

Upgrade

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 Upgrade 6

Updated Information 7

1 SDDC Upgrade Overview 8

Upgrade Policy 8

Upgrade Paths and Application Upgrade Sequence 9

VMware Software Versions in the Upgrade 10

System Requirements for the SDDC Upgrade 11

Best Practices in SDDC Upgrades 12

2 Upgrade the Cloud Management Platform 14

Upgrade vRealize Automation Appliance and the Infrastructure-as-a-Service Components 14

Direct Traffic to the Primary Nodes and Disable Health Monitoring for vRealize Automation on the Load Balancer 17

Upgrade the vRealize Automation Appliances 19

Upgrade the vRealize Automation IaaS Management Agent on Each IaaS Node 22

Upgrade the IaaS Components by Using the Automated Upgrade Shell Script 26

Delete the Snapshots of the vRealize Automation Virtual Machines 29

Re-Enable the Secondary Nodes and Health Monitoring for vRealize Automation on the Load Balancer 30

Upgrade vRealize Business and vRealize Business Data Collectors 31

Upgrade the vRealize Business Server Appliance 31

Upgrade the vRealize Business Remote Data Collectors 33

Delete the Snapshots of the vRealize Business Appliances 35

Upgrade vRealize Orchestrator Cluster 36

Update the vRealize Orchestrator Cluster 36

Delete the Snapshots of the vRealize Orchestrator Appliances 39

Post-Upgrade Configuration of the Cloud Management Platform 40

Rename the Anti-Affinity Rules for vRealize Automation and vRealize Orchestrator Virtual Machines 41

Configure the Load Balancer Application Profiles for vRealize Automation and vRealize Orchestrator 43

Increase the Virtual Memory and the Number of Virtual CPUs of the vRealize Business Appliances 45

Configure Integration of vRealize Operations Manager with vRealize Automation for Workload Reclamation 46

3 Upgrade Operations Management Components 50

- Upgrade vRealize Operations Manager 50
 - Take the vRealize Operations Manager Nodes Offline and Take Snapshots 52
 - Upgrade the Operating System of the vRealize Operations Manager Appliances 53
 - Upgrade the vRealize Operations Manager Software 54
 - Upgrade the vRealize Operations Management Packs 56
 - Delete the Snapshots of the vRealize Operations Manager Appliances 58
 - Post-Upgrade Configuration of vRealize Operations Manager 59
- Upgrade vRealize Log Insight 75
 - Take Snapshots of the vRealize Log Insight Nodes 77
 - Upgrade the vRealize Log Insight Clusters 78
 - Upgrade the vRealize Log Insight Agents 79
 - Delete the Snapshots of the vRealize Log Insight Appliances 82
 - Post-Upgrade Configuration of the vRealize Log Insight 83

4 Upgrade Virtual Infrastructure 96

- Update vSphere Data Protection 96
 - Take Snapshots of the vSphere Data Protection Appliances 98
 - Update the vSphere Data Protection Node 99
 - Post-Upgrade Configuration of vSphere Data Protection 100
- Upgrade the NSX Components for the Management and Shared Edge and Compute Clusters 106
 - Upgrade the NSX Manager Instances 109
 - Upgrade the NSX Controllers 111
 - Upgrade the NSX Components on the ESXi Hosts 113
 - Upgrade NSX Edge Instances 114
 - Post-Upgrade Configuration of NSX for vSphere 115
- Upgrade the Components for the Management Cluster 138
 - Upgrade vSphere and Disaster Recovery Components for the Management Clusters 139
 - Post-Upgrade Configuration of the vSphere Components for the Management Cluster 163
 - Complete vSphere Upgrade for the Management Cluster 193
 - Post-Upgrade Configuration of the Management ESXi Hosts and vSAN Storage 205
- Upgrade the Components for the Shared Edge and Compute Cluster 219
 - Upgrade vSphere for the Shared Edge and Compute Cluster 219
 - Post-Upgrade Configuration of the vCenter Server Components for the Shared Edge and Compute Cluster 233
 - Upgrade the ESXi Hosts in the Shared Edge and Compute Cluster 249
 - Post-Upgrade Configuration of the Shared Edge and Compute ESXi Hosts 261
- Global Post-Upgrade Configuration of the Virtual Infrastructure Components 275
 - Configure the Anti-Affinity Rules for the Platform Services Controller Instances in Region A 277
 - Create Virtual Machine Groups to Define Startup Order in the Management Cluster in Region A 278
 - Deploy the Platform Services Controllers Load Balancer in Region A 279

Repoint the vCenter Server Instances to the Platform Services Controller Load Balancer in Region A	295
Connect the NSX Managers to the Platform Services Controller Load Balancer in Region A	296
Reconnect vSphere Replication to vCenter Server in Region A	297
Reconnect Site Recovery Manager to vCenter Server and Platform Services Controller Instances in Region A	300
Register vSphere Data Protection with the Management vCenter Server in Region A	305
Configure Point in Time in vSphere Replication	306
Clean Up Obsolete Appliances and Snapshots in Region A	308
Configure the Anti-Affinity Rules for the Platform Services Controller Instances in Region B	309
Create Virtual Machine Groups to Define Startup Order in the Management Cluster in Region B	309
Deploy the Platform Services Controllers Load Balancer in Region B	311
Repoint the vCenter Server Instances to the Platform Services Controller Load Balancer in Region B	329
Connect the NSX Managers to the Platform Services Controller Load Balancer in Region B	330
Reconnect vSphere Replication to vCenter Server in Region B	331
Reconnect Site Recovery Manager to vCenter Server and Platform Services Controller Instances in Region B	332
Register vSphere Data Protection with the Management vCenter Server in Region B	335
Clean Up Obsolete Appliances and Snapshots in Region B	336

About VMware Validated Design Upgrade

VMware Validated Design Upgrade provides step-by-step instructions for updating VMware solutions in a software-defined data center (SDDC) that is deployed according to VMware Validated Design™ for Software-Defined Data Center.

Before you start an update in your SDDC, make sure that you are familiar with the update or upgrade planning guidance that is part of this guide.

Note *VMware Validated Design Upgrade* is validated with certain product versions. See *VMware Validated Design Release Notes* and [Upgrade Policy](#) for more information about supported product versions for this release.

Intended Audience

VMware Validated Design Upgrade is intended for infrastructure administrators and cloud administrators who are familiar with and want to keep VMware software up-to-date with the latest versions available.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to <http://www.vmware.com/support/pubs>.

Updated Information

This *VMware Validated Design Upgrade* documentation is updated with each release of the product or when necessary.

This table provides the update history of the *VMware Validated Design Upgrade* documentation.

Revision	Description
EN-002498-01	<ul style="list-style-type: none">■ Optimized documentation structure. The documentation provides separate per-region flows instead of discrete instructions that refer to both regions.■ Added documentation about handling traffic and health checks during a vRealize Automation upgrade operation. See Direct Traffic to the Primary Nodes and Disable Health Monitoring for vRealize Automation on the Load Balancer and Re-Enable the Secondary Nodes and Health Monitoring for vRealize Automation on the Load Balancer.
EN-002498-00	Initial release.

SDDC Upgrade Overview

The VMware Validated Designs reduce risk and time in performing updates and upgrades by validating the procedures and software versions associated with each VMware Validated Design release. Consider the policy, upgrade paths, system requirements and upgrade sequence for successful SDDC upgrade.

This chapter includes the following topics:

- [Upgrade Policy](#)
- [Upgrade Paths and Application Upgrade Sequence](#)
- [VMware Software Versions in the Upgrade](#)
- [System Requirements for the SDDC Upgrade](#)
- [Best Practices in SDDC Upgrades](#)

Upgrade Policy

VMware Validated Designs provide validated instructions for update and upgrade of the SDDC management products according to an upgrade validation policy.

Updates That Are Validated by VMware Validated Designs

VMware Validated Designs follows the lifecycle management principles contextualized around the Software-defined Data Center (SDDC).

Upgrade	Impacts the SDDC design and implementation, ensures interoperability, and introduces new features, functionality, and bug fixes.
Update	Does not impact the SDDC design and implementation, includes bug fixes and ensures interoperability.

The upgrade of the VMware Validated Design is a prescriptive path between each release where, unless specific express patches or hot fixes are required for an environment, deviation is not supported.

Updates That Are Not Validated by VMware Validated Designs

The VMware Validated Design is not scaled or functionally tested against individual patches, express patches or hot fixes. To patch your environment, follow the VMware best practices and KB articles published with the patch you want to apply. If an issue occurs during or after applying a VMware patch, contact VMware Technical Support.

Upgrade Paths and Application Upgrade Sequence

You must comply with the path and sequence for SDDC upgrade to version 4.0 of this VMware Validated Design.

Upgrade Paths

To upgrade to version 4.0.1, you must run version 3.0.2 of this VMware Validated Design.

Currently Installed Version	Upgrade Path
2.0	1 3.0
	2 3.0.2
	3 4.0.1
3.0	1 3.0.2
	2 4.0.1
3.0.2	4.0.1

Upgrade Sequence

The VMware Validated Design upgrade process follows a prescriptive path to properly decouple the VMware components into their respective layers. By following this path, you can incrementally upgrade from one version to another while minimizing the number of context switching between products and user interfaces and minimizing the number of product champions required during maintenance windows. At the same time, the upgrade sequence reduces the overall upgrade window and the impact size in the event of a failed upgrade or update. This sequence also ensures interoperability with the broader components within the SDDC. This way, the upgrade sequence allows for progressive, granular upgrade over the course of time.

Table 1-1. VMware Validated Design Upgrade Sequence

Order	Component	Sub-Component	Layer
1	vRealize Automation	vRealize Automation Appliances	Cloud Management
		vRealize Automation IaaS Components	
2	vRealize Business for Cloud	vRealize Business for Cloud Appliance	

Table 1-1. VMware Validated Design Upgrade Sequence (Continued)

Order	Component	Sub-Component	Layer
		vRealize Business for Cloud Data Collectors	
3	vRealize Orchestrator	-	
4	vRealize Operations Manager	-	Operations Management
5	vRealize Log Insight	vRealize Log Insight Appliances	
		vRealize Log Insight Agents	
6	vSphere Data Protection	-	Business Continuity (Backup and Restore)
7	NSX for vSphere	NSX Managers	Virtual Infrastructure (Networking)
		NSX Controllers	
		NSX Networking Fabric	
		NSX Edges	
8	Platform Services Controller	-	Virtual Infrastructure (Compute Infrastructure)
	vCenter Server	-	
	vSphere Replication	-	Business Continuity (Disaster Recovery)
	Site Recovery Manager	-	
	ESXi	-	Virtual Infrastructure (Compute Infrastructure)
	vSAN	-	Virtual Infrastructure (Storage)

VMware Software Versions in the Upgrade

You upgrade each management products of the SDDC to a specific version according to the software bill of materials of this validated design.

Table 1-2. Upgrade from VMware Validated Design for Software-Defined Data Center 3.0.2 to VMware Validated Design for Software-Defined Data Center 4.0

SDDC Layer	Product Name	Product Version in VMware Validated Design 3.0.2	Product Version in VMware Validated Design 4.0	Operation Type
Cloud Management	vRealize Automation	7.1	7.2	Upgrade
	vRealize Business	7.1	7.2	Update
	vRealize Orchestrator	7.1	7.2	Upgrade
Operations Management	vRealize Operations Manager	6.3	6.4	Upgrade
	vRealize Log Insight	3.6.0	4.0	Upgrade
Virtual Infrastructure	NSX for vSphere	6.2.4	6.3.1	Upgrade

Table 1-2. Upgrade from VMware Validated Design for Software-Defined Data Center 3.0.2 to VMware Validated Design for Software-Defined Data Center 4.0 (Continued)

SDDC Layer	Product Name	Product Version in VMware Validated Design 3.0.2	Product Version in VMware Validated Design 4.0	Operation Type
	vCenter Server	6.0 Update 2	6.5 a	Upgrade
	Platform Services Controller	6.0 Update 2	6.5 a	Upgrade
	ESXi	6.0 Update 2	6.5 a	Upgrade
	vSAN	6.2	6.5	Upgrade
Business Continuity and Disaster Recovery	Site Recovery Manager	6.1.1	6.5	Update
	vSphere Replication	6.1.1	6.5	Upgrade
	vSphere Data Protection	6.1.2	6.1.3	Update

For information about the software components that are available in VMware Validated Design 3.0.2 and VMware Validated Design 4.0, see the *VMware Validated Design Release Notes*.

System Requirements for the SDDC Upgrade

Before you upgrade the layers of the SDDC, verify that your system meets the general system requirements for this operation.

Review the release notes of each VMware product in the SDDC, the *VMware Validated Design Planning and Preparation* documentation and the individual prerequisites for the upgrade of each VMware Validated Design layer to understand the hardware and software requirements that might impact the SDDC upgrade.

- Review the Release Notes for each VMware product in the SDDC.
- Ensure that the server hardware has been certified with vSphere 6.5. For information, see the [VMware Compatibility Guide](#).
- Ensure that the server hardware meets the updated memory requirements of the SDDC. See *ESXi Host Physical Design Specifications* in the *VMware Validated Design Architecture and Design* documentation.
- Review any custom integration that might have occurred outside of VMware Validated Design to ensure compatibility with the new versions of VMware products within the SDDC.
- Review any 3-rd party products that might be used in your environment to ensure compatibility with new versions of VMware products within the SDDC.

Best Practices in SDDC Upgrades

Prepare for the SDDC upgrade and perform certain activities after the upgrade is complete to guarantee the operational state of the environment.

Planning for the SDDC Update or Upgrade

- Schedule a maintenance window that is suitable for your organization and users.

The VMware Validated Design upgrade sequence is organized in such a way that the upgrade of each layer can be executed within a maintenance window.

- Perform backups and snapshots of the VMware management components.
- Allocate time in your maintenance window to run test cases and validate that all integrations, important business functionality, and system performance are acceptable. Add a time buffer for responding to errors without breaching the change window.
- Consider the impact of an update or upgrade to users.

If you properly prepare for the upgrade, existing instances, networking, and storage should continue to operate.

- Performing an upgrade with operational workloads carries risks.

Use vSphere vMotion to temporarily migrate workloads to other compute nodes during upgrade.

- Communicate the upgrade to your users so that they can plan for their own backups.

Considerations on Upgrade Failure

- Contact VMware Technical Support.
- Roll the components back.

In the event of a failure while upgrading one of the components of the SDDC, the order in which the components are organized ensures that backwards compatibility and interoperability are sustained between the layers. You can roll back to a previous version of the components within a layer.

Important Rollback of an entire SDDC after more than one layer has been successfully upgraded is not supported.

Post-Upgrade Operations

Consider the following best practices after you complete the update or upgrade process, evaluating them on a test environment similar to your production SDDC:

- Verify important functionality, integration, and system performance. See the *VMware Validated Design Operational Verification* documentation.

- Conduct a lessons learned meeting. Document improvements and ensure that they are incorporated in the next update or upgrade cycle.

Upgrade the Cloud Management Platform

2

You start the upgrade from VMware Validated Design 3.0.2 to VMware Validated Design 4.0 by upgrading vRealize Automation, vRealize Business for Cloud and vRealize Orchestrator cluster that build up the Cloud Management Platform.

Procedure

1 Upgrade vRealize Automation Appliance and the Infrastructure-as-a-Service Components

When you upgrade the Cloud Management Platform as a part of the upgrade from VMware Validated Design 3.0.2 to VMware Validated Design 4.0, you start with vRealize Automation.

2 Upgrade vRealize Business and vRealize Business Data Collectors

After you upgrade the vRealize Automation nodes, upgrade the vRealize Business for Cloud server in Region A, and the remote data collectors in Region A and Region B.

3 Upgrade vRealize Orchestrator Cluster

After you upgrade the vRealize Automation and vRealize Business components, complete the upgrade the Cloud Management Platform to VMware Validated Design 4.0 by upgrading the vRealize Orchestrator cluster.

4 Post-Upgrade Configuration of the Cloud Management Platform

After you upgrade the components of the Cloud Management Platform, perform the following configuration changes to the environment according to the objectives and deployment guidelines of this validated design.

Upgrade vRealize Automation Appliance and the Infrastructure-as-a-Service Components

When you upgrade the Cloud Management Platform as a part of the upgrade from VMware Validated Design 3.0.2 to VMware Validated Design 4.0, you start with vRealize Automation.

When you update the vRealize Automation instance as a part of the upgrade from VMware Validated Design 3.0.2 to VMware Validated Design 4.0, you first upgrade the vRealize Automation appliances proceeded by an automated upgrade of the Infrastructure-as-a-Service (IaaS) components in Region A and Region B.

Table 2-1. vRealize Automation Nodes in the SDDC

Region	Role	IP Address	Full Qualified Domain Name
Region A	vRealize Automation Server VIP	192.168.11.53	vra01svr01.rainpole.local
	vRealize Automation Server Appliance	192.168.11.51	vra01svr01a.rainpole.local
		192.168.11.52	vra01svr01b.rainpole.local
	vRealize Automation for IaaS Web Server VIP	192.168.11.56	vra01iws01.rainpole.local
	vRealize Automation for IaaS Web Server	192.168.11.54	vra01iws01a.rainpole.local
		192.168.11.55	vra01iws01b.rainpole.local
	vRealize Automation Model Manager IMS VIP	192.168.11.59	vra01ims01.rainpole.local
	vRealize Automation Model Manager IMS	192.168.11.57	vra01ims01a.rainpole.local
		192.168.11.58	vra01ims01b.rainpole.local
	vRealize Automation DEM Workers	192.168.11.60	vra01dem01.rainpole.local
		192.168.11.61	vra01dem01.rainpole.local
	vRealize Automation Proxy Agent	192.168.31.52	vra01ias01.sfo01.rainpole.local
		192.168.31.53	vra01ias02.sfo01.rainpole.local
	MS SQL Server for vRealize Automation	192.168.11.62	vra01mssql01.rainpole.local
Region B	vRealize Automation Proxy Agent	192.168.32.52	vra01ias51.lax01.rainpole.local
		192.168.31.53	vra01ias52.lax01.rainpole.local

Prerequisites

- Perform the operations that are described in *Preparing to Upgrade vRealize Automation 7.1* from the [Preparing to Upgrade vRealize Automation 7.1](#) Guide.

- Verify that the vRealize Automation environment has been quiesced of all activities, including but not limited to, users ordering new virtual machines and third-party integration that may automate the order of new virtual machines. Without quiescing the environment, rollback operations might be disrupted by generate orphaned objects. You might also have to extend the time of the maintenance window.
- Download the vRealize Automation upgrade .iso file to a shared datastore for mounting from the vSphere Web Client.

If you have space on your NFS datastore, upload the file there.

- Download the vRealize Automation IAS Management Agent .msi file to the Windows host that has access to the data center. See the [product download page](#) build 4683764.
- Review health check by using the vRealize Production Test Tool against your vRealize Automation instance to ensure that it is in good health. Remediate any issues prior to beginning of the upgrade. See the [product download page](#) version 1.7.0.
- Verify that all IaaS Windows nodes meet the following requirements:
 - Are connected and available, reporting a status of REGISTERED
 - Have a **Last Connected** status of less than 3 minutes.
 - Have a **Time Offset** status of less than 1 second.
- Verify that both vRealize Automation appliances meet the following requirements:
 - At least 18 GB RAM, 4 vCPUs, Disk1 with 50 GB, Disk3 with 25 GB, and Disk4 with 50 GB before you run the upgrade.
 - At least 5.3 GB of free disk space on the root partition to download and run the upgrade.
 - /storage/log subfolder cleaned of older archived ZIP files to free up disk space.
 - The PostgreSQL database is connected and reporting a Valid status of Yes, indicating synchronization between the master and replica nodes.
- Verify that the primary vRealize IaaS Web Server, Microsoft SQL database, and Model Manager node satisfy the following requirements:
 - Microsoft .NET Framework 4.5.2 version installed.
 - At least 5 GB of free disk space available.
 - JAVA SE Runtime Environment 8 64- bits update 91 or later installed. After you install Java, you must set the environment variable JAVA_HOME to the new version on each server node.
- Verify that you have access to all databases and all load balancers impacted by or participating in the vRealize Automation upgrade.
- Make the system unavailable to end users and any automated components while you perform the upgrade.

Procedure

1 Direct Traffic to the Primary Nodes and Disable Health Monitoring for vRealize Automation on the Load Balancer

Before you upgrade the vRealize Automation appliances and the IaaS nodes, on the NSX load balancer for the management applications you must direct the traffic to the primary nodes of vRealize Automation and to turn off the health check on vRealize Automation traffic. Health checks might interfere with the upgrade and cause unpredictable behavior.

2 Upgrade the vRealize Automation Appliances

When you upgrade the vRealize Automation and the IaaS components in the SDDC, start the update process with upgrading the vRealize Automation Appliance from the virtual appliance management interface using the upgrade .iso file.

3 Upgrade the vRealize Automation IaaS Management Agent on Each IaaS Node

To continue your upgrade of vRealize Automation and the IaaS components in the SDDC, install the automated update process of the IaaS components via Remote Desktop.

4 Upgrade the IaaS Components by Using the Automated Upgrade Shell Script

To complete your upgrade of vRealize Automation and the IaaS components in the SDDC, begin the automated update process of the IaaS components from an SSH session to the primary vRealize Automation virtual appliance.

5 Delete the Snapshots of the vRealize Automation Virtual Machines

After you complete the update of the vRealize Automation nodes, clear the virtual machine snapshots.

6 Re-Enable the Secondary Nodes and Health Monitoring for vRealize Automation on the Load Balancer

After you upgrade the vRealize Automation components, on the server pools of the NSX load balancer for the management applications enable the secondary nodes to distribute traffic between the two nodes in each functional components again and enable the health checks on the vRealize Automation traffic.

What to do next

- Verify that vRealize Automation functions flawlessly after the upgrade. See *Validate vRealize Automation* in the *VMware Validated Design Operational Verification* documentation.

Direct Traffic to the Primary Nodes and Disable Health Monitoring for vRealize Automation on the Load Balancer

Before you upgrade the vRealize Automation appliances and the IaaS nodes, on the NSX load balancer for the management applications you must direct the traffic to the primary nodes of vRealize Automation and to turn off the health check on vRealize Automation traffic. Health checks might interfere with the upgrade and cause unpredictable behavior.

On the NSX load balancer, in the pools that are related to vRealize Automation, you disable the secondary nodes and deselect the monitor for the associated traffic.

Server Pool on the SFOMGMT-LB01 Load Balancer	Secondary Member to Disable
vra-svr-443	vra01svr01a or vra01svr01b according to which one is the primary node.
vra-iaas-web-443	vra01iws01b
vra-iaas-mgr-443	vra01ims01b

Procedure

- 1 Log in to the vRealize Automation appliance management console.
 - a Open a Web Browser and go to **https://vra01svr01a.rainpole.local:5480**.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	vra_appA_root_password

- 2 On **vRA Settings** tab, click the **Database** tab and check which node is labelled as REPLICA.
- 3 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

- 4 Click **Networking & Security**.
- 5 In the **Navigator**, click **NSX Edges**.
- 6 Select **172.16.11.65** from the **NSX Manager** drop-down menu.
- 7 Double-click the **SFOMGMT-LB01** device to open its settings.
- 8 On the **Load Balancer** tab, click **Pools**.
- 9 Select the **vra-svr-443** pool that contains the vRealize Automation appliances and click **Edit**.
- 10 In the **Edit Pool** dialog box, select the secondary node from [Step 2](#), click **Edit**, select **Disable** from the **State** drop-down menu and click **OK**.
- 11 In the **Edit Pool** dialog box, select **NONE** from the **Monitors** drop-down menu and click **OK**.
- 12 Repeat [Step 9](#) to [Step 11](#) on the other load balancer pools.

- 13 To verify that the load balancer works by redirecting the traffic to the primary node of the vRealize Automation appliance, in a Web browser go to **`https://vra01svr01.rainpole.local/vcac`**.

The login page of the vRealize Automation main portal appears.

Upgrade the vRealize Automation Appliances

When you upgrade the vRealize Automation and the IaaS components in the SDDC, start the update process with upgrading the vRealize Automation Appliance from the virtual appliance management interface using the upgrade .iso file.

Prerequisites

- Verify that a backup of the vRealize Automation database exists.
- Mount the upgrade .iso file to the primary virtual appliance svr01vra01.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://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 Take a snapshot of two vRealize Automation appliances.
 - a In the **Navigator**, click **VMs and Templates** and navigate to the vra01svr01a.rainpole.local virtual machine.
 - b Right-click the **vra01svr01a.rainpole.local** virtual machine and select **Snapshot > Take Snapshot**.
 - c In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	<i>Snapshot name</i>
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

- d Repeat these steps for the vra01svr01b.rainpole.local appliance.

- 3 Log in to the Virtual Appliance Management Interface of the primary vRealize Automation appliance
 - a Open a Web browser and go **https://vra01svr01a.rainpole.local:5480**.
 - b Log in using the following credentials

Settings	Value
User Name	root
Password	<i>vra_root_password</i>

- 4 Click the **Update** tab and click the **Settings** button.
- 5 Under the **Update Repository** section, select **Use CD-ROM Updates** and click **Save Settings**.
- 6 Click the **Status** and click **Check Updates** to load the update from the ISO file.
- 7 Validate that the loaded **Available Updates** match the appropriate version defined by the VMware Validated Design Software Components, and click **Install Updates**.
- 8 After the update completes, reboot the primary appliance.
- 9 Ensure the Directory Management has been configured for high availability by using both vRealize Automation appliances before you enable your virtual appliances on your load balancer:
 - a Open a Web browser and log in to
https://vra01svr01.rainpole.local/vcac/org/rainpole.
 - b Log in using the following credentials.

Setting	Value
User Name	ITAC-LocalRainpoleAdmin
Password	<i>itac-localrainpoleadmin_password</i>
Domain	vsphere.local

- c Navigate to **Administration > Directories Management > Directories**.
- d Click the **rainpole.local** directory, and select **Settings**.

- e Click **Identity Providers**, click the name of the identity provider **WorkspaceIDP_2**.
- f Verify that the identity provider has the following settings.

Setting	Expected Value
Connector(s)	<ul style="list-style-type: none"> ■ vra01svr01a.rainpole.local ■ vra01svr01b.rainpole.local
IdP Hostname	vra01svr01.rainpole.local

Infrastructure Service Portal

Welcome, ITAC-LocalRainpoleAdmin | Preferences | Help | Logout

Home | Inbox | Design | Administration | Infrastructure | Containers

Approval Policies

Directories Management >

Users & Groups >

Catalog Management >

Property Dictionary >

Reclamation >

Branding >

Notifications >

Events >

vRO Configuration >

Active Directory Policies

< Back to IdP List

WorkspaceIDP_2

Type: AUTOMATIC

Status: Enabled

Disable IdP

Identity Provider Name

WorkspaceIDP_2

Users

Select which users can authenticate using this IdP. Choose from the available Directories from the list below.

