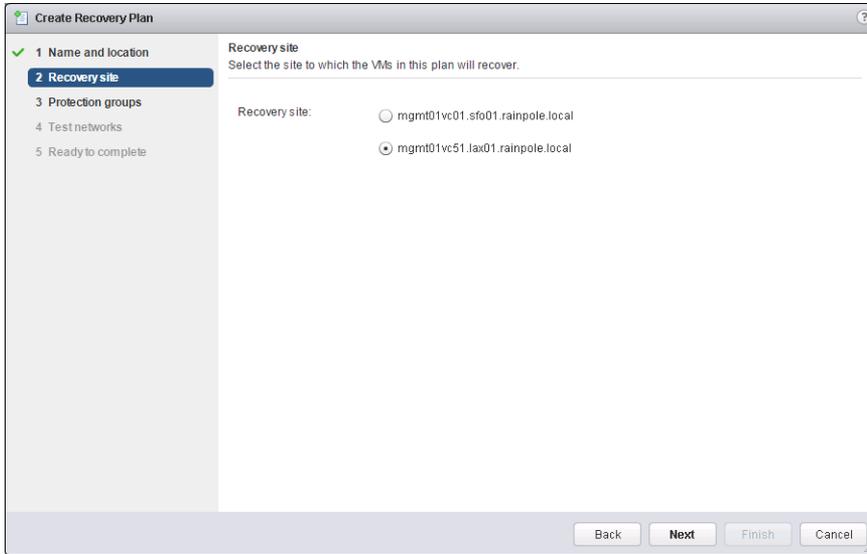
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**
- 3 On the Site Recovery home page, click **Sites** and select **mgmt01vc01.sfo01.rainpole.local**.
- 4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **Create Recovery Plan** icon.
- 5 On the **Name and location** page, configure the following settings and click **Next**.

Property	Value
Name	vROps-RP
Description	Recovery Plan for vROps Cluster
Site pair	mgmt01vc01.sfo01.rainpole.local - mgmt01vc51.lax01.rainpole.local

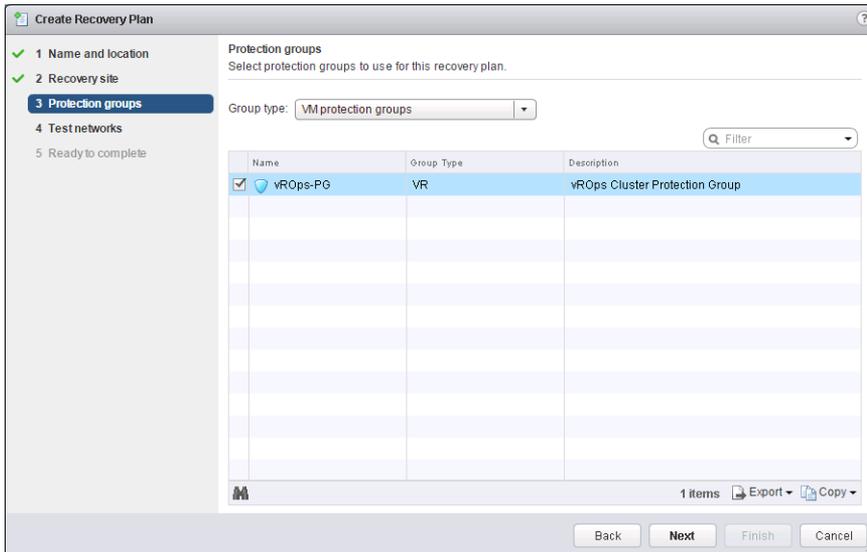


- 6 On the Recovery Site page, select **mgmt01vc51.lax01.rainpole.local** in the **Recovery Site** pane and click **Next**.



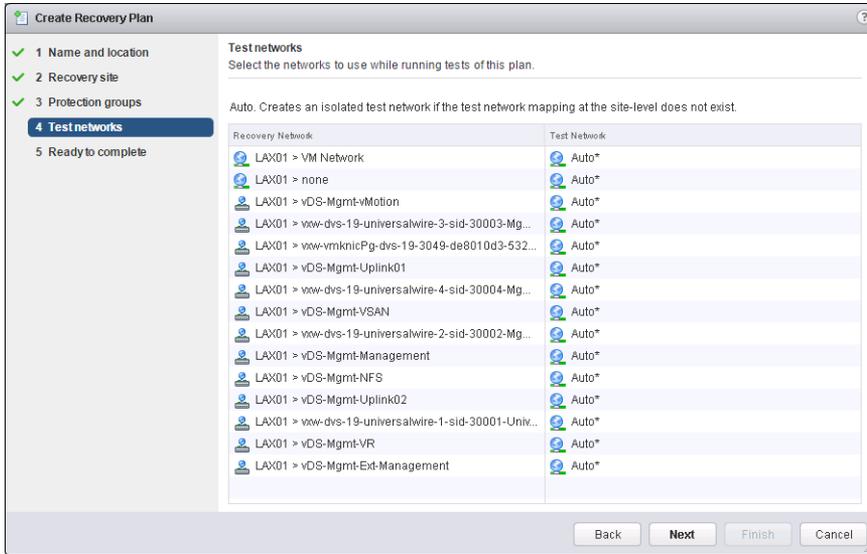
7 On the **Protection group** page, select the protection group for the recovery plan and click **Next**.

Protection Group Option	Value
Group type	VM protection groups
Protection group	vROps-PG



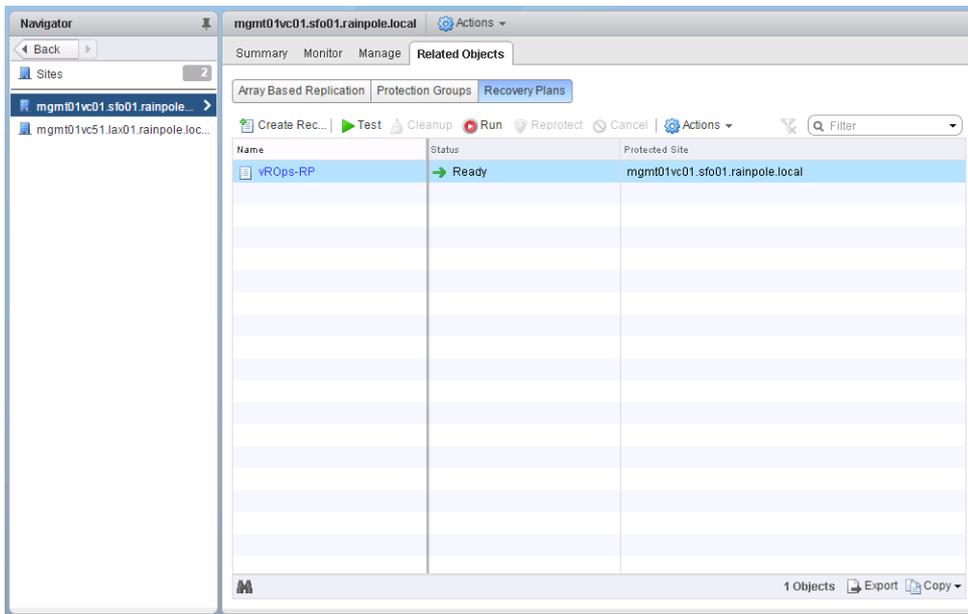
8 On the **Test networks** page, leave the default values and click **Next**.

The default option is to automatically create an isolated network.



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

The vROps-RP recovery plan appears in the list of the recovery plans available in Site Recovery Manager.



Customize the Recovery Plan for vRealize Operations Manager

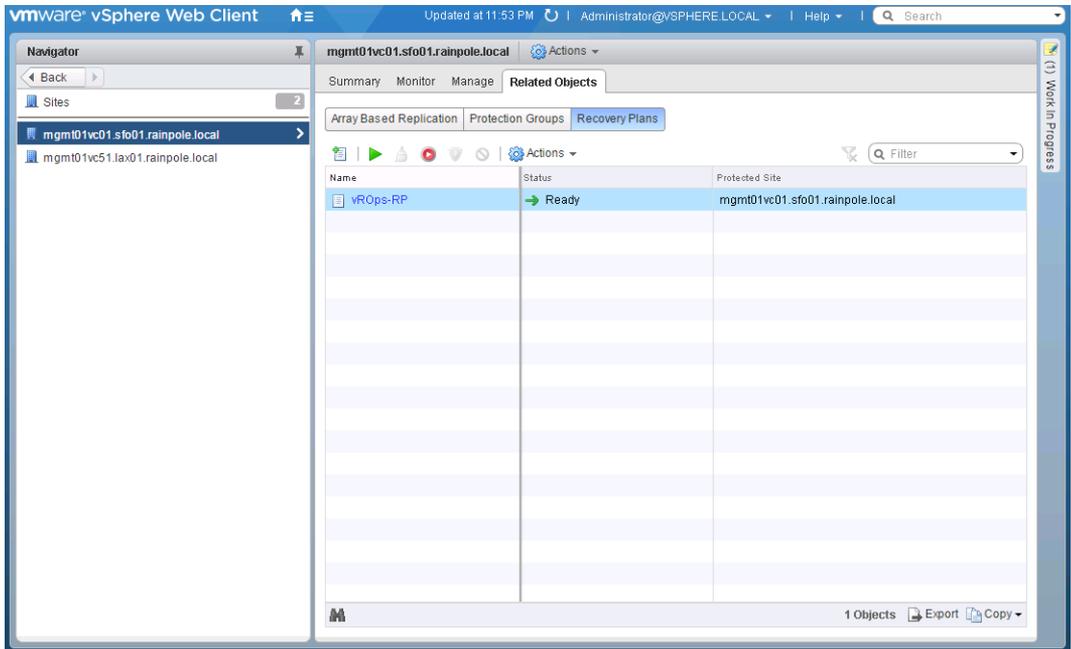
After you create the recovery plan for the vRealize Operations Manager failover, configure the startup priority and the startup and shutdown options for the virtual machines of the analytics cluster.

Procedure

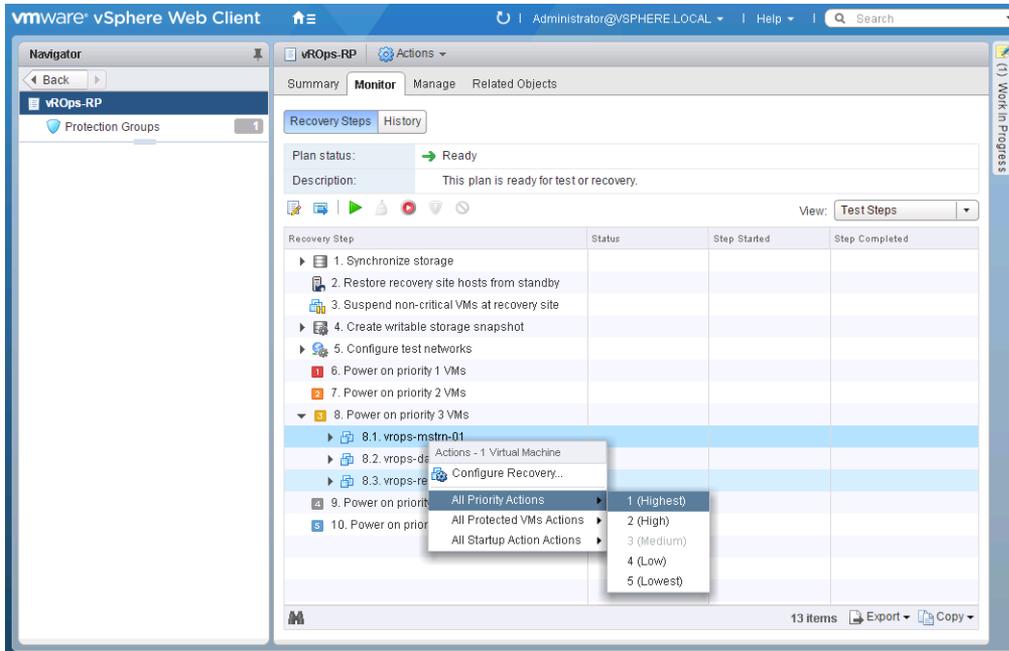
- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Site Recovery**
- 3 On the Site Recovery home page, click **Sites** and select the **mgmt01vc01.sfo01.rainpole.local** protected site.
- 4 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **vROps-RP** recovery plan to open it.

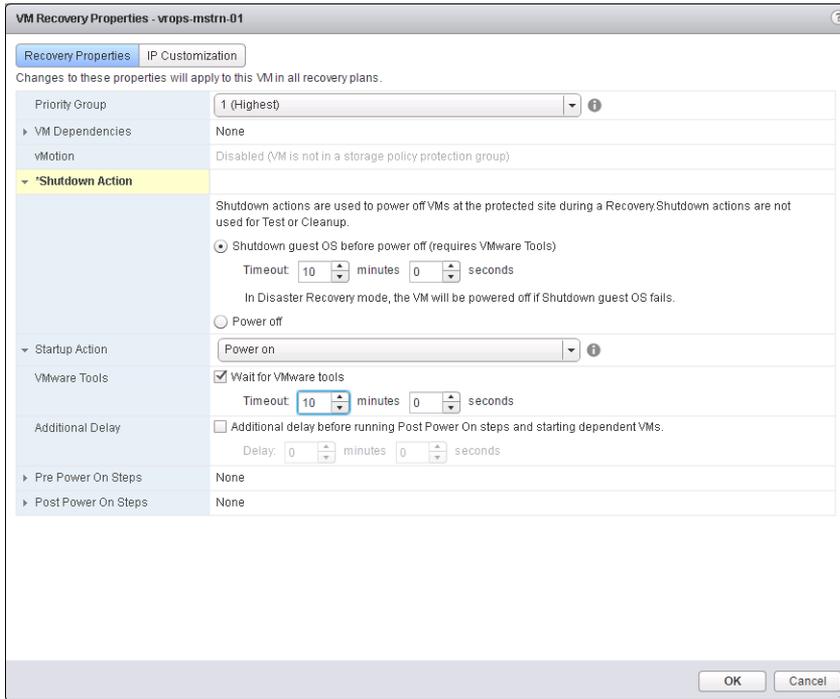


- 5 Change the startup priority of the virtual machine of the master node.
 - a On the recovery plan page, click the **Monitor** tab and click the **Recovery Steps** tab.
 - b Under **Power on priority 3 VMs**, right-click **vrops-mstrn-01** and select **All Priority Actions > 1 > (Highest)**.



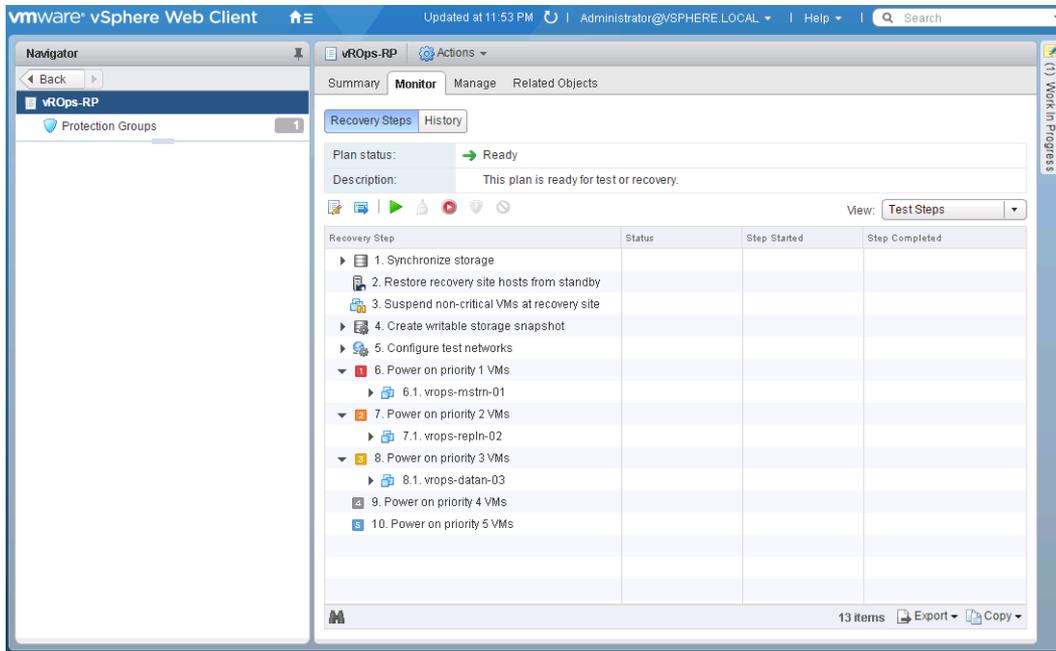
- c In the **Change Priority** dialog box, click **Yes** to confirm.

- 6 Configure startup and shutdown options for the master node.
 - a Right-click **vrops-mstrn-01** and select **Configure Recovery**.
 - b In the **VM Recovery Properties** dialog box, expand **Shutdown Actions** and increase **Shutdown guest OS before power off** to **10 minutes**.
 - c Expand **Startup Actions**, increase the timeout to **10 minutes**, and click **OK**.



- 7 Repeat [Step 5](#) and [Step 6](#) for the other virtual machines of the analytics cluster.

Virtual Machine	Startup Priority Order	Update Timeout Values
vrops-repln-02	2	No
vrops-datan-03	3	Yes



Duplicate the Anti-Affinity Rules for vRealize Operations Manager in Region B

VM anti-affinity rules are not retained during a Site Recovery Manager assisted recovery. You must duplicate the anti-affinity rules for the analytics virtual machines in Region B so that the rules apply after 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Hosts and Clusters** and navigate to the mgmt01vc51.lax01.rainpole.local vCenter Server object.
- 3 Under the **LAX01** data center object, select the **LAX01-Mgmt01** cluster.
- 4 On the **Configure** tab, and under **Configuration**, select **VM/Host Rules**.
- 5 In the **VM/Host Rules** list, click **Add** to create a virtual machine anti-affinity rule.

- 6 In the **Create VM/Host Rule** dialog box, add a new anti-affinity rule for the virtual machines of the master and master replica nodes, and click **OK**.

Setting	Value
Name	anti-affinity-rule-vropsm
Enable Rule	Selected
Type	Separate Virtual Machines
Members	<ul style="list-style-type: none"> ■ vrops-mstrn-01 ■ vrops-repln-02 ■ vrops-datan-03

Configure Failover of the Cloud Management Platform

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

Procedure

- 1 [Replicate the Required VMs of vRealize Automation, vRealize Orchestrator, and vRealize Business](#)
Enable replication of the virtual machines that build up the primary functionality of the cloud management platform to support failover to Region B.
- 2 [Create a Protection Group for the Cloud Management Platform](#)
After you configure replication for the Cloud Management Platform VMs, 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, create a recovery plan. You 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 startup priority.
- 5 [Duplicate the Anti-Affinity Rules for vRealize Automation and vRealize Orchestrator from Region A in Region B](#)
VM anti-affinity rules are not retained during a Site Recovery Manager assisted recovery. You must duplicate the configured anti-affinity rules from Region A in Region B so that the rules apply after failover.

Replicate the Required VMs of vRealize Automation, vRealize Orchestrator, and vRealize Business

Enable replication of the virtual machines that build up the primary functionality of the cloud management platform to support failover to 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://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

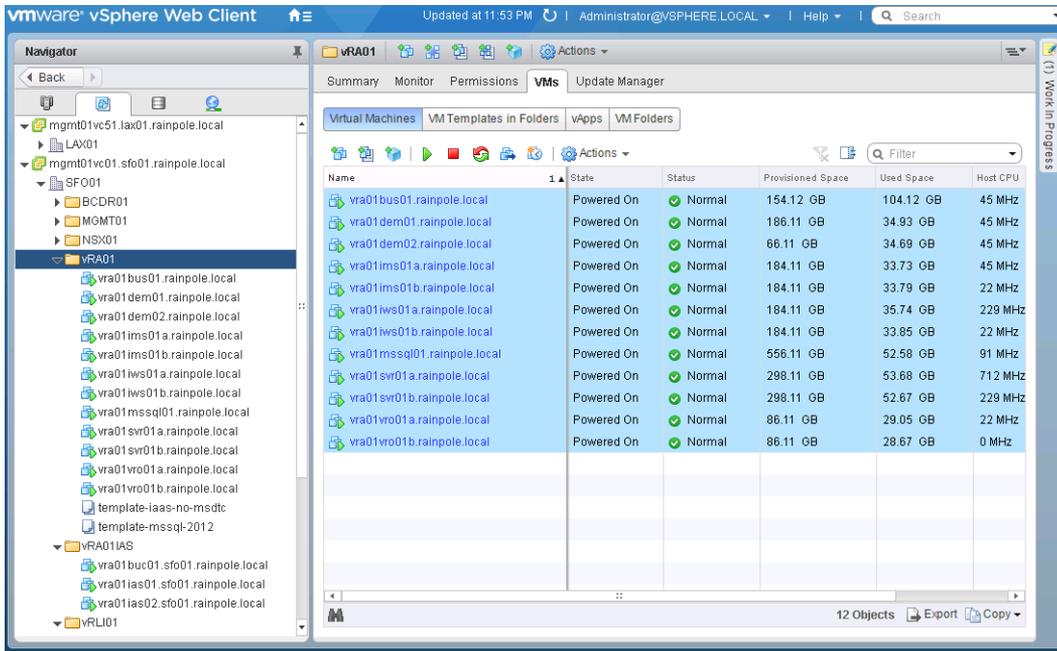
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 On the vSphere Web Client **Home** page, click **VMs and Templates**.
- 3 Navigate to the vRA01 VM folder.

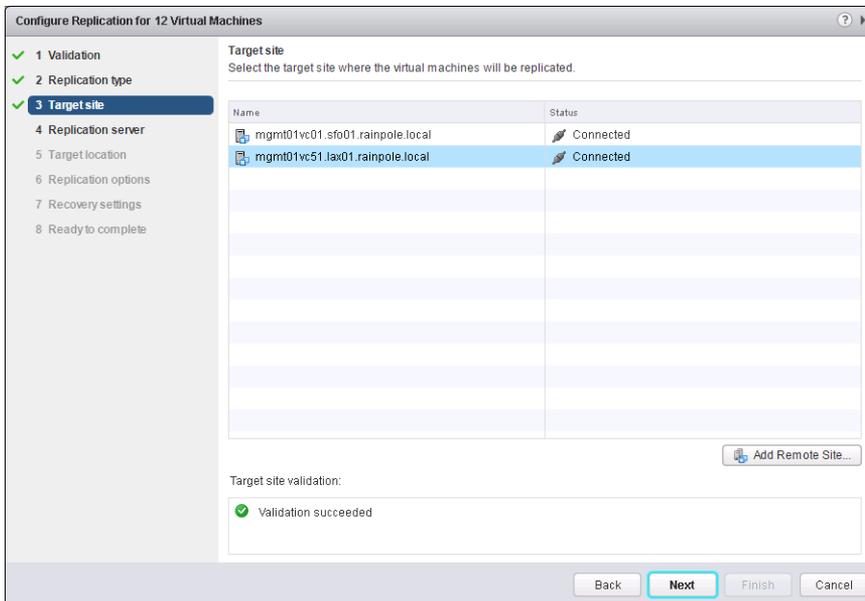
Object	Value
vCenter Server	mgmt01vc01.sfo01.rainpole.local
Data center	SFO01
Folder	vRA01

- 4 On the **vRA01** page, click the **VMs** tab, click **Virtual Machines**, and select the virtual machines of vRealize Automation, vRealize Orchestrator, and the vRealize Business Server.

vRealize Automation Component	VM Name
IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local
IaaS Manager Service and DEM Orchestrator	vra01ims01b.rainpole.local
IaaS Web Server	vra01iws01a.rainpole.local
IaaS Web Server	vra01iws01b.rainpole.local
Microsoft SQL Server	vra01mssql01.rainpole.local
vRealize Appliance	vra01svr01a.rainpole.local
vRealize Appliance	vra01svr01b.rainpole.local
vRealize Automation DEM Worker	vra01dem01.rainpole.local
vRealize Automation DEM Worker	vra01dem02.rainpole.local
vRealize Orchestrator Appliance	vra01vro01a.rainpole.local
vRealize Orchestrator Appliance	vra01vro01b.rainpole.local
vRealize Business Appliance	vra01bus01.rainpole.local



- 5 Right-click the VM selection, and select **All vSphere Replication Actions > Configure Replication**.
- 6 Click **Yes** in the dialog box about performing replication for all objects.
The **Configure Replication for 12 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 **mgmt01vc51.lax01.rainpole.local** vCenter Server in Region B and click **Next**.