☒ rainpole.local

Network

Select which networks this IdP can be accessed from. Choose from the available network ranges from the list below.

☒ ALL RANGES

Authentication Methods

Select which authentication methods the IdP will use to authenticate users.

Authentication Methods	SAML Context
Password	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransp...

Connector(s)

☒ vra01svr01a.rainpole.local

☒ vra01svr01b.rainpole.local

Add a Connector You can deploy external connectors and add them to this IdP for high availability. Create the connector activation code from the Add a Connector page and set up the connector. You can then select that connector for this IdP.

IdP Hostname

vra01svr01.rainpole.local

This is the hostname where the Identity Provider will redirect to for authentication. If you are using a non-standard port other than 443, you can set this to Hostname:Port

Save Cancel

- 10 Synchronize vRealize Automation with the Active Directory immediately if you have just recently added service accounts such as svc-vrops-vra and svc-vra-vrops.
 - a Navigate to **Administration > Directories Management > Directories**
 - b Click **Sync Now**.
 - c Make sure that a green check mark appears after the synchronization is complete.

- d If a **Directory Sync Safeguards** warning appears, review the Active Directory configuration and verify that the new accounts you have created do increase your overall user accounts by more than 5%.
- e Select **Ignore Safeguards** and click **Sync Directory**.

The screenshot shows the vRealize Automation Administration console. The left sidebar contains a navigation menu with options: < Administration, Directories, Policies, Identity Providers, Connectors, User Attributes, Network Ranges, and Password Recovery. The main content area is titled 'Review' and displays a table for group and user synchronization. The table has columns for 'Add', 'Remove', and 'Update'. Below the table, there is a checkbox for 'Ignore Safeguards' and a red warning box with the text: 'Directory Sync Safeguards. You must either ignore or update the threshold for each safeguard violation. • You are attempting to add 19% of users to an existing group, more than your current limit of 5%.'

	Add	Remove	Update	
	0	0	0	Edit User DNS
	0	0	0	Edit Group DNS

After the initial sync, the sync is scheduled to run Once per week. You can change the sync frequency now or you can change it later from the Sync Frequency page. [Edit](#)

☐ Ignore Safeguards

Directory Sync Safeguards
 You must either ignore or update the threshold for each safeguard violation.
 • You are attempting to add 19% of users to an existing group, more than your current limit of 5%.

Upgrade the vRealize Automation IaaS Management Agent on Each IaaS Node

To continue your upgrade of vRealize Automation and the IaaS components in the SDDC, install the automated update process of the IaaS components via Remote Desktop.

You run the upgrade on each IaaS Windows virtual machine. You can start with the first IaaS Web server.

Region	Role	Fully Qualified Domain Name
Region A	vRealize Automation IaaS Web Server	vra01iws01a.rainpole.local
		vra01iws01b.rainpole.local
	vRealize Automation Model Manager Service	vra01ims01a.rainpole.local
		vra01ims01b.rainpole.local
	vRealize Automation DEM Workers	vra01dem01.rainpole.local
		vra01dem02.rainpole.local
Region B	vRealize Automation Proxy Agent	vra01ias01.sfo01.rainpole.local
		vra01ias02.sfo01.rainpole.local
	vRealize Automation Proxy Agent	vra01ias51.lax01.rainpole.local
		vra01ias52.lax01.rainpole.local

Prerequisites

- Download the vRealize Automation IAS Management Agent .msi file to the Windows host that you use to access the data center. See the [product download page](#) build 4683764 or later.

- Verify that each IaaS Windows virtual machine satisfies the following requirements:
 - Installed Microsoft .NET Framework 4.5.2 or later
 - Installed Java SE Runtime Environment 8 64-bit update 91 or later
 - JAVA_HOME environment variable set to the Java home directory

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 Take a snapshot of each IaaS Windows machine.

- a In the **Navigator**, click **VMs and Templates** and navigate to the vra01iws01a.rainpole.local virtual machine.
- b Right-click the **vra01iws01a.rainpole.local** virtual machine and select **Snapshot > Take Snapshot**.
- c In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	<i>Snapshot name</i>
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

- d Repeat these steps for the other machines.
- 3 On the Windows host that has access to the data center, log in to the IaaS Web server by using a Remote Desktop Protocol (RDP) client.
 - a Open an RDP connection to vra01iws01a.rainpole.local.
 - b Log in using the following credentials.

Setting	Value
User name	rainpole.local\svc-vra
Password	svc-vra_password

- 4 Copy the agent installer .msi file to the file system of vra01iws01a.rainpole.local.

- 5 Navigate to the folder where you downloaded the IaaS Management Agent upgrade installer, and start the installed.

The agent installation wizard appears.

- 6 On the **Welcome** page, click **Next**.
- 7 On the **End User License Agreement** page, select the **I agree to the terms in the license agreement** check box, and click **Next**.
- 8 On the **Management Agent Account configuration** page, provide the following settings and click **Next**.

Setting	Value
User name	rainpole.local\svc-vra
Password	svc-vra_password

- 9 On the **Ready to Install** page, click **Install** and allow the installer to complete.
- 10 Reboot the Windows virtual machine.
- 11 Repeat [Step 3](#) to [Step 10](#) on the other IaaS components.
- 12 After you upgrade all IaaS nodes, verify the build number of the management agent on each node. log in to the vRealize Automation Appliance management interface.



VMware vRealize Appliance

vRA Settings

Services

System

Telemetry

Network

Update

Admin

Host Settings

SSO

Licensing

Database

Messaging

Cluster

Logs

IaaS Install

Migration

Xenon

Distributed Deployment Information

Leading Cluster Node*

Admin User*

root

Password*

Status

[2017-03-06 11:21:45] [root] [INFO] Current node in cluster mode

Create Support Bundle



Save a support bundle that includes logs from all nodes connected to this cluster.

Create Support Bundle

There are no collected bundles.

Host / Node Name	Version	Time Offset (sec)	Last Connected	Type	
▶ vra01svr01b.rainpole.local	7.2.0.381		103 seconds ago	VA	Delete
▶ vra01iws01a.rainpole.local	7.2.0.9559	8	20 seconds ago	IAAS	Delete
▶ vra01iws01b.rainpole.local	7.2.0.9559	8	27 seconds ago	IAAS	Delete
▶ vra01ims01a.rainpole.local	7.2.0.9559	8	29 seconds ago	IAAS	Delete
▶ vra01ims01b.rainpole.local	7.2.0.9559	7	27 seconds ago	IAAS	Delete
▶ vra01ias01.sfo01.rainpole.local	7.2.0.9559	9	6 seconds ago	IAAS	Delete

- a Open a Web browser and log in to **https://vra01svr01a.rainpole.local:5480**.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vra_appA_root_password</i>

- c Click **vRA Settings > Cluster** and verify that each of the IaaS components has a **ManagementAgent** build number of 7.2.0.9559 or later.

Upgrade the IaaS Components by Using the Automated Upgrade Shell Script

To complete your upgrade of vRealize Automation and the IaaS components in the SDDC, begin the automated update process of the IaaS components from an SSH session to the primary vRealize Automation virtual appliance.

Prerequisites

- Verify that your primary vRealize IaaS Web Server, Microsoft SQL database, and Model Manager node satisfy the following requirements:
 - Microsoft .NET Framework 4.5.2 version installed.
 - At least 5 GB of free disk space available.
 - JAVA SE Runtime Environment 8 64-bit update 91 or later installed.
 - JAVA_HOME environment variable set to the Java home directory.

Procedure

- 1 Connect to the primary vRealize Automation appliance by using a Secure Shell (SSH) client.
 - a Open an SSH session to `vra01svr01a.rainpole.local`.
 - b Log in using the following credentials

Setting	Value
User Name	root
Password	<i>vra_appA_root_password</i>

- 2 Go to the following directory.

```
cd /usr/lib/vcac/tools/upgrade/
```

- 3 Run the following command to create the `upgrade.properties` file.

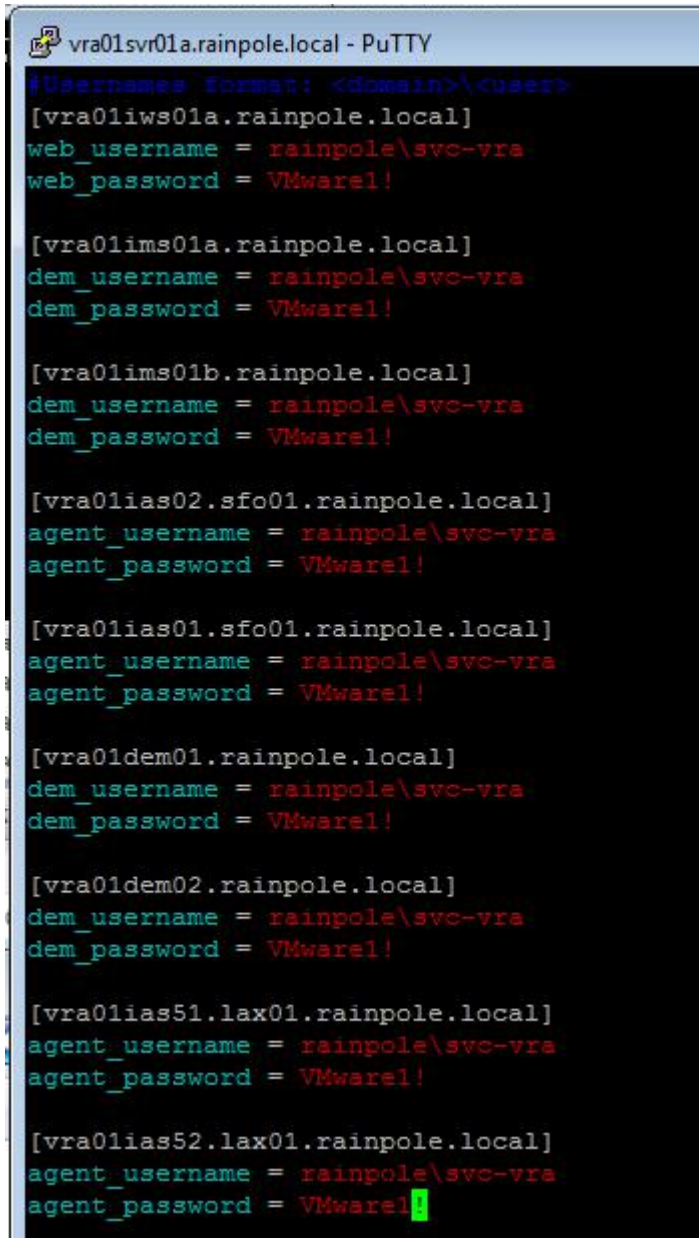
```
./generate_properties
```

- 4 Using the appliance's text editor, open the `upgrade.properties` file.

```
vi upgrade.properties
```

- 5 In the `upgrade.properties` file, update each of the `*_user` and `*_password` fields and save the file.

Node	Setting
vra01iws01a.rainpole.local	web_user = rainpole\svc-vra web_password = <i>svc-vra_password</i>
vra01ims01a.rainpole.local	dem_user = rainpole\svc-vra dem_password = <i>svc-vra_password</i>
vra01ims01b.rainpole.local	dem_user = rainpole\svc-vra dem_password = <i>svc-vra_password</i>
vra01ias01.sfo01.rainpole.local	agent_user = rainpole\svc-vra agent_password = <i>svc-vra_password</i>
vra01ias02.sfo01.rainpole.local	agent_user = rainpole\svc-vra agent_password = <i>svc-vra_password</i>
vra01dem01.rainpole.local	dem_user = rainpole\svc-vra dem_password = <i>svc-vra_password</i>
vra01dem02.rainpole.local	dem_user = rainpole\svc-vra dem_password = <i>svc-vra_password</i>
vra01ias51.lax01.rainpole.local	web_user = rainpole\svc-vra web_password = <i>svc-vra_password</i>
vra01ias52.lax01.rainpole.local	web_user = rainpole\svc-vra web_password = <i>svc-vra_password</i>



```

vra01svr01a.rainpole.local - PuTTY
#Username format: <domain>\<user>
[vra01iws01a.rainpole.local]
web_username = rainpole\svc-vra
web_password = VMware1!

[vra01ims01a.rainpole.local]
dem_username = rainpole\svc-vra
dem_password = VMware1!

[vra01ims01b.rainpole.local]
dem_username = rainpole\svc-vra
dem_password = VMware1!

[vra01ias02.sfo01.rainpole.local]
agent_username = rainpole\svc-vra
agent_password = VMware1!

[vra01ias01.sfo01.rainpole.local]
agent_username = rainpole\svc-vra
agent_password = VMware1!

[vra01dem01.rainpole.local]
dem_username = rainpole\svc-vra
dem_password = VMware1!

[vra01dem02.rainpole.local]
dem_username = rainpole\svc-vra
dem_password = VMware1!

[vra01ias51.lax01.rainpole.local]
agent_username = rainpole\svc-vra
agent_password = VMware1!

[vra01ias52.lax01.rainpole.local]
agent_username = rainpole\svc-vra
agent_password = VMware1!

```

After the upgrade is complete, this file is deleted. No plaintext passwords remain on the disk.

- 6 Start the automated upgrade by running the following command.

```
./upgrade
```

What to do next

Re-enable the health checks on the NSX Load Balancer for vRealize Automation

Re-enable the load balancer pool to allow access to both Primary and Secondary vRealize Automation components.

Cleanup the snapshots used on the vRealize Automation components.

Proceed to updating the vRealize Business components with the Cloud Management Platform. For guidance on performing the update, consult [Upgrade vRealize Business and vRealize Business Data Collectors](#).

Delete the Snapshots of the vRealize Automation Virtual Machines

After you complete the update of the vRealize Automation nodes, clear the virtual machine snapshots.

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 In the **Navigator**, click **VMs and Templates** and navigate to the vrops-mstrn-01.
- 3 Right-click the **vra01svr01a.rainpole.local** virtual machine and select **Manage Snapshots**.
- 4 In the **Snapshot Manager**, click the snapshot that you created before the vRealize Operations Manager update and select **Delete**.
- 5 Click **Yes** in the confirmation dialog box and click **Close** in **Snapshot Manager**.
- 6 Repeat the procedure for the other virtual machines of vRealize Automation.

Region	Virtual Machine Name
Region A	vra01svr01a.rainpole.local
	vra01svr01b.rainpole.local
	vra01iws01a.rainpole.local
	vra01iws01b.rainpole.local
	vra01ims01a.rainpole.local
	vra01ims01b.rainpole.local
	vra01dem01.rainpole.local
	vra01dem01.rainpole.local
	vra01ias01.sfo01.rainpole.local
	vra01ias02.sfo01.rainpole.local
	vra01mssql01.rainpole.local
Region B	vra01ias51.lax01.rainpole.local
	vra01ias52.lax01.rainpole.local

Re-Enable the Secondary Nodes and Health Monitoring for vRealize Automation on the Load Balancer

After you upgrade the vRealize Automation components, on the server pools of the NSX load balancer for the management applications enable the secondary nodes to distribute traffic between the two nodes in each functional components again and enable the health checks on the vRealize Automation traffic.

On the NSX load balancer, in the pools that are related to vRealize Automation, you enable again the secondary nodes and select the monitor for the associated traffic.

Server Pool on the SFOMGMT-LB01 Load Balancer	Secondary Member to Re-Enable	Service Monitor to Re-Associate
vra-svr-443	vra01svr01a or vra01svr01b according to which one is the primary node.	vra-svr-443-monitor
vra-iaas-web-443	vra01iws01b	vra-iaas-web-443-monitor
vra-iaas-mgr-443	-	vra-iaas-mgr-443-monitor

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 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 to open its settings.
- 6 On the **Load Balancer** tab, click **Pools**.
- 7 Select the **vra-svr-443** pool that contains the vRealize Automation appliances and click **Edit**.
- 8 In the **Edit Pool** dialog box, select the secondary node that you disabled before the upgrade, click **Edit**, select **Enable** from the **State** drop-down menu and click **OK**.
- 9 In the **Edit Pool** dialog box, select **vra-svr-443-monitor** from the **Monitors** drop-down menu and click **OK**.

- 10 Repeat [Step 7](#) to [Step 9](#) on the other load balancer pools.

On the vra-iaas-mgr-443 pool, you only re-enable the health checks by associating it with the vra-iaas-mgr-443-monitor monitor.

Upgrade vRealize Business and vRealize Business Data Collectors

After you upgrade the vRealize Automation nodes, upgrade the vRealize Business for Cloud server in Region A, and the remote data collectors in Region A and Region B.

Prerequisites

- Download the vRealize Business upgrade .iso file to a shared datastore for mounting to the virtual appliances.

If you have space on your NFS datastore, upload the file there.

- Allocate 8 GB RAM and 4 vCPUs to the vRealize Business Server appliance.

Procedure

1 [Upgrade the vRealize Business Server Appliance](#)

When you upgrade the vRealize Business Server appliance and the region-specific Data Collectors in the SDDC, start the process from the vRealize Business Server by using the virtual appliance management interface.

2 [Upgrade the vRealize Business Remote Data Collectors](#)

After you upgrade the vRealize Business Server appliance, upgrade the region-specific remote data collectors by using the vRealize Business virtual appliance management interface.

3 [Delete the Snapshots of the vRealize Business Appliances](#)

After you complete the update of the vRealize Business nodes, clear the virtual machine snapshots.

What to do next

- Verify that vRealize Business functions flawlessly after the upgrade. See *Validate the Cloud Management Platform* in the *VMware Validated Design Operational Verification* documentation.

Upgrade the vRealize Business Server Appliance

When you upgrade the vRealize Business Server appliance and the region-specific Data Collectors in the SDDC, start the process from the vRealize Business Server by using the virtual appliance management interface.

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 Take a snapshot of the vRealize Business Server appliance.

- a In the **Navigator**, click **VMs and Templates** and navigate to the vra01bus01.rainpole.local virtual machine.
- b Right-click the **vra01bus01.rainpole.local** virtual machine and select **Snapshot > Take Snapshot**.
- c In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	<i>Snapshot name</i>
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

- 3 Mount the upgrade .iso file to the virtual appliance vra01bus01.rainpole.local.
- 4 Log in to the Virtual Appliance Management Interface of the vRealize Business for Cloud appliance
 - a Open a Web browser and go **`https://vra01bus01.rainpole.local:5480`**.
 - b Log in using the following credentials.

Setting	Value
User Name	root
Password	vrb_root_password

5 Unregister vRealize Business for Cloud from vRealize Automation.

- a On the **Registration** tab, click **vRA**.
- b Enter the following values and click **Unregister**.

Setting	Value
Hostname	vra01svr01.rainpole.local
SSO Default Tenant	rainpole
SSO Admin User	administrator
SSO Admin Password	<i>vra_administrator_password</i>

An Unregistered from vRealize Automation message appears at the top of the page.

6 Start the upgrade of the appliance.

- a Click the **Update** tab and click **Settings**.
- b Under **Update Repository** section, select the **Use CD-ROM Updates** radio button and click **Save Settings**.
- c Click the **Status** button and click **Check Updates** to load the update from the ISO.
- d Click **Install Updates**.

7 After the upgrade is complete, re-register vRealize Business for Cloud with vRealize Automation.

- a On the **Registration** tab, click the **vRA** button
- b Enter the following settings and click **Register**.

Setting	Value
Hostname	vra01svr01.rainpole.local
SSO Default Tenant	rainpole
SSO Admin User	administrator
SSO Admin Password	<i>vra_administrator_password</i>

A Registered with vRealize Automation message appears at the top of the page.

What to do next

Login and verify that the license key for vRealize Business for Cloud is still valid within vRealize Automation. For more information, see the *Update Licenses for vRealize Business for Cloud* section of the [vRealize Business for Cloud 7.2 Install Guide](#).

Upgrade the vRealize Business Remote Data Collectors

After you upgrade the vRealize Business Server appliance, upgrade the region-specific remote data collectors by using the vRealize Business virtual appliance management interface.

You can update the two vRealize Business remote data collectors in Region A and Region B one after the other or in parallel.

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 Take a snapshot of the vRealize Business Server remote data collector.

- a In the **Navigator**, click **VMs and Templates** and navigate to the vra01buc01.sfo01.rainpole.local virtual machine.
- b Right-click the **vra01buc01.sfo01.rainpole.local** virtual machine and select **Snapshot > Take Snapshot**.
- c In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	<i>Snapshot name</i>
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

- 3 Mount the upgrade .iso file to the vra01buc01.sfo01.rainpole.local virtual appliance.
- 4 Log in to the virtual appliance management interface of the vRealize Business data collector appliance.
- a Open a Web browser and go the following URL.

Region	URL
Region A	<code>https://vra01buc01.sfo01.rainpole.local:5480</code>
Region B	<code>https://vra01buc51.lax01.rainpole.local:5480</code>

- b Log in using the following credentials.

Setting	Value
User Name	root
Password	vrb_collector_root_password

- 5 On the **Update** tab, click **Settings**.

- 6 Under the **Update Repository** section, select the **Use CD-ROM Updates** radio button and click **Save Settings**.
- 7 Click **Status**, click **Check Updates** to load the update from the ISO and click **Install Updates**.
- 8 Repeat this operation on the other remote data collector vra01buc51.lax01.rainpole.local.

What to do next

Verify that vRealize Business functions flawlessly after the upgrade. See *Verify the Version, Service Status and Configuration of the vRealize Business VMs* in the *VMware Validated Design Operational Verification* documentation.

Delete the Snapshots of the vRealize Business Appliances

After you complete the update of the vRealize Business nodes, clear the virtual machine snapshots.

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 In the **Navigator**, click **VMs and Templates** and navigate to the vra01bus01.rainpole.local virtual machine.
- 3 Right-click the **vra01bus01.rainpole.local** virtual machine and select **Manage Snapshots**.
- 4 In the **Snapshot Manager**, click the snapshot that you created before the vRealize Business update and select **Delete**.
- 5 Click **Yes** in the confirmation dialog box and click **Close** in **Snapshot Manager**.
- 6 Repeat the procedure for the other virtual machines of vRealize Business.

Role	Virtual Machine Name
Data Collector in Region A	vra01buc01.sfo01.rainpole.local
Data Collector in Region B	vra01buc51.lax01.rainpole.local

Upgrade vRealize Orchestrator Cluster

After you upgrade the vRealize Automation and vRealize Business components, complete the upgrade the Cloud Management Platform to VMware Validated Design 4.0 by upgrading the vRealize Orchestrator cluster.

Table 2-2. vRealize Orchestrator Nodes in the SDDC

Region	Role	IP Address	Fully Qualified Domain Name
Region A	vRealize Orchestrator VIP	192.168.11.65	vra01vro01.rainpole.local
	vRealize Orchestrator	192.168.11.63	vra01vro01a.rainpole.local
	vRealize Orchestrator	192.168.11.64	vra01vro01b.rainpole.local

Prerequisites

- Download the vRealize Orchestrator upgrade .iso file to a shared datastore for mounting to the virtual appliance.
- Allocate 6 GB of memory to the primary and secondary vRealize Orchestrator virtual appliances (vra01vro01a.rainpole.local and vra01vro01b.rainpole.local).

Procedure

1 [Update the vRealize Orchestrator Cluster](#)

When you upgrade the vRealize Orchestrator Cluster in the SDDC, start the update process by picking a primary vRealize Orchestrator node, and beginning the upgrade via the Virtual Appliance Management Interface.

2 [Delete the Snapshots of the vRealize Orchestrator Appliances](#)

After you complete the upgrade of the vRealize Orchestrator nodes, clear the virtual machine snapshots.

What to do next

- Verify that vRealize Orchestrator functions flawlessly after the upgrade. See *Validate the Cloud Management Platform* in the *VMware Validated Design Operational Verification* documentation.

Update the vRealize Orchestrator Cluster

When you upgrade the vRealize Orchestrator Cluster in the SDDC, start the update process by picking a primary vRealize Orchestrator node, and beginning the upgrade via the Virtual Appliance Management Interface.

Prerequisites

Verify that a backup of the vRealize Orchestrator database exists.

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 In the Navigator, click **VMs and Templates**.
- 3 Expand the mgmt01vc01.sfo01.rainpole.local vCenter Server tree.
- 4 Shut down each vRealize Orchestrator node in the cluster.
 - a Navigate to the one of following virtual machines.

Designation	Object Name
Primary	vra01vro01a.rainpole.local
Secondary	vra01vro01b.rainpole.local

- b Right-click the virtual machine, select **Power > Shut Down Guest OS** and click **Yes** in the confirmation dialog box that appears.
- 5 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

- 6 Verify that both vRealize Orchestrator nodes vra01vro01a.rainpole.local and vra01vro01b.rainpole.local have their memory increased to 6 GB.
 - a In the **Navigator**, click **VMs and Templates** and navigate to the vra01vro01a.rainpole.local virtual machine.
 - b Right-click the **vra01vro01a.rainpole.local** virtual machine and select **Edit Settings**.

- c In the **Edit Settings** dialog box, ensure the following resources have been allocated to the virtual machine and click **OK**.

Setting	Value
CPU	2
Memory	6144 MB (6 GB)

- d Repeat these steps for vra01vro01b.rainpole.local.

7 Take a snapshot of each node in the cluster.

- a In the **Navigator**, click **VMs and Templates** and navigate to the vra01vro01a.rainpole.local virtual machine.
- b Right-click the **vra01vro01a.rainpole.local** virtual machine and select **Snapshot > Take Snapshot**.
- c In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	<i>Snapshot name</i>
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

- d Repeat these steps for vra01vro01b.rainpole.local.

8 Verify that a backup of the vRealize Orchestrator database exists.

9 Mount the upgrade .iso file to the vra01vro01a.rainpole.local virtual appliance.

10 Right-click the vra01vro01a.rainpole.local virtual machine, and select **Power > Power On**.

11 Log in to the virtual appliance management interface of the primary vRealize Orchestrator appliance.

- a Open a Web browser and go **https://vra01vro01a.rainpole.local:5480**.
- b Log in using the following credentials.

Setting	Value
User Name	root
Password	<i>vro_root_password</i>

12 On the **Update** tab, click **Settings**.

13 Under **Update Repository** section, select the **Use CD-ROM Updates** radio button and click **Save Settings**.

14 Click **Status**, click **Check Updates** to load the update from the ISO and click **Install Updates**.

- 15 After the update completes, restart the primary vRealize Orchestrator appliance.
 - a On the **System** Tab, click **Information**.
 - b Click **Reboot**.
 - c In the **System Reboot** dialog box, click **Reboot**.
- 16 Verify that the vRealize Orchestrator node configuration is valid in the vRealize Orchestrator Control Center.
 - a Open a Web browser and log in to
`https://vra01vro01a.rainpole.local:8283/vco-controlcenter`.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vro_appliance_A_root_pwd</i>

- c Click the **Validate Configuration** icon and verify that all configuration settings are valid except the cluster section.

You have not upgraded the secondary node yet.