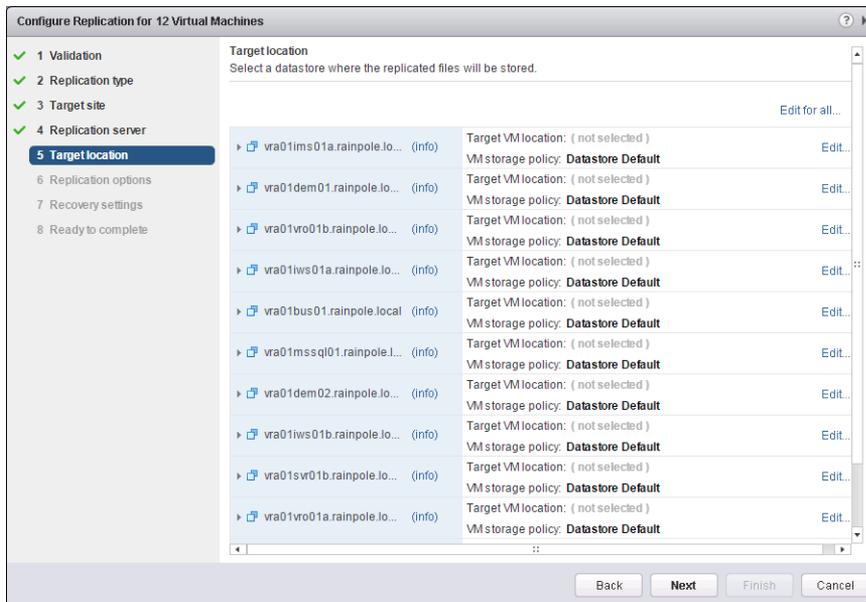


10 On the **Replication server** page, select **Auto-assign vSphere Replication server** and click **Next**.

If the environment contains several replications servers, selecting this option makes use of any of these replication servers.

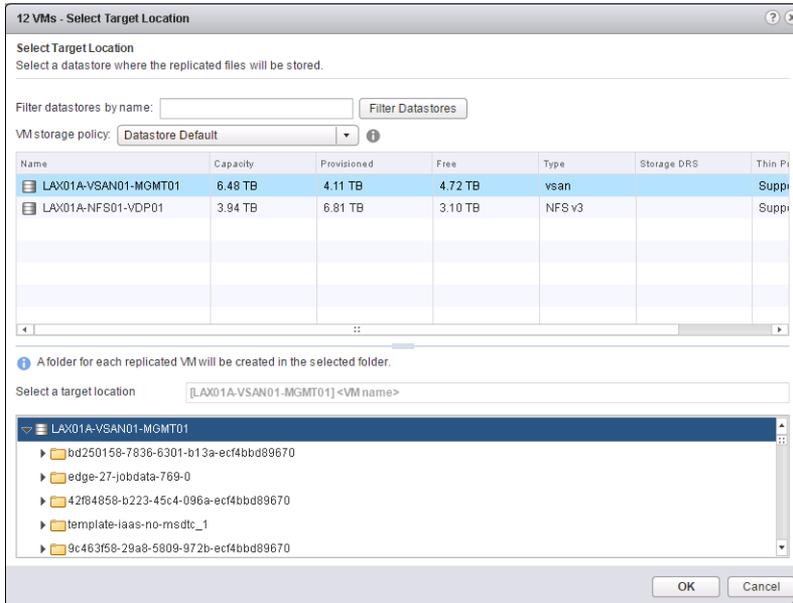
11 On the **Target location** page, set the location on the vSAN datastore in Region B to store replicated VM files.

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

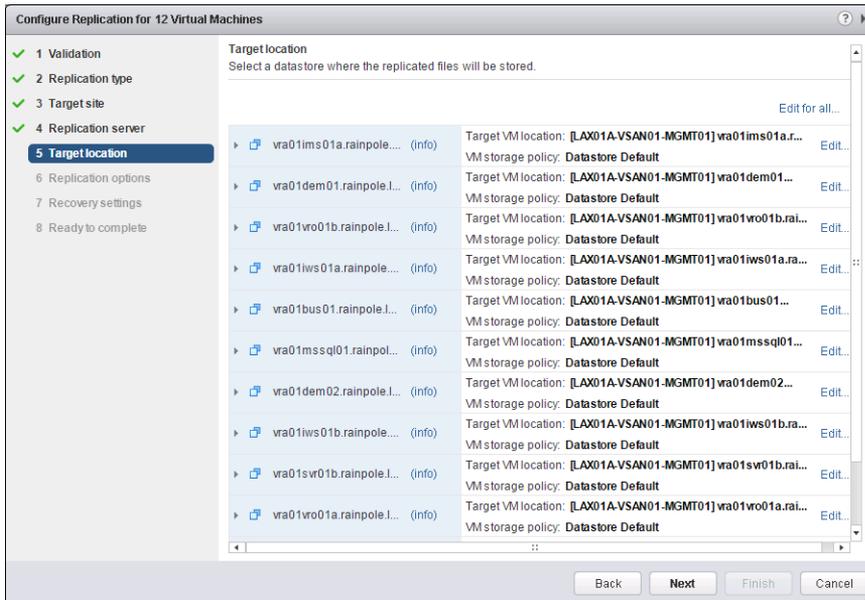


b In the **Select Target Location** dialog box, select **LAX01A-VSAN01-MGMT01** as datastore for replicated files.

- c In the **Select a target location** pane, select **LAX01A-VSAN01-MGMT01** to select the root folder of the datastore and click **OK**.



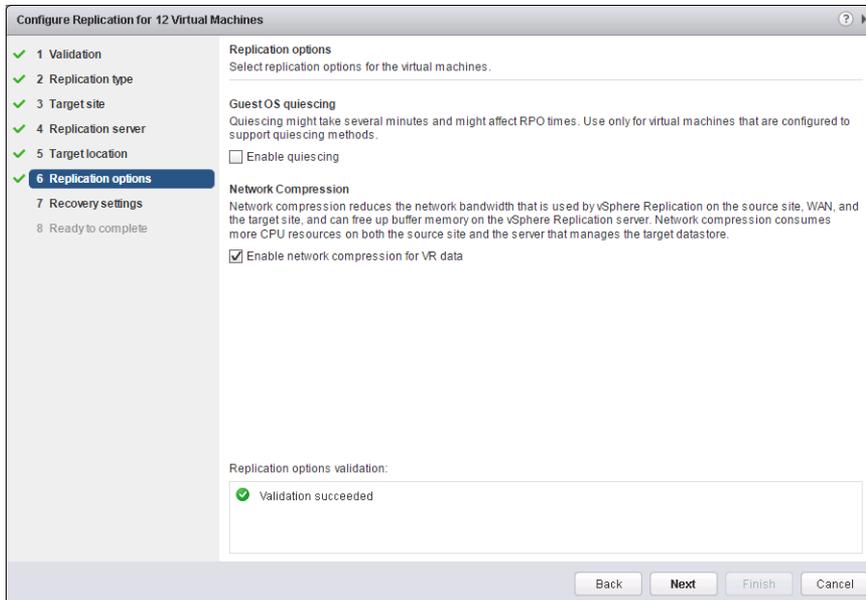
- d On the **Target Location** page, click **Next**.



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

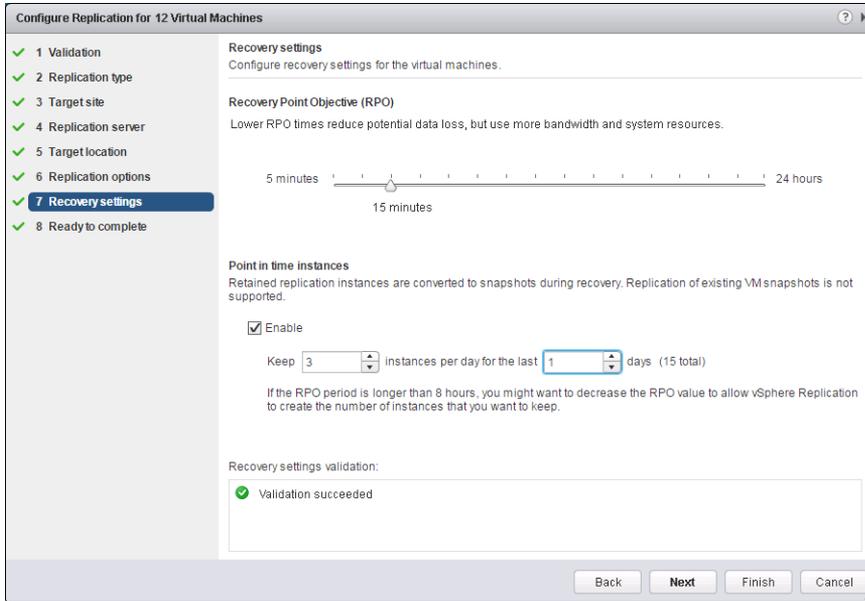
Important

- Do not enable guest OS quiescing because some of the vRealize Automation and vRealize Orchestrator databases do not support quiescing. Quiescing might result in a cluster failure because virtual disks remain in 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**.

- a Set the **Recovery Point Objective (RPO)** to **15 minutes**.
- b Select **Enable** under **Point in time instances** and keep **3** instances per day for the last **1** days.

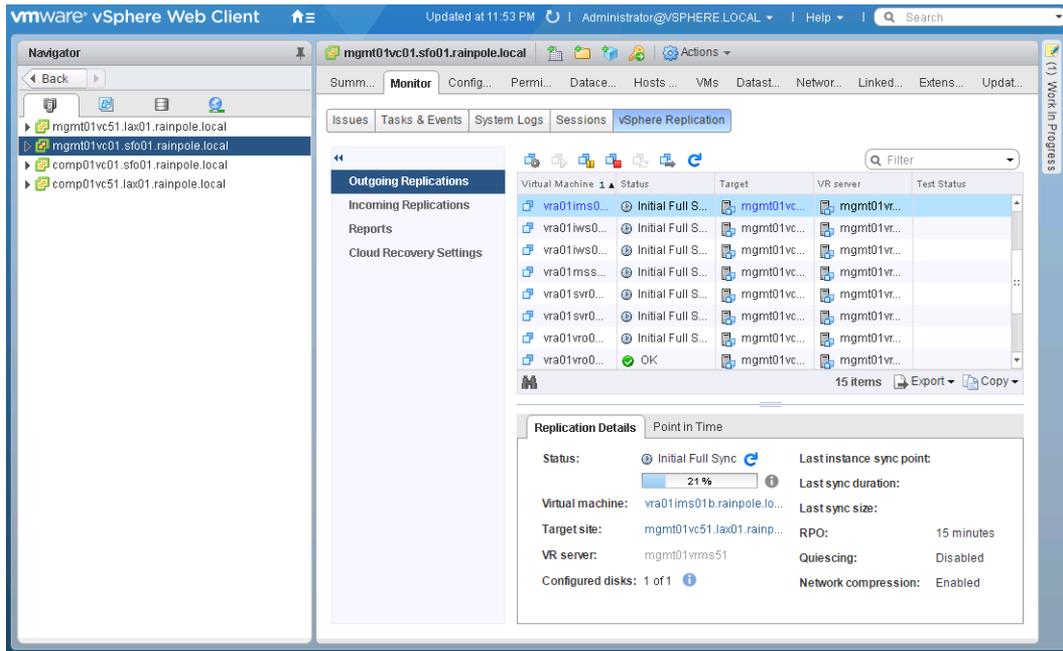


14 On the **Ready to complete** page, review the configuration and click **Finish**.

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

15 (Optional) Monitor the replication progress.

- a From the **Home** menu, select **vSphere Replication** and click the **Home** tab.
- b Select the **mgmt01vc01.sfo01.rainpole.local** and click **Monitor** to open the replication configuration page for this vCenter Server instance
- c On the **Monitor** tab, click the **vSphere Replication** tab, and select **Outgoing Replications**.



Create a Protection Group for the Cloud Management Platform

After you configure replication for the Cloud Management Platform VMs, 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://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

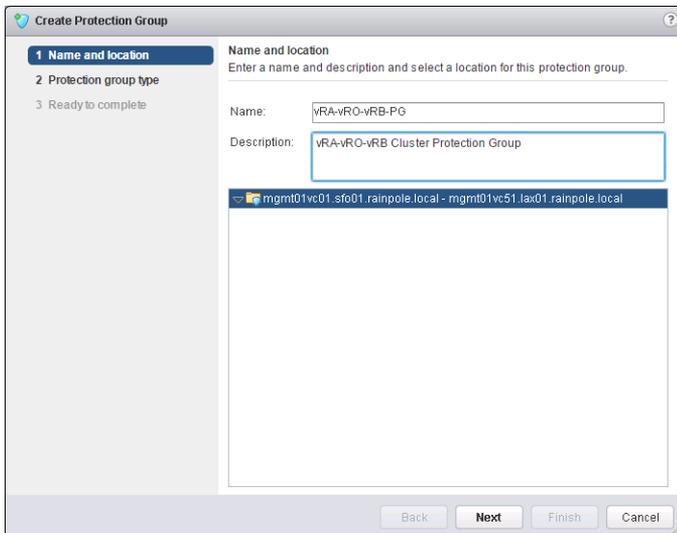
- 2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.
- 3 On the Site Recovery home page, click **Sites** and select the **mgmt01vc01.sfo01.rainpole.local** protected site.

- 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.

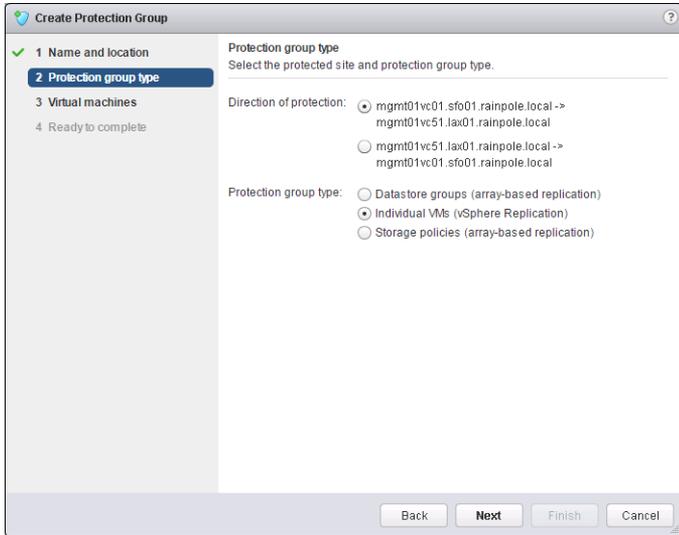
- On the **Related Objects** tab, click the **Protection Groups** tab and click **Create Protection Group**. The **Create Protection Group** wizard appears.
- On the **Name and location** page, configure the following settings and click **Next**.

Setting	Value
Name	vRA-vRO-vRB-PG
Description	vRA-vRO-vRB Cluster Protection Group
Site pair	mgmt01vc01.sfo01.rainpole.local - mgmt01vc51.lax01.rainpole.local



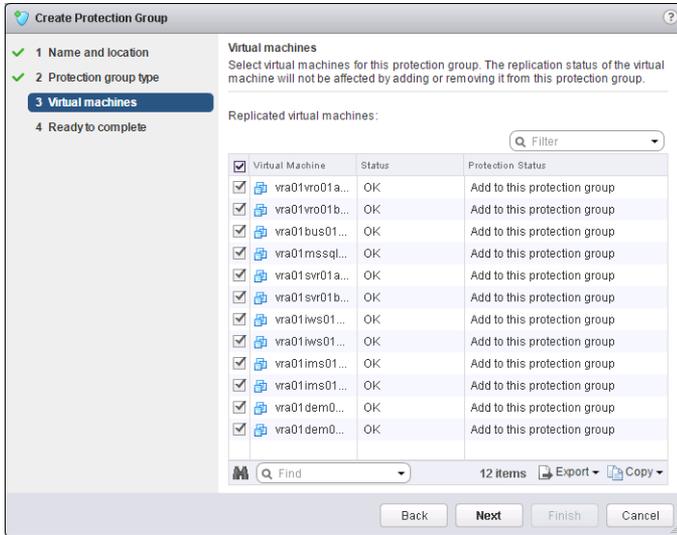
- On the **Protection group type** page, configure the following settings and click **Next**.

Setting	Value
Direction of protection	mgmt01vc01.sfo01.rainpole.local -> mgmt01vc51.lax01.rainpole.local
Protection group type	Individual VMs (vSphere Replication)



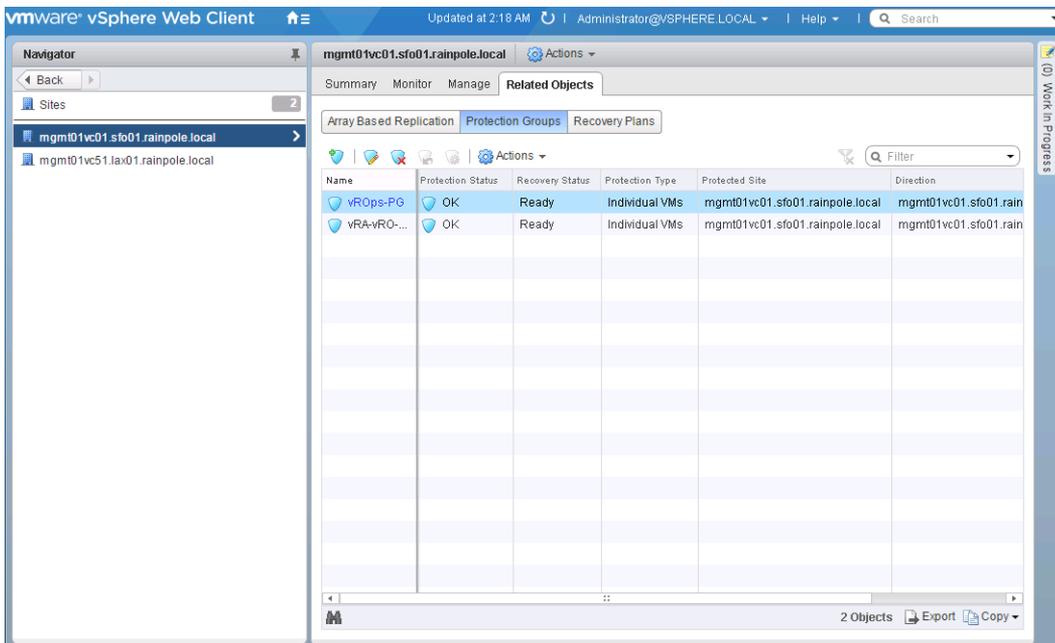
- 8 On the **Virtual machines** page, select the virtual machines of vRealize Automation, vRealize Orchestrator and the vRealize Business Server VM, from the list of replicated machines and click **Next**.

VM Name
vra01ims01a.rainpole.local
vra01ims01b.rainpole.local
vra01iws01a.rainpole.local
vra01iws01b.rainpole.local
vra01mssql01.rainpole.local
vra01svr01a.rainpole.local
vra01svr01b.rainpole.local
vra01dem01.rainpole.local
vra01dem02.rainpole.local
vra01vro01a.rainpole.local
vra01vro01b.rainpole.local
vra01bus01.rainpole.local



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

The vRA-vRO-vRB-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, create a recovery plan. You use this plan to configure dependencies between the virtual machines.

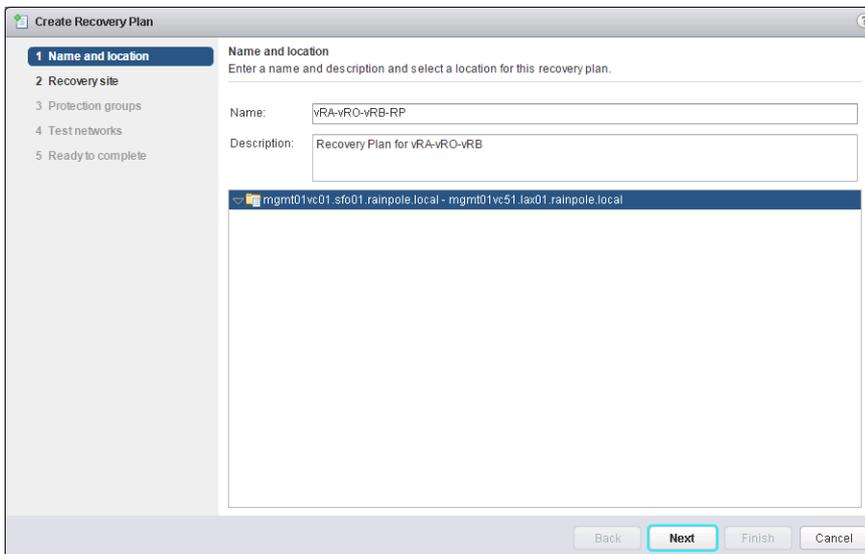
Procedure

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

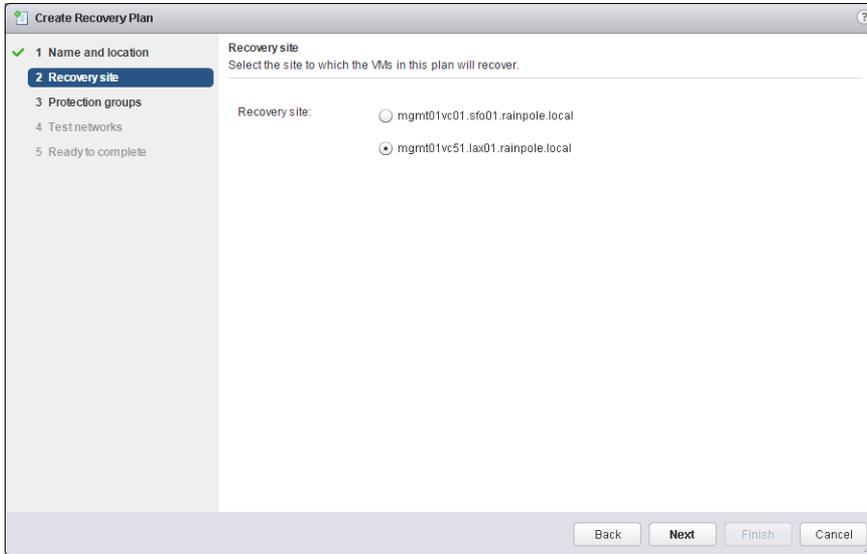
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.
- 3 On the Site Recovery home page, click **Sites** and select **mgmt01vc01.sfo01.rainpole.local**.
- 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	vRA-vRO-vRB-RP
Description	Recovery Plan for vRA-vRO-vRB
Site pair	mgmt01vc01.sfo01.rainpole.local - mgmt01vc51.lax01.rainpole.local

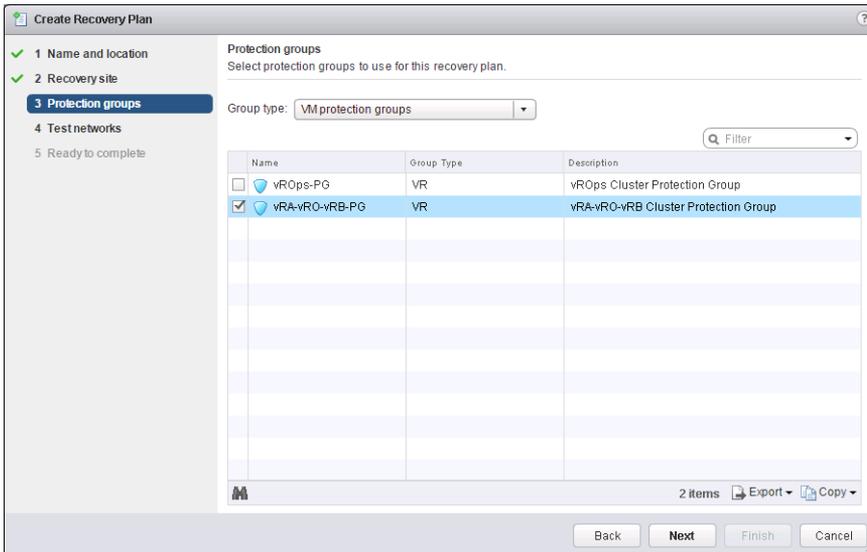


- 6 On the **Recovery Site** page, select **mgmt01vc51.lax01.rainpole.local** as the recovery site and click **Next**.

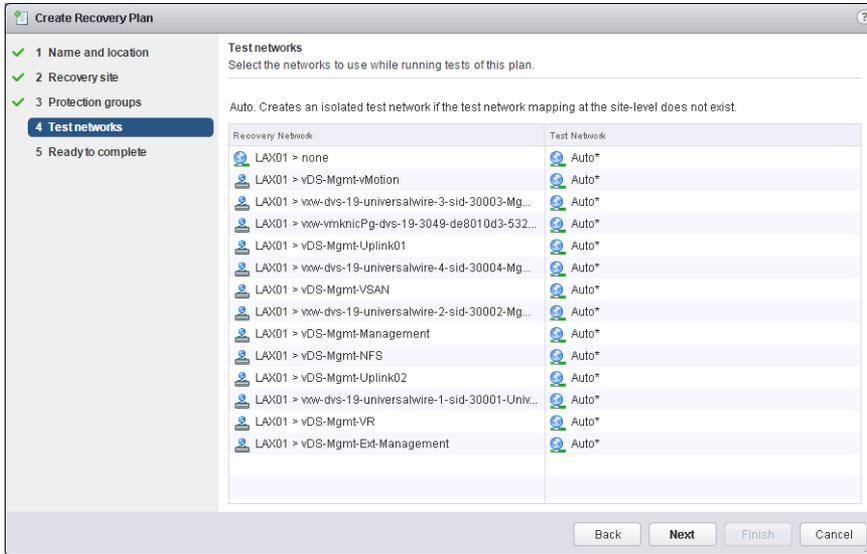


7 On the **Protection groups** page, select the protection group for the recovery plan and click **Next**.

Protection Group Setting	Value
Group type	VM protection groups
Protection group	vRA-vRO-vRB-PG

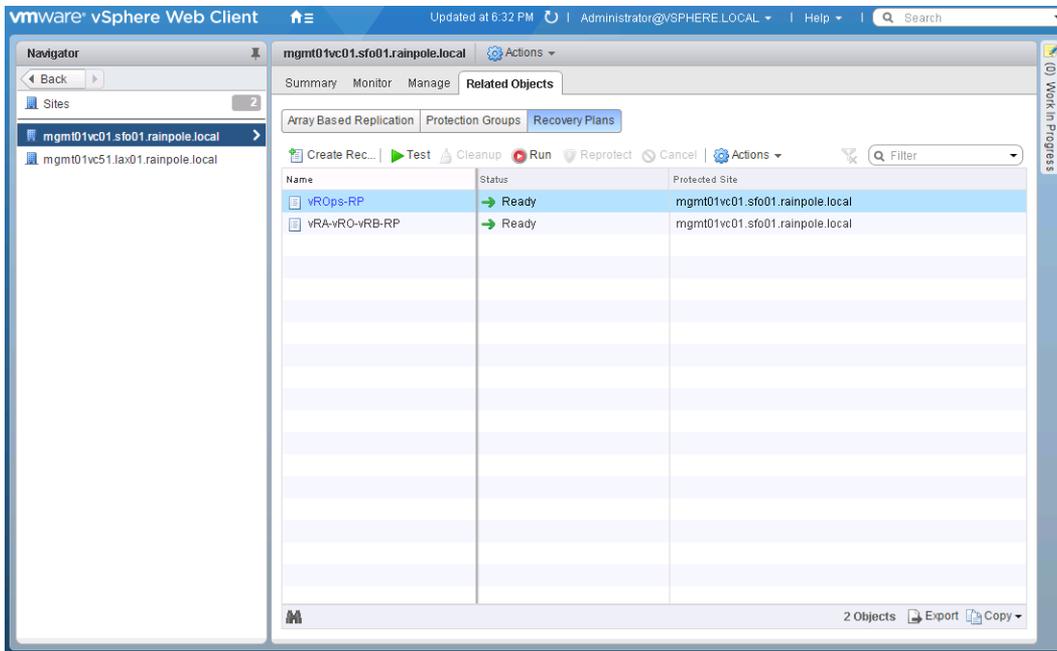


8 On the **Test networks** page, leave the default values and click **Next**.



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

The vRA-vRO-vRB-RP recovery plan appears in the list of the recovery plans available in Site Recovery Manager.



Customize the Recovery Plan for the Cloud Management Platform

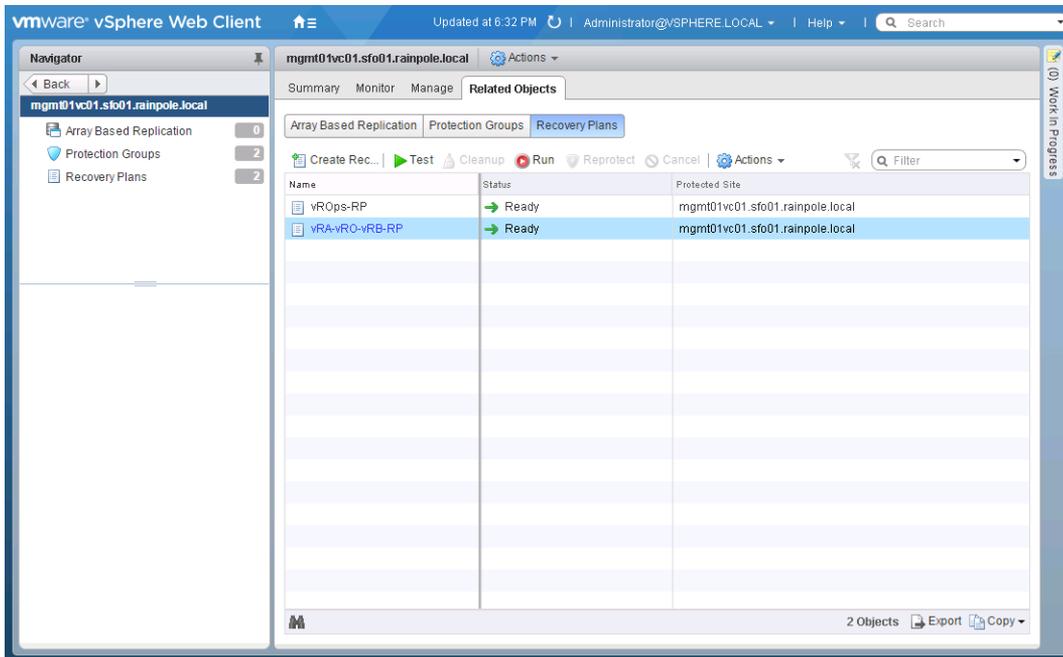
After you create the recovery plan for the Cloud Management Platform VMs, configure startup priority.

Procedure

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

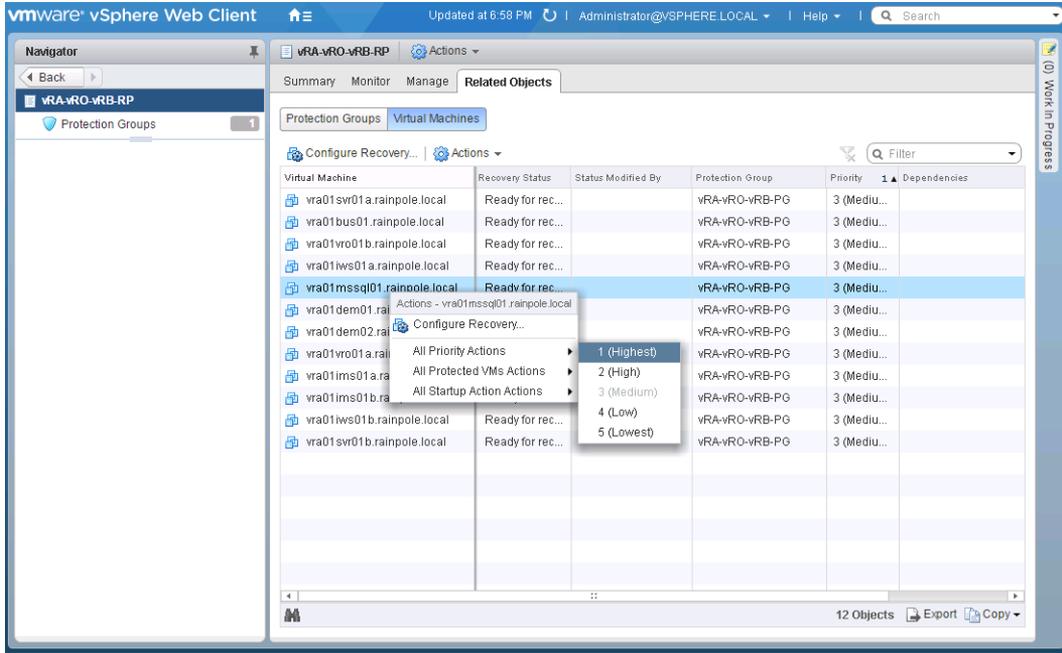
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Site Recovery**.
- 3 On the Site Recovery home page, click **Sites** and select the **mgmt01vc01.sfo01.rainpole.local** protected site.
- 4 On the **Related Objects** tab, click **Recovery Plans** and click the **vRA-vRO-vRB-RP** recovery plan to open it.



- 5 On the **Recovery Plan** page, click the **Related Objects** tab and click **Virtual Machines**.

- 6 Change the priority of the vra01mssql01.rainpole.local VM.
 - a Under **Virtual Machine**, right-click **vra01mssql01.rainpole.local** and select **All Priority Actions > 1 (Highest)**.

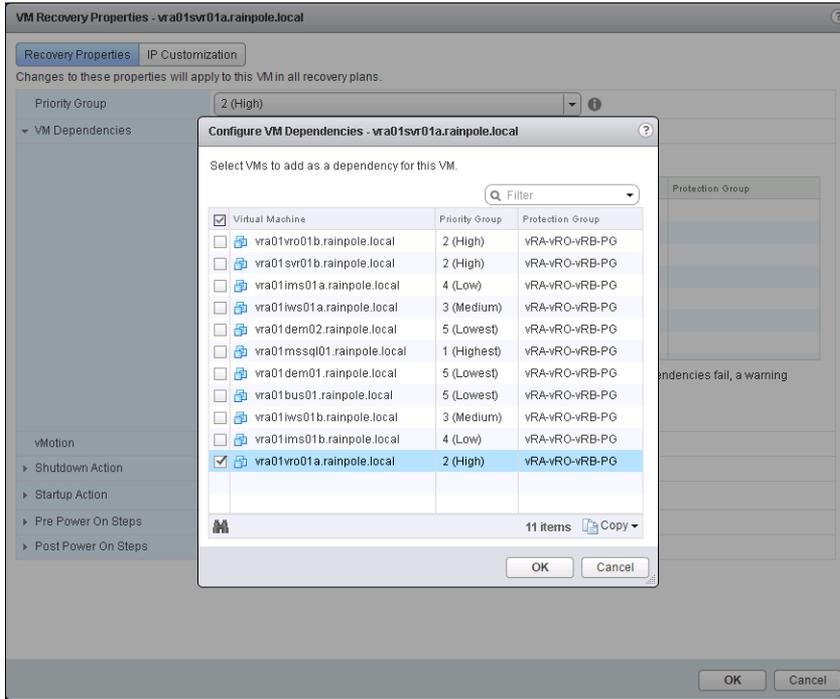


- b In the **Change Priority** dialog box, click **Yes** to confirm.
- 7 Repeat the previous step to reconfigure the priorities of the following VMs.

VM Name	Priority
vra01vro01a.rainpole.local	2
vra01vro01b.rainpole.local	2
vra01svr01a.rainpole.local	2
vra01svr01b.rainpole.local	2
vra01iws01a.rainpole.local	3
vra01iws01b.rainpole.local	3
vra01ims01a.rainpole.local	4
vra01ims01b.rainpole.local	4
vra01dem01.rainpole.local	5
vra01dem02.rainpole.local	5
vra01bus01.rainpole.local	5

8 Configure the VM dependencies.

- a Right-click **vra01svr01a.rainpole.local** 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 **vra01vro01a.rainpole.local**, click **OK**, and click **OK**.

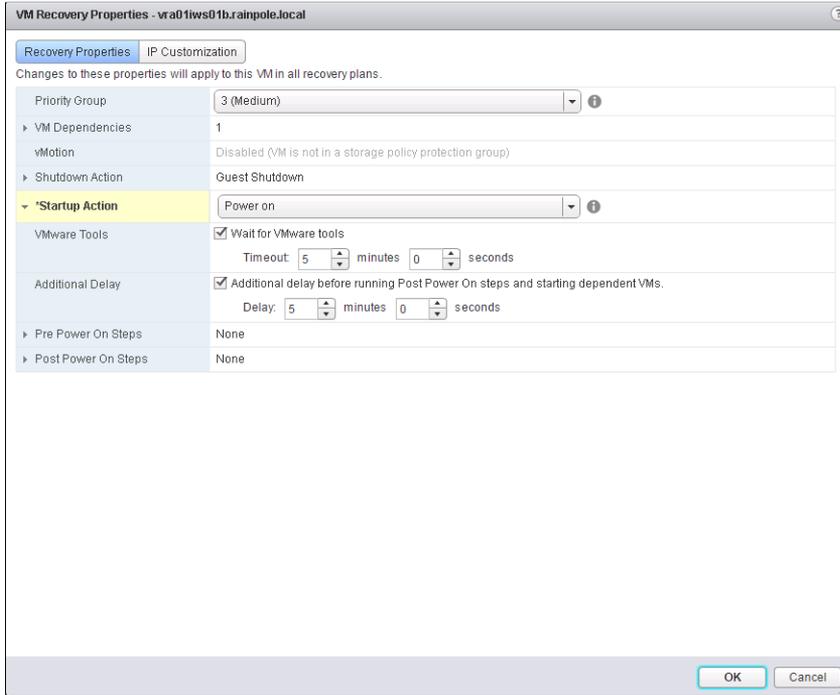


9 Repeat the previous step to configure additional VM dependencies for the following VMs.

VM Name	Priority	VM Dependencies
vra01svr01b.rainpole.local	2	Depends on vra01vro01a.rainpole.local
vra01iws01b.rainpole.local	3	Depends on vra01iws01a.rainpole.local
vra01ims01b.rainpole.local	4	Depends on vra01ims01a.rainpole.local

10 Configure additional startup delay for the second IaaS Web Server instance and the IaaS Manager Service.

- a Right-click **vra01iws01b.rainpole.local** and select **Configure Recovery**.
- b In the **VM Recovery Properties** dialog box, expand the **Startup Action** section and under **Additional Delay**, set **Delay** to 5 minutes, and click **OK**.



- c Repeat the step to configure additional delay of 5 minutes for the vra01ims01b.rainpole.local VM.

Duplicate the Anti-Affinity Rules for vRealize Automation and vRealize Orchestrator from Region A in Region B

VM anti-affinity rules are not retained during a Site Recovery Manager assisted recovery. You must duplicate the configured anti-affinity rules from Region A in Region B so that the rules apply after failover.

Table 3-1. Anti-Affinity Rules for the Cloud Management Platform

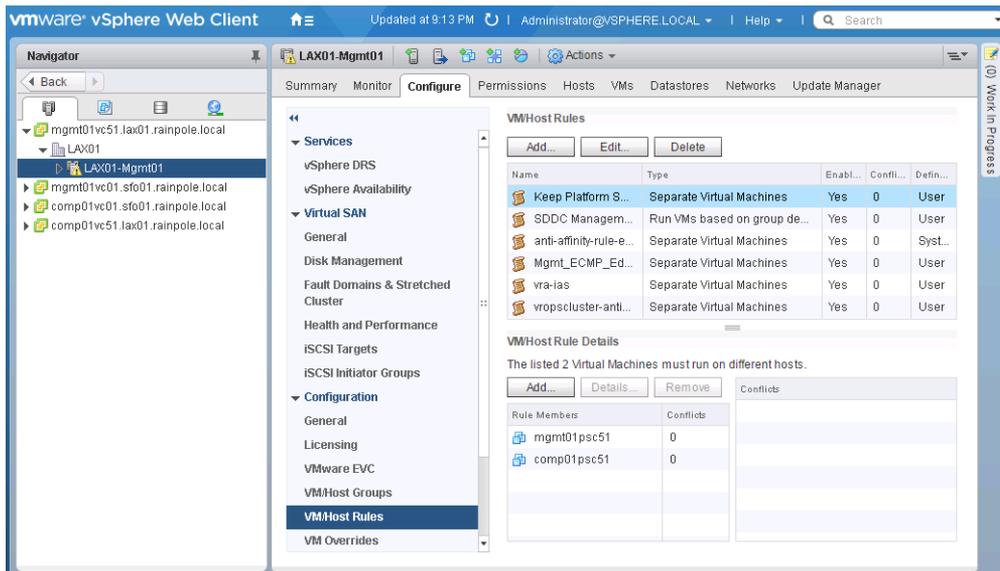
Name	Type	Members
vra-svr	Separate Virtual Machines	vra01svr01a.rainpole.local, vra01svr01b.rainpole.local
vra-dem	Separate Virtual Machines	vra01dem01.rainpole.local, vra01dem02.rainpole.local
vra-ims	Separate Virtual Machines	vra01ims01a.rainpole.local, vra01ims01b.rainpole.local
vra-iws	Separate Virtual Machines	vra01iws01a.rainpole.local, vra01iws01b.rainpole.local
vra-vro	Separate Virtual Machines	vra01vro01a.rainpole.local, vra01vro01b.rainpole.local

Procedure

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

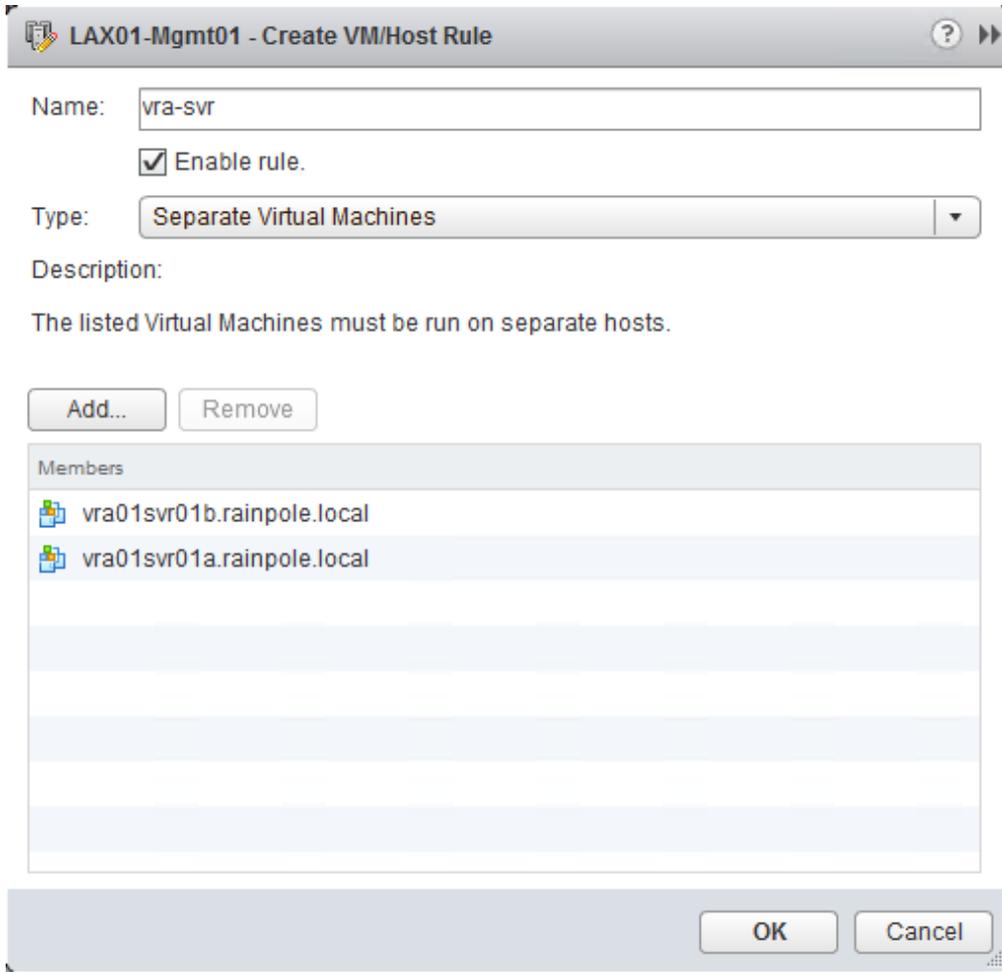
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Hosts and Clusters**.
- 3 Under mgmt01vc51.lax01.rainpole.local, expand **LAX01** and click **LAX01-Mgmt01**.
- 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 virtual appliances, click **OK**, and click **OK**.

Setting	Value
Name	vra-svr
Enable rule	Selected
Type	Separate Virtual Machines
Members	vra01svr01a.rainpole.local, vra01svr01b.rainpole.local



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

Test the Failover of Management Applications

Test the recovery plan for the management applications in the SDDC to eliminate potential problems during a future failover.

Test the Failover of vRealize Operations Manager

Test the recovery plan for vRealize Operations Manager to eliminate potential problems during a future failover.