- 17 Repeat [Step 9](#) to [Step 16](#) to upgrade the vra01vro01b.rainpole.local vRealize Orchestrator appliance.
- 18 Verify that the configuration of vRealize Orchestrator nodes is valid in the vRealize Orchestrator Control Center.
 - a Open a Web browser and log in to
`https://vra01vro01a.rainpole.local:8283/vco-controlcenter`.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vro_appliance_A_root_pwd</i>

- c Click the **Validate Configuration** icon and verify that all configuration settings are valid.
- d Repeat the step on **`https://vra01vro01b.rainpole.local:8283/vco-controlcenter`**.

What to do next

On the vRealize Orchestrator Control Center, upgrade the vRealize Automation default plugins, which include the NSX plugin

Delete the Snapshots of the vRealize Orchestrator Appliances

After you complete the upgrade of the vRealize Orchestrator nodes, clear the virtual machine snapshots.

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 In the **Navigator**, click **VMs and Templates** and navigate to the vra01vro01a.rainpole.local virtual machine.
- 3 Right-click the **vra01vro01a.rainpole.local** virtual machine and select **Manage Snapshots**.
- 4 In the **Snapshot Manager**, click the snapshot that you created before the vRealize Business update and select **Delete**.
- 5 Click **Yes** in the confirmation dialog box and click **Close** in **Snapshot Manager**.
- 6 Repeat the procedure for the vra01vro01b.rainpole.local virtual machine.

Post-Upgrade Configuration of the Cloud Management Platform

After you upgrade the components of the Cloud Management Platform, perform the following configuration changes to the environment according to the objectives and deployment guidelines of this validated design.

Procedure

- 1 **Rename the Anti-Affinity Rules for vRealize Automation and vRealize Orchestrator Virtual Machines**
After you update the vRealize Automation and vRealize Orchestrator appliances, rename the anti-affinity rules for these components in vSphere DRS to implement a configuration that matches the deployment guidelines in this validated design.
- 2 **Configure the Load Balancer Application Profiles for vRealize Automation and vRealize Orchestrator**
After you complete the upgrade of vRealize Automation and vRealize Orchestrator, configure the application profiles on the NSX load balancer according to the deployment guidelines of this validated design.
- 3 **Increase the Virtual Memory and the Number of Virtual CPUs of the vRealize Business Appliances**
After you complete the update of the vRealize Business appliance, increase its compute resources so that the appliance can handle the number of tenant workloads according to this VMware Validated Design objectives.

4 Configure Integration of vRealize Operations Manager with vRealize Automation for Workload Reclamation

Connect vRealize Automation with vRealize Operations Manager to collect metrics that vRealize Automation can use to identify tenant workloads for reclamation according to the objectives and deployment guidelines of this validated design.

Rename the Anti-Affinity Rules for vRealize Automation and vRealize Orchestrator Virtual Machines

After you update the vRealize Automation and vRealize Orchestrator appliances, rename the anti-affinity rules for these components in vSphere DRS to implement a configuration that matches the deployment guidelines in this validated design.

Perform the procedure six times starting with the rule for the vRealize Automation appliances.

Table 2-3. Anti-Affinity Rules Configuration After Cloud Management Platform Update

Region	Old Rule Name	New Rule Name	Members	vCenter Server Cluster
Region A	anti-affinity-rule-svr	anti-affinity-rule-vra-svr	vra01svr01a.rainpole.local, vra01svr01b.rainpole.local	mgm01vc01.sfo01.rainpole.local > SFO01 > SFO01-Mgmt
	anti-affinity-rule-iws	anti-affinity-rule-vra-iws	vra01iws01a.rainpole.local, vra01iws01b.rainpole.local	
	anti-affinity-rule-ims	anti-affinity-rule-vra-ims	vra01ims01a.rainpole.local, vra01ims01b.rainpole.local	
	anti-affinity-rule-dem	anti-affinity-rule-vra-dem	vra01dem01.rainpole.local, vra01dem02.rainpole.local	
	anti-affinity-rule-ias	anti-affinity-rule-vra-ias	vra01ias01.sfo01.rainpole.local, vra01ias02.sfo01.rainpole.local	
	anti-affinity-rule-vro	anti-affinity-rule-vro	vra01vro01a.rainpole.local, vra01vro01b.rainpole.local	
Region B	anti-affinity-rule-ias	anti-affinity-rule-vra-ias	vra01ias51.lax01.rainpole.local, vra01ias52.lax01.rainpole.local	mgm01vc51.lax01.rainpole.local > LAX01 > LAX01-Mgmt

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** page, click **Hosts and Clusters**.
- 3 In the **Navigator**, expand **mgmt01vc01.sfo01.rainpole.local > SFO01** and click **SFO01-Mgmt01**.
- 4 On the **Manage** tab, select **VM/Host Rules** under **Configuration**.

- 5 Rename the anti-affinity rules for the vRealize Automation appliances.
 - a Select the **anti-affinity-rule-svr** from the **VM/Host Rules** list and click **Edit**.
 - b In the **Edit VM/Host Rule** dialog box, enter **anti-affinity-rule-vra-svr** in the **Name** text box and click **OK**.

SFO01-Mgmt01 - Edit VM/Host Rule

Name:

☒ Enable rule.

Type: Separate Virtual Machines

Description:

The listed Virtual Machines must be run on separate hosts.

Members	
	vra01svr01a.rainpole.local
	vra01svr01b.rainpole.local

- 6 Repeat [Step 5](#) to rename the remaining anti-affinity rules in Region A and Region B.

Configure the Load Balancer Application Profiles for vRealize Automation and vRealize Orchestrator

After you complete the upgrade of vRealize Automation and vRealize Orchestrator, configure the application profiles on the NSX load balancer according to the deployment guidelines of this validated design.

You repeat this procedure twice to create two application profiles.

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 **Networking & Security**.
- 3 On the **NSX Home** page, click **NSX Edges** and select **172.16.11.65** from the **NSX Manager** drop-down menu at the top of the **NSX Edges** page.
- 4 Double-click the **SFOMGMT-LB01** NSX Edge to manage its network settings, and on the **Manage** tab, click the **Load Balancer** tab.
- 5 Rename the existing application profile for vRealize Automation and create a new non-persistent one.
 - a On the **Load Balancer** page, click **Application Profiles**.
 - b Select the **vRealize-https** profile, click the **Edit** icon, change the following values, and click **OK**.

Setting	Value
Name	vRealize-https-persist
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	Source IP
Expires in (Seconds)	1800

- c Click the **New** icon, enter the following values in the **New Profile** dialog box, and click **OK**.

Setting	Value
Name	vRealize-https
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	None

- 6 Change the algorithm for load balancing of vRealize Automation and vRealize Orchestrator.
 - a On the **Load Balancer** page, click **Pools**.
 - b Select **vra-svr-443** and click **Edit**.

- c In the **Edit Pool** dialog box, select **ROUND-ROBIN** from the **Algorithm** drop-down menu and click **OK**.
 - d Repeat the steps to change the algorithm to **ROUND-ROBIN** on the following server pools.
 - vra-iaas-web-443
 - vra-iaas-mgr-443
 - vra-vro-8281
 - vra-svr-8444
- 7 Rename the virtual servers for the vRealize Automation Appliance UI, vRealize Automation IaaS Web UI and vRealize Automation Remote Console Proxy.
- a On the **Load Balancer** page, click **Virtual Servers**.
 - b Select **vra-svr-443** , click **Edit**.
 - c In the **Edit Virtual Server** dialog box, from the **Application Profile** drop-down menu, select **vRealize-https-persist** and click **OK**.
 - d Repeat the steps to change the application profile to **vRealize-https-persist** on the following virtual servers.
 - vra-iaas-web-443
 - vra-svr-8444

Increase the Virtual Memory and the Number of Virtual CPUs of the vRealize Business Appliances

After you complete the update of the vRealize Business appliance, increase its compute resources so that the appliance can handle the number of tenant workloads according to this VMware Validated Design objectives.

You increase the amount of virtual memory and number of virtual CPUs of all vRealize Business nodes. You start with the vRealize Business appliance first.

Table 2-4. Compute Post-Upgrade Configuration for the vRealize Business Nodes

vRealize Business Node	Memory	Number of Virtual CPUs
vra01bus01.rainpole.local	8 GB	8
vra01buc01.sfo01.rainpole.local	8 GB	8
vra01buc51.lax01.rainpole.local	8 GB	8

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 Change the amount of virtual memory and number of virtual CPUs of the vRealize Business virtual appliance.
 - a In the **Navigator**, navigate to the vra01bus01.rainpole.local virtual machine.
 - b Right-click the **vra01bus01.rainpole.local** virtual machine and select **Power > Power Off**.
 - c Right-click the virtual machine and select **Edit Settings**.
 - d In the **Edit Settings** dialog box, click the **Virtual Hardware** tab, and in the **CPU** text box increase the number of virtual CPU to 4.
 - e In the **Memory** text box, change the amount of memory to 8 GB, and click **OK**.
 - f Right-click the **vra01bus01.rainpole.local** virtual machine and select **Power > Power On**.
- 3 Repeat [Step 2](#) to configure the compute resources for the other vRealize Business nodes.

Configure Integration of vRealize Operations Manager with vRealize Automation for Workload Reclamation

Connect vRealize Automation with vRealize Operations Manager to collect metrics that vRealize Automation can use to identify tenant workloads for reclamation according to the objectives and deployment guidelines of this validated design.

Procedure

- 1 [Configure User Privileges on vRealize Operations Manager for Tenant Workload Reclamation](#)

After you update the Cloud Management Platform, configure read-only privileges for the svc-vra-vrops@rainpole.local service account on vRealize Operations Manager for compliance with the setup of this validated design. You configure these privileges so that vRealize Automation can pull metrics from vRealize Operations Manager for reclamation of tenant workloads in Region A and Region B.

- 2 [Add vRealize Operations Manager as a Metrics Provider in vRealize Automation](#)

After you upgrade vRealize Automation and configure a service account on vRealize Operations Manager for pulling statistics, connect vRealize Automation to vRealize Operations Manager to start retrieving metrics for reclamation of tenant workloads.

Configure User Privileges on vRealize Operations Manager for Tenant Workload Reclamation

After you update the Cloud Management Platform, configure read-only privileges for the `svc-vra-vrops@rainpole.local` service account on vRealize Operations Manager for compliance with the setup of this validated design. You configure these privileges so that vRealize Automation can pull metrics from vRealize Operations Manager for reclamation of tenant workloads in Region A and Region B.

Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.
 - b Log in using the following credentials.

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

- 2 In the left pane of vRealize Operations Manager, click **Administration**, and click **Access Control**.
- 3 On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.
- 4 On the **Import Users** page, import the `svc-vra-vrops@rainpole.local` service account.
 - a From the **Import From** drop-down menu, select **RAINPOLE.LOCAL**.
 - b Select the **Basic** option for the search query.
 - c In the **Search String** text box, enter **`svc-vra-vrops`** and click **Search**.
The search results contain the `svc-vra-vrops` user account.
 - d Select **`svc-vra-vrops@rainpole.local`** and click **Next**.

Import Users

1 Import Users

2 Assign Groups and Permissions

Import From: RAINPOLE.LOCAL

Change Credentials

Basic Advanced

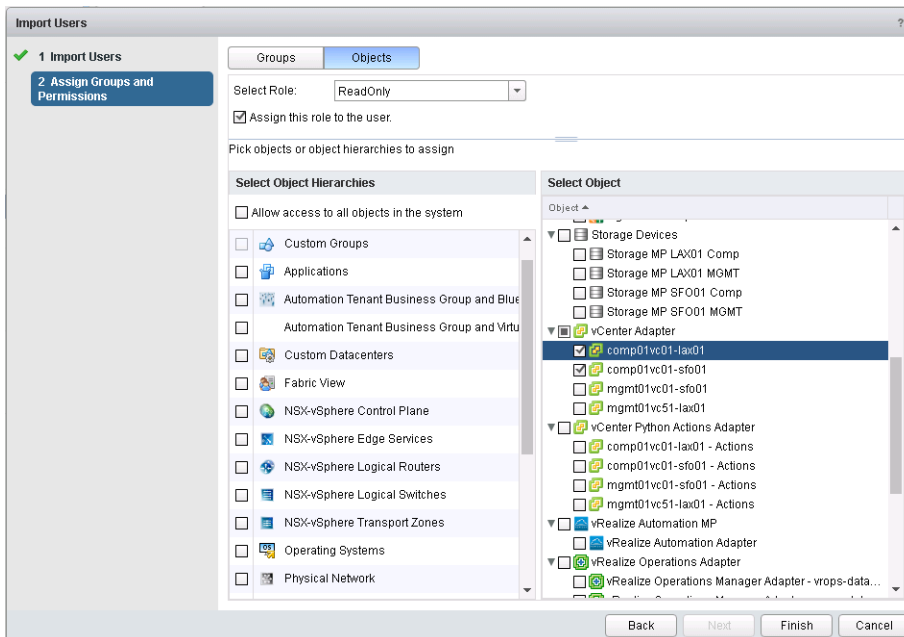
Search String: svc-vra-vrops Search

User Name	First Name	Last Name	Distinguished Name	Email Address
svc-vra-vrops@rainpole.local	svc-vra-vr...		CN=svc-vra-vrops,CN=U...	

Back Next Finish Cancel

- 5 On the **Assign Groups and Permissions** page, to assign the ReadOnly role to the svc-vra-vrops@rainpole.local service account, click the **Objects** tab, configure the following settings and click **Finish**.

Setting	Value
Select Role	ReadOnly
Assign this role to the user	Selected
Select Object	<ul style="list-style-type: none"> ■ vCenter Adapter > comp01vc01-sfo01 ■ vCenter Adapter > comp01vc51-lax01
Select Object Hierarchies	Adapter Instance This option is automatically selected after you select the adapter instance.



Add vRealize Operations Manager as a Metrics Provider in vRealize Automation

After you upgrade vRealize Automation and configure a service account on vRealize Operations Manager for pulling statistics, connect vRealize Automation to vRealize Operations Manager to start retrieving metrics for reclamation of tenant workloads.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	Rainpole.local

- 2 Navigate to **Administration > Reclamation > Metrics Provider**.
- 3 On the **Metrics Provider** page, configure the vRealize Operations Manager settings.

Infrastructure Service Portal

Welcome, ITAC-TenantAdmin. Preferences Help Logout

Home Catalog Items Requests Inbox Design Administration Infrastructure Containers Business Management

Administration

Deployments

Reclamation Requests

Metrics Provider

Metrics Provider

Select a metrics provider for vSphere virtual machine metrics.

✓ vSphere metrics provider updated successfully

☐ vRealize Automation metrics provider

☒ vRealize Operations Manager endpoint

* URL:

* Username:

* Password:

Test Connection Save Cancel

- a Select **vRealize Operations Manager endpoint**.
- b Configure the following settings for vRealize Operations Manager.

Setting	Value
URL	https://vrops-cluster-01.rainpole.local/suite-api/
Username	svc-vra-vrops@rainpole.local
Password	<i>svc-vra-vrops_password</i>

- c Click **Test Connection**, verify that the test connection is successful, and click **Save**.
- d In the certificate warning message box, click **OK**.

The vSphere metrics provider updated successfully message appears.

Upgrade Operations Management Components

3

After you upgrade the Cloud Management Platform, upgrade vRealize Operations Manager and vRealize Log Insight, the components of the Operations Management stack, the to start using their monitoring capabilities.

- [Upgrade vRealize Operations Manager](#)

You update the virtual appliances and management packs of the vRealize Operations Manager deployment. You perform additional configuration on the adapters of the installed management packs, on vSphere DRS and the SDDC dashboards to make the environment complaint with the objectives and deployment guidelines of this version of the validated design.

- [Upgrade vRealize Log Insight](#)

Upgrade the vRealize Log Insight clusters and agents in Region A and Region B so that you can use the new features of and have an environment that is compliant with version 4.0 of this VMware Validated Design.

Upgrade vRealize Operations Manager

You update the virtual appliances and management packs of the vRealize Operations Manager deployment. You perform additional configuration on the adapters of the installed management packs, on vSphere DRS and the SDDC dashboards to make the environment complaint with the objectives and deployment guidelines of this version of the validated design.

When you upgrade the virtual appliances of vRealize Operations Manager in your SDDC, you perform the update operation manually only on the master node in the cluster. All other nodes are updated automatically. After the update of the virtual appliances is complete, update all installed management packs.

Table 3-2. vRealize Operations Manager Nodes in the SDDC

Region	Role	IP Address	Fully Qualified Domain Name
Region A	Master Node	192.168.11.31	vrops-mstrn-01.rainpole.local
	Master Replica Node	192.168.11.32	vrops-repln-02.rainpole.local
	Data Node 1	192.168.11.33	vrops-datan-03.rainpole.local
	Data Node 2	192.168.11.34	vrops-datan-04.rainpole.local
	Remote Collector Node 1	192.168.31.31	vrops-rmtcol-01.sfo01.rainpole.local

Table 3-2. vRealize Operations Manager Nodes in the SDDC (Continued)

Region	Role	IP Address	Fully Qualified Domain Name
Region B	Remote Collector Node 2	192.168.31.32	vrops-rmtcol-02.sfo01.rainpole.local
	Remote Collector Node 1	192.168.32.31	vrops-rmtcol-51.lax01.rainpole.local
	Remote Collector Node 2	192.168.32.32	vrops-rmtcol-52.lax01.rainpole.local

Prerequisites

- Download the following software packages on the Windows host that has access to the data center.

Table 3-1. PAK Files That Are Required for vRealize Operations Manager Upgrade

PAK Type	PAK File
OS update .pak file	vRealize_Operations_Manager-VA-OS-xxx.pak
Software update .pak file	vRealize_Operations_Manager-VA-xxx.pak
Management Pack for NSX for vSphere	vmware-MPforNSX-vSphere-xxx.pak
vRealize Operations Manager Management Pack for vRealize Automation	vmware-MPforStorageDevices-xxx.pak
vRealize Operations Manager Management Pack for Storage Devices	vmware-MPforvRealizeAutomation-xxx.pak

- Clone any customized content to preserve it.
Customized content can include alert definitions, symptom definitions, recommendations, and views.

Procedure**1 Take the vRealize Operations Manager Nodes Offline and Take Snapshots**

Before you start the update, take the nodes of vRealize Operations Manager offline and take a snapshot of each node so that you can roll the update back if a failure occurs.

2 Upgrade the Operating System of the vRealize Operations Manager Appliances

When you upgrade the vRealize Operation Manager analytics cluster and the region-specific remote collectors in the SDDC, start the upgrade process from the vRealize Operations Manager administration interface of the master node.

3 Upgrade the vRealize Operations Manager Software

After you upgrade the operating system of the vRealize Operations Manager appliance, continue with the upgrade of the software on the vRealize Operations Manager nodes.

4 Upgrade the vRealize Operations Management Packs

Upgrade the management packs for vRealize Operations Manager to provide ongoing interoperability with the different components of the SDDC.

5 Delete the Snapshots of the vRealize Operations Manager Appliances

After you complete the update of the vRealize Operations Manager nodes, clear the virtual machine snapshots.

6 Post-Upgrade Configuration of vRealize Operations Manager

After you update the components of the vRealize Operations Manager deployment, perform the configuration changes to the environment according to the objectives and deployment guidelines of this validated design.

What to do next

- 1 Verify that vRealize Operations Manager functions flawlessly after the upgrade. See *Validate vRealize Operations Manager* in the *VMware Validated Design Operational Verification* documentation.

Take the vRealize Operations Manager Nodes Offline and Take Snapshots

Before you start the update, take the nodes of vRealize Operations Manager offline and take a snapshot of each node so that you can roll the update back if a failure occurs.

Procedure

- 1 Log in to the master node vRealize Operations Manager administrator interface of your cluster.
 - a Open a Web browser and go to **`https://vrops-mstrn-01.rainpole.local/admin`**.
 - b Log in using the following credentials.

Setting	Value
User Name	admin
Password	<code>vrops_admin_password</code>

- 2 Take all nodes offline.
 - a On the main page, click **System Status**.
 - b Click **Take Offline** under **Cluster Status**.
- 3 Wait until all nodes in the analytics cluster are offline.
- 4 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	<code>vsphere_admin_password</code>

- 5 Take a snapshot of each node in the cluster.
 - a In the **Navigator**, click **VMs and Templates** and navigate to the vrops-mstrn-01 virtual machine.
 - b Right-click the **vrops-mstrn-01** virtual machine and select **Snapshot > Take Snapshot**.

- c In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	<i>Snapshot name</i>
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

- d Repeat these steps for the other nodes in vRealize Operations Manager.

Region	Role	Virtual Machine Name
Region A	Master Replica Node	vrops-repln-02
	Data Node 1	vrops-datan-03
	Data Node 2	vrops-datan-04
	Remote Collector 1	vrops-rmtcol-01
	Remote Collector 2	vrops-rmtcol-02
Region B	Remote Collector 1	vrops-rmtcol-51
	Remote Collector 2	vrops-rmtcol-52

Upgrade the Operating System of the vRealize Operations Manager Appliances

When you upgrade the vRealize Operation Manager analytics cluster and the region-specific remote collectors in the SDDC, start the upgrade process from the vRealize Operations Manager administration interface of the master node.

Procedure

- 1 Log in to the administrator interface of the vRealize Operations Manager master node.
 - a Open a Web browser and go to **`https://vrops-mstrn-01.rainpole.local/admin`**.
 - b Log in using the following credentials.

Setting	Value
User Name	admin
Password	<i>vrops_admin_password</i>

- 2 Click **Software Update** in the left pane and click **Install a Software Update** on the **Software Update** page.
- 3 Click **Browse**, locate `vRealize_Operations_Manager-VA-OS-xxx.pak` on the local file system.

Add Software Update

1 Select Software Update

2 End User License Agreement

3 Update Information

4 Install Software Update

Select a Software Update to Install

Browse your file system to select a PAK file for the software update you want to install.

vRealize_Operations_Manager-VA-OS-... .pak

✓ The selected file is ready to upload and install. Click Upload to continue.

☒ Install the PAK file even if it is already installed

☐ Reset Default Content, overwriting to a newer version provided by this update. User modifications to DEFAULT Alert Definitions, Symptoms, Recommendations, Policy Definitions, Views, Dashboards, Widgets and Reports will be overwritten. If you are installing a product software update, clone or backup the content before you proceed.

- 4 Select **Install the PAK file even if it is already installed**, click **Upload** and click **Next**.

The upload might take several minutes

- 5 Read and accept the end user license agreement, and click **Next**.
- 6 Review the **Important Update and Release Information** and click **Next**.
- 7 Click **Install**.

- 8 Wait until the update of the operation system is complete.

You are logged out from the administrator interface of the master node because this operation restarts each of the virtual machines of the vRealize Operations Manager deployment.

- 9 After the software update is complete, log back in to the administrator interface of the master node.

The main **Cluster Status** page appears and cluster becomes online automatically.

Upgrade the vRealize Operations Manager Software

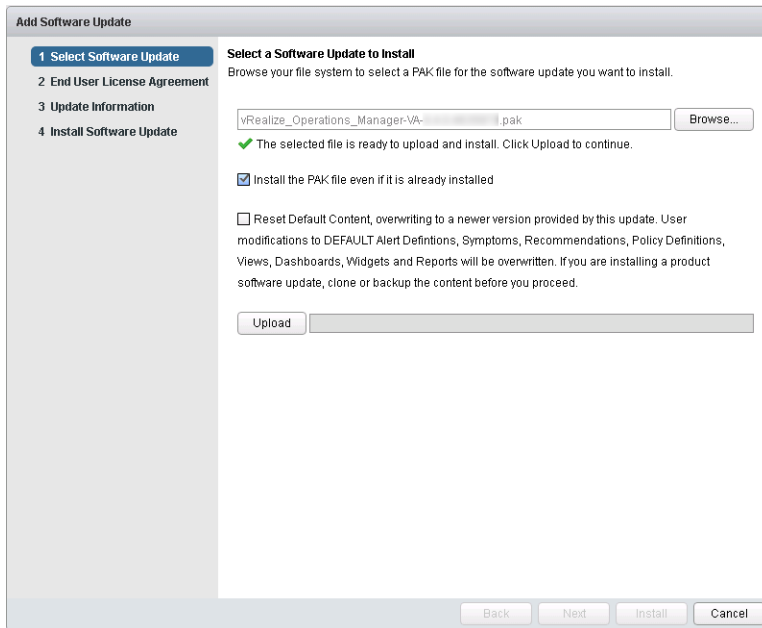
After you upgrade the operating system of the vRealize Operations Manager appliance, continue with the upgrade of the software on the vRealize Operations Manager nodes.

Procedure

- 1 Log in to the administrator interface of the vRealize Operations Manager master node.
 - a Open a Web browser and go to **https://vrops-mstrn-01.rainpole.local/admin**.
 - b Log in using the following credentials.

Setting	Value
User Name	admin
Password	vrops_admin_password

- 2 Take all nodes offline.
 - a On the main page, click **System Status**.
 - b Click **Take Offline** under **Cluster Status**.
- 3 Click **Software Update** in the **Administration** pane and click **Install a Software Update** on the **Software Update** page.
- 4 Click **Browse**, locate vRealize_Operations_Manager-VA-xxx.pak on the local file system.



- 5 Select **Install the PAK file even if it is already installed**, click **Upload** and click **Next**.

If you have customized content like alert definitions, symptom definitions, recommendations, and views, select **Reset Default Content**.

The upload might take several minutes .

- 6 Read and accept the end user license agreement, and click **Next**.
- 7 Review the **Important Update and Release Information** and click **Next**.

8 Click **Install**.

Wait for the operating system update to complete. You are logged out from the administrator interface because this operation restarts each of the virtual machines of the vRealize Operations Manager deployment.

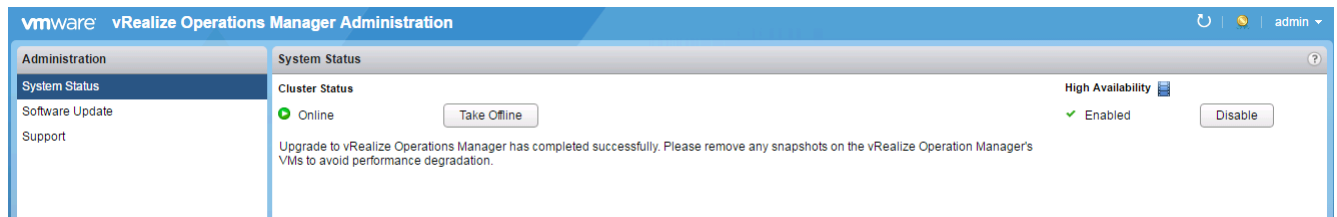
9 After the software update is complete, log back in to the administrator interface of the master node.

The main **Cluster Status** page appears and cluster becomes online automatically.

10 Clear the cache of your Web browser, and if the browser page does not refresh automatically, refresh the page.

The cluster status changes to **Going Online**. When the cluster status changes to **Online**, the upgrade is complete.

A message indicating that the upgrade completed successfully appears in the main pane.



11 On the **Administration** pane, click **Software Update** to verify that the upgrade is done.

Upgrade the vRealize Operations Management Packs

Upgrade the management packs for vRealize Operations Manager to provide ongoing interoperability with the different components of the SDDC.

You upgrade the management packs for integration with NSX for vSphere, Storage Devices and vRealize Automation. You can start with upgrade the management pack of NSX for vSphere.

Management Pack	File Name
vRealize Operations Management Pack for NSX for vSphere	vmware-MPforNSX-vSphere-xxx.pak
vRealize Operations Management Pack for Storage Devices	vmware-MPforStorageDevices-xxx.pak
vRealize Operations Management Pack for vRealize Automation	vmware-MPforvRealizeAutomation-xxx.pak

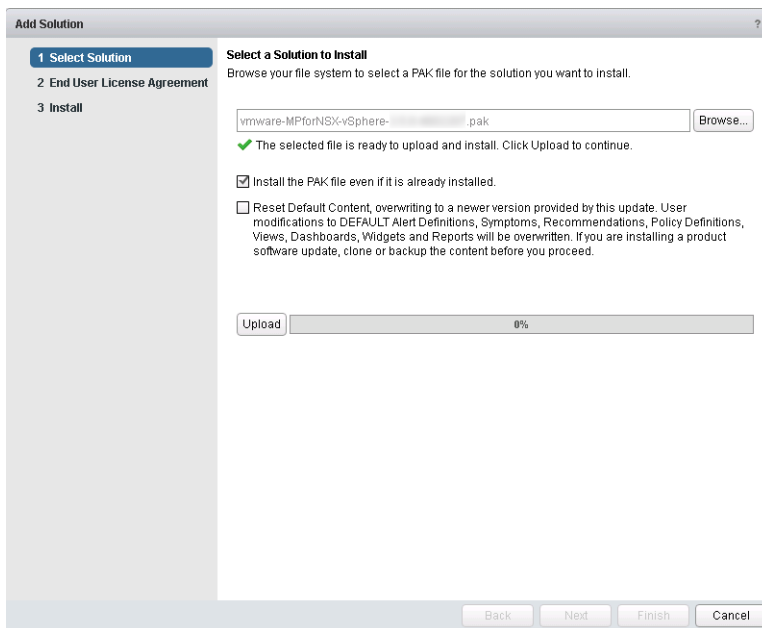
After you update the management pack software, you must reconnect the adapter instances to NSX for vSphere, vCenter Server and vRealize Automation.

Procedure

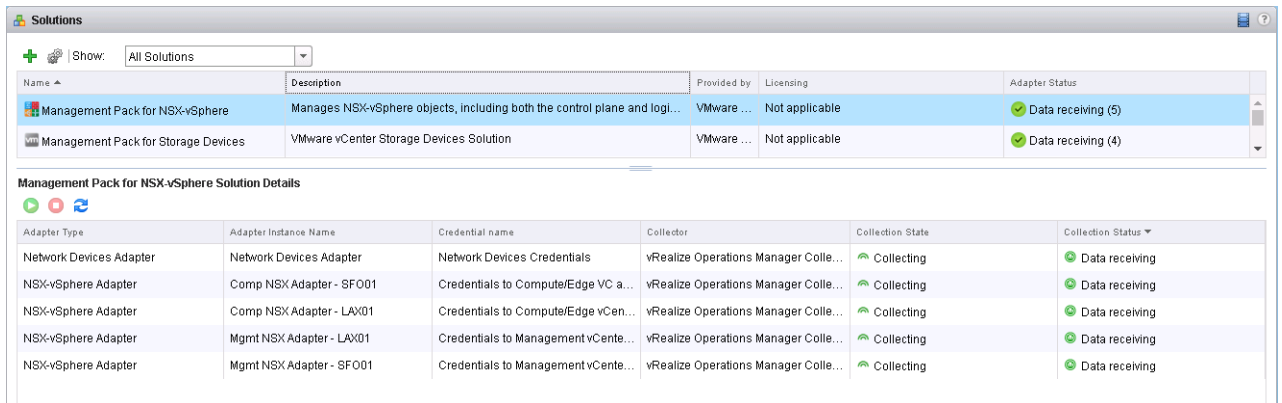
- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.
- 3 On the **Solutions** page, click **Add** .
The **Add Solution** wizard appears.
- 4 On the **Select a Solution** page, browse your file system and locate the management pack .pak file for NSX for vSphere.



- 5 Select **Install the PAK file even if it is already installed**, click **Upload** and click **Next**.
The upload might take several minutes.
- 6 Read and accept the end user license agreement, and click **Next**.
- 7 After the upgrade is complete, click **Finish**.
- 8 On the **Solutions** page in the vRealize Operations Manager user interface, select **Management Pack for NSX-vSphere** from the solution table, and click **Configure**.



- 9 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, select the **NSX-vSphere** adapter instance and click **Test Connection** to validate the connection.

Region	Adapter Instance	Adapter Type
Region A	Mgmt NSX Adapter - SFO01	NSX-vSphere
	Comp NSX Adapter - SFO01	
	Network Devices Adapter	Network Devices Adapter
Region B	Mgmt NSX Adapter - LAX01	NSX-vSphere
	Comp NSX Adapter - LAX01	

Accept the NSX Manager certificates if prompted.

- 10 Repeat the step for each NSX-vSphere adapter instance and Network Device adapter instance.
- 11 Click **Save Settings**.
- Accept the certificates if prompted.
- 12 Click **OK**.
- 13 Repeat this procedure for the other management packs.

Delete the Snapshots of the vRealize Operations Manager Appliances

After you complete the update of the vRealize Operations Manager nodes, clear the virtual machine snapshots.

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 In the **Navigator**, click **VMs and Templates** and navigate to the vrops-mstrn-01.
- 3 Right-click the **vrops-mstrn-01** virtual machine and select **Manage Snapshots**.
- 4 In the **Snapshot Manager**, click the snapshot that you created before the vRealize Operations Manager update and select **Delete**.
- 5 Click **Yes** in the confirmation dialog box and click **Close** in **Snapshot Manager**.
- 6 Repeat the procedure for the other virtual machines of vRealize Operations Manager.

Region	Role	Virtual Machine Name
Region A	Master Replica Node	vrops-repln-02
	Data Node 1	vrops-datan-03
	Data Node 2	vrops-datan-04
	Remote Collector 1	vrops-rmtcol-01
	Remote Collector 2	vrops-rmtcol-02
Region B	Remote Collector 1	vrops-rmtcol-51
	Remote Collector 2	vrops-rmtcol-52

Post-Upgrade Configuration of vRealize Operations Manager

After you update the components of the vRealize Operations Manager deployment, perform the configuration changes to the environment according to the objectives and deployment guidelines of this validated design.

Procedure

- 1 [Configure Global User Privileges in vSphere for Integration with vRealize Operations Manager](#)
After you upgrade vRealize Operations Manager, assign global permissions to the operations service accounts svc-vrops and svc-mpsd-vrops to access monitoring data from the Management vCenter Server and Compute vCenter Server with vRealize Operations Manager.
- 2 [Configure vRealize Operations Manager Integration with NSX for vSphere](#)
After you update vRealize Operations Manager, configure the collection of data metrics from the NSX components according to the objectives and deployment guidelines of this validated design.

3 Configure the Integration between vRealize Operations and vRealize Automation

After you update vRealize Operations Manager, configure the collection of data metrics from vRealize Automation according to the objectives and deployment guidelines of this validated design.

4 Rename the DRS Anti-Affinity Rule for vRealize Operations Manager

To protect the vRealize Operations Manager virtual machines from a host-level failure, configure vSphere DRS to run all virtual machines of the vRealize Operations Manager Analytics cluster and of the remote collectors on different hosts in the management cluster.

5 Update the Physical Network I/O Widget Configuration in the SDDC Overview Dashboard in vRealize Operations Manager

After you update vRealize Operations Manager, reconfigure the Physical Network I/O widget of the SDDC Overview dashboard according to the metrics support in the new version of vRealize Operations Manager so that you can continue collecting analytics data about network I/O free capacity of the management hosts.

Configure Global User Privileges in vSphere for Integration with vRealize Operations Manager

After you upgrade vRealize Operations Manager, assign global permissions to the operations service accounts svc-vrops and svc-mpsdc-vrops to access monitoring data from the Management vCenter Server and Compute vCenter Server with vRealize Operations Manager.

The svc-vrops user has read-only access on all objects in vCenter Server. The svc-mpsdc-vrops user has rights that are specifically required for access to storage device information in vRealize Operations Manager on all objects in vCenter Server.

Prerequisites

- Verify that the Management vCenter Server and Compute vCenter Server for Region A are connected to the Active Directory domain.
- Verify that the users and groups from the rainpole.local domain are available in the Management vCenter Server and in the Compute vCenter Server for Region A.

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.

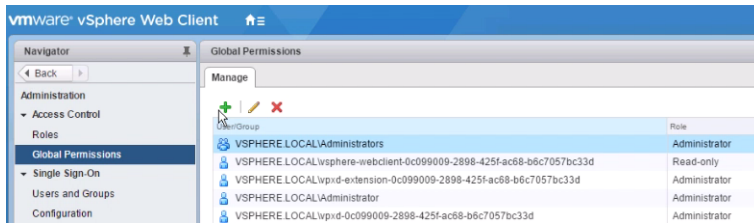
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Administration**.

- 3 Assign global permissions to the `svc-vrops@rainpole.local` and `svc-mpsd-vrops@rainpole.local` users according to their roles.

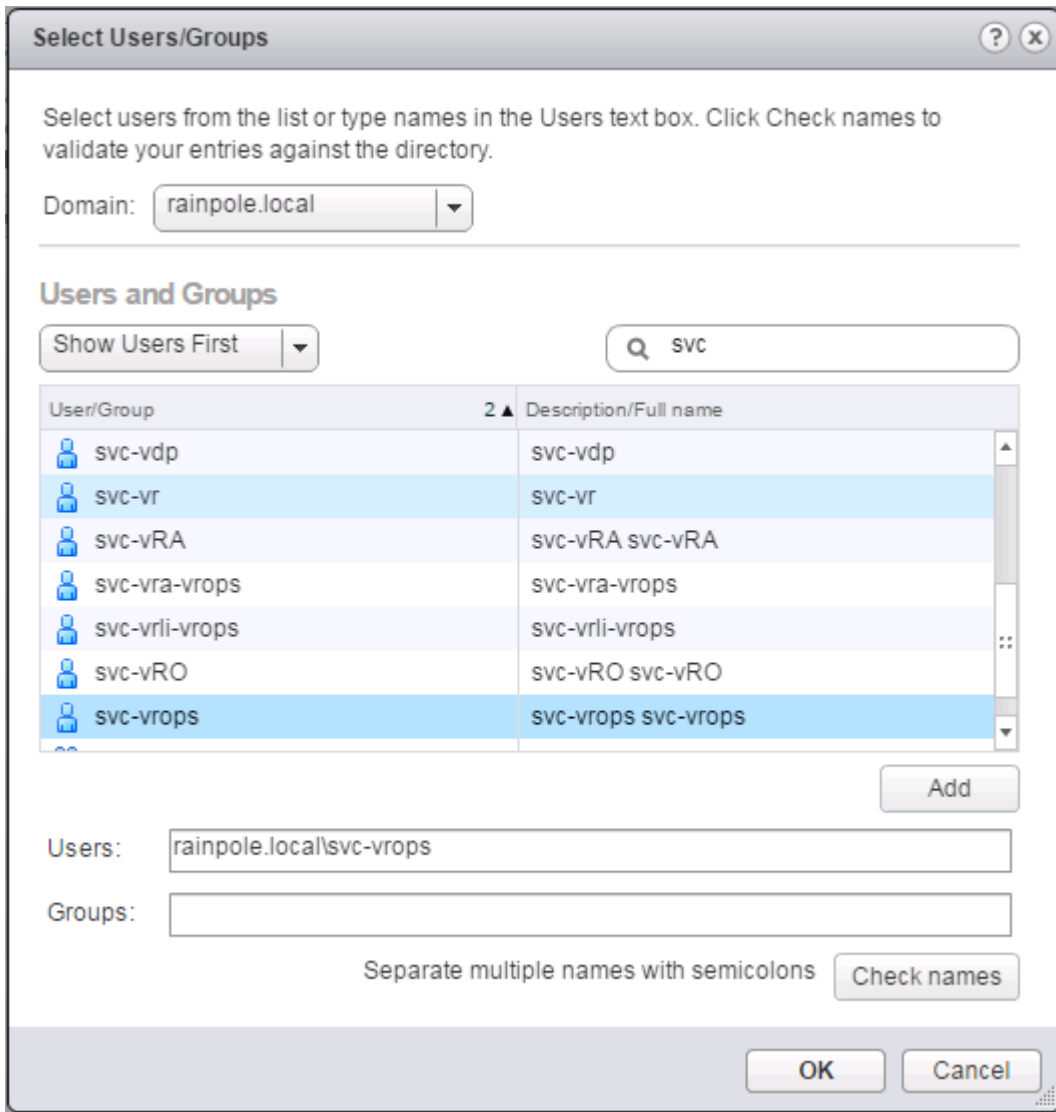
User	Role
<code>svc-vrops@rainpole.local</code>	Read-Only
<code>svc-mpsd-vrops@rainpole.local</code>	MPSD Metrics User

- In the vSphere Web Client, navigate **Administration** and click **Global Permissions**.
- Click **Add Permission**.



- In the **Global Permissions Root - Add Permission** dialog box, click **Add** to associate a user or a group with a role.
- In the **Select Users/Groups** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc** and press Enter.

- e From the list of users and groups, select **svc-vrops**, click **Add** , and click **OK**.



- f In the **Global Permissions Root - Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **Read-only**, ensure that **Propagate to children** is selected, and click **OK**.
- g Repeat the steps to assign the MPSP Metrics User role to the svc-mpsd-vrops user.

The global permissions of svc-vrops and svc-mpsd-vrops propagate to all linked vCenter Server instances.

Configure vRealize Operations Manager Integration with NSX for vSphere

After you update vRealize Operations Manager, configure the collection of data metrics from the NSX components according to the objectives and deployment guidelines of this validated design.

Procedure

1 Configure User Privileges in NSX Manager for Integration with vRealize Operations Manager

After you upgrade vRealize Operations Manager, assign the permissions that are required to access monitoring data from the Management NSX Manager and Compute NSX Manager in Region A and Region B in vRealize Operations Manager to the operations local service account svc-vrops-nsx.

2 Reconfigure the NSX-vSphere Adapter Instances in vRealize Operations Manager with the NSX Service Account

After you update vRealize Operations Manager, reconfigure the NSX-vSphere Adapters to use the svc-vrops-nsx service account and disable log forwarding of NSX-related data to vRealize Log Insight.

Configure User Privileges in NSX Manager for Integration with vRealize Operations Manager

After you upgrade vRealize Operations Manager, assign the permissions that are required to access monitoring data from the Management NSX Manager and Compute NSX Manager in Region A and Region B in vRealize Operations Manager to the operations local service account svc-vrops-nsx.

Prerequisites

- Ensure that SSH has been enabled on the Management NSX Manager and Compute NSX Manager in Region A.
- On a Windows host that has access to you data center, install a REST client, such as the RESTClient add-on for Firefox.

Procedure

- 1 Log in to the NSX Manager by using a Secure Shell (SSH) client.
 - a Open an SSH connection to the NSX Manager virtual machine.

Region	NSX Manager	Host name
Region A	NSX Manager for the management cluster	mgmt01nsxm01.sfo01.rainpole.local
	NSX Manager for the shared compute and edge cluster	comp01nsxm01.sfo01.rainpole.local
Region B	NSX Manager for the management cluster	mgmt01nsxm51.lax01.rainpole.local
	NSX Manager for the shared compute and edge cluster	comp01nsxm51.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<ul style="list-style-type: none"> ■ <i>mngnsx_admin_password</i> ■ <i>compnsx_admin_password</i>

2 Create the local service account svc-vrops-nsx on the NSX Manager instances.

- a Run the following command to switch to Privileged mode of the NSX Manager.

```
enable
```

- b Enter the admin password when prompted and press Enter.
- c Switch to Configuration mode.

```
configure terminal
```

- d Create the service account svc-vrops-nsx.

```
user svc-vrops-nsx password plaintext svc-vrops-nsx_password
```

- e Assign the svc-vrops-nsx user access to NSX Manager from the vSphere Web Client.

```
user svc-vrops-nsx privilege web-interface
```

- f Leave the Configuration mode

```
exit
```

- g Commit these updates to the NSX Managers:

```
copy running-config startup-config
```

3 Assign the security_admin role to the svc-vrops-nsx service account.

- a Log in to the Windows host that has access to your data center.
- b In a Firefox browser, go to **chrome://restclient/content/restclient.html**
- c From the **Authentication** drop-down menu, select **Basic Authentication**
- d In the **Basic Authorization** dialog box, enter the following credentials, select **Remember me** and click **Okay**.

Setting	Value
User name	admin
Password	<ul style="list-style-type: none"> ■ mngnsx_admin_password ■ compnsx_admin_password

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

- e In the **Request** pane, 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.

- f In the **Request** pane, from the **Method** drop-down menu, select **POST**, and in the **URL** text box, enter the following URL.

Region	NSX Manager	POST URL
Region A	NSX Manager for the management cluster	https://mgmt01nsxm01.sfo01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true
	NSX Manager for the shared edge and compute cluster	https://comp01nsxm01.sfo01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true
Region B	NSX Manager for the management cluster	https://mgmt01nsxm51.lax01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true
	NSX Manager for the shared edge and compute cluster	https://comp01nsxm51.lax01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true

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

```
<accessControlEntry>
  <role>security_admin</role>
  <resource>
    <resourceId>globalroot-0</resourceId>
  </resource>
</accessControlEntry>
```

The screenshot shows a REST client interface with the following details:

- Method:** POST
- URL:** https://mgmt01nsxm01.sfo01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli
- Headers:**
 - Content-Type: application/xml
 - Authorization: Basic YWRtaW46Vk1...
- Body:**

```
<accessControlEntry>
  <role>security_admin</role>
  <resource>
    <resourceId>globalroot-0</resourceId>
  </resource>
</accessControlEntry>
```
- Response:**
 - Status Code: 204 No Content
 - Cache-Control: no-cache
 - Date: Tue, 07 Feb 2017 14:40:38 GMT
 - Strict-Transport-Security: max-age=31536000; includeSubDomains
 - X-Frame-Options: SAMEORIGIN

The Status changes to 204 No Content.

- h Repeat the step for the other NSX Manager instances in Region A and Region B.

Reconfigure the NSX-vSphere Adapter Instances in vRealize Operations Manager with the NSX Service Account

After you update vRealize Operations Manager, reconfigure the NSX-vSphere Adapters to use the svc-vrops-nsx service account and disable log forwarding of NSX-related data to vRealize Log Insight.

You update the NSX-vSphere adapter for the NSX Manager for the management cluster and NSX-vSphere adapter for the NSX Manager for the shared edge and compute cluster in each region. To stop the log forwarding to vRealize Log Insight, you disable integration with Log Insight in the settings of each NSX-vSphere adapter.

Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.
- 3 On the **Solutions** page, select **Management Pack for NSX-vSphere** from the solution table, and click **Configure**.

The screenshot shows the 'Solutions' page in vRealize Operations Manager. A table lists two management packs: 'Management Pack for NSX-vSphere' and 'Management Pack for Storage Devices'. The first pack is selected, and its details are expanded below. The details include a table of adapters and their collection states.

Name	Description	Provided by	Licensing	Adapter Status
Management Pack for NSX-vSphere	Manages NSX-vSphere objects, including both the control plane and logi...	VMware ...	Not applicable	✔ Data receiving (5)
Management Pack for Storage Devices	VMware vCenter Storage Devices Solution	VMware ...	Not applicable	✔ Data receiving (4)

Management Pack for NSX-vSphere Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
Network Devices Adapter	Network Devices Adapter	Network Devices Credentials	vRealize Operations Manager Colle...	Collecting	✔ Data receiving
NSX-vSphere Adapter	Comp NSX Adapter - SF001	Credentials to Compute/Edge VC a...	vRealize Operations Manager Colle...	Collecting	✔ Data receiving
NSX-vSphere Adapter	Comp NSX Adapter - LAX01	Credentials to Compute/Edge vCen...	vRealize Operations Manager Colle...	Collecting	✔ Data receiving
NSX-vSphere Adapter	Mgmt NSX Adapter - LAX01	Credentials to Management vCente...	vRealize Operations Manager Colle...	Collecting	✔ Data receiving
NSX-vSphere Adapter	Mgmt NSX Adapter - SF001	Credentials to Management vCente...	vRealize Operations Manager Colle...	Collecting	✔ Data receiving

- 4 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, from the **Adapter Type** table at the top, select **NSX-vSphere Adapter**.

5 Update the NSX-vSphere adapter instances according to the guidelines of this validated design.

- a Under **Instance Settings**, select the NSX-vSphere adapter instance.

Region	NSX Manager	Display Name
Region A	NSX Manager for the management cluster	Mgmt NSX Adapter - SFO01
	NSX Manager for the shared compute and edge cluster	Comp NSX Adapter - SFO01
Region B	NSX Manager for the management cluster	Mgmt NSX Adapter - LAX01
	NSX Manager for the shared compute and edge cluster	Comp NSX Adapter - LAX01

- b Disable log forwarding of NSX-related data to vRealize Log Insight.

Setting	Value
Enable Log Insight integration if configured	false

- c Click the **Edit** icon next to the **Credential** text box, and change the credentials for the connection to NSX Manager and vCenter Server to use the svc-vrops-nsx service account, and click **OK**.

Setting	Value
NSX User Name	svc-vrops-nsx
NSX Manager Password	svc-vrops-nsx_password

- d Click **Test Connection** to validate the connection to the NSX Manager.
The NSX Manager certificate appears.
- e In the **Review and Accept Certificate** dialog box, verify the certificate information and click **OK**.
- f Click **OK** in the **Test Connection Information** dialog box.
- g Click **Save Settings**.

- h Click **OK** in the information box that appears.
- i Repeat these steps to reconfigure an NSX-vSphere Adapter for other NSX Manager instances in Region A and Region B.

6 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, click **Close**.

The NSX-vSphere Adapters are available on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of each NSX-vSphere adapters is **Collecting** and the **Collection Status** is **Data receiving**.

Configure the Integration between vRealize Operations and vRealize Automation

After you update vRealize Operations Manager, configure the collection of data metrics from vRealize Automation according to the objectives and deployment guidelines of this validated design.

Procedure

1 [Configure User Privileges in vRealize Automation for Integration with vRealize Operations Manager](#)

After you upgrade the Cloud Management Platform and vRealize Operations Manager, assign the permissions that are required to access monitoring data from vRealize Automation in vRealize Operations Manager to the svc-vrops-vra operations service account.

2 [Reconfigure vRealize Automation Adapter in vRealize Operations Manager with Service Account](#)

After you update vRealize Operations Manager, reconfigure the vRealize Automation adapter to use the svc-vrops-vra service account to collect monitoring data from vRealize Automation.

Configure User Privileges in vRealize Automation for Integration with vRealize Operations Manager

After you upgrade the Cloud Management Platform and vRealize Operations Manager, assign the permissions that are required to access monitoring data from vRealize Automation in vRealize Operations Manager to the svc-vrops-vra operations service account.

Procedure

1 Log in to the vRealize Automation portal.

- a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
- b Log in using the following credentials.

Setting	Value
User name	administrator
Password	vra_administrator_password
Domain	vsphere.local

2 On the **Tenants** tab, click the **Rainpole** tenant.

- 3 Click the **Administrators** tab to assign Tenant administrator and IaaS administrator roles to the svc-vrops-vra service account.
 - a Enter **svc-vrops-vra** in the **Tenant administrators** search text box, click **Search**, and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** that shows in the search result list to assign the role to the account.
 - b Enter **svc-vrops-vra** in the **IaaS administrators** search text box, click **Search**, and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** that appears in the search result list to assign the role to the account.
 - c Click **Finish**.
- 4 Log out of the vRealize Automation Default tenant portal.
- 5 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	Rainpole.local

- 6 Add the software architect role to the svc-vrops-vra user.
 - a Navigate to **Administration > Users & Groups > Directory Users and Groups**.
 - b Enter **svc-vrops-vra** in the search text box and click **Search**.
 - c Click on the user name **svc-vrops-vra@rainpole.local** that appears in the search result list.
 - d On the **General** tab, select **Software Architect** from the **Add roles to this User** list and click **Finish**.
- 7 Navigate to **Infrastructure > Endpoints > Fabric Groups** to assign the fabric administrator role to the svc-vrops-vra service account.
 - a On the **Fabric Groups** page, click **SFO Fabric Group**.
 - b On **Edit Fabric Group** page, enter **svc-vrops-vra** in the **Fabric Administrators** search text box and click **Search**.
 - c Click **svc-vrops-vra@rainpole.local** in the search result list to assign the fabric administrator role to the account and click **OK**.
 - d Repeat the steps for the **LAX Fabric Group** to assign the fabric administrator role for Region B to the svc-vrops-vra service account.

Reconfigure vRealize Automation Adapter in vRealize Operations Manager with Service Account

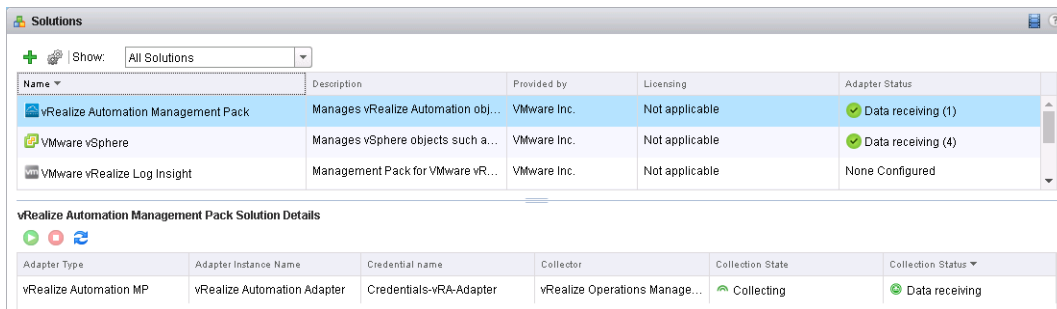
After you update vRealize Operations Manager, reconfigure the vRealize Automation adapter to use the svc-vrops-vra service account to collect monitoring data from vRealize Automation.

Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.
- 3 From the **Solutions** page, select **vRealize Automation Management Pack** from the solution table and click **Configure**.



- 4 In the **Manage Solution - vRealize Automation Management Pack** dialog box, from the **Adapter Type** table at the top, select **vRealize Automation MP**.
- 5 Reconfigure the vRealize Automation adapter to use the svc-vrops-vra service account for connection to vRealize Automation.
 - a Under **Instance Settings**, select **vRealize Automation Adapter**.
 - b Click the **Edit** icon next to the **Credential** text box, enter the credentials of the svc-vrops-vra service account for SuperUser account, and click **OK**.