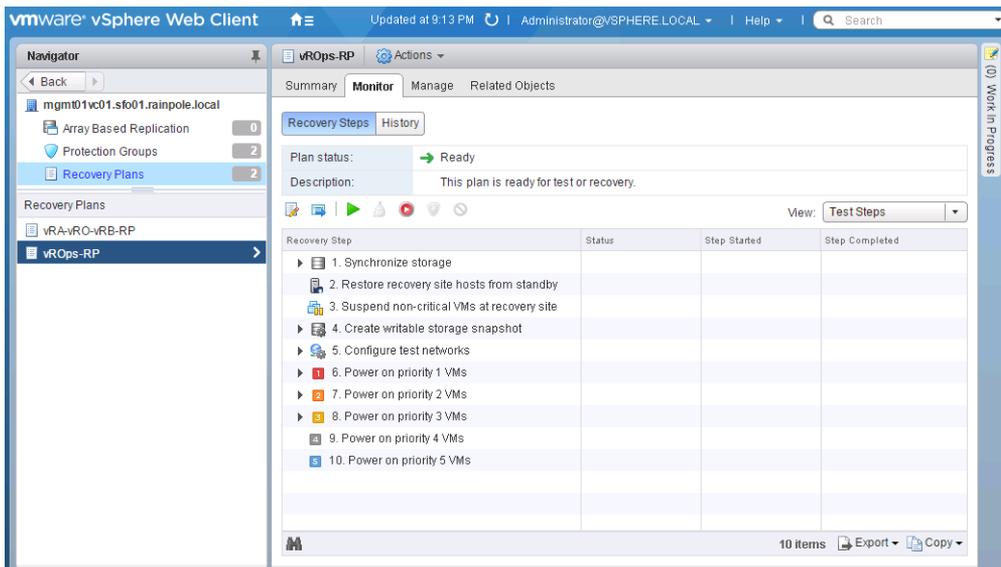
Site Recovery Manager runs the analytics virtual machines on the test network and on a temporary snapshot of replicated data in Region B.

Procedure

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

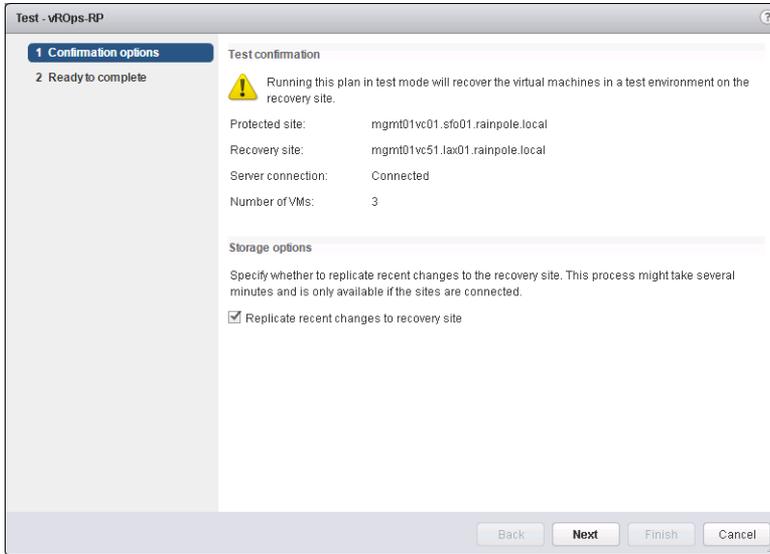
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Site Recovery**.
- 3 On the Site Recovery home page, click **Sites** and double-click the **mgmt01vc01.sfo01.rainpole.local** protected site.
- 4 If the **Log In Site** dialog box appears, re-authenticate by using the **administrator@vsphere.local** user name and the **vsphere_admin_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 Click the **Recovery Plans** and click the **vROps-RP** recovery plan.
- 6 On the **vROps-RP** page, click the **Monitor** tab and click **Recovery Steps**.
- 7 Click the **Test Recovery Plan** icon to run a test recovery.

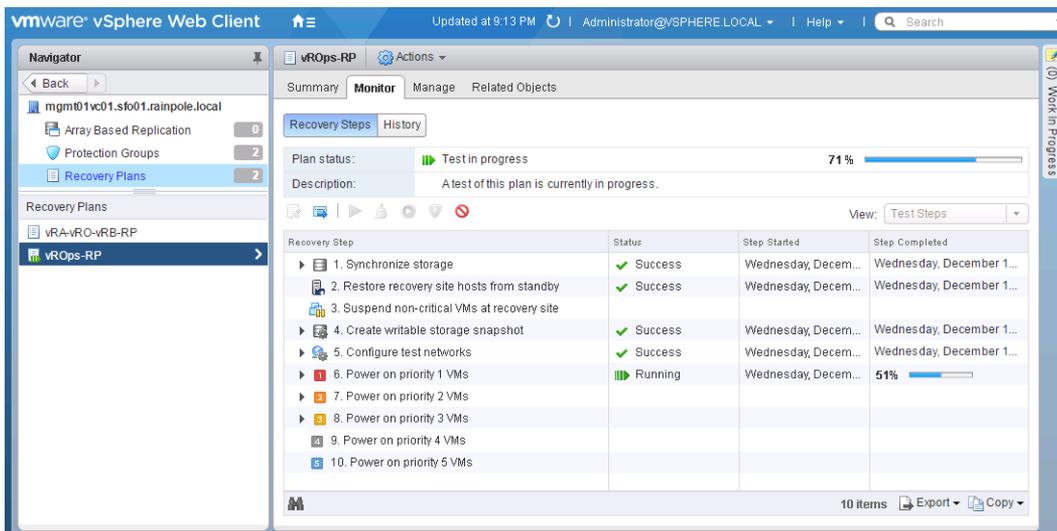


The **Test** wizard appears.

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

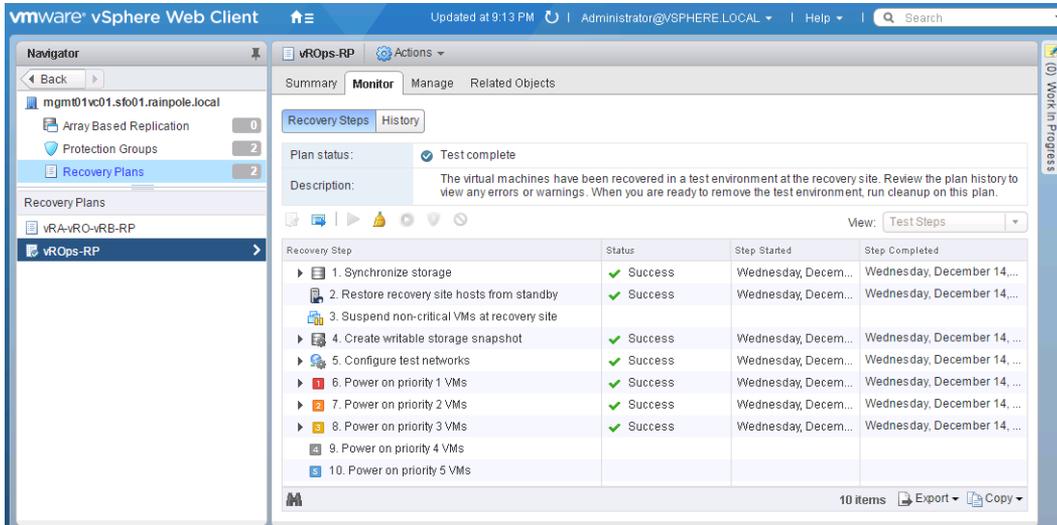


9 On the **Ready to complete** page, click **Finish** to start the test recovery.



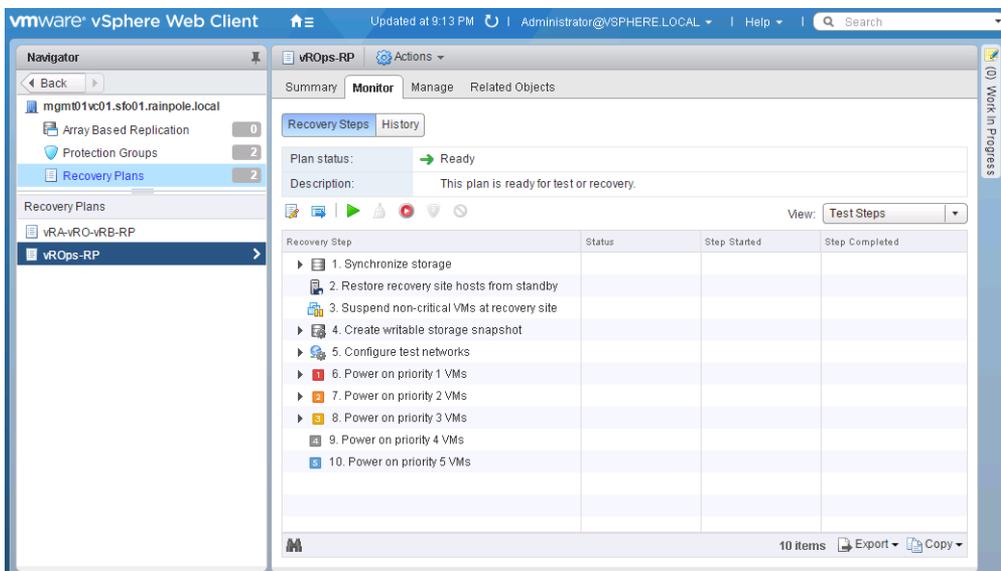
Test failover starts. You can follow the progress on the **Recovery Steps** page.

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.



Test the Failover of the Cloud Management Platform

Test the recovery plan for vRealize Automation, vRealize Orchestrator, and vRealize Business to validate the configuration.

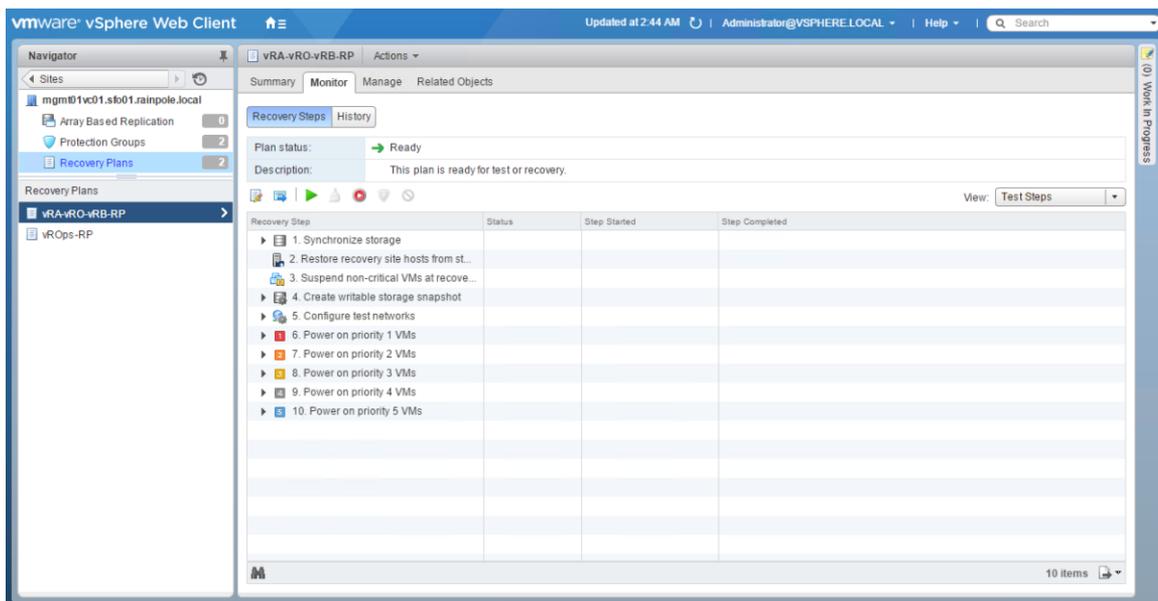
Site Recovery Manager runs the virtual machines on the test **network** and on a temporary snapshot of replicated data in Region B.

Procedure

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

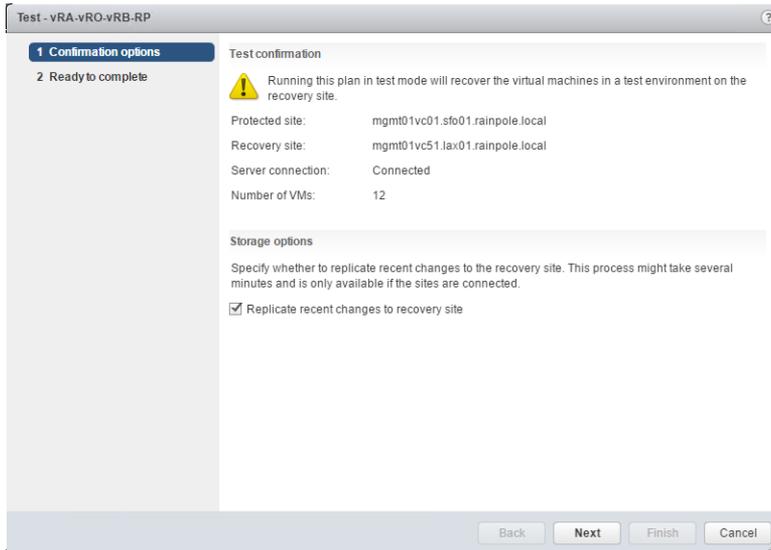
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the menu of the vSphere Web Client, select **Site Recovery**.
- 3 On the Site Recovery home page, click **Sites** and double-click the **mgmt01vc01.sfo01.rainpole.local** protected site.
- 4 If the **Log In Site** dialog box appears, re-authenticate by using the **administrator@vsphere.local** user name and the **vsphere_admin_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 Click **Recovery Plans** and click the **vRA-vRO-vRB-RP** recovery plan.
- 6 On the **vRA-vRO-vRB-RP** page, click the **Monitor** tab and click **Recovery Steps**.
- 7 Click the **Test Recovery Plan** icon to run a test recovery.

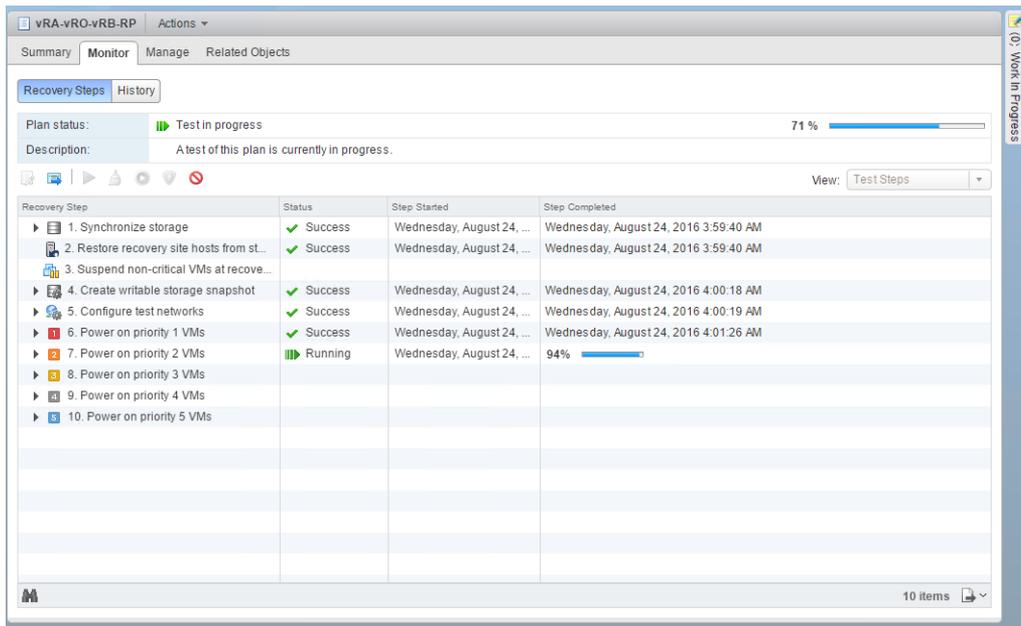


The **Test** wizard appears.

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



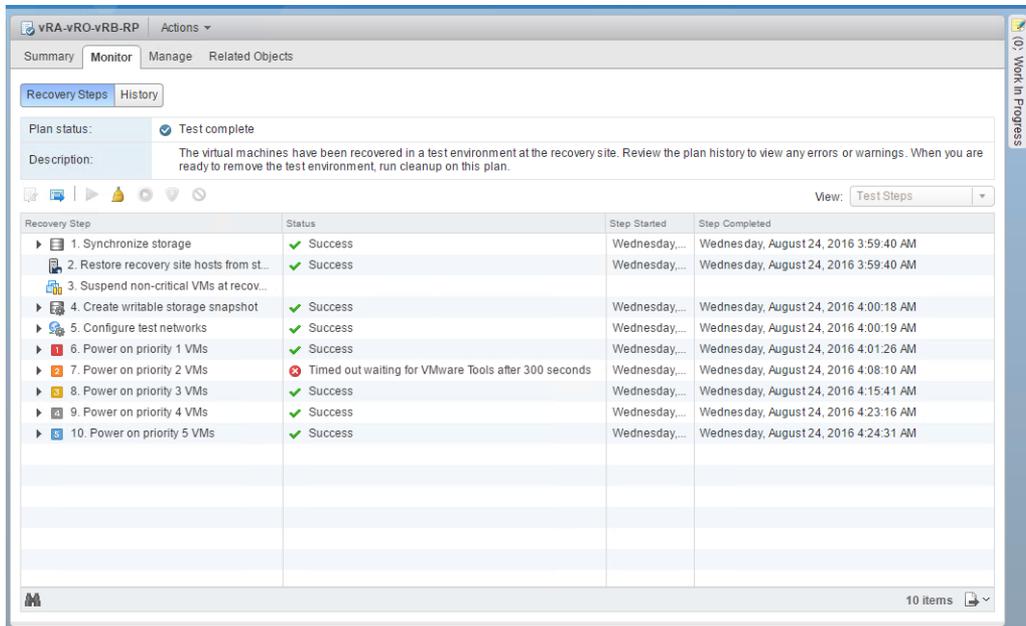
- On the **Ready to complete** page, click **Finish** to start the test recovery.



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

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

Note Because recovered VMs are using the Test network, VMware Tools in vra01svr01a.rainpole.local and vra01svr01b.rainpole.local VMs might not become online within the default timeout value. Increase the timeout value for the VMs 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.

Perform Planned Migration of Management Applications

After you have successfully configured and tested failover of the management applications, start the migration process from Region A to Region B.

Initiate a Planned Migration of vRealize Operations Manager

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

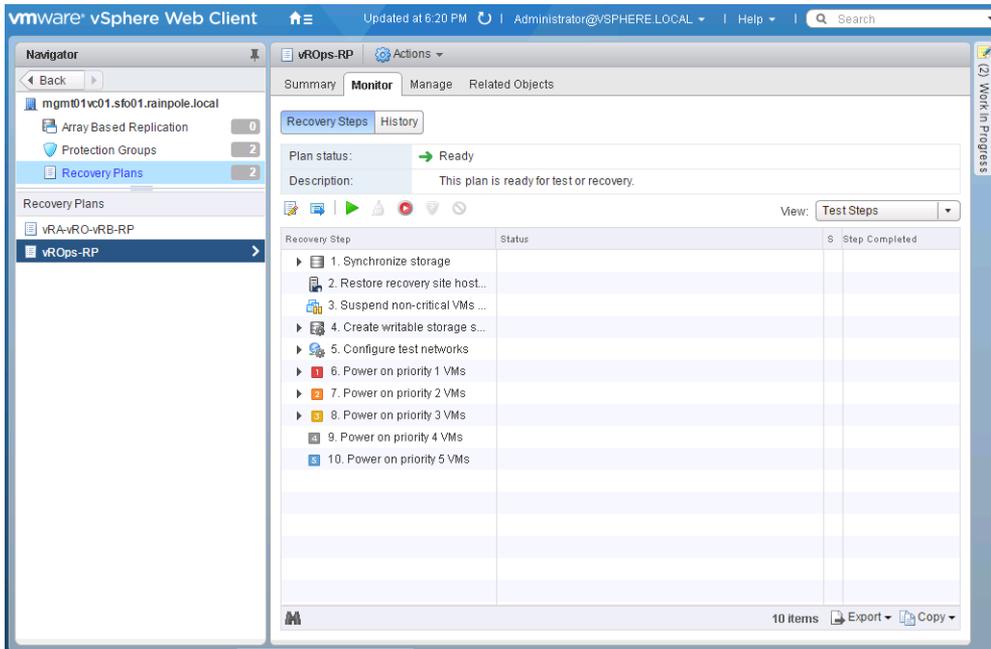
Procedure

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

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

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

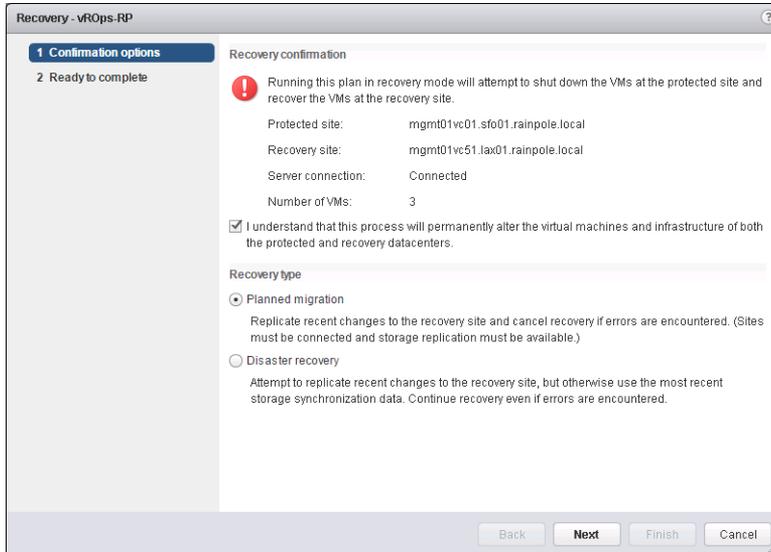
- 3 On the Site Recovery home page, click **Sites** and double-click the **mgmt01vc01.sfo01.rainpole.local** vCenter Server object to open its site configuration.
- 4 Click **Recovery Plans** and click the **vROps-RP** recovery plan.
- 5 On the **vROps-RP** page, click the **Monitor** tab and click **Recovery 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**.

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	Planned migration



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

What to do next

Perform the steps required to verify the operation of and reprotect the system.

- Verify that vRealize Operations Manager is up and functions flawlessly after failover. See *Validate vRealize Operations Manager* in the *Operational Verification* documentation.
- Prepare vRealize Operations Manager for failback by reprotecting the virtual machines of the analytics cluster in Site Recovery Manager. See [Reprotect vRealize Operations Manager](#).

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, vRealize Orchestrator and vRealize Business from Region A to Region B. You can also run a recovery plan under unplanned circumstances if Region A suffers an unforeseen event that might result in data loss.