Setting	Value
SuperUser Username	svc-vrops-vra@rainpole.local
SuperUser Password	svc_vrops_vra_password

- c Click **Test Connection** to validate the connection to vRealize Automation.
- d In the **Review and Accept Certificate** dialog box, verify the vRealize Automation certificate information and click **OK**.

- e Click **OK** in the **Test Connection Information** dialog box.
- f Click **Save Settings**.
- g Click **OK** in the information box that appears.

6 In the **Manage Solution - vRealize Automation Management Pack** dialog box, click **Close**.

The **Collection State** of the **vRealize Automation MP** adapter is **Collecting** and the **Collection Status** is **Data receiving**.

Rename the DRS Anti-Affinity Rule for vRealize Operations Manager

To protect the vRealize Operations Manager virtual machines from a host-level failure, configure vSphere DRS to run all virtual machines of the vRealize Operations Manager Analytics cluster and of the remote collectors on different hosts in the management cluster.

In this validated design, you use two anti-affinity rules for the analytics virtual machines: one for the analytics nodes and one for the remote collector nodes. As a result, you must reconfigure the rules after vRealize Operations Manager update to make your environment compliant with the objectives and deployment guidelines of this design version.

This rule configuration also accommodates the case when you place a host from the management cluster in maintenance mode.

Table 3-3. Anti-Affinity Rules Configuration After vRealize Operations Manager Update

Region	Old Rule Name	New Rule Name	vCenter Server Cluster
Region A	vropsmastern-antiaffinity-rule	anti-affinity-rule-vropsm	mgm01vc01.sfo01.rainpole.local > SFO01 > SFO01-Mgmt01
	vropsdatan-antiaffinity-rule	no longer needed	
	vropscollectors-antiaffinity-rule	anti-affinity-rule-vropsr	
Region B	vropscollectors-antiaffinity-rule	anti-affinity-rule-vropsr	mgm01vc51.lax01.rainpole.local > LAX01 > LAX01-Mgmt01

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 Navigate to the mgmt01vc01.sfo01.rainpole.local vCenter Server object, and under the **SFO01** data center object select the **SFO01-Mgmt01** cluster.
- 3 On the **Manage** tab, select **VM/Host Rules** under **Configuration**.
- 4 Delete **vropsdatan-antiaffinity-rule** from **VM/Host Rules**.
 - a Select the **vropsdatan-antiaffinity-rule** and click **Delete**.
 - b Click the **Yes** button on the popup warning message.
- 5 Rename and reconfigure the anti-affinity rule for the vRealize Operations Manager analytics cluster nodes.
 - a Select the **vropsmastern-antiaffinity-rule** from the **VM/Host Rules** list and click **Edit**.
 - b In the **Edit VM/Host Rule** dialog box, enter **anti-affinity-rule-vropsm** in the **Name** text box.
 - c Click **Add**.
 - d Type in **vrops** in the search text box and press enter.
 - e Select all virtual machines whose names start with vrops-datan- and click **OK**.
 - f Click **OK** button.

SFO01-Mgmt01 - Edit VM/Host Rule

Name:

☒ Enable rule.

Type:

Description:

The listed Virtual Machines must be run on separate hosts.

Members	
	vrops-datan-03
	vrops-datan-04
	vrops-repln-02
	vrops-mstrn-01

- 6 Rename the anti-affinity rule for the remote collectors in Region A.
 - a Select the **vropscollectors-antiaffinity-rule** rule from the **VM/Host Rules** list and click **Edit**.
 - b In the **Edit VM/Host Rule** dialog box, enter **anti-affinity-rule-vropsr** in the **Name** text box and click **OK**.
- 7 Rename the anti-affinity rule for the remote collectors in Region B by repeating step 6 by logging in to <http://mgmt01vc51.lax01.rainpole.local/vsphere-client>.

Update the Physical Network I/O Widget Configuration in the SDDC Overview Dashboard in vRealize Operations Manager

After you update vRealize Operations Manager, reconfigure the Physical Network I/O widget of the SDDC Overview dashboard according to the metrics support in the new version of vRealize Operations Manager so that you can continue collecting analytics data about network I/O free capacity of the management hosts.

Prerequisites

Verify that the SDDC Overview dashboard that tracks the overall state of the SDDC exists in vRealize Operations Manager.

Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **<https://vrops-cluster-01.rainpole.local>**.
 - b Log in using the following credentials.

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

- 2 Click **Home**.
- 3 On the **Home** page, from the **Dashboard List** drop-down menu select the **SDDC Overview** dashboard.

- 4 Change **Physical Network I/O** heatmap to use the network demand host metric.
 - a Locate the **Physical Network I/O** heatmap in the SDDC Overview dashboard and click **Edit**.
 - b Update the following widget settings and click **Save**.

Widget Setting	Value
Attribute type	Network I/O > Demand (%)
Min Value (Color)	80 (green)
Max Value (Color)	100 (red)

Edit Physical Network I/O

Title: Physical Network I/O

Refresh Content: ☒ On ☐ Off

Refresh Interval: 300 (seconds)

Configurations: Management Hosts

Name: Management Hosts

Group by: Datacenter

Then by:

Mode: ☒ Instance ☐ General

Object Type: Host System

Attribute type: Network I/O Demand (%)

Color:
 Min. Value Max. Value

Filter:

- Collectors (Full Set)
- Applications (Full Set)
- Adapter Types
- Adapter Instances
- Object Types
- Recently Added Objects
- Object Statuses
- Collection States
- Health Ranges
- Application
- Cluster Compute Resource

Save Cancel

Upgrade vRealize Log Insight

Upgrade the vRealize Log Insight clusters and agents in Region A and Region B so that you can use the new features of and have an environment that is compliant with version 4.0 of this VMware Validated Design.

Upgrade both of the vRealize Log Insight clusters in Region A and Region B from the user interface of the master nodes. All the other nodes are upgraded automatically. Upgrade by using the Integrated Load Balancer IP address is not supported.

You must also upgrade the Log Insight agents on the management components that send log data to vRealize Log Insight over the Ingestion API.

After the virtual appliances and agents are upgraded, upgrade all installed content packs.

Table 3-4. vRealize Log Insight Nodes in the SDDC

Region	Role	IP Address	FQDN
Region A	Integrated load balancer VIP	192.168.31.10	vrli-cluster-01.sfo01.rainpole.local
	Master node	192.168.31.11	vrli-mstr-01.sfo01.rainpole.local
	Worker node 1	192.168.31.12	vrli-wrkr-01.sfo01.rainpole.local
	Worker node 2	192.168.31.13	vrli-wrkr-02.sfo01.rainpole.local
Region B	Integrated load balancer VIP	192.168.32.10	vrli-cluster-51.lax01.rainpole.local
	Master node	192.168.32.11	vrli-mstr-51.lax01.rainpole.local
	Worker node 1	192.168.32.12	vrli-wrkr-51.lax01.rainpole.local
	Worker node 2	192.168.32.13	vrli-wrkr-51.lax01.rainpole.local

Prerequisites

- Download the vRealize Log Insight product upgrade .pak file on the Windows host that has access to the data center.
- Verify that you have a user with the **Edit Admin** permission for the vRealize Log Insight Web Interface.

Procedure**1 Take Snapshots of the vRealize Log Insight Nodes**

Before you start the upgrade, take snapshots of the nodes of vRealize Log Insight so that you can roll their state back in the case of an upgrade failure.

2 Upgrade the vRealize Log Insight Clusters

When you upgrade the vRealize Log Insight instances in Region A and Region B in the SDDC, start the update process from the vRealize Log Insight user interface of the master node.

3 Upgrade the vRealize Log Insight Agents

After upgrading the vRealize Log Insight, upgrade the individual vRealize Log Insight Agents on the Windows hosts within the environment to take advantage of the latest features.

4 Delete the Snapshots of the vRealize Log Insight Appliances

After you complete the update of the vRealize Log Insight nodes, clean up the virtual machine snapshots.

5 Post-Upgrade Configuration of the vRealize Log Insight

After you upgrade the operations management components of the SDDC, configure the environment according to the objectives and deployment guidelines of this validated design.

What to do next

- Verify that vRealize Log Insight functions flawlessly after the upgrade. See *Validate vRealize Log Insight* in the *VMware Validated Design Operational Verification* documentation.

Take Snapshots of the vRealize Log Insight Nodes

Before you start the upgrade, take snapshots of the nodes of vRealize Log Insight so that you can roll their state back in the case of an upgrade failure.

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 Take a snapshot of each node in the cluster.
 - a In the **Navigator**, click **VMs and Templates** and navigate to the vrli-mstr-01 virtual machine.
 - b Right-click the **vrli-mstr-01** virtual machine and select **Snapshot > Take Snapshot**.
 - c In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	<i>Snapshot name</i>
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

- d Repeat these steps for the other nodes in the cluster in Region A.

Role	Virtual Machine Name
Worker Node 1	vrli-wrkr-01
Worker Node 2	vrli-wrkr-02

- 3 Repeat the procedure for the nodes in Region B under the mgmt01vc51.lax01.rainpole.local vCenter Server in the vSphere Web Client.

Role	Virtual Machine Name
Master Node	vrli-mstr-51
Worker Node 1	vrli-wrkr-51
Worker Node 2	vrli-wrkr-52

Upgrade the vRealize Log Insight Clusters

When you upgrade the vRealize Log Insight instances in Region A and Region B in the SDDC, start the update process from the vRealize Log Insight user interface of the master node.

If upgrade the two vRealize Log Insight clusters in Region A or Region B, you can upgrade two vRealize Log Insight instances one after the other or in parallel.


Procedure


- 1 Log in to the vRealize Log Insight user interface of the master node.
 - a Open a Web browser and go the master node for the cluster that you are updating.

Region	URL
Region A	https://vrli-mstr-01.sfo01.rainpole.local
Region B	https://vrli-mstr-51.lax01.rainpole.local

- b Log in using the following credentials.











Setting	Value
User name	admin
Password	vrli_admin_password

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Management**, click **Cluster** and click **Upgrade Cluster**.

Cluster 


Nodes



Filter by host




Host	Uptime	Version	Monitor	Status	Actions
vrli-mstr-01.sfo01.rainpole.local (Master)	15 days 23 hours	3.6.0	Monitor 	 Connected	
192.168.31.12	15 days 22 hours	3.6.0	Monitor 	 Connected	 
192.168.31.13 (ILB)	15 days 22 hours	3.6.0	Monitor 	 Connected	 

To add a node, deploy a new Log Insight instance and choose "Join Deployment" in the startup wizard.

Upgrade Cluster
Download Support Bundle

Integrated Load Balancer 

 New Virtual IP Address
 Delete Virtual IP Address

	IP	FQDN	Tags	Status
 	192.168.31.10	vrli-cluster-01.sfo01.rainpole.local	No tags	 Available

- 4 Browse to the location of the vRealize Log Insight .pak file on your local file system and click **Open**.

- 5 In the **Upgrade Log Insight** dialog box, click **Upgrade** and wait until the .pak file uploads to the master appliance.
- 6 On the **End User License Agreement** page, click **Accept**.

The **Upgrade Log Insight** progress dialog box opens.

- 7 After the upgrade of the master node completes, in the **Upgrade Successful** dialog box that appears, click **OK**.

The upgrade of all other nodes in the cluster starts automatically.

Cluster

Nodes Filter by host

Host	Uptime	Version	Monitor	Status	Actions
vrl-mstr-01.sfo01.rainpole.local (Master)	3 minutes	4.0.0	Monitor	Connected	
192.168.31.12 (ILB)	15 days 23 hours	3.6.0	Monitor	Upgrade Pending	
192.168.31.13	N/A	N/A	Monitor	Transferring PAK	

To add a node, deploy a new Log Insight instance and choose 'Join Deployment' in the startup wizard.

[UPGRADE CLUSTER](#) [DOWNLOAD SUPPORT BUNDLE](#)

Integrated Load Balancer

[+ NEW VIRTUAL IP ADDRESS](#) [x DELETE VIRTUAL IP ADDRESS](#)

IP	FQDN	Tags	Status
192.168.31.10	vrl-cluster-01.sfo01.rainpole.local	No tags	Unavailable

- 8 After the upgrade process for the whole cluster completes, the Integrated Load Balancer will come back online.
- 9 After the Integrated Load Balancer becomes Available, repeat the procedure on the cluster in Region B.

Upgrade the vRealize Log Insight Agents

After upgrading the vRealize Log Insight, upgrade the individual vRealize Log Insight Agents on the Windows hosts within the environment to take advantage of the latest features.

You download the latest agents from the vRealize Log Insight clusters for each region and upgrade them on the Windows management nodes in each region. You can start with downloading and updating the agents in Region A. Then repeat this task with downloading and updating the agents in Region B.


Procedure

- 1 Log in to the vRealize Log Insight user interface of the master node.
 - a Open a Web browser and go the master node of the cluster that you are updating.

Region	URL
Region A	https://vrli-mstr-01.sfo01.rainpole.local
Region B	https://vrli-mstr-51.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Management**, click **Agents**.
- 4 Click the **Download Log Insight Agent Version 4.0.0** button.
- 5 In the **Download Log Insight Agent Version 4.0.0** dialog box, download the following agent files.



- a For the Windows hosts in the SDDC in Region A, on the Region A vRealize Log Insight cluster, click **Window MSI (32-bit/64-bit)** and save the `VMware-Log-Insight-Agent-4.0.0-build_number_Region_A_vRealize_Log_Insight_VIP_address.msi` on the Windows host that you use to access the data center.
 - b For the Windows hosts in the SDDC in Region B, on the RegionB vRealize Log Insight cluster, click **Window MSI (32-bit/64-bit)** and save the `VMware-Log-Insight-Agent-4.0.0-build_number_Region_B_vRealize_Log_Insight_VIP_address.msi` on the Windows host that you use to access the data center.

6 Upgrade the vRealize Log Insight Windows Agents in Region A.

- a Open a Remote Desktop Protocol (RDP) connection to each of the following Windows virtual machines.

SDDC Layer	Role	Host Name
Cloud Management	IaaS Web Server	vra01iws01a.rainpole.local
		vra01iws01b.rainpole.local
	IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local
		vra01ims01b.rainpole.local
	IaaS DEM Worker	vra01dem01.rainpole.local
		vra01dem02.rainpole.local
	vSphere Proxy Agent	vra01ias01.sfo01.rainpole.local
		vra01ias02.sfo01.rainpole.local
	Microsoft SQL Server	vra01mssql01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	Windows administrator
Password	<i>windows_administrator_password</i>

- c Copy the `VMware-Log-Insight-Agent-4.0.0-build_number_Region_A_vRealize_Log_Insight_VIP_address.msi` file from the Windows host to the Windows virtual machine.
- d Double-click the `.msi` file to run the installer.
- e In the **VMware vRealize Log Insight Agent Setup** wizard, accept the license agreement and click **Next**.
- f With the Log Insight host name `vrli-cluster-01.sfo01.rainpole.local` shown in the **Host** text box, click **Install**.
- g When the installation is complete, click **Finish**.
- h Repeat the steps on the other Windows virtual machines.

7 Upgrade the vRealize Log Insight Windows Agents in Region B.

- a Open a Remote Desktop Protocol (RDP) connection to each of the following Windows virtual machines.

SDDC Layer	Role	Host Name
Cloud Management	vSphere Proxy Agent	vra01ias51.lax01.rainpole.local
		vra01ias52.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	Windows administrator
Password	<i>windows_administrator_password</i>

- c Copy the `VMware-Log-Insight-Agent-4.0.0-build_number_Region_B_vRealize_Log_Insight_VIP_address.msi` file from the Windows host to the Windows virtual machine.
- d Double-click the `.msi` file to run the installer.
- e In the **VMware vRealize Log Insight Agent Setup** wizard, accept the license agreement and click **Next**.
- f With the Log Insight host name `vrli-cluster-51.lax01.rainpole.local` shown in the **Host** text box, click **Install**.
- g When the installation is complete, click **Finish**.
- h Repeat the steps on the other Windows virtual machines.

Delete the Snapshots of the vRealize Log Insight Appliances

After you complete the update of the vRealize Log Insight nodes, clean up the virtual machine snapshots.

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	<i>vsphere_admin_password</i>

- 2 In the **Navigator**, click **VMs and Templates** and navigate to the `vrli-mstr-01` under `mgmt01vc01.sfo01.rainpole.local`.

- 3 Right-click the **vrli-mstr-01** virtual machine and select **Manage Snapshots**.
- 4 In the **Snapshot Manager**, click the snapshot that you created before the vRealize Log Insight update and select **Delete**.
- 5 Click **Yes** in the confirmation dialog box and click **Close** in **Snapshot Manager**.
- 6 Repeat the procedure on the other virtual machines of vRealize Log Insight in Region A.

Role	Virtual Machine Name
Worker Node 1	vrli-wrkr-01
Worker Node 2	vrli-wrkr-02

- 7 Repeat the procedure on the virtual machines of vRealize Log Insight in Region B under the mgmt01vc51.lax01.rainpole.local vCenter Server.

Role	Virtual Machine Name
Master Node	vrli-mstr-51
Worker Node 1	vrli-wrkr-51
Worker Node 2	vrli-wrkr-52

Post-Upgrade Configuration of the vRealize Log Insight

After you upgrade the operations management components of the SDDC, configure the environment according to the objectives and deployment guidelines of this validated design.

Procedure

- 1 [Configure User Privileges in vSphere for Integration with vRealize Log Insight](#)
Assign global permissions to the operations service account svc-loginsight to access monitoring data from the Management vCenter Server and Compute vCenter Server with vRealize Log Insight.
- 2 [Reconnect vRealize Log Insight to vRealize Operations Manager](#)
This version of this validated design uses service accounts for controlled communication between the management components of the SDDC. Connect vRealize Log Insight to vRealize Operations Manager using such a service account to make your environment compliant with this validated design.
- 3 [Complete vRealize Log Insight Integration with vRealize Automation](#)
After you configure vRealize Log Insight to use a service account in the communication with vSphere and vRealize Operations Manager, complete the configuration of vRealize Log Insight for communication with vRealize Automation.
- 4 [Rename the DRS Anti-Affinity Rule for vRealize Log Insight](#)
To protect the vRealize Log Insight virtual machines from a host-level failure, configure vSphere DRS to run both the virtual machines on different hosts in the management cluster.

Configure User Privileges in vSphere for Integration with vRealize Log Insight

Assign global permissions to the operations service account svc-loginsight to access monitoring data from the Management vCenter Server and Compute vCenter Server with vRealize Log Insight.

The svc-loginsight user account is specifically dedicated to collecting log information from vCenter Server and ESXi.

Prerequisites

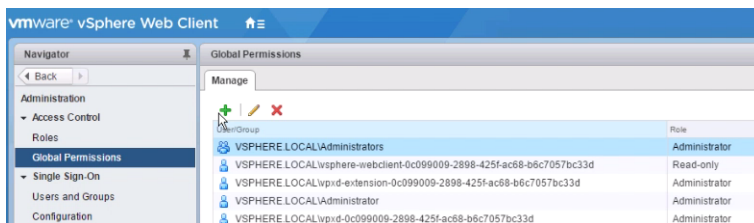
- Verify that the Management vCenter Server and Compute vCenter Server for Region A are connected to the Active Directory domain.
- Verify that the users and groups from the rainpole.local domain are available in the Management vCenter Server and in the Compute vCenter Server for Region A.

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.

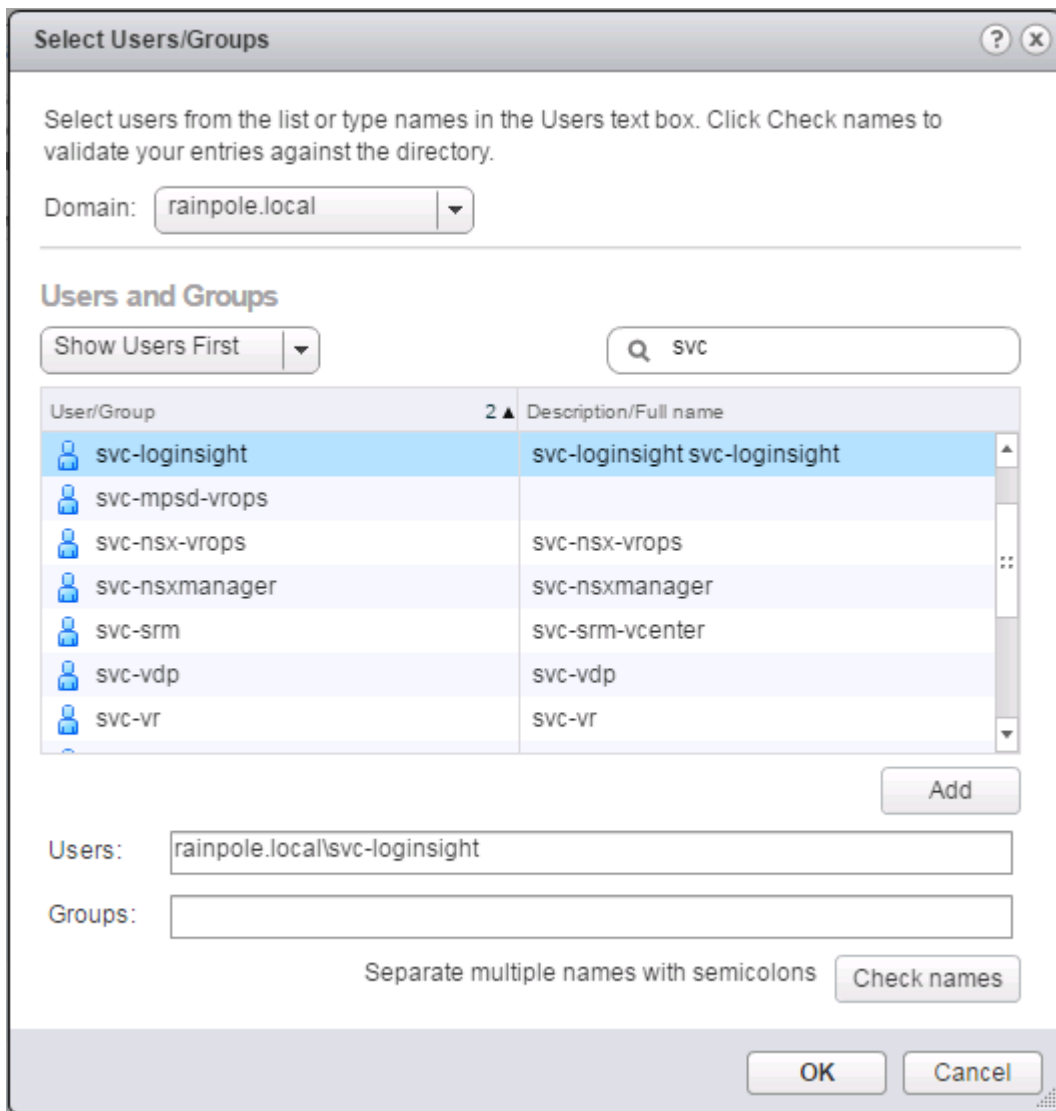
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Administration**.
- 3 Assign global permissions to the svc-loginsight@rainpole.local service account.
 - a In the vSphere Web Client, select **Administration** from the **Home** menu and click **Global Permissions** under **Access Control**.
 - b On the **Manage** tab, click **Add Permission**.



- c In the **Global Permissions Root - Add Permission** dialog box, click **Add** to associate a user or a group with a role.
- d In the **Select Users/Groups** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.

- e From the list of users and groups, select the **svc-loginsight** user, click **Add**, and click **OK**.



- f In the **Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **LogInsight**, select **Propagate to children**, and click **OK**.

The global permissions of the svc-loginsight@rainpole.local user propagate to all vCenter Server instances.

Reconnect vRealize Log Insight to vRealize Operations Manager

This version of this validated design uses service accounts for controlled communication between the management components of the SDDC. Connect vRealize Log Insight to vRealize Operations Manager using such a service account to make your environment compliant with this validated design.

Procedure

1 Configure User Privileges on vRealize Operations Manager for Integration with vRealize Log Insight

Configure read-only privileges for the `svc-vrli-vrops@rainpole.local` service account on vRealize Operations Manager. You configure these privileges so that you can open vRealize Log Insight from within vRealize Operations Manager to examine log data and send alerts from vRealize Log Insight to vRealize Operations Manager.

2 Configure the Log Insight Agent Groups for vRealize Operations Manager components

After you reconfigure the service account used to connect vRealize Log Insight to vRealize Operations Manager, configure the Log Insight agent group for the Realize Operations Manager components for the vRealize Log Insight in Region A. Repeat this operations in for the vRealize Operations Manger components in Region B.

Configure User Privileges on vRealize Operations Manager for Integration with vRealize Log Insight

Configure read-only privileges for the `svc-vrli-vrops@rainpole.local` service account on vRealize Operations Manager. You configure these privileges so that you can open vRealize Log Insight from within vRealize Operations Manager to examine log data and send alerts from vRealize Log Insight to vRealize Operations Manager.

Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.
 - b Log in using the following credentials.

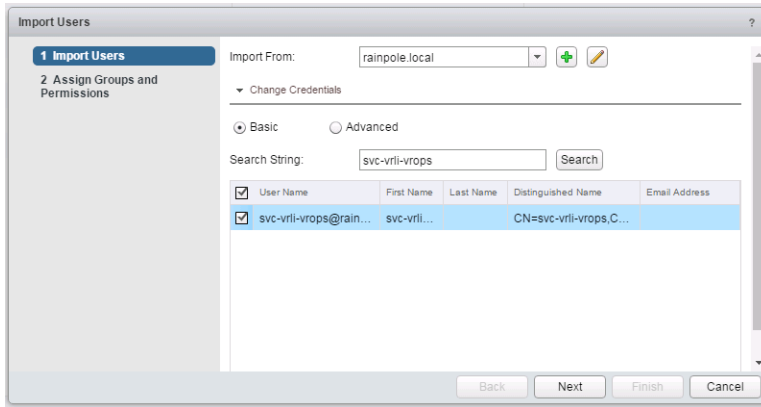
Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 In the left pane of vRealize Operations Manager, click **Administration**, and click **Access Control**.
- 3 On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.
- 4 On the **Import Users** page, import the `svc-vrli-vrops@rainpole.local` service account.
 - a From the **Import From** drop-down menu, select **RAINPOLE.LOCAL**.
 - b Select the **Basic** option for the search query.

- c In the **Search String** text box, enter **svc-vrli-vrops** and click **Search**.