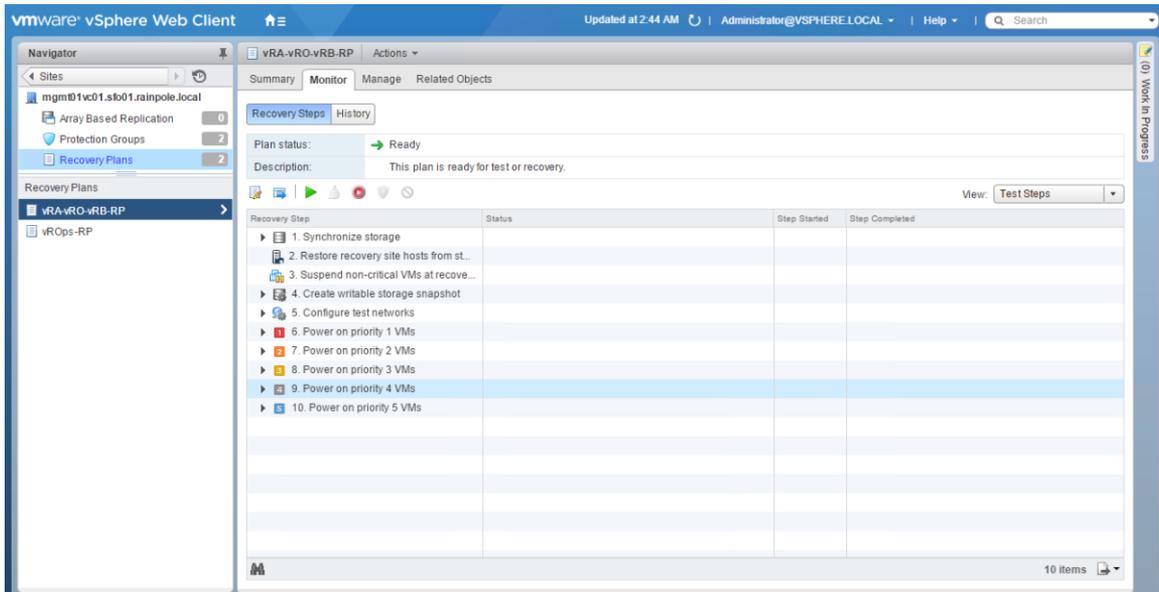
Procedure

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

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

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

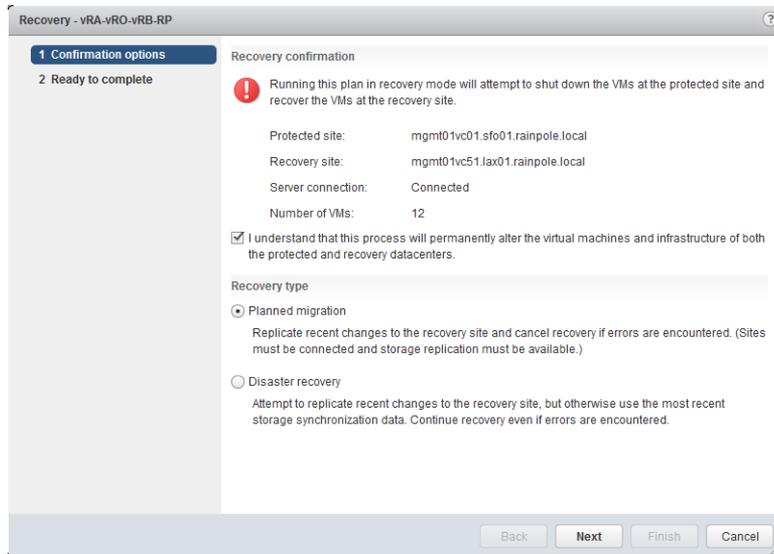
- 3 On the Site Recovery home page, click **Sites** and double-click the **mgmt01vc01.sfo01.rainpole.local** vCenter Server object to open its site configuration.
- 4 Click **Recovery Plans** and click the **vRA-vRO-vRB-RP** recovery plan.
- 5 On the **vRA-vRO-vRB-RP** page, click the **Monitor** tab 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**.

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	Planned migration



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

What to do next

Perform the steps required to verify the operation of and reprotect the system.

- Verify that vRealize Automation, vRealize Orchestrator and vRealize Business VMs are up and function flawlessly after failover. See *Validate the Cloud Management Platform* in the *Operational Verification* documentation.
- Prepare vRealize Automation, vRealize Orchestrator and vRealize Business Server for failback by reprotecting the virtual machines of the vRealize Automation components in Site Recovery Manager. See [Reprotect the Cloud Management Platform](#).

Perform Disaster Recovery of Management Applications

Prepare networking in Region B and perform failover of Realize Automation, vRealize Orchestrator, vRealize Business, and vRealize Operations Manager to Region B if Region A becomes unavailable in the event of a disaster or if you plan a graceful migration.

Reconfigure the NSX Instance for the Management Cluster in Region B

In the event of a site failure, when Region A becomes unavailable, prepare the network layer in Region B for failover of management applications.

Change the role of the NSX Manager to primary, deploy 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 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**, click **Installation**.
 - c On the **Management** tab, 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** confirmation dialog box, click **Yes**.
The NSX Manager gets the Transit role.
 - f On the **Management** tab, select the **172.17.11.65** instance again.
 - g From the **Actions** menu, select **Assign Primary Role**.
 - h In the **Assign Primary Role** confirmation dialog box, click **Yes**.
- 3 Configure an IP pool for the new universal controller cluster.
 - a In the **Navigator**, click **NSX Managers**.
 - b Under **NSX Managers**, click the **172.17.11.65** instance.
 - c On the **Manage** tab, click **Grouping Objects**, click **IP Pools**, and click the **Add New IP Pool** icon.
 - d In the **Add Static IP Pool** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	Mgmt01-NSXC51
Gateway	172.17.11.253
Prefix Length	24
Primary DNS	172.17.11.5
DNS Suffix	lax01.rainpole.local
Static IP Pool	172.17.11.118-172.17.11.120

4 Deploy the universal controller cluster in Region B.

- a In the **Navigator**, click **Networking & Security** and click **Installation**.
- b 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 **OK**.

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

Setting	Value
Name	nsx-controller-mgmt-51
NSX Manager	172.17.11.65
Datacenter	LAX01
Cluster/Resource Pool	LAX01-Mgmt01
Datastore	LAX01A-VSAN01-MGMT01
Connected To	vDS-Mgmt-Management
IP Pool	Mgmt01-NSXC51
Password	<i>mgmtnsx_controllers_password</i>
Confirm Password	<i>mgmtnsx_controllers_password</i>

- d After the **Status** of the controller node changes to Connected, deploy the remaining two NSX Controller nodes.

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

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** , and expand the **mgmt01vc51.lax01.rainpole.local** tree.
- b Select the **LAX01-Mgmt01** cluster and click the **Configure** tab.
- c Under **Configuration**, click **VM/Host Rules** and click **Add** under the **VM/Host Rules** section.
- d In the **LAX01-Mgmt01 - Create VM/Host Rule** dialog box, enter the following settings and click **Add**.

Setting	Value
Name	Mgmt_NSX_Controllers
Enable rule	Selected
Type	Separate Virtual Machines

- e In the **Add Rule Member** dialog box, select all three NSX Controller virtual machines, click **OK**, and click **OK**.

- 6 Use the update controller state mechanism on the NSX Manager to synchronize the state of the newly deployed controllers.
 - a From the **Home** menu of the vSphere Web Client, select **Networking & Security**.
 - b In the **Navigator**, click **Installation**.
 - c On the **Management** tab, select the **172.17.11.65** instance.
 - d From the **Actions** menu, select **Update Controller State**.
 - e In the **Update Controller State** confirmation dialog box, click **Yes**.

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

Because of the failure of Region A, dynamic routing in Region B is not available. Deploy a Control VM for the universal dynamic logical router UDLR01 in Region B to recover dynamic routing in the environment.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.
- 5 Double-click **UDLR01**.
- 6 Re-deploy the universal distributed logical router control VM and enable high availability.
 - 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
Datacenter	LAX01
Cluster/Resource Pool	LAX01-Mgmt01
Datastore	LAX01A-VSAN01-MGMT01

- d Click the **Add** icon to deploy another NSX Edge device with the same configuration.

7 Configure high availability for the control VM.

- a On the **Configuration** page for SFOMGMT-UDLR01, click **Change** under **HA Configuration**, configure the following settings and click **OK**.

Setting	Value
HA Status	Enable
Connected To	vDS-Mgmt-Management
Enable Logging	Selected

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

8 Configure the CLI credentials for the control VM.

- a In the **Navigator**, click **NSX Edges**.
- b Select **172.17.11.65** from the **NSX Manager** drop-down menu.
- c Right-click **SFOMGMT-UDLR01** 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	<i>udlr_admin_password</i>
Enable SSH access	Selected

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

Configure the universal distributed logical router UDLR01 and NSX Edges LAXMGMT-ESG01 and LAXMGMT-ESG02 to use dynamic routing in Region B.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 From the **Home** menu of the vSphere Web Client, select **Networking & Security** and click **NSX Edges** in the **Navigator**.
- 3 Select **172.17.11.65** from the **NSX Manager** drop-down menu.

- 4 Verify the routing configuration for the universal distributed logical router.
 - a Double-click **UDLR01**.
 - b Click the **Manage** tab and click **Routing**.
 - c Verify that **ECMP** is **Enabled**.
 - d Verify that **192.168.10.3** (Uplink) is configured as the **Router ID** under **Dynamic Routing Configuration**.

- 5 On the left side, select **BGP** to verify BGP configuration .
 - a On the **BGP** page, verify the following settings.

Setting	Value
Status	Enabled
Local AS	65003
Graceful Restart	Enabled

- b Select **192.168.10.50** (LAXMGMT-ESG01) neighbor and click **Edit** icon.
- c In the **Edit Neighbour** 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	LAXMGMT-ESG01 Value
IP Address	192.168.10.50
Forwarding Address	192.168.10.3
Protocol Address	192.168.10.4
Remote AS	65003
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	<i>BGP_password</i>

- d On the **BGP** page, select **192.168.10.51** (LAXMGMT-ESG02) neighbor, click **Edit** to change the following settings for the second ECMP NSX Edge, and click **OK**.

Setting	LAXMGMT-ESG02 Value
IP Address	192.168.10.51
Forwarding Address	192.168.10.3
Protocol Address	192.168.10.4
Remote AS	65003
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	<i>BGP_password</i>

- e Click **Publish Changes**.

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

- a Verify the following settings under **Route Redistribution Status**.

Setting	Value
OSPF	Deselected
BGP	Selected

- b Verify the following settings under **Route Redistribution table**.

Setting	Value
Learner	BGP
From	Connected
Perfix	Any
Action	Permit

- 7 Reconfigure the routing and weight value of LAXMGMT-ESG01 and LAXMGMT-ESG02 edges.

- a In the **Navigator**, click **NSX Edges**.
- b Select **172.17.11.65** from the **NSX Manager** drop-down menu.
- c Double-click **LAXMGMT-ESG01**.
- d Click the **Manage** tab and click **Routing**.
- 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 Neighbour** dialog box, change **Weight** value to **60** and click **OK**.
- g Click **Publish Changes**.
- h Repeat the step for the LAXMGMT-ESG02 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.

Procedure

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

- a Open an SSH connection to **UDLR01**.
- b Log in using the following credentials.

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

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 (LAXMGMT-ESG01) and 192.168.10.51 (LAXMGMT-ESG02).

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 B

Enable the network connectivity of LAXMGMT-LB01 load balancer.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.65** from the **NSX Manager** drop-down menu.
- 5 Double-click the **LAXMGMT-LB01** 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 of vRealize Operations Manager in Region B

If a disaster event occurs in Region A, initiate the Disaster Recovery of vRealize Operations Manager to fail over it 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Site Recovery**.
- 3 On the Site Recovery home page, click **Sites** and double-click the **mgmt01vc51.lax01.rainpole.local** vCenter Server object to open its site configuration.
- 4 Click **Recovery Plans** and click the **vROps-RP** recovery plan.
- 5 On the **vROps-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 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 vRealize Operations Manager failover.
 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 the operation of and reprotect the system.

- 1 Verify that vRealize Operations Manager is up and functions flawlessly after failover. See *Validate vRealize Operations Manager* in the *Operational Verification* documentation.
- 2 Prepare vRealize Operations Manager for failback by reprotecting the virtual machines of the analytics cluster in Site Recovery Manager. See [Reprotect vRealize Operations Manager](#).

Initiate Disaster Recovery of the Cloud Management Platform in Region B

In the event of a disaster in Region A, initiate the Disaster Recovery of vRealize Automation, vRealize Orchestrator and vRealize Business components to fail over them 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Site Recovery**.
- 3 On the Site Recovery home page, click **Sites** and double-click the **mgmt01vc51.lax01.rainpole.local** vCenter Server object to open its site configuration.

- 4 Click **Recovery Plans** and click the **vRA-vRO-vRB-RP** recovery plan.
- 5 On the **vRA-vRO-vRB-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

Perform the steps required to verify the operation of and reprotect the system.

- 1 Verify that vRealize Automation, vRealize Orchestrator and vRealize Business VMs are up and function flawlessly after failover. See *Validate the Cloud Management Platform* in the *Operational Verification* documentation.
- 2 Prepare vRealize Automation, vRealize Orchestrator and vRealize Business for failback by reprotecting the virtual machines of the cloud management platform in Site Recovery Manager. See [Reprotect the Cloud Management Platform](#).

Post-Failover Configuration of Management Applications

After failover of the cloud management platform and vRealize Operations Manager, you must perform certain tasks to ensure that applications perform as expected.

Procedure

- 1 [Configure the NSX Controllers and the 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. You can use a REST client, such as the RESTClient add-on for Firefox, to enable log forwarding.

- 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 Reconfigure the NSX Instance for the Management Cluster in Region A after Failover

After Region A comes back online, you must perform additional configuration of the networking layer to avoid conflicts.

Configure the NSX Controllers and the 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. You can use a REST client, such as the RESTClient add-on for Firefox, to enable log forwarding.

Prerequisites

On a Windows host that has access to your data center, install a REST client, such as the RESTClient add-on for Firefox.

Procedure

- 1 Log in to the Windows host that has access to your data center.
- 2 In a Firefox browser, go to `chrome://restclient/content/restclient.html`.
- 3 Specify the request headers for requests to the NSX Manager.
 - a From the **Authentication** drop-down menu, select **Basic Authentication**.
 - b In the **Basic Authorization** dialog box, enter the following credentials, select **Remember me** and click **Okay**.

Authentication Attribute	Value
Username	admin
Password	<i>mngnsx_admin_password</i>

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

- c From the **Headers** drop-down menu, select **Custom Header**.
- d In the **Request Header** dialog box, enter the following header details and click **Okay**.

Request Header Attribute	Value
Name	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 In the **Request** pane, from the **Method** drop-down menu, select **GET**.
 - b In the **URL** text box, enter `https://mgmt01nsxm51.lax01.rainpole.local/api/2.0/vdn/controller` and click **Send**.

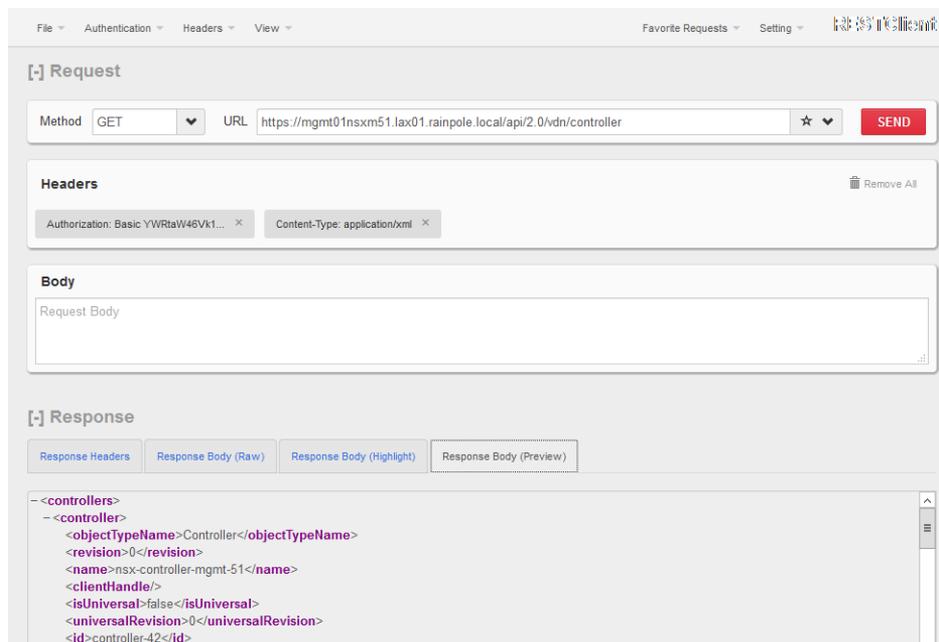
The RESTClient sends a query to the NSX Manager about the installed NSX controllers.

- c After the NSX Manager sends a response back, click the **Response Body (Preview)** tab under **Response**.

The response body contains a root <controllers> XML element, which 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-2`.



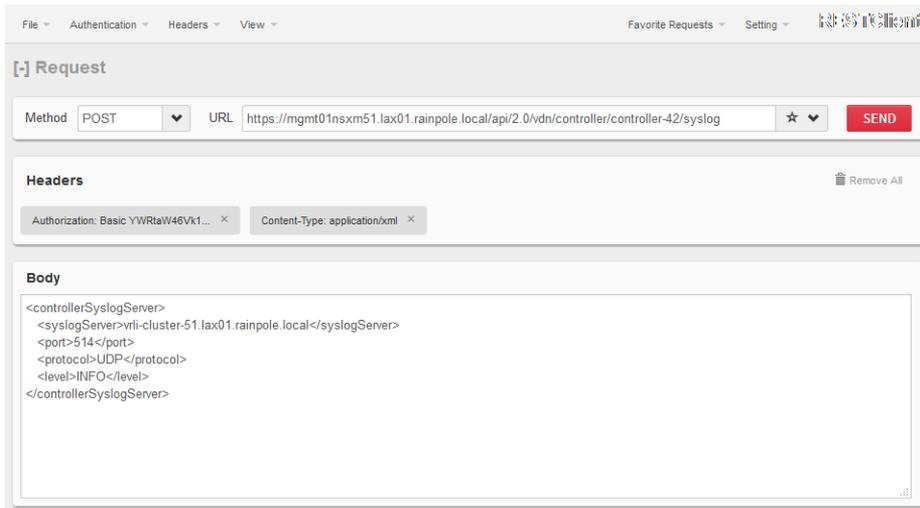
- 5 For each NSX Controller, send a request to configure vRealize Log Insight as a remote syslog server.
 - a In the **Request** pane, from the **Method** drop-down menu, select **POST**, and in the **URL** text box, enter the following URL.

NSX Manager	NSX Controller in the Controller Cluster	POST URL
NSX Manager for the management cluster	NSX Controller 1	https://mgmt01nsxm51.lax01.rainpole.local/api/2.0/vdn/controller/<controller1-id>/syslog
	NSX Controller 2	https://mgmt01nsxm51.lax01.rainpole.local/api/2.0/vdn/controller/<controller2-id>/syslog
	NSX Controller 3	https://mgmt01nsxm51.lax01.rainpole.local/api/2.0/vdn/controller/<controller3-id>/syslog

- b In the **Request** pane, paste the following request body in the **Body** text box and click **Send**.

```
<controllerSyslogServer>
  <syslogServer>vrli-cluster-51.lax01.rainpole.local</syslogServer>
  <port>514</port>
  <protocol>UDP</protocol>
  <level>INFO</level>
</controllerSyslogServer>
```

- c Repeat the steps for the next NSX Controller.

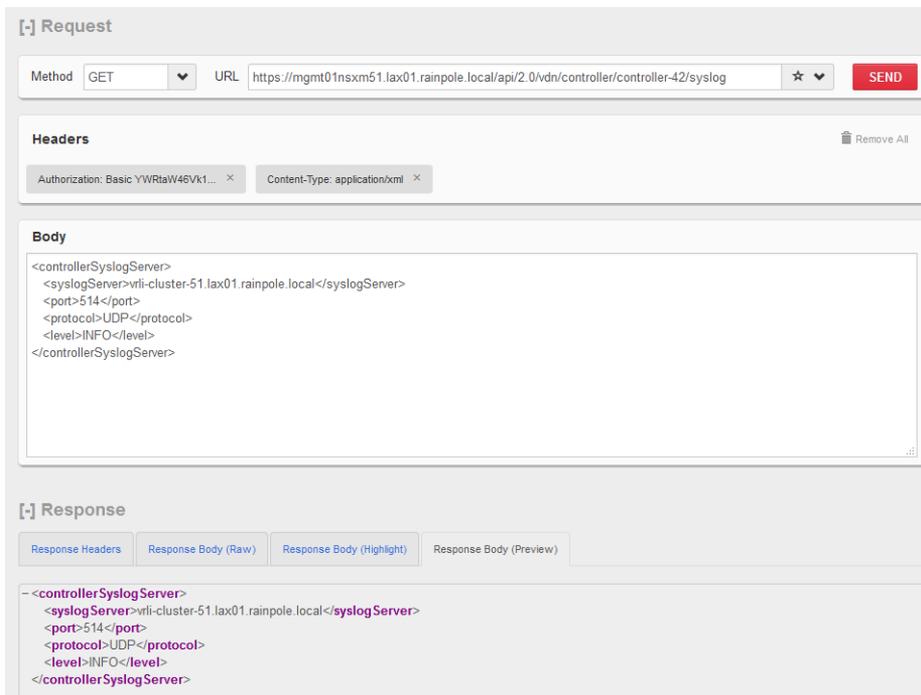


6 Verify the syslog configuration on each NSX Controller.

- a In the **Request** pane, from the **Method** drop-down menu, select **GET**, and in the **URL** text box, enter the controller-specific syslog URL from [Step 5](#), and click the **SEND** button.
- b After the NSX Manager returns a response, click the **Response Body (Preview)** 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 `vrl-cluster-51.lax01.rainpole.local`.
- d Repeat the steps for the next NSX Controller.



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

- a Open a Web browser and go to <https://mgmt01vc51.lax01.rainpole.local/vsphere-client>.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 8 Configure the newly deployed UDLR control VM 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 **UDLR01**.
 - 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, in the **Syslog Server 1** text box, enter **192.168.32.10** and from the **Protocol** drop-down menu, select **udp**.
 - h Click **OK**.

Update the vRealize Log Insight Logging Address after Failover

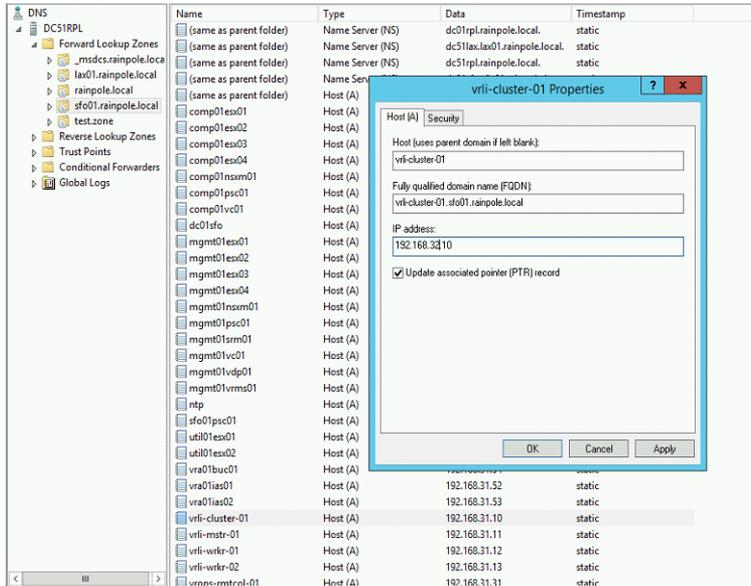
After you fail over the management applications in the SDDC to Region B, update the address configured on the management applications for vRealize Log Insight. All management applications are still configured to send logs to the vRealize Log Insight instance in Region A.

You update the DNS entry for `dc51rpl.rainpole.local` to point to the IP address `192.168.32.10` of `vrli-cluster-51.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 `vrli-cluster-01` record on the right side.
- 4 Double-click the **vrli-cluster-01** 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)	vrli-cluster-01.sfo01.rainpole.local
IP Address	192.168.32.10
Update associated pointer (PTR) record	Selected



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

After Region A comes back online, you must perform additional configuration of the networking layer to avoid conflicts.

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://mgmt01vc01.sfo01.rainpole.local/vsphere-client>.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Networking & Security**.
- 3 In the **Navigator**, click **Installation** and click the **Management** tab.
You see that both NSX Managers 172.16.11.65 and 172.17.11.65 are assigned the primary role.
- 4 Force the removal of the registered secondary NSX Manager before removing the primary role.
 - a Select the **172.16.11.65** instance, and select **Actions > Remove Secondary NSX Manager**.
 - b Select the **Perform operation even if the NSX manage is inaccessible** check box and click **OK**.

- 5 Demote the original primary site NSX Manager 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.
- 6 Delete the NSX controllers in the primary site.
 - a Select the **nsx-controller-mgmt-01** node and click **Delete**.
 - b In the **Delete Controller** confirmation dialog box, click **Yes**.
 - c Repeat the step to delete the remaining two NSX Controller nodes.
 - d Select **Forcefully remove the controller** when you delete the last controller.
- 7 Delete the UDLR01 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 **UDLR01** and click **Delete**.
 - d In the **Delete NSX Edge** confirmation dialog box, click **Yes**.
- 8 Assign the Region A management cluster NSX Manager the secondary role to the already promoted primary NSX Manager in Region B.
 - a In the **Navigator**, click **Installation**.
 - b On the **Management** tab select the primary **172.17.11.65** instance.
 - c Select **Actions > Add Secondary NSX Manager**.
 - d In the **Add secondary NSX Manager** dialog box, enter the following settings and click **OK**.

Setting	Value
NSX Manager	172.16.11.65
User Name	admin
Password	<i>mgmtnsx_admin_password</i>
Confirm Password	<i>mgmtnsx_admin_password</i>

- e In the **Trust Certificate confirmation** dialog box, click **Yes**.
- 9 Disable network connectivity for the NSX load balancer in Region A.
 - a In the **Navigator**, click **NSX Edges**.
 - b Select **172.16.11.65** from the **NSX Manager** drop-down menu.
 - c Double-click the **SFOMGMT-LB01** 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**.

10 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 **UDLR01**.
- 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	SFOMGMT-ESG01 Value	SFOMGMT-ESG02 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	<i>BGP_password</i>	<i>BGP_password</i>

- 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 **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
MTU	9000
Admin Distance	1

- k Click **Publish Changes**.

11 Reconfigure the weight value of SFOMGMT-ESG01 and SFOMGMT-ESG02 edges.

- a In the **Navigator**, click **NSX Edges**.
- b Select **172.16.11.65** from the **NSX Manager** drop-down menu.

- c Double-click **SFOMGMT-ESG01**.
- d Click the **Manage** tab and click **Routing**.
- e On the left, select **BGP**, select the **192.168.10.4** neighbour and click **Edit**.
- f In the **Edit Neighbour** dialog box, change the **Weight** value to **10** and click **OK**.
- g Click **Publish Changes**.
- h Repeat the step for the SFOMGMT-ESG02 edge.

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

- a Log in to the SFOMGMT-ESG01 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 will display `Established UP` if you have successfully peered with UDLR01.
- c Run the `show ip route` command to verify that you are receiving routes using BGP.
- d Repeat the step for the SFOMGMT-ESG02 NSX Edge device.

Failback of the SDDC Management Applications

4

Configure and perform failback of the management applications in the SDDC from the protected region, Region B, to the recovery region, Region A.

You failback the following management components:

- Analytics cluster of vRealize Operations Manager
- Primary components of vRealize Automation, vRealize Orchestrator, and vRealize Business

The remote collector nodes of vRealize Operations Manager are not failed back. You deploy a separate pair of remote collectors in each region in an application isolated network. The vSphere Proxy Agents of vRealize Automation and the vRealize Business data collector are not failed back. You deploy a separate pair of agents and collector in each region in an application isolated network.

Procedure

1 [Test the Failback of Management Applications](#)

Test the recovery plan for the management applications in the SDDC to eliminate potential problems during a future failback.

2 [Perform Failback as Planned Migration of Management Applications](#)

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

3 [Perform Failback as Disaster Recovery of Management Applications](#)

Prepare networking in Region A and perform failback of vRealize Automation, vRealize Orchestrator, vRealize Business, and vRealize Operations Manager to Region A if Region B becomes unavailable in the event of a disaster or if you plan a graceful migration.

4 [Post-Failback Configuration of Management Applications](#)

After failback of the cloud management platform and vRealize Operations Manager, you must perform certain tasks to ensure that applications perform as expected.

Test the Failback of Management Applications

Test the recovery plan for the management applications in the SDDC to eliminate potential problems during a future failback.

Test the Failback of vRealize Operations Manager

Test the recovery plan for vRealize Operations Manager to prevent potential problems during a future failback.

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

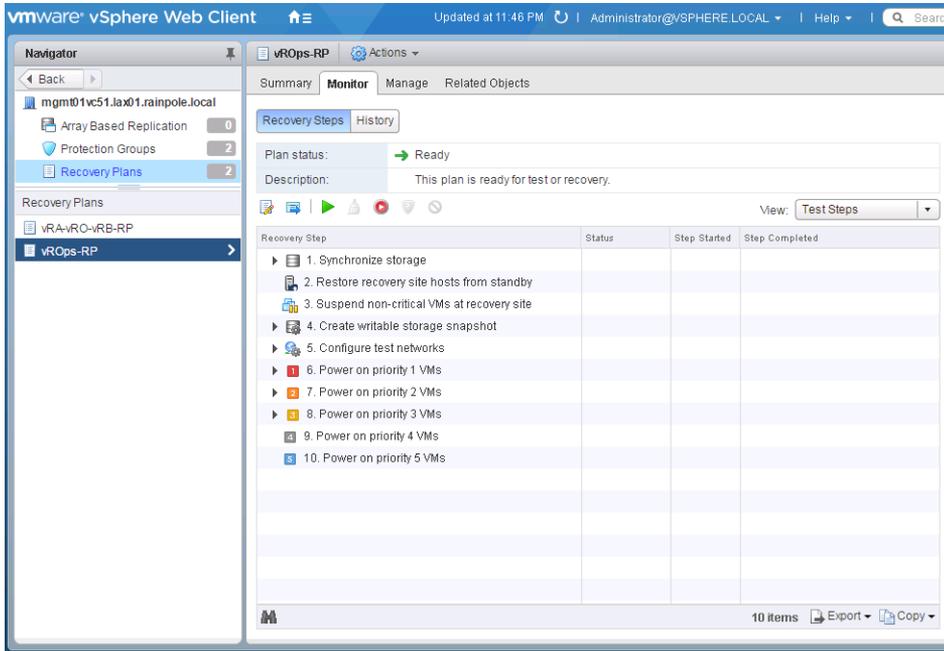
Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

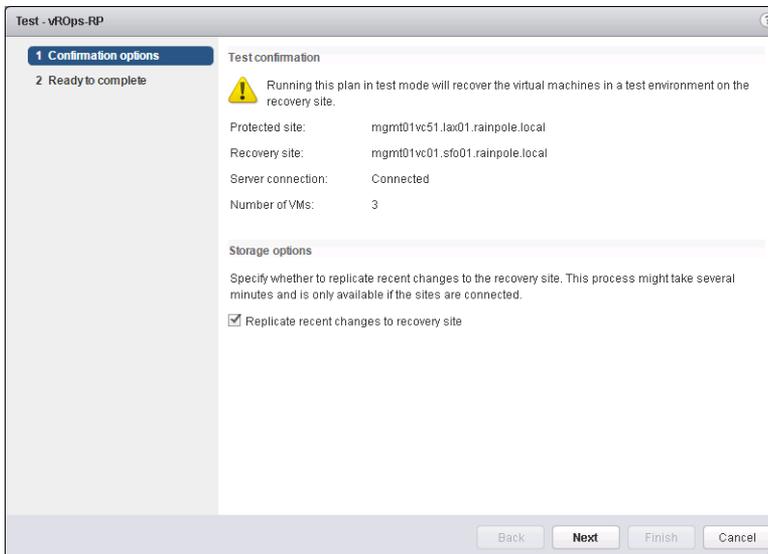
- 2 From the **Home** menu, select **Site Recovery**.
- 3 On the Site Recovery home page, click **Sites** and double-click the **mgmt01vc51.lax01.rainpole.local** protected site.
- 4 If the **Log In Site** dialog box appears, re-authenticate by using the **administrator@vsphere.local** user name and the *vsphere_admin_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 Click **Recovery Plans** and click the **vROps-RP** recovery plan.
- 6 On the **vROps-RP** page, click the **Monitor** tab and click **Recovery Steps**.
- 7 Click the **Test Recovery Plan** icon to run a test recovery.

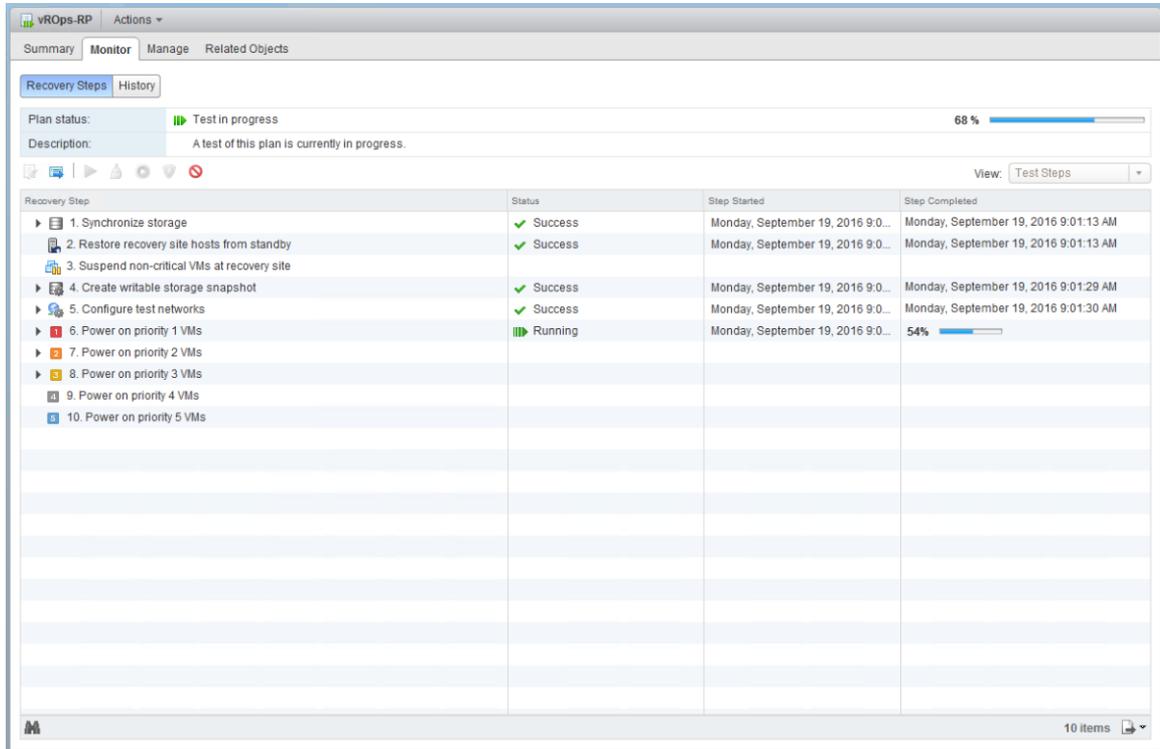


The **Test** wizard appears.

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

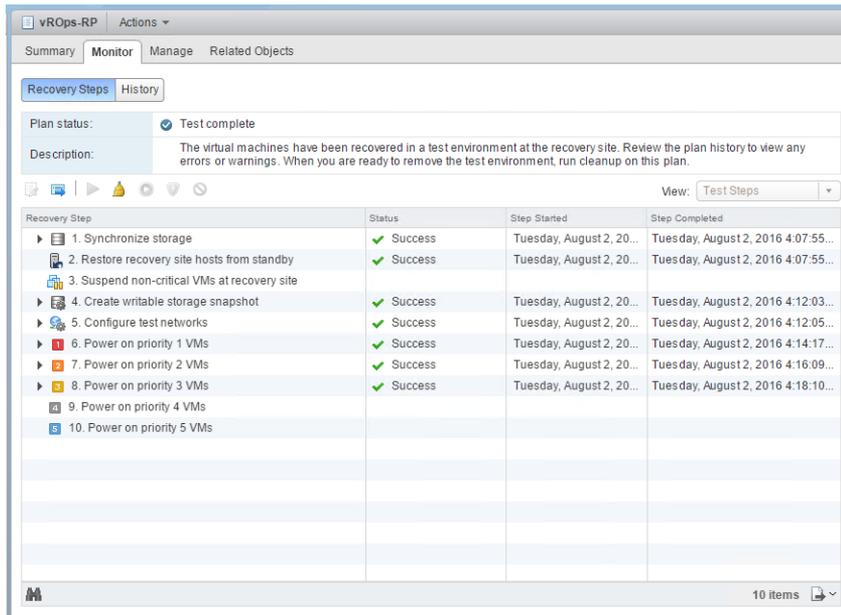


- On the **Ready to complete** page, click **Finish** to start the test recovery.



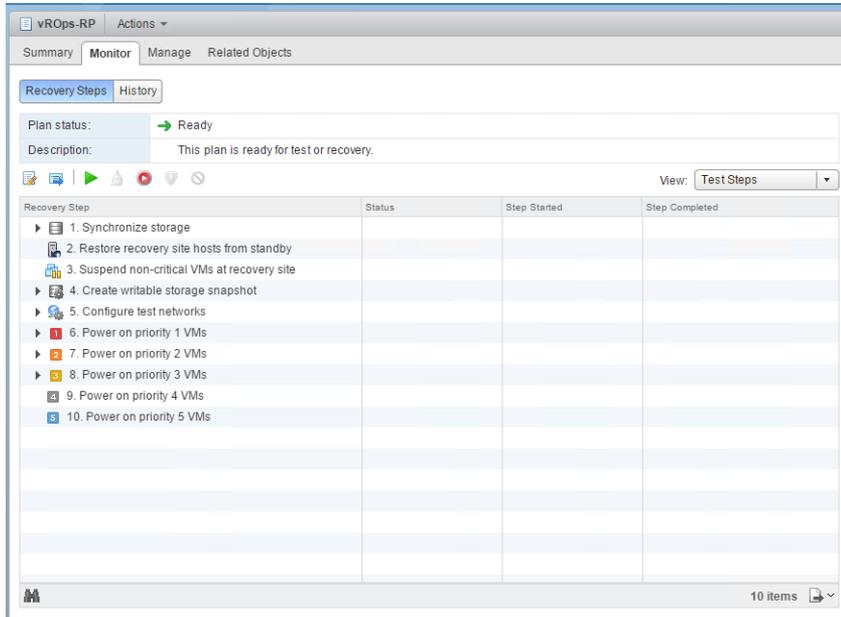
Test failback starts. You can follow the progress on the **Recovery Steps** page.

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



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

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



Test the Failback of the Cloud Management Platform

Test the recovery plan for vRealize Automation, vRealize Orchestrator and vRealize Business to validate the configuration.

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

Procedure

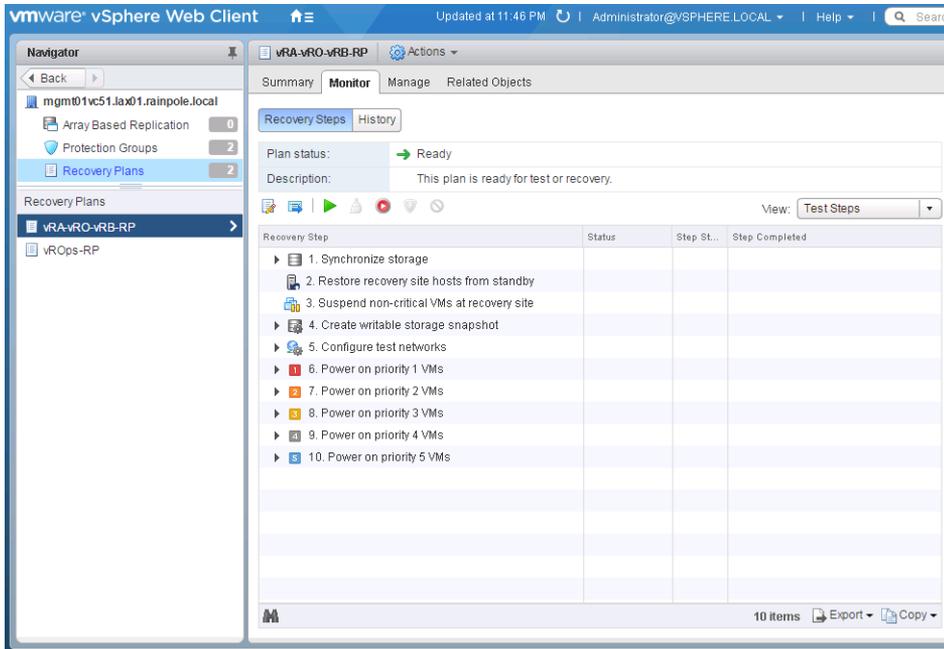
- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Site Recovery**
- 3 On the Site Recovery Home page, click **Sites** and select the **mgmt01vc51.lax01.rainpole.local** protected site.
- 4 If the **Log In Site** dialog box appears, re-authenticate by using the **administrator@vsphere.local** user name and the *vsphere_admin_password* password.

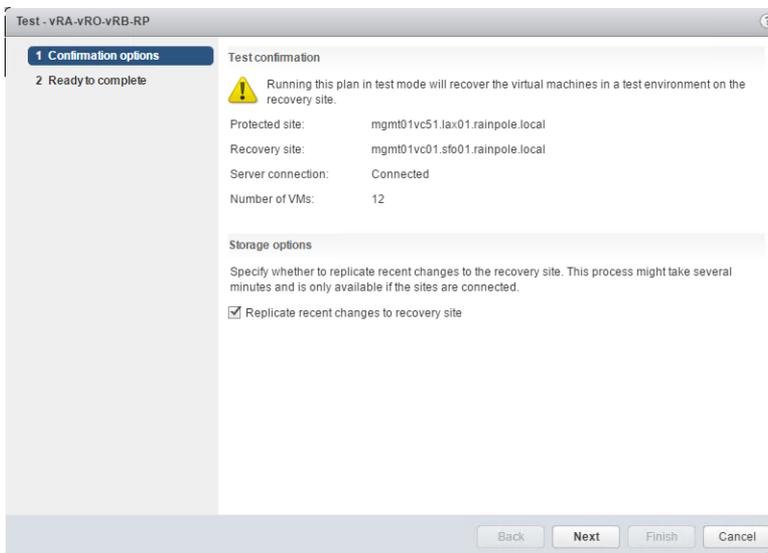
Re-authentication is required if the network connection between Region A and Region B has been interrupted after the last successful authentication.

- 5 Click **Recovery Plans** and click the **vRA-vRO-vRB-RP** recovery plan.
- 6 On the **vRA-vRO-vRB-RP** page, click the **Monitor** tab and click **Recovery Steps**.
- 7 Click the **Test Recovery Plan** icon to run a test recovery.

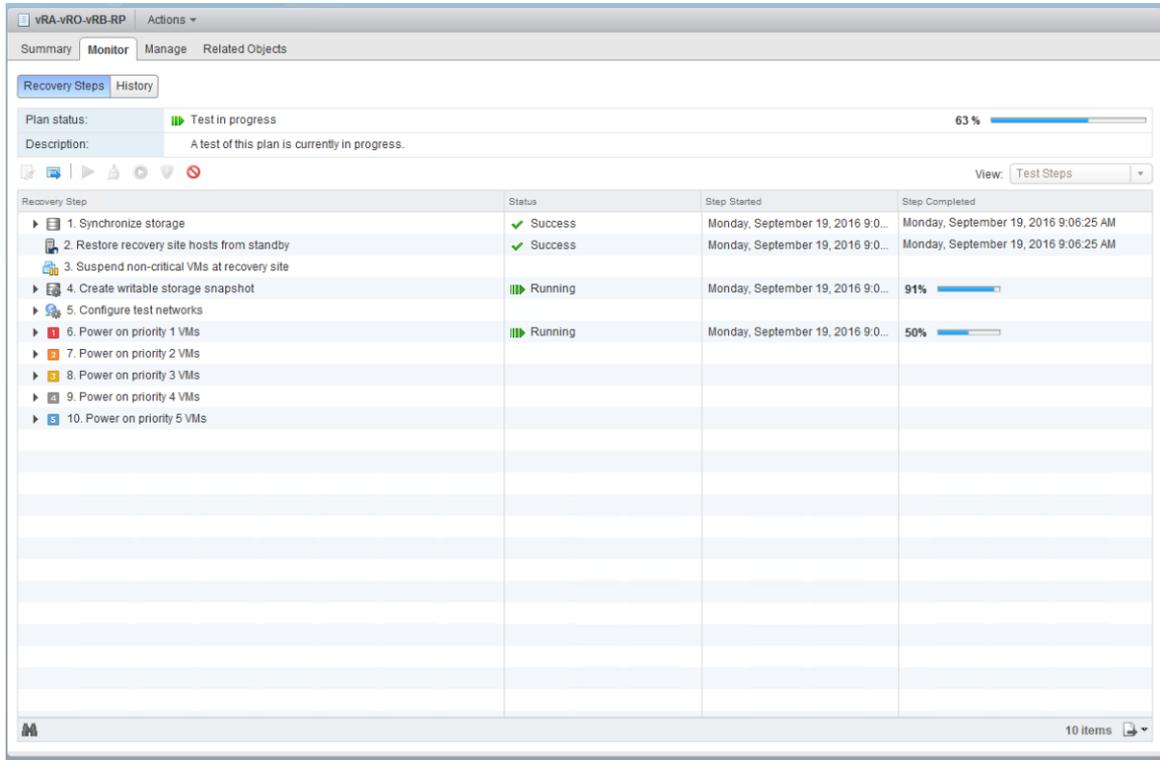


The **Test** wizard appears.

- 8 In the **Confirmation options** page of the **Test** wizard, leave the **Replicate recent changes to recover site** check box selected and click **Next**.