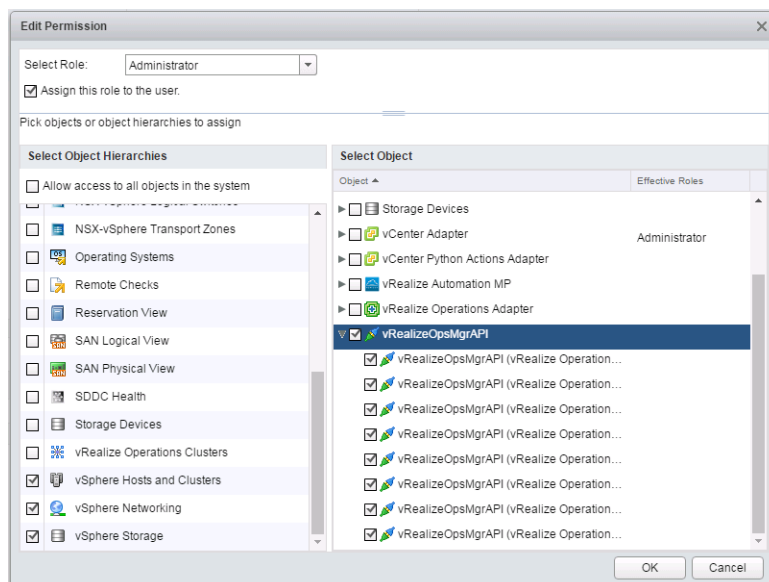
The search results contain the svc-vrli-vrops user account.

- d Select **svc-vrli-vrops@rainpole.local** and click **Next**.




- 5 On the **Assign Groups and Permissions** page, to assign the ReadOnlY role to the svc-vrli-vrops@rainpole.local service account, click the **Objects** tab, configure the following settings and click **Finish**.

Setting	Value
Select Role	Administrator
Assign this role to the user	Selected
Select Object	vRealizeOpsMgrAPI Adapter Instance becomes automatically selected under Select Object Hierarchies .
Select Object Hierarchies	<ul style="list-style-type: none"> ■ vSphere Hosts and Clusters ■ vSphere Networking ■ vSphere Storage



- 6 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **https://vrli-cluster-01.sfo01.rainpole.local**.
 - b Log in using the following credentials.

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

- 7 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.
- 8 Under **Integration**, click **vRealize Operations**.
- 9 On the **vRealize Operations Manager** pane, change the integration settings for vRealize Operations Manager.
 - a Enter the host name and the svc-vrli-vrops@rainpole.local user credentials for the vRealize Operations Manager instances.

vRealize Operations Manager Option	Value
Hostname	vrops-cluster-01.rainpole.local
Username	svc-vrli-vrops@rainpole.local
Password	<i>svc-vrli-vrops_password</i>
Enable alerts integration	Selected
Enable launch in context	Selected

- b Click **Test Connection**.
- c Click **Save**.

A progress dialog box appears.

Configure the Log Insight Agent Groups for vRealize Operations Manager components


After you reconfigure the service account used to connect vRealize Log Insight to vRealize Operations Manager, configure the Log Insight agent group for the Realize Operations Manager components for the vRealize Log Insight in Region A. Repeat this operations in for the vRealize Operations Manger components in Region B.

Procedure

- 1 Configure the Linux Agent Group for Region A for the vRealize Operations Manager components from the vRealize Log Insight Web user interface.

- a Open a Web browser and go to **https://vrli-cluster-01.sfo01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- c Click the configuration drop-down menu icon  and select **Administration**.
- d Under **Management**, click **Agents**.
- e From the drop-down menu at the top, select **vRops 6.x - Sample** from the **Available Templates** section and click **Copy Template**.
- f In the **Copy Agent Group** dialog box, enter **vRops6 – Agent Group** in the name text box and click **Copy**.
- g In the **agent filter** fields, enter the following values pressing Enter after each host name.

Filter	Operator	Values
Hostname	matches	<ul style="list-style-type: none"> ■ vrops-mstrn-01.rainpole.local ■ vrops-repln-02.rainpole.local ■ vrops-datan-03.rainpole.local ■ vrops-datan-04.rainpole.local ■ vrops-rmtcol-01.sfo01.rainpole.local ■ vrops-rmtcol-02.sfo01.rainpole.local


Note New deployment of the VMware Validated Design do not deploy the secondary analytics node (vrops-datan-04.rainpole.local). For customers coming from previously releases that are upgrading to VMware Validated Design 4.0.x, include the secondary analytics node in the agent group.

- h Click **Refresh** and verify that all the agents in the filter appear in the **Agents** list.
- i Click **Save New Group** at the bottom of the page.

- 2 Configure the Linux Agent Group for Region B for the vRealize Operations Manager components from the vRealize Log Insight Web user interface.

- a Open a Web browser and go to **https://vrli-cluster-51.lax01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- c Click the configuration drop-down menu icon  and select **Administration**.
- d Under **Management**, click **Agents**.
- e From the drop-down menu at the top, select **vRops 6.x - Sample** from the **Available Templates** section and click **Copy Template**.
- f In the **Copy Agent Group** dialog box, enter **vRops6 – Agent Group** in the name text box and click **Copy**.
- g In the **agent filter** fields, enter the following values pressing Enter after each host name.

Filter	Operator	Values
Hostname	matches	<ul style="list-style-type: none"> ■ vrops-rmtcol-51.lax01.rainpole.local ■ vrops-rmtcol-52.lax01.rainpole.local

- h Click **Refresh** and verify that all the agents in the filter appear in the **Agents** list.
- i Click **Save New Group** at the bottom of the page.

Complete vRealize Log Insight Integration with vRealize Automation

After you configure vRealize Log Insight to use a service account in the communication with vSphere and vRealize Operations Manager, complete the configuration of vRealize Log Insight for communication with vRealize Automation.

Procedure

- 1 [Install the new vRealize Log Insight Content Pack for the Cloud Management Platform](#)

Install the new content pack for Microsoft SQL Server to add the dashboards for viewing log information about the database platform hosting the Cloud Management Platform in vRealize Log Insight.

- 2 [Configure the Log Insight Agent Group for vRealize Orchestrator components](#)

Configure the Log Insight agent group for the Realize Orchestrator components for the vRealize Log Insight in Region A.

Install the new vRealize Log Insight Content Pack for the Cloud Management Platform

Install the new content pack for Microsoft SQL Server to add the dashboards for viewing log information about the database platform hosting the Cloud Management Platform in vRealize Log Insight.


You install the following content packs:

- Microsoft - SQL Server


Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **https://vrli-cluster-01.sfo01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under Content Pack Marketplace, select **Marketplace**.
- 4 In the list of content packs, locate the **Microsoft - SQL Server** content pack and click its icon.
- 5 In the Install Content Pack dialog box, click **Install**.
 After the installation is complete, the Microsoft - SQL Server content pack appears in the Installed Content Packs list on the left
- 6 Repeat the procedure to on vrli-cluster-51.lax01.rainpole.local
- 7 In the vRealize Log Insight Web user interface, configure the Log Insight Windows Agent Group for the Microsoft SQL Server component that is used by vRealize Automation.
 - a Open a Web browser and go to **https://vrli-cluster-01.sfo01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- c Click the configuration drop-down menu icon  and select **Administration**.
- d Under **Management**, click **Agents**.
- e From the drop down on the top, select **Microsoft - SQL Server** from the **Available Templates** section..
- f Click **Copy Template**.
- g In the **Copy Agent Group** dialog box, enter **vRA7 – Microsoft SQL Server Agent Group** in the name text box and click **Copy**.

- h In the agent filter fields, use the following selections.

Use ENTER to separate the host name values.

Filter	Operator	Values
Hostname	matches	vra01mssql01.rainpole.local

- i Under **Agent Configuration**, click **Edit**
- j Locate `directory=C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log` and change it to `directory=C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Log`

Note In this VMware Validated Design, Microsoft SQL Server 2012 R2 has been installed in the default location on the Windows Server virtual machine.

- k Click **Refresh** and verify that all the agents listed in the filter appear in the Agents list.
- l Click **Save New Group** at the bottom of the page.

Configure the Log Insight Agent Group for vRealize Orchestrator components


Configure the Log Insight agent group for the Realize Orchestrator components for the vRealize Log Insight in Region A.

Procedure

- ◆ Configure the Linux Agent Group for Region A for the vRealize Orchestrator components from the vRealize Log Insight Web user interface

- a Open a Web browser and go to **`https://vrli-cluster-01.sfo01.rainpole.local`**
- b Log in using the following credentials.

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

- c Click the configuration drop-down menu icon  and select **Administration**.
- d Under **Management**, click **Agents**.
- e From the drop-down menu at the top, select **vRealize Orchestrator 7.0.1** from the **All Agents** section and click **Copy Template**.
- f In the **Copy Agent Group** dialog box, enter **vrO 7.0.1** in the name text box and click **Copy**.

- g In the **agent filter** fields, enter the following values pressing Enter after each host name to determine which agents receive the configuration.

Filter	Operator	Values
Hostname	matches	■ vra01vro01a.rainpole.local ■ vra01vro01b.rainpole.local

- h Click **Refresh** and verify that in the **Agents** list vRealize Log Insight receives data from the two agents in the filter.

The screenshot shows the vRealize Log Insight interface. On the left is a navigation menu with options like Management, System Monitor, Cluster, Access Control, User Alerts, Hosts, Agents (selected), Event Forwarding, License, Integration, vSphere, vRealize Operations, Configuration, General, Time, Authentication, SMTP, Archiving, and SSL. The main area is titled 'Agents' and shows a filter for 'vRO 7.0.1 (Not Seved)' with a 'REFRESH' button. Below the filter, it says 'Use filters to select which agents receive the Agent Configuration below.' and shows the filter 'Hostname matches vra01vro01a.rainpole.local vra01vro01b.rainpole.local'. There are 2 agents listed in a table:

IP Address	Hostname	Version	OS	Last Active	Events Sent	Events Sent/...	Events Dropp...	Uptime	Status
192.168.11.63	vra01vro01a.rainpole.local	3.3.0.3516686	SUSE Linux Enterprise Server 11 (x86_64)	Less than 1 minute ago	4,935	3	0	3 days 8 hours	Active
192.168.11.64	vra01vro01b.rainpole.local	3.3.0.3516686	SUSE Linux Enterprise Server 11 (x86_64)	Less than 1 minute ago	3,207	2	0	3 days 8 hours	Active

Below the table is the 'Agent Configuration' section with 'Build' and 'Edit' tabs. The 'General' tab is selected, showing a file path 'file:///usr/share/vmware-loginsight/agents/agent.conf'.

- i Click **Save Agent Group** at the bottom of the page.

Rename the DRS Anti-Affinity Rule for vRealize Log Insight

To protect the vRealize Log Insight virtual machines from a host-level failure, configure vSphere DRS to run both the virtual machines on different hosts in the management cluster.

You use an anti-affinity rules for the vRealize Log Insight virtual machines. This rule configuration also accommodates the case when you place a host from the management cluster in maintenance mode.

Region	Old Rule Name	New Rule Name	vCenter Server Cluster
Region A	vrli-antiaffinity-rule	anti-affinity-rule-vrli	mgmt01vc01.sfo01.rainpole.local> SFO01 > SFO01-Mgmt
Region B	vrli-antiaffinity-rule	anti-affinity-rule-vrli	mgmt01vc51.lax01.rainpole.local> LAX01 > LAX01-Mgmt

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 Navigate to the mgmt01vc01.sfo01.rainpole.local vCenter Server object, and under the **SFO01** data center object select the **SFO01-Mgmt01** cluster.
- 3 Click **Configure** tab.
- 4 Under the **Configuration** group of settings, select **VM/Host Rules**.
- 5 Select the vrli-antiaffinity-rule from the **VM/Host Rules** list and click **Edit**
- 6 In the **Edit VM/Host Rule** dialog box, enter **anti-affinity-rule-vrli** in the **Name** text box and click **OK**

SFO01-Mgmt01 - Edit VM/Host Rule

Name:

☒ Enable rule.

Type:

Description:

The listed Virtual Machines must be run on separate hosts.

Members

- vrli-wrkr-02
- vrli-wrkr-01
- vrli-mstr-01

- 7 Repeat the procedure for Region B by logging in to <http://mgmt01vc51.lax01.rainpole.local/vsphere-client> and configuring the LAX01-Mgmt cluster.

Upgrade Virtual Infrastructure

After you upgrade the Cloud Management Platform and operations management component, you must upgrade the components of the virtual infrastructure layer of the SDDC.

Procedure

1 [Update vSphere Data Protection](#)

When you update the vSphere Data Protection instances for version 4.0 of this VMware Validated Design, you update the instance in Region A and then in Region B, or update the two vSphere Data Protection instances in parallel.

2 [Upgrade the NSX Components for the Management and Shared Edge and Compute Clusters](#)

When you upgrade the NSX instances in the SDDC, you upgrade each functional group of components of the NSX deployment in Region A and Region B.

3 [Upgrade the Components for the Management Cluster](#)

When you upgrade the virtual infrastructure layer of the SDDC, you upgrade the components that support the management cluster first.

4 [Upgrade the Components for the Shared Edge and Compute Cluster](#)

After you upgrade the components that support the management cluster, you upgrade the components for the shared edge and compute cluster to complete the upgrade of the SDDC virtual infrastructure layer.

5 [Global Post-Upgrade Configuration of the Virtual Infrastructure Components](#)

After you upgrade all virtual infrastructure components, perform global post-upgrade configuration according to the dependencies between these components.

Update vSphere Data Protection

When you update the vSphere Data Protection instances for version 4.0 of this VMware Validated Design, you update the instance in Region A and then in Region B, or update the two vSphere Data Protection instances in parallel.

Perform the upgrade outside of the backup windows.

Upgrading vSphere Data Protection is a single-step operation in which you upgrade the virtual appliances in each region. .

Table 4-1. vSphere Data Protection Nodes in the SDDC

Region	Role	IP Address	Fully Qualified Domain Name
Region A	Backup Node	172.16.11.81	mgmt01vdp01.sfo01.rainpole.local
Region B	Backup Node	172.17.11.81	mgmt01vdp51.lax01.rainpole.local

Prerequisites

Note If you are not using vSphere Data Protection ensure that the 3rd party software has been validated from your vendor and is compatible to work with vSphere 6.5, then follow the vendor's prescribed upgrade documentation.

- Download the vSphere Data Protection upgrade .iso file to a shared datastore for mounting to the virtual appliances.
If you have space on your NFS datastore, upload the file there.
- Verify that approximately 2 GB are free on Hard Disk 1.
Use the `mccli server show-prop` command on each appliance over SSH.
- Verify that the maintenance window is in a time period in which no backup jobs are running or scheduled to run.
- Verify that no alarms on the vSphere Data Protection virtual appliances exist in both the vSphere Web Client and the vSphere Data Protection configuration interface.

Procedure

1 Take Snapshots of the vSphere Data Protection Appliances

Before you start the upgrade, take the nodes of vRealize Operations Manager offline and take a snapshot of each node so that you can roll the update back if a failure occurs.

2 Update the vSphere Data Protection Node

When you upgrade the vSphere Data Protection instances in Region A and Region B in the SDDC, start the update process from the vSphere Data Protection configuration interface. Because no interdependencies between the vSphere Data Protection nodes in each region exist, you can perform the update in parallel or sequentially starting with Region A.

3 Post-Upgrade Configuration of vSphere Data Protection

After you upgrade vSphere Data Protection, perform additional configuration of the environment in compliance with the objectives and deployment guidelines of version 4.0 of this validated design.

What to do next

- Verify that vSphere Data Protection functions flawlessly after the upgrade. See *Validate vSphere Data Protection* in the *Operational Verification* documentation.

Take Snapshots of the vSphere Data Protection Appliances

Before you start the upgrade, take the nodes of vRealize Operations Manager offline and take a snapshot of each node so that you can roll the update back if a failure occurs.

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 In the **Navigator**, click **VMs and Templates**, expand the mgmt01vc01.sfo01.rainpole.local tree and navigate to the mgmt01vdp01 virtual machine.
- 3 Right-click the **mgmt01vdp01** virtual machine and select **Power > Shut Down Guest OS** and click **Yes** in the confirmation dialog box that appears.
- 4 After the appliance is powered off, change the disk mode of the vSphere Data Protection appliance.
 - a Right-click **mgmt01vdp01** and select **Edit Settings**.
 - b On the **Virtual Hardware** tab, expand Hard disk 2, select **Dependent** from the **Disk Mode** drop-down menu.
 - c Repeat the step to change the disk mode on Hard Disk 3 to Hard disk 7 and click **OK**.
- 5 Take a snapshot of each node in the cluster.
 - a Right-click the **mgmt01vdp01** virtual machine and select **Snapshot > Take Snapshot**.
 - b In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	<i>Snapshot name</i>
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

- 6 After the snapshot is taken, right-click the **mgmt01vdp01** virtual machine and select **Power > Power On**.
- 7 Repeat the procedure on mgmt01vdp51 under the mgmt01vc51.lax01.rainpole.local vCenter Server in Region B.

Update the vSphere Data Protection Node

When you upgrade the vSphere Data Protection instances in Region A and Region B in the SDDC, start the update process from the vSphere Data Protection configuration interface. Because no interdependencies between the vSphere Data Protection nodes in each region exist, you can perform the update in parallel or sequentially starting with Region A.

Procedure

- 1 Log in to the vSphere Data Protection configuration interface.

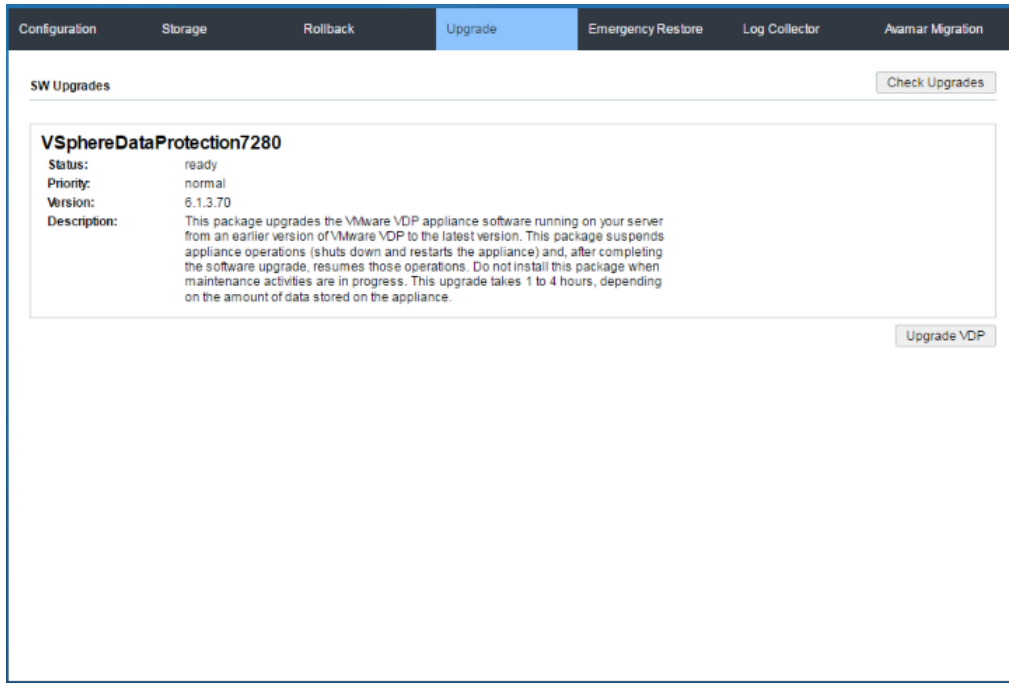
- a Open a Web browser and go to the following URLs.

Region	URL
Region A	https://mgmt01vdp01.sfo01.rainpole.local:8543/vdp-configure/
Region B	https://mgmt01vdp51.lax01.rainpole.local:8543/vdp-configure/

- b Log in use the following credentials.

Setting	Value
User Name	root
Password	<i>vdp_root_password</i>

- 2 Mount the upgrade .iso file to the vSphere Data Protection appliance.
- 3 On the **Configuration** tab, verify that all the services are running.
If all of the services are not running, the upgrade might fail.
- 4 Click the **Upgrade** tab.



The upgrades that are available on the upgrade ISO image you mounted appear in the **SW Upgrades** pane.

- 5 Select the upgrade you want to install and click **Upgrade VDP**.
- 6 Repeat the procedure for the other vSphere Data Protection appliance.

Post-Upgrade Configuration of vSphere Data Protection

After you upgrade vSphere Data Protection, perform additional configuration of the environment in compliance with the objectives and deployment guidelines of version 4.0 of this validated design.

Procedure

1 [Configure Service Account Access in vSphere for Integration with vSphere Data Protection](#)

After you upgrade vSphere Data Protection, configure an operations service account with permissions that are required to enable vSphere Data Protection access to provide backup operations on the Management vCenter Server instances in Region A and Region B.

2 [Place vSphere Data Protection in a Dedicated VM and Templates Folder](#)

Create a folder on the Management vCenter Server in each region to group vSphere Data Protection instance together with Site Recovery Manager and vSphere Replication for easier management, and move the appliance there.

Configure Service Account Access in vSphere for Integration with vSphere Data Protection

After you upgrade vSphere Data Protection, configure an operations service account with permissions that are required to enable vSphere Data Protection access to provide backup operations on the Management vCenter Server instances in Region A and Region B.

Procedure

1 Define a User Role in vSphere for Integration with vSphere Data Protection

In vSphere, create a user role with privileges that are required for performing backup operations against for the management virtual machines in vSphere Data Protection in Region A.

2 Configure User Privileges in vSphere for Integration with vSphere Data Protection

Assign global permissions to the operations service account svc-vdp so that you can manage and perform backups by using vSphere Data Protection.

Define a User Role in vSphere for Integration with vSphere Data Protection

In vSphere, create a user role with privileges that are required for performing backup operations against for the management virtual machines in vSphere Data Protection 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://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 **Home** page of the vSphere Web Client, select **Roles** under **Administration**.

3 Create a new role for managing backups.

- a On the **Roles** page, click the **Create role action** icon.
- b In the **Create Role** dialog box, configure the role using the following configuration settings, and click **OK**.

Setting	Value
Role name	vSphere Data Protection User
Privilege	<ul style="list-style-type: none"> ■ Alarms.Create Alarm ■ Alarms.Modify Alarms ■ Datastore.Allocate space ■ Datastore.Browse datastore ■ Datastore.Configure datastore ■ Datastore.Low level file operations ■ Datastore.Move datastore ■ Datastore.Remove datastore ■ Datastore.Remove file ■ Datastore.Rename datastore ■ Extension.Register extension ■ Extension.Update extensions ■ Folder.Create folder ■ Global.Cancel task ■ Global.Disable methods ■ Global.Enable methods ■ Global.Licenses ■ Global.Log event ■ Global.Manage custom attributes ■ Global.Settings ■ Network.Assign network ■ Network.Configure ■ Resource.Assign virtual machine to resource pool ■ Session.Validate session ■ Tasks.Create task ■ Tasks.Update task ■ Virtual Machine.Configuration.Add existing disk ■ Virtual Machine.Configuration.Add new disk ■ Virtual Machine.Configuration.Add or remove device ■ Virtual Machine.Configuration.Advanced ■ Virtual Machine.Configuration.Change cpu count ■ Virtual Machine.Configuration.Change resource ■ Virtual Machine.Configuration.Disk change tracking ■ Virtual Machine.Configuration.Disk lease ■ Virtual Machine.Configuration.Extend virtual disk ■ Virtual Machine.Configuration.Host USB device ■ Virtual Machine.Configuration.Memory ■ Virtual Machine.Configuration.Modify device settings ■ Virtual Machine.Configuration.Raw device

Setting	Value
	<ul style="list-style-type: none"> ■ Virtual Machine.Configuration.Reload from path ■ Virtual Machine.Configuration.Remove disk ■ Virtual Machine.Configuration.Rename ■ Virtual Machine.Configuration.Reset guest information ■ Virtual Machine.Configuration.Set annotation ■ Virtual Machine.Configuration.Settings ■ Virtual Machine.Configuration.Swapfile placement ■ Virtual Machine.Configuration.Upgrade virtual machine compatibility ■ Virtual Machine.Guest Operations.Guest Operation Modifications ■ Virtual Machine.Guest Operations.Guest Operations Program execution ■ Virtual Machine.Guest Operations.Guest Operation Queries ■ Virtual Machine.Interaction.Console interaction ■ Virtual Machine.Interaction.Device connection ■ Virtual Machine.Interaction.Guest operating system management by VIX API ■ Virtual Machine.Interaction.Power off ■ Virtual Machine.Interaction.Power on ■ Virtual Machine.Interaction.Reset ■ Virtual Machine.Interaction.ViMware tools install ■ Virtual Machine.Inventory.Create new ■ Virtual Machine.Inventory.Register ■ Virtual Machine.Inventory.Remove ■ Virtual Machine.Inventory.Unregister ■ Virtual Machine.Provisioning.Allow disk access ■ Virtual Machine.Provisioning.Allow read-only disk access ■ Virtual Machine.Provisioning.Allow virtual machine download ■ Virtual Machine.Provisioning.Mark as template ■ Virtual Machine.Snapshot management.Create snapshot ■ Virtual Machine.Snapshot management.Remove snapshot ■ Virtual Machine.Snapshot management.Revert snapshot ■ vApp.Export ■ vApp.Import ■ vApp.vApp application configuration

This role inherits the **System.Anonymous System.View**, and **System.Read** permissions.

- 4 The Management vCenter Server for Region A propagates the role to the other linked vCenter Server instances.

Configure User Privileges in vSphere for Integration with vSphere Data Protection

Assign global permissions to the operations service account svc-vdp so that you can manage and perform backups by using vSphere Data Protection.

The svc-vdp user has access rights that are specifically required for performing backups of vCenter Server inventory.

Prerequisites

- Verify that the Management vCenter Server for Region A are connected to the Active Directory domain.
- Verify that the users and groups from the rainpole.local domain are available on the Management vCenter Server or Region A.