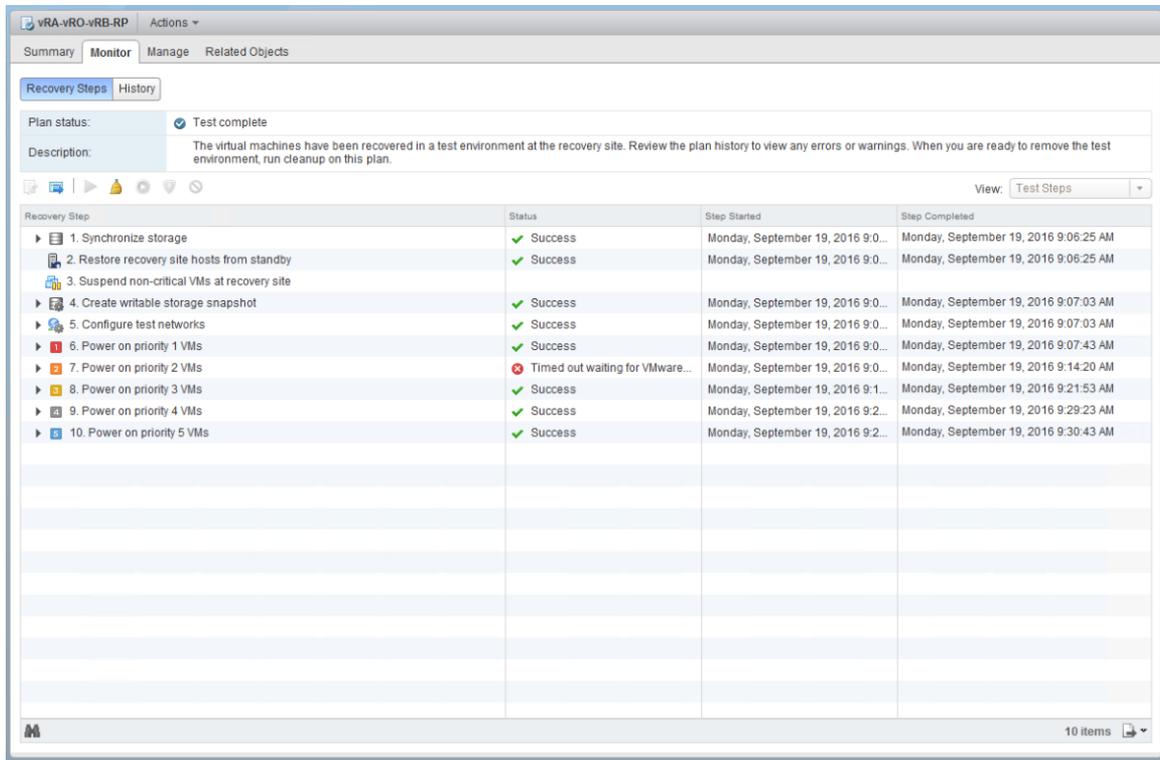
- 9 On the **Ready to complete** page, click **Finish** to start the test recovery.



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

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

Note Because the recovered VMs are using the Test network, VMware Tools in vra01svr01a.rainpole.local and vra01svr01b.rainpole.local VMs might not become online within the default timeout value. Increase the timeout value for the VMs 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.

Perform Failback as Planned Migration of Management Applications

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

Initiate Failback as Planned Migration of vRealize Operations Manager

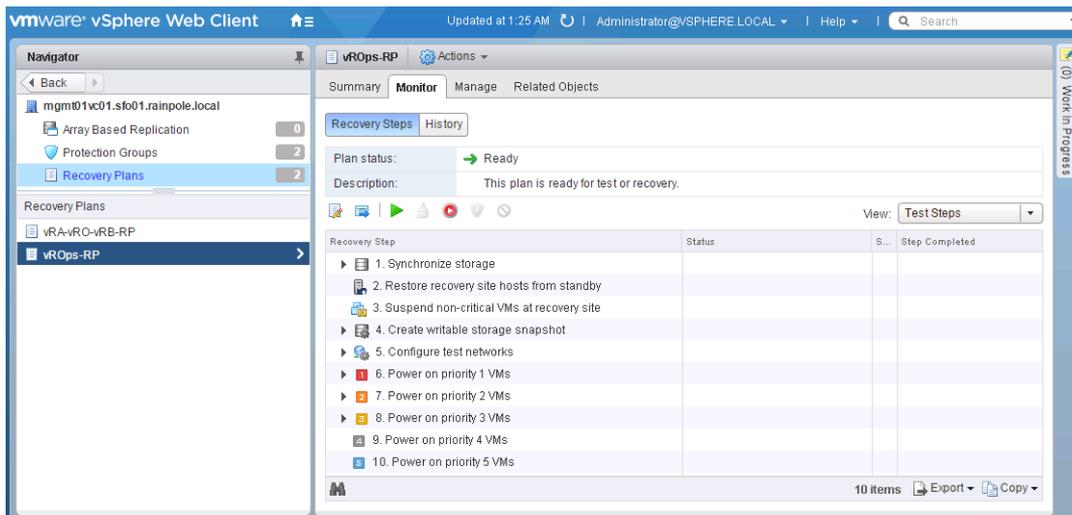
You can run a recovery plan under planned circumstances to migrate the virtual machines of the analytics cluster of vRealize Operations Manager from Region B to Region A. You can also run a recovery plan under unplanned circumstances if Region B suffers an unforeseen event that might result in data loss.

Procedure

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

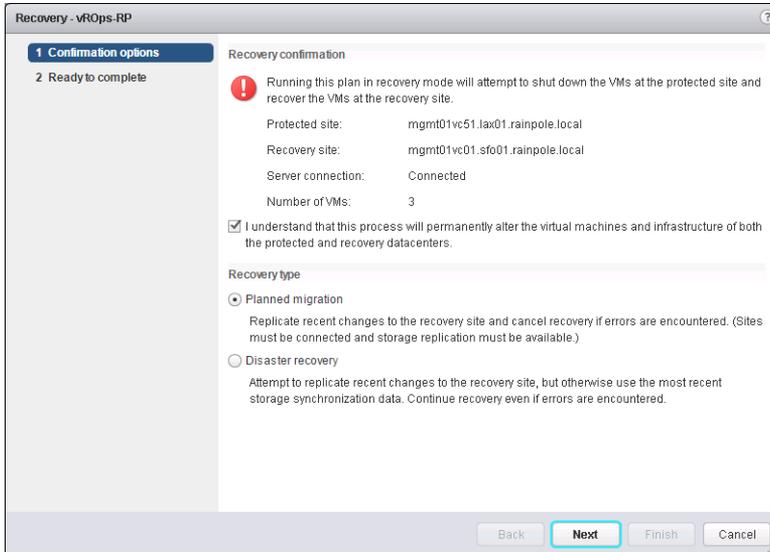
- 2 From the **Home** menu, select **Site Recovery**.
- 3 On the Site Recovery Home page, click **Sites** and click the **mgmt01vc01.sfo01.rainpole.local** vCenter Server object to open its configuration in Site Recovery Manager.
- 4 Click **Recovery Plans** and click the **vROps-RP** recovery plan.
- 5 On the vROps-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.



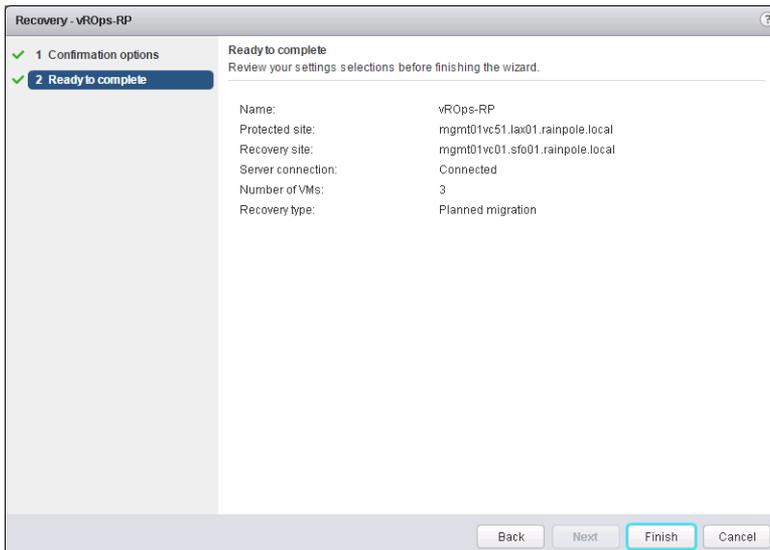
The **Recovery** wizard appears.

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

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	Planned Migration



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



- 9 Perform the steps required to verify the operation of and reprotect the system.
- a Verify that vRealize Operations Manager is up and functions flawlessly after failback.
See *Validate vRealize Operations Manager* in the *Operational Verification* documentation.
 - b Prepare vRealize Operations Manager for failover by reprotecting the virtual machines of the analytics cluster in Site Recovery Manager.
See *Reprotect vRealize Operations Manager* in the *Reprotect of the SDDC Management Applications* documentation.

Initiate Failback as Planned Migration of the Cloud Management Platform

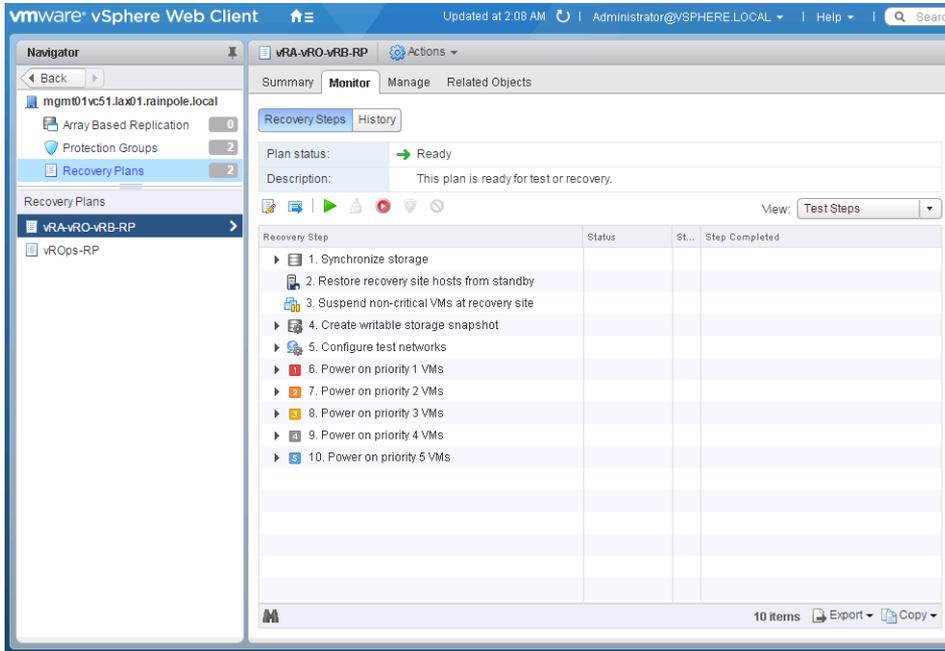
You can run a recovery plan under planned circumstances to migrate the virtual machines of vRealize Automation, vRealize Orchestrator and vRealize Business from Region B to Region A. You can also run a recovery plan under unplanned circumstances if Region B suffers an unforeseen event that might result 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://mgmt01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

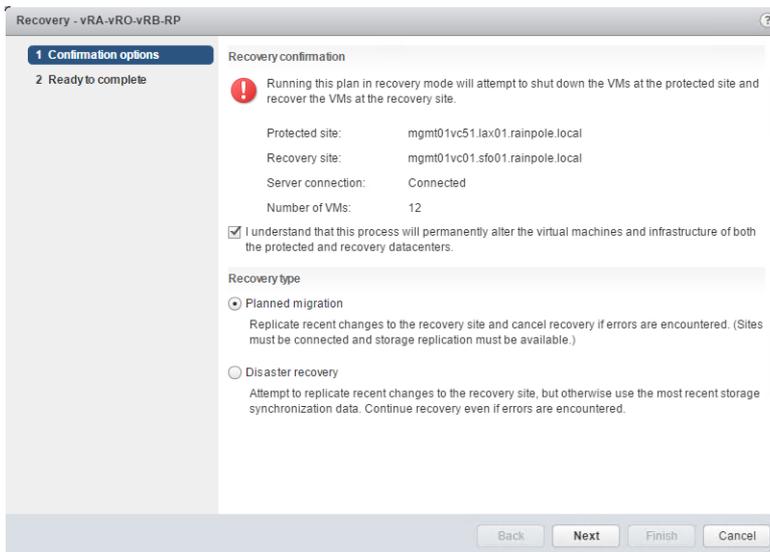
- 2 From the vSphere Web Client **Home** menu, click **Site Recovery**.
- 3 On the Site Recovery home page, click **Sites** and double-click the **mgmt01vc51.lax01.rainpole.local** vCenter Server object to open its site configuration.
- 4 Click **Recovery Plans** and click the **vRA-vRO-vRB-RP** recovery plan.
- 5 On the **vRA-vRO-vRB-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.

- 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 datacenters	Selected
Recovery type	Planned Migration



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

- 9 Perform the steps required to verify the operation of and reprotect the system.
 - a Verify that vRealize Automation, vRealize Orchestrator and vRealize Business VMs are up and function flawlessly after failback.

See *Validate vRealize Automation* in the *Operational Verification* document.
 - b Prepare vRealize Automation, vRealize Orchestrator 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* in the *Reprotect of the SDDC Management Applications* documentation.

Perform Failback as Disaster Recovery of Management Applications

Prepare networking in Region A and perform failback of vRealize Automation, vRealize Orchestrator, vRealize Business, and vRealize Operations Manager to Region A if Region B becomes unavailable in the event of a disaster or if you plan a graceful migration.

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.
- 2 [Recover the Control VM of the Universal Distributed Logical Router in Region A](#)

Because of the failure of Region B, dynamic routing in Region A is not available. Deploy a Control VM for the universal dynamic logical router UDLR01 in Region A to recover dynamic routing in the environment.
- 3 [Reconfigure the Universal Distributed Logical Router and NSX Edges for Dynamic Routing in Region A](#)

Configure the universal distributed logical router UDLR01, and NSX Edges SFOMGMT-ESG01 and SFOMGMT-ESG02 to use dynamic routing in Region A.
- 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.
- 5 [Enable Network Connectivity for the NSX Load Balancer in Region A](#)

Enable the network connectivity on SFOMGMT-LB01 load balancer.
- 6 [Initiate Disaster Recovery of vRealize Operations Manager in Region A](#)

If a disaster event occurs in Region B, initiate the Disaster Recovery of vRealize Operations Manager in Region A to fail back vRealize Operations Manager to Region A.

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

In the event of a disaster in Region B, initiate the Disaster Recovery of vRealize Automation, vRealize Orchestrator and vRealize Business in Region A to fail back the cloud management platform to Region A.

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 to primary, deploy 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://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Promote the NSX Manager for the management cluster in Region A to the primary role.

You must 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**.
 - c On the **Management** tab, 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** confirmation dialog box, click **Yes**.
The NSX Manager gets the **Transit** role.
 - f On the **Management** tab, select the **172.16.11.65** instance again.
 - g Click **Actions** and select **Assign Primary Role**.
 - h In the **Assign Primary Role** confirmation dialog box, click **Yes**.

3 Deploy the universal controller cluster in Region A.

- a In the **Navigator**, click **Networking & Security**, and click **Installation**.
- b 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 **OK**.

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

Setting	Value
Name	nsx-controller-mgmt-01
NSX Manager	172.16.11.65
Datacenter	SFO01
Cluster/Resource Pool	SFO01-Mgmt01
Datastore	SFO01A-VSAN01-MGMT01
Connected To	vDS-Mgmt-Management
IP Pool	Mgmt01-NSXC01
Password	<i>mgmtnsx_controllers_password</i>
Confirm Password	<i>mgmtnsx_controllers_password</i>

- d After the status of the controller node changes to Connected, deploy the remaining two NSX Controller nodes.

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** and expand the **mgmt01vc01.sfo01.rainpole.local** tree. .
- b Select the **SFO01-Mgmt01** cluster and click the **Configure** tab.
- c Under **Configuration**, click **VM/Host Rules** and click **Add** under the **VM/Host Rules** section.
- d In the **SFO01-Mgmt01 - Create VM/Host Rule** dialog box, enter the following settings and click **Add**.

Setting	Value
Name	Mgmt_NSX_Controllers
Enable rule	Selected
Type	Separate Virtual Machines

- e In the **Add Rule Member** dialog box, select all three NSX Controller virtual machines, click **OK**, and click **OK**.

- 5 Use the update controller state mechanism on the NSX Manager to synchronize the state of the newly deployed controllers.
 - a From the **Home** menu, select **Networking & Security**.
 - b In the **Navigator**, click **Installation**.
 - c On the **Management** tab, select the **172.16.11.65** instance.
 - d Click the **Actions** menu and select **Update Controller State**.
 - e In the **Update Controller State** confirmation dialog box, click **Yes**.

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

Because of the failure of Region B, dynamic routing in Region A is not available. Deploy a Control VM for the universal dynamic logical router UDLR01 in Region A to recover dynamic routing in the environment.

Procedure

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

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 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 **UDLR01**.
- 6 Re-deploy 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
Datacenter	SFO01
Cluster/Resource Pool	SFO01-Mgmt01
Datastore	SFO01A-VSAN01-MGMT01

- d Click the **Add** icon to deploy another NSX Edge device with the same configuration.

7 Configure high availability for the control VM.

- a On the **Configuration** page for UDLR01, click **Change** under **HA Configuration**, configure the following settings and click **OK**.

Setting	Value
HA Status	Enable
Connected To	vDS-Mgmt-Management
Enable Logging	Selected

- b In the **Change HA confirmation** 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 **UDLR01** 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	<i>udlr_admin_password</i>
Enable SSH access	Selected

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

Configure the universal distributed logical router UDLR01, and NSX Edges SFOMGMT-ESG01 and SFOMGMT-ESG02 to use dynamic routing in 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://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 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 **UDLR01**.
 - b Click the **Manage** tab and click **Routing**.
 - c Verify that **ECMP** is **Enabled**.
 - d Verify that **192.168.10.3** (Uplink) is configured as the Router ID under **Dynamic Routing Configuration**.

- 5 On the left side, select **BGP** to verify the BGP configuration.
 - a On the **BGP** page, verify the following settings.

Setting	Value
Status	Enabled
Local AS	65003
Graceful Restart	Enabled

- b Select the **192.168.10.1** (SFOMGMT-ESG01) neighbor and click **Edit** icon.
- c In the **Edit Neighbour** 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	SFOMGMT-ESG01 Value
IP Address	192.168.10.1
Forwarding Address	192.168.10.3
Protocol Address	192.168.10.4
Remote AS	65003
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	<i>BGP_password</i>

- d Select the **192.168.10.2** (SFOMGMT-ESG02) neighbor and click **Edit** icon.

- e In the **Edit Neighbour** 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	SFOMGMT-ESG02 Value
IP Address	192.168.10.2
Forwarding Address	192.168.10.3
Protocol Address	192.168.10.4
Remote AS	65003
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	<i>BGP_password</i>

- f Click **Publish Changes**.

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

- a Verify the following settings under **Route Redistribution Status** .

Setting	Value
OSPF	Deselected
BGP	Selected

- b Verify the following settings under **Route Redistribution table**.

Setting	Value
Learner	BGP
From	Connected
Perfix	Any
Action	Permit

7 Reconfigure the routing and weight value of SFOMGMT-ESG01 and SFOMGMT-ESG02 edges.

- a In the **Navigator**, click **NSX Edges**.
- b Select **172.16.11.65** from the **NSX Manager** drop-down menu.
- c Double-click **SFOMGMT-ESG01**.
- 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 Neighbour** dialog box, change **Weight** value to **60** and click **OK**.
- g Click **Publish Changes**.
- h Repeat the step for the SFOMGMT-ESG02 edge.

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

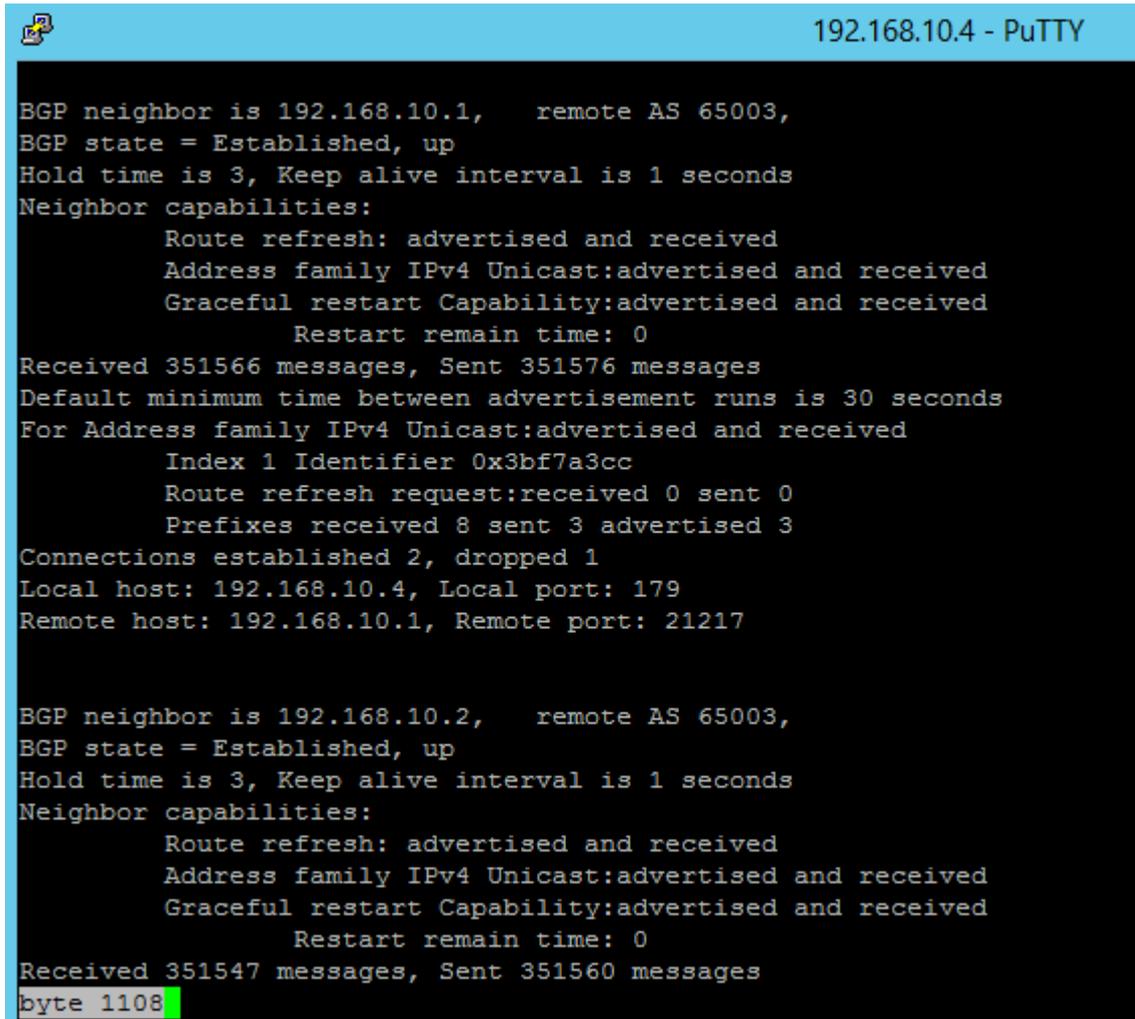
Verify that the UDLR for the management applications is successfully peering, and that BGP routing has been established in Region A.

Procedure

- 1 Log in to the UDLR virtual appliance by using a Secure Shell (SSH) client.
 - a Open an SSH connection to UDLR01.
 - b Log in using the following credentials.

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

- 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 (SFOMGMT-ESG01) and 192.168.10.2 (SFOMGMT-ESG02).



```
192.168.10.4 - PuTTY

BGP neighbor is 192.168.10.1, remote AS 65003,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 351566 messages, Sent 351576 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 1 Identifier 0x3bf7a3cc
  Route refresh request:received 0 sent 0
  Prefixes received 8 sent 3 advertised 3
Connections established 2, dropped 1
Local host: 192.168.10.4, Local port: 179
Remote host: 192.168.10.1, Remote port: 21217

BGP neighbor is 192.168.10.2, remote AS 65003,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 351547 messages, Sent 351560 messages
byte 1108
```

- 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.

```

UDLR01-0> show ip route

Codes: O - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 16

B       0.0.0.0/0           [200/0]       via 192.168.10.1
B       0.0.0.0/0           [200/0]       via 192.168.10.2
B       10.159.4.0/23       [200/0]       via 192.168.10.1
B       10.159.4.0/23       [200/0]       via 192.168.10.2
C       169.254.1.0/30      [0/0]         via 169.254.1.1
B       172.16.11.0/24      [200/0]       via 192.168.10.1
B       172.16.11.0/24      [200/0]       via 192.168.10.2
B       172.16.21.0/24      [200/0]       via 192.168.10.1
B       172.16.21.0/24      [200/0]       via 192.168.10.2
B       172.16.21.0/24      [200/0]       via 192.168.10.1
B       172.16.21.0/24      [200/0]       via 192.168.10.2
B       172.17.11.0/24      [200/0]       via 192.168.10.1
B       172.17.11.0/24      [200/0]       via 192.168.10.2
B       172.17.21.0/24      [200/0]       via 192.168.10.1
B       172.17.21.0/24      [200/0]       via 192.168.10.2
B       172.27.11.0/24      [200/0]       via 192.168.10.1
B       172.27.11.0/24      [200/0]       via 192.168.10.2
B       172.27.12.0/24      [200/0]       via 192.168.10.1
B       172.27.12.0/24      [200/0]       via 192.168.10.2
B       172.27.14.0/24      [200/0]       via 192.168.10.1
B       172.27.14.0/24      [200/0]       via 192.168.10.2
B       172.27.15.0/24      [200/0]       via 192.168.10.1
B       172.27.15.0/24      [200/0]       via 192.168.10.2
B       172.27.22.0/24      [200/0]       via 192.168.10.1
B       172.27.22.0/24      [200/0]       via 192.168.10.2
C       192.168.10.0/24      [0/0]         via 192.168.10.4
C       192.168.11.0/24      [0/0]         via 192.168.11.1
C       192.168.31.0/24      [0/0]         via 192.168.31.1
C       192.168.32.0/24      [0/0]         via 192.168.32.1

UDLR01-0>
  
```

Enable Network Connectivity for the NSX Load Balancer in Region A

Enable the network connectivity on SFOMGMT-LB01 load balancer.

Procedure

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

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 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 **SFOMGMT-LB01** 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 of vRealize Operations Manager in Region A

If a disaster event occurs in Region B, initiate the Disaster Recovery of vRealize Operations Manager in Region A to fail back vRealize Operations Manager 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://mgmt01vc01.sfo01.rainpole.local/vsphere-client>.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Site Recovery**.

- 3 On the Site Recovery home page, click **Sites** and click the **mgmt01vc01.sfo01.rainpole.local** vCenter Server object to open its configuration in Site Recovery Manager.
- 4 Click **Recovery Plans** and click the **vROps-RP** recovery plan.
- 5 On the **vROps-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 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 vRealize Operations Manager failback.
After disaster recovery, the status of the recovery plan is **Disaster Recovery Completed**.

What to do next

Perform the steps required to verify the operation of and reprotect the system.

- 1 Verify that vRealize Operations Manager is up and functions flawlessly after failback. See *Validate vRealize Operations Manager* in the *Operational Verification* documentation.
- 2 Prepare vRealize Operations Manager for failover by reprotecting the virtual machines of the analytics cluster in Site Recovery Manager. See [Reprotect vRealize Operations Manager](#).

Initiate Disaster Recovery of the Cloud Management Platform in Region A

In the event of a disaster in Region B, initiate the Disaster Recovery of vRealize Automation, vRealize Orchestrator and vRealize Business in Region A to fail back the cloud management platform 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://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Site Recovery**.
- 3 On the Site Recovery home page, click **Sites** and double-click the **mgmt01vc01.sfo01.rainpole.local** vCenter Server object to open its site configuration.
- 4 Click **Recovery Plans** and click the **vRA-vRO-vRB-RP** recovery plan.
- 5 On the **vRA-vRO-vRB-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.

What to do next

Perform the steps required to verify the operation of and reprotect the system.

- 1 Verify that vRealize Automation, vRealize Orchestrator and vRealize Business VMs are up and function flawlessly after failback. See *Validate the Cloud Management Platform* in the *Operational Verification* document.
- 2 Prepare vRealize Automation, vRealize Orchestrator 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 Management Applications

After failback of the cloud management platform and vRealize Operations Manager, you must perform certain tasks to ensure that applications perform as expected.

Procedure

- 1 [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. You can use a REST client, such as the RESTClient add-on for Firefox, to enable log forwarding.

- 2 [Update the vRealize Log Insight Logging Address after Failback](#)

After you failback the management applications in the SDDC to Region A, 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 B.

- 3 [Reconfigure the NSX Instance for the Management Cluster in Region B after Failback](#)

After Region B comes back online, you must perform additional configuration of the networking layer to avoid conflicts.

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. You can use a REST client, such as the RESTClient add-on for Firefox, to enable log forwarding.

Prerequisites

On a Windows host that has access to your data center, install a REST client, such as the RESTClient add-on for Firefox.

Procedure

- 1 Log in to the Windows host that has access to your data center.
- 2 In a Firefox browser, go to `chrome://restclient/content/restclient.html`.

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

- a From the **Authentication** drop-down menu, select **Basic Authentication**.
- b In the **Basic Authorization** dialog box, enter the following credentials, select **Remember me** and click **Okay**.

Authentication Attribute	Value
Username	admin
Password	<i>mngnsx_admin_password</i>

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

- c From the **Headers** drop-down menu, select **Custom Header**.
- d In the **Request Header** dialog box, enter the following header details and click **Okay**.

Request Header Attribute	Value
Name	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 In the **Request** pane, from the **Method** drop-down menu, select **GET**.
- b In the **URL** text box, enter **https://mgmt01nsxm01.sfo01.rainpole.local/api/2.0/vdn/controller** and click **Send**.

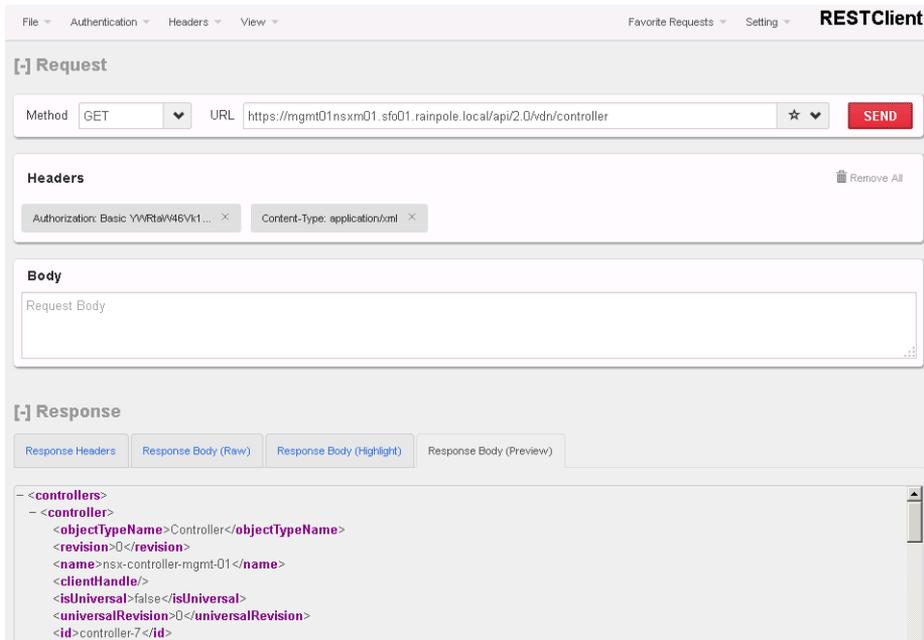
The RESTClient sends a query to the NSX Manager about the installed NSX controllers.

- c After the NSX Manager sends a response back, click the **Response Body (Preview)** tab under **Response**.

The response body contains a root <controllers> XML element, which 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-2`.



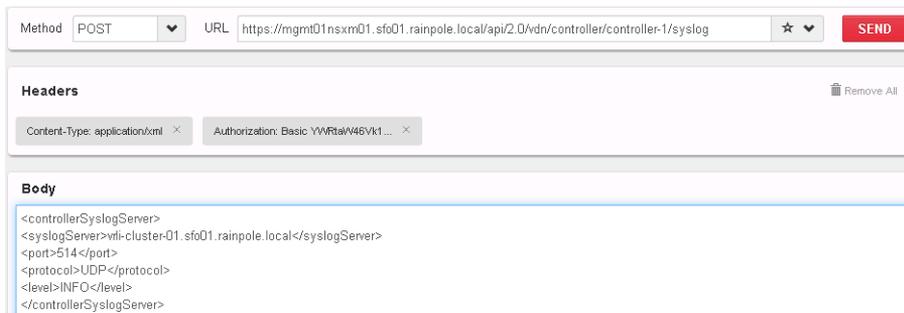
- 5 For each NSX Controller, send a request to configure vRealize Log Insight as a remote syslog server.
 - a In the **Request** pane, from the **Method** drop-down menu, select **POST**, and in the **URL** text box, enter the following URL.

NSX Manager	NSX Controller in the Controller Cluster	POST URL
NSX Manager for the management cluster	NSX Controller 1	https://mgmt01nsm01.sfo01.rainpole.local/api/2.0/vdn/controller/<controller1-id>/syslog
	NSX Controller 2	https://mgmt01nsm01.sfo01.rainpole.local/api/2.0/vdn/controller/<controller2-id>/syslog
	NSX Controller 3	https://mgmt01nsm01.sfo01.rainpole.local/api/2.0/vdn/controller/<controller3-id>/syslog

- b In the **Request** pane, paste the following request body in the **Body** text box and click **Send**.

```
<controllerSyslogServer>
  <syslogServer>vrli-cluster-01.sfo01.rainpole.local</syslogServer>
  <port>514</port>
  <protocol>UDP</protocol>
  <level>INFO</level>
</controllerSyslogServer>
```

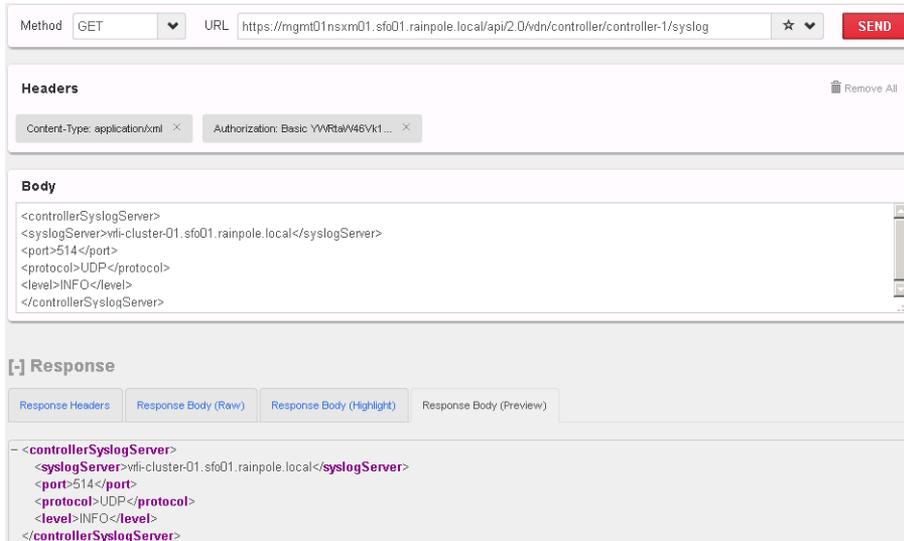
- c Repeat the steps for the next NSX Controller.



- 6 Verify the syslog configuration on each NSX Controller.
 - a In the **Request** pane, from the **Method** drop-down menu, select **GET**, and 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 returns a response, click the **Response Body (Preview)** 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 vrl-cluster-01.sfo01.rainpole.local.
- d Repeat the steps for the next NSX Controller.



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

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 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 **UDLR01**.
 - 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, in the **Syslog Server 1** text box, enter **192.168.31.10** and from the **Protocol** drop-down menu, select **udp**.
 - h Click **OK**.

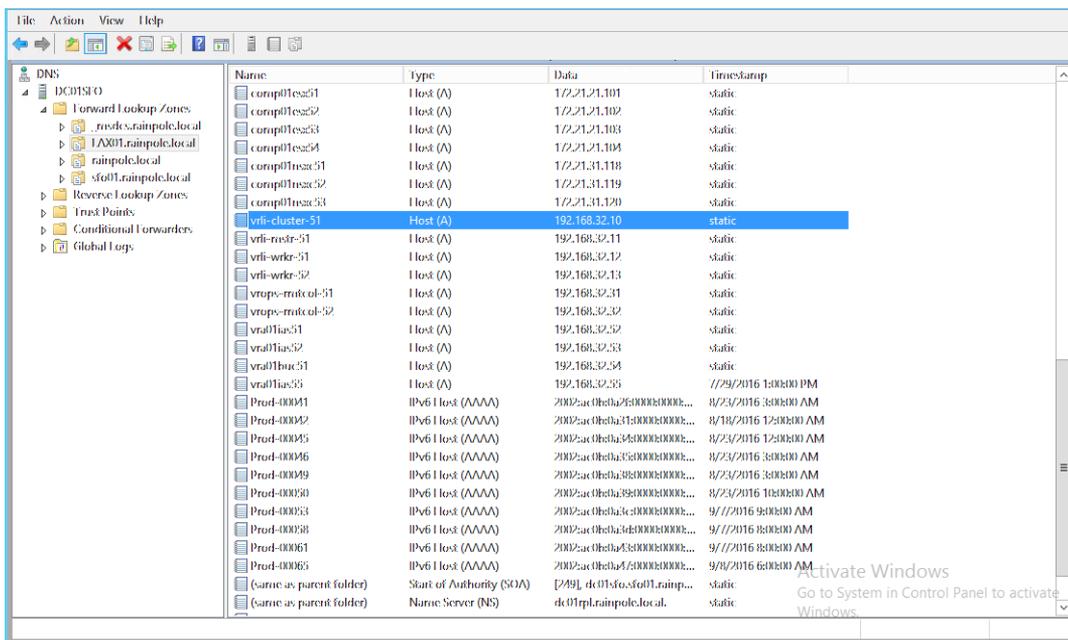
Update the vRealize Log Insight Logging Address after Failback

After you failback the management applications in the SDDC to Region A, 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 B.

You update the DNS entry for `vrli-cluster-51.lax01.rainpole.local` to point to the IP address `192.168.31.10` of `vrli-cluster-01.sfo01.rainpole.local` in Region A.

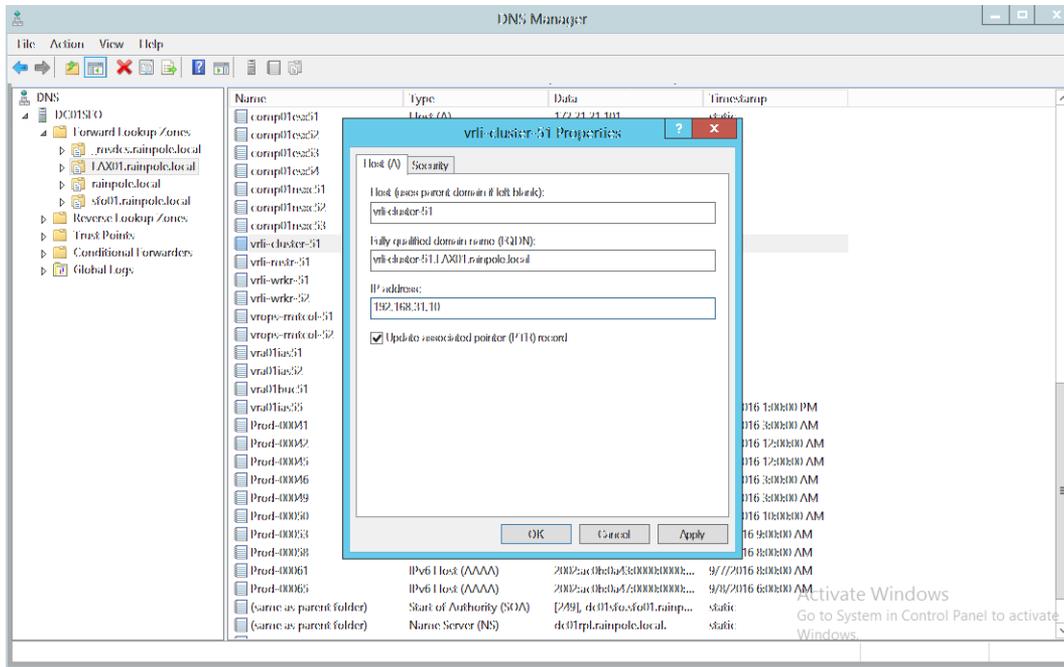
Procedure

- 1 Log in to the DNS server `dc01sfo.sfo01.rainpole.local` that resides in the `sfo01.rainpole.local` domain.
- 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 `lax01.rainpole.local` domain and locate the `vrli-cluster-51` record on the right.



- 4 Double-click the `vrli-cluster-51` record, 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)	vrli-cluster-51.lax01.rainpole.local
IP Address	192.168.31.10
Update associated pointer (PTR) record	Selected



Reconfigure the NSX Instance for the Management Cluster in Region B after Failback

After Region B comes back online, you must perform additional configuration of the networking layer to avoid conflicts.

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://mgmt01vc01.sfo01.rainpole.local/vsphere-client>.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu from the vSphere Web Client, click **Networking & Security**.
- 3 In the **Navigator**, click **Installation** and click the **Management** tab.

You see that 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 NSX Manager** .
 - b Select the **Perform operation even if the NSX manage is inaccessible** check box and click **OK**.
- 5 Demote the original primary site NSX Manager to the transit role.
 - a Select the **172.17.11.65** instance, click **Actions > Remove Primary Role**.
 - b Click **Yes** in the confirmation dialog box.
- 6 Delete the NSX controllers in the primary site.
 - a Select the **nsx-controller-mgmt-51** node and click **Delete**.
 - b In the **Delete Controller** confirmation dialog box, click **Yes**.
 - c Repeat step to delete the remaining two NSX Controller nodes.
 - d Select **Forcefully remove the controller** when you delete the last controller.
- 7 Delete the UDLR01 edge in the protected site.
 - a In the **Navigator**, click **NSX Edges**.
 - b Select **172.17.11.65** from the **NSX Manager** drop-down menu.
 - c Select the **UDLR01** and click **Delete**.
 - d In the **Delete NSX Edge** confirmation dialog box, click **Yes**.
- 8 Assign the Region B management cluster NSX Manager the secondary role to the already promoted primary NSX Manager in Region A.
 - a In the **Navigator**, click **Installation**.
 - b On the **Management** tab select the primary **172.16.11.65** instance.
 - c Select **Actions > Add Secondary NSX Manager**.
 - d In the **Add secondary NSX Manager** dialog box, enter the following settings and click **OK**.

Setting	Value
NSX Manager	172.17.11.65
User Name	admin
Password	<i>mgmtnsx_admin_password</i>
Confirm Password	<i>mgmtnsx_admin_password</i>

- e In the **Trust Certificate** confirmation dialog box, click **Yes**.
- 9 Disable network connectivity for the NSX load balancer 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 the **LAXMGMT-LB01** 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**.

10 Configure the routing for the universal distributed logical router in Region A.

- a In the **Navigator**, click **NSX Edges**.
- b Select **172.16.11.65** from the **NSX Manager** drop-down menu.
- c Double-click **UDLR01**.
- 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	LAXMGMT-ESG01 Value	LAXMGMT-ESG02 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	<i>BGP_password</i>	<i>BGP_password</i>

- 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 **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 LAXMGMT-ESG01 and LAXMGMT-ESG02 edges.

- a In the **Navigator**, click **NSX Edges**.
- b Select **172.17.11.65** from the **NSX Manager** drop-down menu.
- c Double-click **LAXMGMT-ESG01**.
- d Click the **Manage** tab and click **Routing**.
- e On the left, select **BGP**, select the **192.168.10.4** neighbour and click **Edit**.
- f In the **Edit Neighbour** dialog box, change the **Weight** value to **10** and click **OK**.
- g Click **Publish Changes**.
- h Repeat the step for the LAXMGMT-ESG02 edge.

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

- a Log in to the LAXMGMT-ESG01 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 will display `Established`, `UP` if you have successfully peered with UDLR01.
- c Run the `show ip route` command to verify that you are receiving routes using BGP.
- d Repeat the step for the LAXMGMT-ESG02 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 virtual machines 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 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 completes.

- [Prerequisites for Performing Reprotect](#)

To reprotect the virtual machines of the SDDC management applications, your environment must meet certain requirements for availability of the original protected region and state of recovery plans.

- [Reprotect vRealize Operations Manager](#)

Prepare vRealize Operations Manager for failback or failover by reprotecting the virtual machines in Site Recovery Manager.

- [Reprotect the Cloud Management Platform](#)

Prepare vRealize Automation, vRealize Orchestrator and vRealize Business Server 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 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.

You cannot restore the original region if, for example, a physical catastrophe destroyed it. 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, make sure that all steps of the recovery plan finish successfully. If errors occur during the recovery, resolve the problems that caused the errors and re-run the recovery plan. When you re-run 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*. Re-run the recovery plans for the Cloud Management Platform and vRealize Operations Manager again in the *Recovery Required* state so that Site Recovery Manager can perform actions on the original region which were 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 re-run the planned migration until it succeeds.

Reprotect vRealize Operations Manager

Prepare vRealize Operations 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://mgmt01vc51.lax01.rainpole.local/vsphere-client
Reprotect after failback	https://mgmt01vc01.sfo01.rainpole.local/vsphere-client

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 In the vSphere Web Client, select **Home > Site Recovery** .

3 Click **Recovery Plans**, right-click the **vROps-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 that 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 **vROps-RP** recovery plan and click the **Monitor > Recovery Steps** tab to monitor the progress of the reprotect operation.
- 7 If the status of the vROps-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 vROps-RP recovery plan changes to **Ready**, click **Monitor > History** and click the **Export report for selected history item** button.

The recovery plan can return to the ready state even if errors occurred during the reprotect operation. Check the history report for the reprotect operation to make sure that no errors occurred. If errors occurred during reprotect, attempt to fix the errors and run a test recovery to make sure that the errors are fixed. If you do not fix errors and you subsequently attempt to run a planned migration or disaster recovery, 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 from the new protected site to the new recovery site

Reprotect the Cloud Management Platform

Prepare vRealize Automation, vRealize Orchestrator and vRealize Business Server 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://mgmt01vc51.lax01.rainpole.local/vsphere-client
Reprotect after failback	https://mgmt01vc01.sfo01.rainpole.local/vsphere-client

- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the vSphere Web Client, select **Home > Site Recovery**.
- 3 Click **Recovery Plans**, right-click the **vRA-vRO-vRB-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 that 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 **vRA-vRO-vRB-RP** recovery plan and click the **Monitor > Recovery Steps** tab to monitor the progress of the reprotect operation.
- 7 If the status of the vRA-vRO-vRB-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 vRA-vRO-vRB-RP recovery plan changes to **Ready**, click **Monitor > History** and click the **Export report for selected history item** button.

The recovery plan can return to the ready state even if errors occurred during the reprotect operation. Check the history report for the reprotect operation to make sure that no errors occurred. If errors occurred during reprotect, attempt to fix the errors and run a test recovery to make sure that the errors are fixed. If you do not fix the errors and you subsequently attempt to run a planned migration or disaster recovery, 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