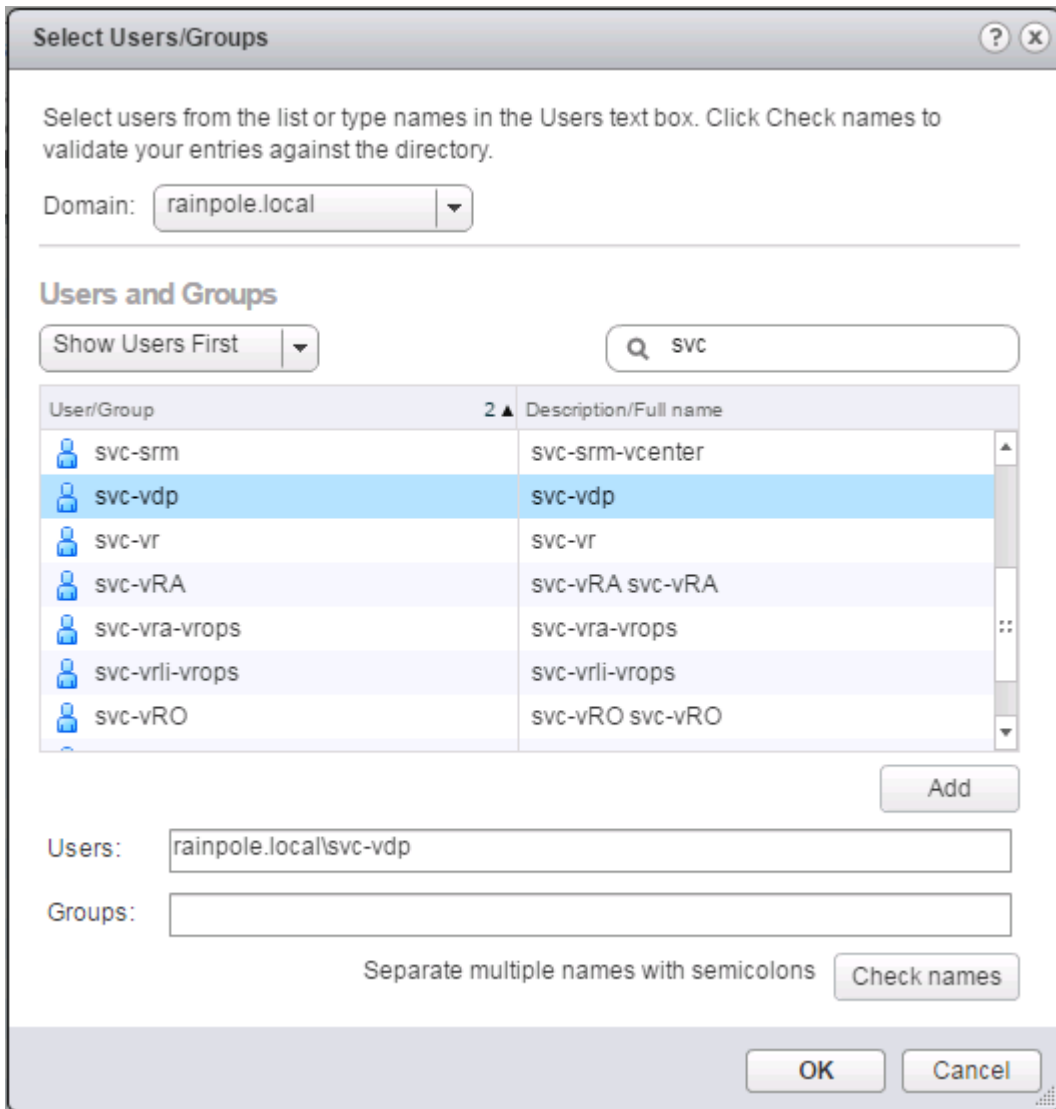
Procedure

- 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, select **Administration**.
- 3 Assign global permissions to the svc-vdp@rainpole.local service account.
 - a In the vSphere Web Client, select navigate **Administration** from the **Home** menu and click **Global Permissions** under **Access Control**.
 - b On the **Manage** tab, click **Add Permission**.
 - c In the **Global Permissions Root - Add Permission** dialog box, click **Add** to associate a user or a group with a role.
 - d In the **Select Users/Groups** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.

- e From the list of users and groups, select the **svc-vdp** user, click **Add**, and click **OK**.



- f In the **Global Permissions Root - Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **vSphere Data Protection User**, select **Propagate to children**, and click **OK**.

The global permissions of the svc-vdp service account propagate to all linked vCenter Server instances.

Place vSphere Data Protection in a Dedicated VM and Templates Folder

Create a folder on the Management vCenter Server in each region to group vSphere Data Protection instance together with Site Recovery Manager and vSphere Replication for easier management, and move the appliance there.

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 If the BCDR01 folder is not available, create it.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **mgmt01vc01.sfo01.rainpole.local** tree.
 - c Right-click the **SFO01** data center, and select **New Folder > New VM and Template Folder**.
 - d In the **New Folder** dialog box enter **BCDR01** as the name to label the folder and click **OK**.
- 3 Move the vSphere Data Protection to the BCDR01 folder.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **mgmt01vc01.sfo01.rainpole.local** tree.
 - c Expand the **Discovered Virtual Machines** folder.
 - d Drag **mgmt01vdp01** to the BCDR01 folder.
- 4 Repeat [Step 2](#) and [Step 3](#) to place the **mgmt01vdp51** virtual machine in the BCDR51 folder on the Management vCenter Server in Region B mgmt01vc51.lax01.rainpole.local under the LAX01 data center.

Upgrade the NSX Components for the Management and Shared Edge and Compute Clusters

When you upgrade the NSX instances in the SDDC, you upgrade each functional group of components of the NSX deployment in Region A and Region B.

Upgrading NSX for vSphere is a multi-step operation where you must upgrade the NSX Managers paired instances for Cross-vCenter Networking and Security, the NSX Controller nodes, the ESXi VIBs, and the NSX Edge devices. This upgrade operation is split between the management cluster pairs and the shared edge and compute cluster pairs. You might perform the upgrades of these components in different maintenance windows.

Table 4-2. NSX Nodes in the SDDC

Role	IP Address	FQDN	Region
NSX Manager for the management cluster that is running as primary	172.16.11.65	mgmt01nsx01.sfo01.rainpole.local	Region A
NSX Controller 1 for the management cluster	172.16.11.118	-	
NSX Controller 2 for the management cluster	172.16.11.119	-	
NSX Controller 3 for the management cluster	172.16.11.120	-	
NSX Manager for the shared edge and compute cluster that is running as primary	172.16.11.66	comp01nsx01.sfo01.rainpole.local	
NSX Controller 1 for the shared edge and compute cluster	172.16.31.118	-	
NSX Controller 2 for the shared edge and compute cluster	172.16.31.119	-	
NSX Controller 3 for the shared edge and compute cluster	172.16.31.120	-	
NSX Manager for the management cluster that is running as secondary	172.17.11.65	mgmt01nsx51.lax01.rainpole.local	Region B
NSX Manager for the shared edge and compute cluster that is running as secondary	172.17.11.66	comp01nsx51.lax01.rainpole.local	

Important You might receive a number of false alerts from vRealize Operations Manager and vRealize Log Insight during this upgrade procedure of NSX components.

Prerequisites

- Download the NSX update bundle on the Windows host that has access to your data center.
- Review [Operational Impacts of NSX Upgrade](#) from *NSX Upgrade Guide* to understand the impact that each component might have on your VMware Validated Design environment.
- Verify that any virtual networking integration within the environment has been quiesced of all activities, including but not limited to: users ordering new virtual machines backed by virtual wires over the Cloud Management Platform (CMP); third-party integration that automates the ordering or deployment of new virtual machines that are backed by virtual wires; and administrators manually creating new NSX-based components.

Without quiescing the environment, rollback operations might be disrupted by generated orphaned objects. You might also have to extend the time of the maintenance windows.

- Validate the NSX Manager file system usage, and perform a cleanup if file system usage is at 100 percent.
 - a Open an SSH connection using the admin account to the NSX Manager instance you are upgrading and run the `show filesystems` command to show the filesystem usage.
 - b If the usage is 100 percent, enter Privileged mode and clean the logs up by running the following commands.

```
enable
purge log manager
purge log system
```

- c Reboot the NSX Manager appliance for the log cleanup to take effect.
- Back up the NSX configuration and download technical support logs before upgrading. See *Backing Up and Restoring the NSX Instances in Region A* and *Backing Up and Restoring the NSX Instances in Region B* from the *VMware Validated Design Backup and Restore* documentation.
- Take a backup of the NSX Manager pair, both the primary and secondary, and of NSX Controller virtual machines. For more information, see [Preparing for the NSX Upgrade](#) from *NSX Upgrade Guide*.
- Verify that all of the controllers are in normal, connected state.
- Get the current version of the NSX VIBs on the hosts in the management cluster and in the shared edge and compute cluster.
 - a Log in to one of the hosts in the cluster and run the `esxcli software vib list | grep esx` command.
 - b Note the current version of the following VIBs.
 - esx-vsip

- esx-vxlan

Procedure

1 Upgrade the NSX Manager Instances

When you upgrade the NSX components in Region A and Region B, upgrade the NSX Manager instances first.

2 Upgrade the NSX Controllers

After you upgrade the NSX Manager instance, upgrade the NSX Controller instances for the management cluster and for the shared edge and compute cluster.

3 Upgrade the NSX Components on the ESXi Hosts

After you upgrade the NSX Manager and NSX Controller instances in Region A and Region B, update the NSX Virtual Infrastructure Bundles (VIBs) on each ESXi host in the management, and in the shared edge and compute cluster.

4 Upgrade NSX Edge Instances

Upgrade the NSX Edge services gateways, universal distributed logical router and load balancer instances.

5 Post-Upgrade Configuration of NSX for vSphere

After you upgrade the components of NSX for vSphere, perform additional configuration for compliance with the objectives and deployment guidelines of version 4.0 of this validated design.

What to do next

Verify that NSX components function flawlessly after the upgrade. See *Validate NSX for vSphere* in the *Operational Verification* documentation.

Upgrade the NSX Manager Instances

When you upgrade the NSX components in Region A and Region B, upgrade the NSX Manager instances first.

You start with the NSX Manager nodes for the management cluster first and then continue with the NSX Manager nodes for the shared edge and compute cluster.

Table 4-3. NSX Manager Details

Order	NSX Manager Instance	NSX Appliance URL	vCenter Server URL	Region
1	NSX Manager for the management cluster that is configured running as primary	https://mgmt01nsxm01.sfo01.rainpole.local	mgmt01vc01.sfo01.rainpole.local	Region A
2	NSX Manager for the management cluster that is running as secondary	https://mgmt01nsxm51.lax01.rainpole.local	mgmt01vc51.lax01.rainpole.local	Region B

Table 4-3. NSX Manager Details (Continued)

Order	NSX Manager Instance	NSX Appliance URL	vCenter Server URL	Region
3	NSX Manager for the shared edge and compute cluster that is running as primary	https://comp01nsxm01.sfo01.rainpole.local	comp01vc01.sfo01.rainpole.local	Region A
4	NSX Manager for the shared edge and compute cluster that is running as secondary.	https://comp01nsxm51.lax01.rainpole.local	comp01vc51.lax01.rainpole.local	Region B

Procedure

- 1 Log in to the Management NSX Manager appliance user interface.
 - a Open a Web browser and go to **https://mgmt01nsxm01.sfo01.rainpole.local**.
 - b Log in using the following credentials.

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

- 2 In the appliance user interface, click **Upgrade**.
- 3 On the **Upgrade** page, click **Upgrade** and browse your file system to locate the **.tar.gz** upgrade bundle.
- 4 Once the file has been located, click **Open** and click **Continue**.
The NSX Manager starts uploading the bundle.
- 5 After the upload is complete, in the **Upgrade** dialog box, select **Yes** next to **Do you want to enable SSH?** and **Do you want to join the VMware Customer Experience Program**, and click **Upgrade**.
- 6 After the upgrade is complete, if not already logged in, log in to the NSX Manager instance for the management cluster again and verify that the **Upgrade** tab shows the following configuration.

Setting	Expected Value
Upgrade State	Complete
Current Software Version	<i>the version and build in the upgrade bundle you installed</i>

- a Open a Web browser and go to **https://mgmt01nsxm01.sfo01.rainpole.local**.
- b Log in using the following credentials.

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

- 7 After you upgrade the NSX Manager, restart the vSphere Web Client to trigger upgrade of the NSX plug-ins.

- a Open an SSH connection to the mgmt01vc01.sfo01.rainpole.local vCenter Server Appliance.
- b Log in using the following credentials.

Credential	Value
User name	root
Password	mgmtvc_root_password

- c Run the following commands to restart the vSphere Web Client.

```
service-control --stop vsphere-client
service-control --start vsphere-client
```

- 8 Perform a fresh backup of the primary NSX Manager because the old backups can not be restored to the new NSX Manager version.

See the *VMware Validated Design Backup and Restore* documentation.

- 9 Repeat the steps for the secondary NSX Manager mgmt01nsxm51.lax01.rainpole.local to complete the NSX Manager upgrade in the management cluster.

- 10 Perform a fresh backup of the secondary NSX Manager because the old backups can not be restored to the new NSX Manager version.

See the *VMware Validated Design Backup and Restore* documentation.

- 11 Repeat the procedure for the shared edge and compute cluster.

You start with the primary NSX Manager comp01nsxm01.sfo01.rainpole.local and complete the upgrade with the secondary NSX Manager comp01nsxm51.lax01.rainpole.local.

Upgrade the NSX Controllers

After you upgrade the NSX Manager instance, upgrade the NSX Controller instances for the management cluster and for the shared edge and compute cluster.

For each NSX Manager that has the primary role, you start an upgrade for the connected NSX Controller cluster. During the upgrade, an upgrade file is downloaded to each controller node. The controllers are upgraded one at a time so that high availability remains persistent during the upgrade.

You upgrade the NSX Controller cluster for the management cluster in Region A first. Repeat the upgrade procedure for the NSX Controller cluster for the shared edge and compute cluster in Region A. You can perform these operations in the same or separate maintenance windows.

Table 4-4. NSX Controller Properties in Region A

Order	NSX Manager	NSX Manager IP Address	NSX Controller IP Address	Region
1	Primary NSX Manager for the management cluster	172.16.11.65	172.16.11.118	Region A
			172.16.11.119	
			172.16.11.120	
2	Primary NSX Manager for the shared edge and compute cluster	172.16.11.66	172.16.31.118	Region A
			172.16.31.119	
			172.16.31.120	

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 In the **Navigator**, click **Networking & Security**, and click **Installation**.
- 3 Under NSX Managers, select the **172.16.11.65** NSX Manager instance and click **Upgrade Available** in the **Controller Cluster Status** column.
- 4 In the **Upgrade Controller** dialog, click **Yes**.

The **Upgrade Status** column in the NSX Controller nodes pane displays the upgrade status for each controller. The status starts with Downloading upgrade file, then changes to Upgrade in progress, and finally to Rebooting. After a controller is upgraded, the status becomes Upgraded.

- 5 After the upgrade is complete for each NSX Controller, confirm that all are connected to the NSX Manager, verify that the NSX Controller has the following configuration the **NSX Controller nodes** section of the **Installation** page.

Setting	Expected Value
Status	Connected
Software Version	6.3

- 6 After the upgrade of the NSX Controller cluster of the management cluster is complete, repeat the procedure to on the NSX Controller nodes for the shared edge and compute cluster in Region A.

Upgrade the NSX Components on the ESXi Hosts

After you upgrade the NSX Manager and NSX Controller instances in Region A and Region B, update the NSX Virtual Infrastructure Bundles (VIBs) on each ESXi host in the management, and in the shared edge and compute cluster.

For each NSX Manager instance in Region A and Region B, you run an upgrade for each associated cluster. You run the upgrade on the hosts of the management cluster in Region A first and proceed with the other clusters in the two regions.

Table 4-5. NSX Manager Instances and Associated Host Clusters

Region	NSX Manager	NSX Manager IP Address	Host Clusters
Region A	NSX Manager for the management cluster	172.16.11.65	mgm01vc01.sfo01.rainpole.local > SFO01 > SFO01-Mgmt01
	NSX Manager for the shared edge and compute cluster	172.16.11.66	mgm01vc01.sfo01.rainpole.local > SFO01 > SFO01-Comp01
Region B	NSX Manager for the management cluster	172.17.11.65	mgm01vc51.lax01.rainpole.local > LAX01 > LAX01-Mgmt01
	NSX Manager for the shared edge and compute cluster	172.17.11.66	mgm01vc51.lax01.rainpole.local > LAX01 > LAX01-Comp01

Prerequisites

- Verify that vSphere DRS is enabled on the host clusters, and is set to Fully Automated.
- Verify that vSphere vMotion functions correctly between all ESXi hosts within the cluster.
- Verify that all ESXi hosts are in a connected state with vCenter Server.

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 In the **Navigator**, click **Networking & Security**.
- 3 In the **Navigator**, click **Installation** and click the **Host Preparation** tab.
- 4 From the **NSX Manager** drop-down menu, select the IP address **172.16.11.65** of the NSX Manager for the management cluster in Region A.

- 5 Under **NSX Components Installation on Hosts**, click **Upgrade available** next to the SFO01-Mgmt01 cluster.
- 6 In the confirmation dialog, click **Yes**.

If the hosts must be in maintenance mode, for example, because of high availability requirements or DRS rules, the upgrade process stops and the cluster **Installation Status** becomes Not Ready.
- 7 If the **Installation Status** is Not Ready because the hosts must be in maintenance mode, manually move all virtual machines from the hosts, select the cluster again and click the **Resolve** action.
- 8 Repeat the steps to update the NSX components on the clusters in Region A and Region B.

Upgrade NSX Edge Instances

Upgrade the NSX Edge services gateways, universal distributed logical router and load balancer instances.

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 **Networking & Security**.
- 3 From the **Networking & Security** menu on the left, click **NSX Edges**.
- 4 On the **NSX Edges** page, select the IP address of the NSX Manager instance from the **NSX Manager** drop-down menu.

NSX Manager Instance	Region	IP Address
NSX Manager for the management cluster	Region A	172.16.11.65
NSX Manager for the shared edge and compute cluster	Region A	172.16.11.66
NSX Manager for the management cluster	Region B	172.17.11.65
NSX Manager for the shared edge and compute cluster	Region B	172.17.11.66

The edge devices in the scope of the NSX Manager appear.

- 5 For each NSX Edge instance, select **Upgrade Version** from the **Actions** menu and in the **Upgrade Edge** confirmation dialog box, click **Yes**.

Perform the upgrade in the following order as to minimize disruption on both the management and shared and edge compute pods.

Order	Management Edge in Region A	Management Edge in Region B	Compute Edge in Region A	Compute Edge in Region B
1	SFOMGMT-ESG01			
2		LAXMGMT-ESG01		
3	SFOMGMT-ESG02			
4		LAXMGMT-ESG02		
5	SFOMGMT-LB01			
6		LAXMGMT-LB01		
7	UDLR01	-		
8			SFOCOMP-ESG01	
9				LAXCOMP-ESG01
10			SFOCOMP-ESG02	
11				LAXCOMP-ESG02
12			UDLR01	-

After all the NSX edges are upgraded successfully, verify that for the edge device the **Status** column shows Deployed, and the **Version** column contains the upgraded version.

Post-Upgrade Configuration of NSX for vSphere

After you upgrade the components of NSX for vSphere, perform additional configuration for compliance with the objectives and deployment guidelines of version 4.0 of this validated design.

Procedure

1 [Enable Health Check on the vSphere Distributed Switches](#)

Turn on the health check of whether the VLAN settings on the distributed switches match the trunk port configuration on the connected physical switch ports and of whether the physical access switch port MTU jumbo frame setting matches the MTU setting on the switches.

2 [Configure Global Transport Zones for the Shared Edge and Compute Clusters](#)

Configure the global transport zones for the shared edge and compute clusters to enable networking provisioning in Region A and Region B from vRealize Automation.

3 [Configure NSX Managers to Use a Service Account for Connection to vCenter Server](#)

After you upgrade NSX for vSphere, reconnect the NSX Manager instances to vCenter Server using a dedicated service account for better access control.

4 [Configure the Anti-Affinity Rules for the NSX Components](#)

After you update the NSX components, rename the anti-affinity rules for these components in vSphere DRS to implement a configuration that matches the deployment guidelines in this validated design.

5 Place the NSX Manager Appliances in a VM and Templates Folder

Create a folder on the Management vCenter Server in each region to group NSX Manager instances together for easier management, and move the appliances there.

6 Deploy and Configure Distributed Logical Routers for the Shared Edge and Compute Clusters

After you update NSX for vSphere, deploy the distributed logical routers that are required for network provisioning in vRealize Automation.

Enable Health Check on the vSphere Distributed Switches

Turn on the health check of whether the VLAN settings on the distributed switches match the trunk port configuration on the connected physical switch ports and of whether the physical access switch port MTU jumbo frame setting matches the MTU setting on the switches.

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 Enable vSphere Distributed Switch health checks in Region A

- a In the **Navigator**, click **Networking** and expand the **SFO01** data center under the mgmt01vc01.sfo01.rainpole.local vCenter Server.
- b Select the **vDS-Mgmt** distributed switch and click the **Manage** tab.
- c On the **Manage** tab, select **Health check** on the **Settings** tab and click the **Edit** button.
- d Configure the following settings and click **OK**.

Setting	Value
VLAN and MTU	Enabled
Teaming and failover	Enabled

- e Repeat the step to enable health checks on the vDS-Comp01 switch under the **SFO01** data center of the under the comp01vc01.sfo01.rainpole.local vCenter Server.
- 3 Repeat the procedure to enable the health checks on the vDS-Mgmt and vDS-Comp01 switches under the LAX01 data centers of the mgmt01vc51.lax01.rainpole.local and comp01vc51.lax01.rainpole.local vCenter Server.

Configure Global Transport Zones for the Shared Edge and Compute Clusters

Configure the global transport zones for the shared edge and compute clusters to enable networking provisioning in Region A and Region B from vRealize Automation.

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 vSphere Web Client Home menu, click **Networking & Security** and click **Installation** in the **Navigator**.
- 3 Configure the global transport zone.
 - a Click the **Logical Network Preparation** tab and click **Transport Zones**.
 - b Select NSX Manager for the region, click the **Add New Transport zone** icon, enter the following settings, and click **OK**.

Setting	Value for Region A	Value for Region B
NSX Manager	172.16.11.66	172.17.11.66
Name	Comp Global Transport Zone	Comp Global Transport Zone
Replication mode	Hybrid	Hybrid
Select clusters part of the Transport Zone	SFO01-Comp01	LAX01-Comp01

Name	Description	Scope	Control Plane Mode	CDO Mode	Logical Switches
Comp Global Transport Zone		Global	Hybrid	Disabled	1
Comp Universal Transport Z...		Universal	Hybrid	Disabled	1

- c Repeat the steps to add a global transport zone for the shared edge and compute cluster in Region B.

Configure NSX Managers to Use a Service Account for Connection to vCenter Server

After you upgrade NSX for vSphere, reconnect the NSX Manager instances to vCenter Server using a dedicated service account for better access control.

Procedure

1 Assign User Privileges to the NSX Service Account in vCenter Server

After you upgrade NSX for vSphere, configure user privileges for access to the vSphere to vCenter Server inventory to the svc-nsxmanager service account.

2 Configure NSX Managers with Service Account for Communication with vCenter Server

After you assign administrator privileges to access to the vCenter Server inventory, configure the NSX Manager instances to use the svc-nsxmanager for authentication to vCenter Server.

Assign User Privileges to the NSX Service Account in vCenter Server

After you upgrade NSX for vSphere, configure user privileges for access to the vSphere to vCenter Server inventory to the svc-nsxmanager service account.

Procedure

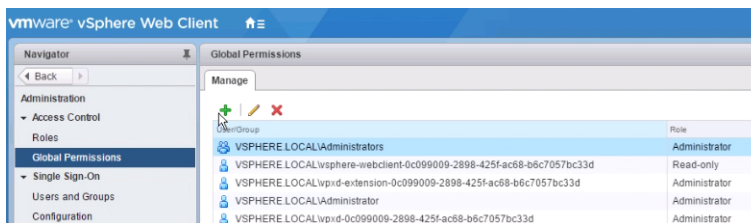
1 Log in to the Management vCenter Server by using the vSphere Web Client.

- 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 **Administration** and click **Global Permissions**.

3 Click the **Add** icon.



4 In the **Global Permission Root - Add Permission** dialog box, click **Add**.

5 In the **Select Users/Groups** dialog box, select **rainpole.local** from the **Domain** drop-down menu.

6 In the search box, enter **svc-nsxmanager** and press **Enter**.

- 7 Select **svc-nsxmanager**, click **Add** and click **OK**.

Select Users/Groups

Select users from the list or type names in the Users text box. Click Check names to validate your entries against the directory.

Domain: rainpole.local

Users and Groups

Show Users First

svc-nsxmanager

User/Group	Description/Full name
svc-nsxmanager	svc-nsxmanager

Add

Users: rainpole.local\svc-nsxmanager

Groups:

Separate multiple names with semicolons

Check names

OK Cancel

- 8 In the **Global Permission Root - Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **Administrator**, select **Propagate to children**, and click **OK**.
- 9 Click **OK**.

Configure NSX Managers with Service Account for Communication with vCenter Server

After you assign administrator privileges to access to the vCenter Server inventory, configure the NSX Manager instances to use the svc-nsxmanager for authentication to vCenter Server.

You configure the svc-nsxmanager service account on the four NSX Manager instances in the two regions.

NSX Manager	URL	Connected vCenter Server
NSX Manager for the management cluster in Region A	https://mgmt01nsxm01.sfo01.rainpole.local	mgmt01vc01.sfo01.rainpole.local
NSX Manager for the shared edge and compute cluster in Region A	https://comp01nsxm01.sfo01.rainpole.local	comp01vc01.sfo01.rainpole.local
NSX Manager for the management cluster in Region B	https://mgmt01nsxm51.lax01.rainpole.local	mgmt01vc51.lax01.rainpole.local
NSX Manager for the shared edge and compute cluster in Region B	https://comp01nsxm51.lax01.rainpole.local	comp01vc51.lax01.rainpole.local

Procedure

- 1 Log in to the Management NSX Manager appliance user interface.
 - a Open a Web browser and go to **https://mgmt01nsxm01.sfo01.rainpole.local**.
 - b Log in using the following credentials.

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

- 2 Click **Manage vCenter Registration**.
- 3 Under **vCenter Server**, click **Edit**.
- 4 In the **vCenter Server** dialog box, change the user account for connecting to vCenter Server, and click **OK**.

Setting	Value
vCenter Server	mgmt01vc01.sfo01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	svc-nsxmanager_password

- 5 In the **Trust Certificate?** dialog box, click **Yes**.
- 6 Wait for the **Status** indicator for vCenter Server to change to the Connected status.
- 7 Repeat to procedure to configure the other NSX Manager instances with the svc-nsxmanager service account.

Configure the Anti-Affinity Rules for the NSX Components

After you update the NSX components, rename the anti-affinity rules for these components in vSphere DRS to implement a configuration that matches the deployment guidelines in this validated design.

You rename the rules for the NSX controllers and add new rules of the NSX Edge device pairs for north-south routing in the two regions.

Table 4-6. Anti-Affinity Rules Configuration After NSX Update

Region	Old Rule Name	New Rule Name	Members	vCenter Server Cluster
Region A	Mgmt_NSX_Contr ollers	anti-affinity-rule- nsxcontrollers	NSX controllers in the management cluster	mgm01vc01.sfo01.rainpole.local > SFO01 > SFO01-Mgmt01
	Comp_NSX_Cont rollers	anti-affinity-rule- nsxcontrollers	NSX controllers in the shared edge and compute cluster	comp01vc01.sfo01.rainpole.local > SFO01 > SFO01-Comp01
	-	anti-affinity-rule- ecmpedges	SFOMGMT-ESG01, SFOMGMT-ESG02	mgm01vc01.sfo01.rainpole.local > SFO01 > SFO01-Mgmt01
	-	anti-affinity-rule- ecmpedges	SFOCOMP-ESG01, SFOCOMP-ESG02	comp01vc01.sfo01.rainpole.local > SFO01 > SFO01-Comp01
Region B	-	anti-affinity-rule- ecmpedges	LAXMGMT-ESG01, LAXMGMT-ESG02	mgmt01vc51.lax01.rainpole.local > LAX01 > LAX01-Mgmt01
	-	anti-affinity-rule- ecmpedges	LAXCOMP-ESG01, LAXCOMP-ESG02	comp01vc51.lax01.rainpole.local > LAX01 > LAX01-Comp01

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** page of the vSphere Web Client, click **Hosts and Clusters**.
- 3 In the **Navigator**, expand **mgmt01vc01.sfo01.rainpole.local > SFO01** and click **SFO01-Mgmt01**.
- 4 On the **Manage** tab, select **VM/Host Rules** under **Configuration**.
- 5 Rename the anti-affinity rules for the NSX Controller virtual machines.
 - a Select the **Mgmt_NSX_Controllers** rule from the **VM/Host Rules** list and click **Edit**.
 - b In the **Edit VM/Host Rule** dialog box, enter **anti-affinity-rule-nsxcontrollers** in the **Name** text box and click **OK**.
 - c Repeat the steps to rename the **Comp_NSX_Controllers** rule.

- 6 Create an anti-affinity rule for the NSX Edge devices for north-south routing for the management cluster in Region A.
 - a Under **VM/Host Rules**, click **Add**.
 - b In the **SFO01-Mgmt01 - Create VM/Host Rule** dialog box, enter the following settings and click **Add**.

Setting	Value
Name	anti-affinity-rule-ecmpedges
Enable rule	Selected
Type	Separate Virtual Machine
 - c In the **Add Rule Member** dialog box, select the check box next to each of the two SFOMGMT-ESG01 and SFOMGMT-ESG02 virtual machines, and click **OK**.
 - d In the SFO01-Mgmt01 - Create VM/Host Rule dialog box, click **OK**.
- 7 Repeat [Step 6](#) to create an anti-affinity rule for the other NSX Edge devices for north-south routing in Region A and Region B.

Place the NSX Manager Appliances in a VM and Templates Folder

Create a folder on the Management vCenter Server in each region to group NSX Manager instances together for easier management, and move the appliances there.

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 Create the NSX01 folder.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **mgmt01vc01.sfo01.rainpole.local** tree.
 - c Right-click the **SFO01** data center, and select **New Folder > New VM and Template Folder**.
 - d In the **New Folder** dialog box enter **NSX01** as the name to label the folder and click **OK**.

- 3 Move the NSX Manager for the management cluster and for the shared edge and compute cluster to the NSX01 folder.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **mgmt01vc01.sfo01.rainpole.local** tree.
 - c Drag **mgmt01nsxm01** and **comp01nsxm01.sfo01** to the NSX01 folder.
- 4 Repeat [Step 2](#) and [Step 3](#) to place the **mgmt01nsxm51** and **comp01nsxm51** virtual machines in the NSX51 folder on the Management vCenter Server in Region B mgmt01vc51.lax01.rainpole.local under the LAX01 data center.

Deploy and Configure Distributed Logical Routers for the Shared Edge and Compute Clusters

After you update NSX for vSphere, deploy the distributed logical routers that are required for network provisioning in vRealize Automation.

Procedure

- 1 [Configure a Logical Switch and Deploy Distributed Logical Router for the Shared Edge and Compute Cluster in Region A](#)
Configure a logical switch and deploy the distributed logical routers (DLR).
- 2 [Configure Distributed Logical Router for Dynamic Routing in Shared Edge and Compute Cluster in Region A](#)
Configure the distributed logical router (DLR) in the shared edge and compute cluster to use dynamic routing.
- 3 [Connect the NSX Edge Devices in the Shared Edge and Compute Cluster to the Distributed Logical Router in Region A](#)
After you deploy a distributed logical router for the shared edge and compute cluster in Region A according to this design, you configure an interface and update BGP on the SFOCOMP-ESG01 and SFOCOMP-ESG02 NSX Edge devices for connection to the router.
- 4 [Configure a Logical Switch and Deploy the Distributed Logical Router for the Shared Edge and Compute Cluster in Region B](#)
Configure a logical switch and deploy the distributed logical router (DLR).
- 5 [Configure Distributed Logical Router for Dynamic Routing in Shared Edge and Compute Cluster in Region B](#)
Configure the distributed logical router (DLR) in the shared edge and compute cluster to use dynamic routing.
- 6 [Connect the NSX Edge Devices in the Shared Edge and Compute Cluster to the Distributed Logical Router in Region B](#)
After you deploy a distributed logical router for the shared edge and compute cluster in Region B according to this design, you configure an interface and update BGP on the LAXCOMP-ESG01 and LAXCOMP-ESG02 NSX Edge devices for connection to the router.

Configure a Logical Switch and Deploy Distributed Logical Router for the Shared Edge and Compute Cluster in Region A

Configure a logical switch and deploy the distributed logical routers (DLR).

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://comp01vc01.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 Client **Home** menu, select **Networking & Security**.
- 3 In the **Navigator**, click **Logical Switches**.
- 4 Select **172.16.11.66** from the **NSX Manager** drop-down menu and click the **Add** icon.
- 5 In the **New Logical Switch** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	Global Transit Network
Transport Zone	Comp Global Transport Zone
Replication Mode	Hybrid

- 6 In the **Navigator**, click **NSX Edges**.
- 7 Select **172.16.11.66** from the **NSX Manager** drop-down menu.
- 8 Click the **Add** icon to create a new distributed logical router.

The **New NSX Edge** wizard appears.

- 9 On the **Name and description** page, enter the following settings, and click **Next**.

Setting	Value
Logical (Distributed) Router	Selected
Name	SFOCOMP-DLR01
Deploy Edge Appliance	Selected
Enable High Availability	Selected

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

Setting	Value
User Name	admin
Password	<i>dlr_admin_password</i>
Enable SSH access	Selected
Enable FIPS mode	Deselected
Edge Control Level logging	INFO

- 11 On the **Configure deployment** page, and click the **Add** icon.

The **Add NSX Edge Appliance** dialog box appears.

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

Setting	Value
Cluster/Resource Pool	SDDC-EdgeRP01
Datastore	<i>sfo01_shared_edge_and_compute_datastore</i>

- 13 On the **Configure deployment** page, click the **Add** icon a second time to add a second NSX Edge device.

The **Add NSX Edge Appliance** dialog box appears.

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

Setting	Value
Resource Pool	SDDC-EdgeRP01
Datastore	<i>sfo01_shared_edge_and_compute_datastore</i>

- 15 Click **Next**.

- 16 On the **Configure interfaces** page, under **HA Interface Configuration**, click **Select** and connect to **vDS-Comp01-Management**.

17 On the **Configure interfaces** page, enter the following configuration settings and click **Next**.

Setting	Value
Primary IP Address	1.3.1.1
Subnet Prefix Length	24

- a Click the **Add** icon.

The **Add Interface** dialog box appears.

- b Enter the following settings in the **Add Interface** dialog box, and click **OK**.

Setting	Value
Name	Uplink
Type	Uplink
Connected To	Global Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.101.3
Subnet Prefix Length	24
MTU	9000

18 On the **Default gateway settings** page, deselect **Configure Default Gateway** and click **Next**.

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

Configure Distributed Logical Router for Dynamic Routing in Shared Edge and Compute Cluster in Region A

Configure the distributed logical router (DLR) in the shared edge and compute cluster to use dynamic routing.

Procedure

- 1** Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://comp01vc01.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 Client **Home** menu, select **Networking & Security**.
- 3** In the **Navigator**, click **NSX Edges**.
- 4** Select **172.16.11.66** from the **NSX Manager** drop-down menu.

5 Configure the routing for the Distributed Logical Router.

- a Double-click **SFOCOMP-DLR01**.
- b Click the **Manage** tab and click **Routing**.
- c On the **Global Configuration** page, perform the following configuration steps.
- d Click the **Enable** button for **ECMP**.
- e Click the **Edit** button under **Dynamic Routing Configuration**, select **Uplink** as the Router ID, and click **OK**.
- f Click **Publish Changes**.

6 On the left, select **BGP** to configure it.

- a On the **BGP** page, click the **Edit** button.

The **Edit BGP Configuration** dialog box appears.

- b In the **Edit BGP Configuration** dialog box, enter the following settings and click **OK**.

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Local AS	65000

Edit BGP Configuration

☒ Enable BGP

☒ Enable Graceful Restart

(Enables/Disables the ability to preserve forwarding state during restart of the BGP process)

Local AS * 65000

OK Cancel

- c Click the **Add** icon to add a Neighbor.

The **New Neighbor** dialog box appears.

- d In the **New Neighbor** dialog box, enter the following values for both NSX Edge devices, and click **OK**.

Repeat this step two times to configure the DLR for both NSX Edge devices: SFOCOMP-ESG01 and SFOCOMP-ESG02.

Setting	SFOCOMP-ESG01 Value	SFOCOMP-ESG02 Value
IP Address	192.168.101.1	192.168.101.2
Forwarding Address	192.168.101.3	192.168.101.3
Protocol Address	192.168.101.4	192.168.101.4
Remote AS	65000	65000
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	<i>bgp_password</i>	<i>bgp_password</i>

- e Click **Publish Changes**.

The screenshot shows the NSX Manager interface for SFOCOMP-DLR01. The 'Manage' tab is selected, and the 'Routing' sub-tab is active. On the left, the 'BGP' configuration is expanded. The main area shows the BGP Configuration with the following details:

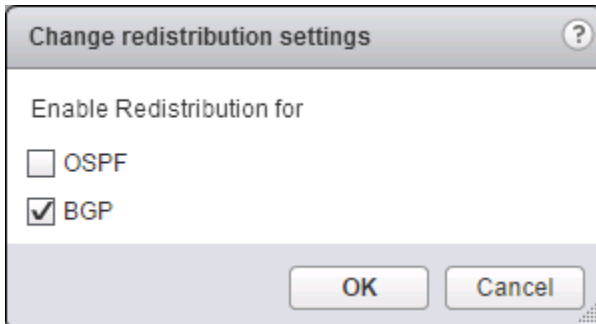
- Status: Enabled
- Local AS: 65000
- Graceful Restart: Enabled

Below the BGP Configuration, the 'Neighbors' section is displayed with a table of configured neighbors:

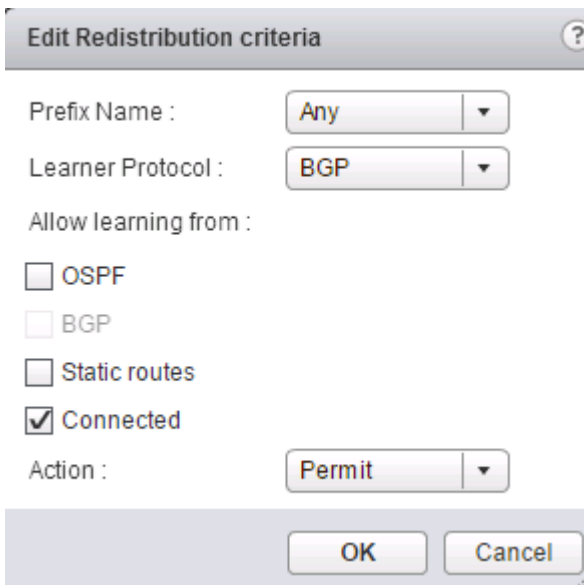
Forwarding Address	Protocol Address	IP Address	Remote AS	Weight	Keep Alive Ti...	Hold Down Time (...)
192.168.101.3	192.168.101.4	192.168.101.1	65000	60	1	3
192.168.101.3	192.168.101.4	192.168.101.2	65000	60	1	3

- 7 On the left, select **Route Redistribution** to configure it.
 - a Click the **Edit** button.
 - b In the **Change redistribution settings** dialog box, enter the following settings, and click **OK**.

Setting	Value
OSPF	Deselected
BGP	Selected



- c On the **Route Redistribution** page, select the default **OSPF** entry and click the **Edit** button.
 - d Select **BGP** from the **Learner Protocol** drop-down menu, and click **OK**.



- e Click **Publish Changes**.

Connect the NSX Edge Devices in the Shared Edge and Compute Cluster to the Distributed Logical Router in Region A

After you deploy a distributed logical router for the shared edge and compute cluster in Region A according to this design, you configure an interface and update BGP on the SFOCOMP-ESG01 and SFOCOMP-ESG02 NSX Edge devices for connection to the router.

Perform this procedure two times to configure the two NSX Edge devices in Region B: SFOCOMP-ESG01 and SFOCOMP-ESG02.

Table 4-7. NSX Edge Devices and DLR Interface Settings for Region B

Parameter	Value for Region B
NSX Edge Device 1	SFOCOMP-ESG01
NSX Edge Device 2	SFOCOMP-ESG02
DLR Interface	SFOCOMP-DLR01
Primary DLR IP Address for NSX Edge Device 1	192.168.101.1
Primary DLR IP Address for NSX Edge Device 2	192.168.101.2

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://comp01vc01.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 Client **Home** menu, select **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.
- 5 Double-click the **SFOCOMP-ESG01** NSX Edge device to open its settings.
- 6 On the **Manage** tab, click the **Settings** tab.

7 Configure an interface to distributed router.

- a On the **Settings** tab for the NSX Edge, click **Interfaces**.
- b Select the **vnic3** interface and click **Edit**.
- c In the **Edit NSX Edge Interface** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	SFOCOMP-DLR01
Type	Internal
Connected To	Global Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.101.1
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

8 Add the distributed logical router to the BGP configuration of the SFOCOMP-ESG01 device.

- a On the **Routing** tab, click **BGP** to add the distributed router as a neighbor to the NSX Edge.
- b Click the **Add** icon to add another neighbor.
The **New Neighbor** dialog box appears.
- c Configure the distributed logical router (DLR) as a neighbor.

- d In the **New Neighbor** dialog box, enter the following values, and click **OK**.

Setting	Value
IP Address	192.168.101.4
Remote AS	65000
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	<i>BGP_password</i>

New Neighbour

IP Address : * 192.168.101.4

Remote AS : * 65000

Weight : 60

Keep Alive Time : 1 (Seconds)

Hold Down Time : 3 (Seconds)

(BGP Keep alive timer value needs to be one third of hold down timer)

Password : *****

BGP Filters :

Direction	Action	Network	IP Prefix GE	IP Prefix LE

0 items Copy

OK Cancel

- e Click **Publish Changes**.
- 9 Repeat [Step 5](#) to [Step 8](#) on the other NSX Edge device to configure the interface to the distributed logical router and add the router as a BGP neighbor.

Configure a Logical Switch and Deploy the Distributed Logical Router for the Shared Edge and Compute Cluster in Region B

Configure a logical switch and deploy the distributed logical router (DLR).

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 vSphere Web Client **Home** menu, select **Networking & Security**.
- 3 In the Navigator, click **Logical Switches**.
- 4 Select **172.17.11.66** from the **NSX Manager** drop-down menu and click the **Add** icon.
- 5 In the **New Logical Switch** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	Global Transit Network
Transport Zone	Comp Global Transport Zone
Replication Mode	Hybrid

- 6 In the **Navigator**, click **NSX Edges**.
- 7 Select **172.17.11.66** from the **NSX Manager** drop-down menu.
- 8 Click the **Add** icon to create a new DLR.
- 9 On the **Name and description** page, enter the following settings and click **Next**.

Setting	Value
Logical (Distributed) Router	Selected
Name	LAXCOMP-DLR01
Deploy Edge Appliance	Selected
Enable High Availability	Selected

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

Setting	Value
User Name	admin
Password	dlr_admin_password
Enable SSH access	Selected
Enable FIPS mode	Deselected
Edge Control Level logging	INFO

- 11 On the **Configure deployment** page, click the **Add** icon.

The **Add NSX Edge Appliance** dialog box appears.

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

Setting	Value
Cluster/Resource Pool	SDDC-EdgeRP51
Datastore	<i>lax01_shared_edge_and_compute_datastore</i>

- 13 On the **Configure deployment** page, click the **Add** icon a second time to add a second NSX Edge device.

The **Add NSX Edge Appliance** dialog box appears.

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

Setting	Value
Cluster/Resource Pool	SDDC-EdgeRP51
Datastore	<i>lax01_shared_edge_and_compute_datastore</i>

- 15 Click **Next**.

- 16 On the **Configure interfaces** page, under **HA Interface Configuration**, click **Select** and connect to **vDS-Comp01-Management**.

- 17 On the **Configure interfaces** page enter the following configuration settings and click **Next**.

- a Click the **Add** icon.

Setting	Value
Primary IP Address	1.4.1.1
Subnet Prefix Length	24

- b Enter the following settings in the **Add Interface** dialog box, and click **OK**.

Setting	Value
Name	Uplink
Type	Uplink
Connected To	Global Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.102.3
Subnet Prefix Length	24
MTU	9000

- 18 On the **Default gateway settings** page, deselect **Configure Default Gateway** and click **Next**.

- 19 On the **Ready to complete** page, click **Finish**.

Configure Distributed Logical Router for Dynamic Routing in Shared Edge and Compute Cluster in Region B

Configure the distributed logical router (DLR) in the shared edge and compute cluster to use dynamic routing.

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 Under **Inventories**, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.
- 5 Configure the routing for the Distributed Logical Router.
 - a Double-click **LAXCOMP-DLR01**.
 - b Click the **Manage** tab and click **Routing**.
 - c On the **Global Configuration** page, perform the following configuration steps.
 - d Click the **Enable** button for **ECMP**.
 - e Click the **Edit** button under **Dynamic Routing Configuration**, select **Uplink** as the Router ID, and click **OK**.
 - f Click **Publish Changes**.
- 6 On the left, select **BGP** to configure it.
 - a On the **BGP** page, click the **Edit** button.
The **Edit BGP Configuration** dialog box appears.
 - b In the **Edit BGP Configuration** dialog box, enter the following settings and click **OK**.

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Local AS	65000

- c Click the **Add** icon to add a Neighbor.
The **New Neighbor** dialog box appears.

- d In the **New Neighbor** dialog box, enter the following values for both NSX Edge devices, and click **OK**.

You repeat this step two times to configure the DLR for both NSX Edge devices: LAXCOMP-ESG01 and LAXCOMP-ESG02.

Setting	LAXCOMP-ESG01 Value	LAXCOMP-ESG02 Value
IP Address	192.168.102.1	192.168.102.2
Forwarding Address	192.168.102.3	192.168.102.3
Protocol Address	192.168.102.4	192.168.102.4
Remote AS	65000	65000
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	<i>bgp_password</i>	<i>bgp_password</i>

- e Click **Publish Changes**.

- 7 On the left, select **Route Redistribution** to configure it.

- a Click the **Edit** button.
- b In the **Change redistribution settings** dialog box, enter the following settings, and click **OK**.

Setting	Value
OSPF	Deselected
BGP	Selected

- c On the **Route Redistribution** page, select the default **OSPF** entry and click the **Edit** button.
- d Select **BGP** from the **Learner Protocol** drop-down menu, and click **OK**.
- e Click **Publish Changes**.

Connect the NSX Edge Devices in the Shared Edge and Compute Cluster to the Distributed Logical Router in Region B

After you deploy a distributed logical router for the shared edge and compute cluster in Region B according to this design, you configure an interface and update BGP on the LAXCOMP-ESG01 and LAXCOMP-ESG02 NSX Edge devices for connection to the router.

Perform this procedure two times to configure the two NSX Edge devices in Region B: LAXCOMP-ESG01 and LAXCOMP-ESG02.

Table 4-8. NSX Edge Devices and DLR Interface Settings for Region B

Parameter	Value for Region B
NSX Edge Device 1	LAXCOMP-ESG01
NSX Edge Device 2	LAXCOMP-ESG02
DLR Interface	LAXCOMP-DLR01

Table 4-8. NSX Edge Devices and DLR Interface Settings for Region B (Continued)

Parameter	Value for Region B
Primary DLR IP Address for NSX Edge Device 1	192.168.102.1
Primary DLR IP Address for NSX Edge Device 2	192.168.102.2

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, select **Networking & Security**.
- 3 In the **Navigators**, click **NSX Edges**.
- 4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.
- 5 Double-click the **LAXCOMP-ESG01** NSX Edge device to open its settings.
- 6 On the **Manage** tab, click the **Settings** tab.
- 7 Configure an interface to distributed router.
 - a On the **Settings** tab for the NSX Edge, click **Interfaces**.
 - b Select the **vnic3** interface and click **Edit**.
 - c In the **Edit NSX Edge Interface** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	LAXCOMP-DLR01
Type	Internal
Connected To	Global Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.102.1
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- 8 Add the distributed logical router to the BGP configuration of the LAXCOMP-ESG01 device.
 - a On the **Routing** tab, click **BGP** to add the distributed router as a neighbor to the NSX Edge.
 - b Click the **Add** icon to add another neighbor.
The **New Neighbor** dialog box appears.
 - c Configure the distributed logical router (DLR) as a neighbor.
 - d In the **New Neighbor** dialog box, enter the following values, and click **OK**.

Setting	Value
IP Address	192.168.102.4
Remote AS	65000
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	<i>BGP_password</i>

- e Click **Publish Changes**.
- 9 Repeat [Step 5](#) to [Step 8](#) on the other NSX Edge device to configure the interface to the distributed logical router and add the router as a BGP neighbor.

Upgrade the Components for the Management Cluster

When you upgrade the virtual infrastructure layer of the SDDC, you upgrade the components that support the management cluster first.

Procedure

1 [Upgrade vSphere and Disaster Recovery Components for the Management Clusters](#)

When you update the vSphere layer for the management instances in the SDDC, you upgrade the Management Platform Services Controller, Management vCenter Server, vSphere Replication Appliance and Site Recovery Manager system in Region A, and then repeat this operation in Region B.

2 [Post-Upgrade Configuration of the vSphere Components for the Management Cluster](#)

After you upgrade the vCenter Server and Platform Services Controller instances for the management cluster, configure the environment according to the objectives and deployment guidelines of this validated design.

3 [Complete vSphere Upgrade for the Management Cluster](#)

After you upgrade the vCenter Server and Platform Services Controller, and vSphere Data Protection and Site Recovery Manager, upgrade the ESXi hosts and Virtual SAN storage.

4 Post-Upgrade Configuration of the Management ESXi Hosts and vSAN Storage

After you complete the upgrade of the vSphere management components, perform a final update of the configuration of vCenter Server and ESXi according to the objectives and deployment guidelines of this validated design.

Upgrade vSphere and Disaster Recovery Components for the Management Clusters

When you update the vSphere layer for the management instances in the SDDC, you upgrade the Management Platform Services Controller, Management vCenter Server, vSphere Replication Appliance and Site Recovery Manager system in Region A, and then repeat this operation in Region B.

Upgrading the VMware Validated Design vSphere and disaster recovery layers for the management clusters is a multi-step operation in which you must upgrade the Management Platform Services Controller, Management vCenter Server, vSphere Replication Appliance and Site Recovery Manager system in Region A before you repeat this operation in Region B, accordingly. This sequence ensures least impact on your ability to perform disaster recovery operations in the SDDC.

Table 4-9. Management vSphere and Disaster Recovery Nodes In the SDDC

Region	Role	IP Address	Fully Qualified Domain Name
Region A	Management Platform Services Controller	172.16.11.61	mgmt01psc01.sfo01.rainpole.local
	Management vCenter	172.16.11.62	mgmt01vc01.sfo01.rainpole.local
	vSphere Replication	172.16.11.123	mgmt01vrms01.sfo01.rainpole.local
	Site Recovery Manager	172.16.11.124	mgmt01srm01.sfo01.rainpole.local
Region B	Management Platform Services Controller	172.17.11.61	mgmt01psc51.lax01.rainpole.local
	Management vCenter	172.17.11.62	mgmt01vc51.lax01.rainpole.local
	vSphere Replication	172.17.11.123	mgmt01vrms51.lax01.rainpole.local
	Site Recovery Manager	172.17.11.124	mgmt01srm51.lax01.rainpole.local

Prerequisites

- For Management vCenter Server and Platform Services Controller instances
 - Download the vCenter Server Appliance .iso file.
 - Verify that vSphere DRS is set to Partially Automated for the duration of the upgrade operations.
 - Verify that the static IP addresses 172.16.11.70 and 172.17.11.70 are available for use in the temporary network settings of the appliances.
 - Verify that all management ESXi hosts have the lockdown mode disabled for the duration of the upgrade.

- Ensure any integration with the Management vCenter Server instances within environment has been quiesced of all activities, including but not limited to, users performing active backups of components or provisioning of new virtual machines within vRealize Automation. Without quiescing the environment, rollback operations may be disrupted by generated orphaned objects. You might have to extend the time of the maintenance windows too.
- Create a snapshot of all Platform Services Controller appliances that you want to upgrade as a precaution in case of failure during the upgrade process.
- Create a snapshot of the Management vCenter Server appliances that you want to upgrade as a precaution in case of failure during the upgrade process.
- Create a backup copy of all Platform Services Controllers and Management vCenter Servers.
- For complete information about the prerequisites to upgrading vSphere, see [Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance](#) in the *vSphere 6.5 Upgrade* documentation.
- For vSphere Replication
 - Download the vSphere Replication Upgrade .iso file to a shared datastore for mounting to the virtual appliances. If you have space on your NFS datastore, upload the file there.
 - Create a snapshot of the each vSphere Replication Appliance that has been configured as a pair.
 - Create a backup of the each vSphere Replication Appliance that has been configured as a pair.
 - Verify that the Management Platform Services Controllers and Management vCenter Servers are successfully upgraded.
 - Verify that all services on the Management Platform Services Controllers and Management vCenter Servers are running.
- For Site Recovery Manager
 - Download the Site Recovery Manager Upgrade .msi file.
 - Create a snapshot of the each Site Recovery Manager system that has been configured as a pair.
 - Create a backup of the each Site Recovery Manager system that has been configured as a pair.
 - Verify that the Management Platform Services Controller and Management vCenter Server instances are successfully upgraded.
 - Verify that all services on the Management Platform Services Controllers and Management vCenter Servers are running.
 - For information about the prerequisites to upgrading Site Recovery Manager, see [Prerequisites and Best Practices for Site Recovery Manager Upgrade](#) in the *Upgrading Site Recovery Manager* documentation.

Procedure

- 1 [Upgrade Management Platform Services Controller in Region A](#)
- 2 [Upgrade Management vCenter Server in Region A](#)

3 Upgrade Management vSphere Replication Appliance in Region A

After you upgrade the Management Platform Services Controller and vCenter Server, upgrade to vSphere Replication appliance in Region A.

4 Upgrade Management Site Recovery Manager in Region A

After you upgrade the vSphere Replication appliance in Region A, proceed to Site Recovery Manager in Region A.

5 Upgrade Management Platform Services Controller in Region B

6 Upgrade Management vCenter Server in Region B

7 Upgrade Management vSphere Replication Appliance in Region B

To continue your upgrade of the vSphere and disaster recovery instances in the SDDC, after you upgrade the Management Platform Services Controller and vCenter Server, proceed to the vSphere Replication appliance in Region B.

8 Upgrade Management Site Recovery Manager in Region B

To continue your update of the Foundation Layer for Management instances in the SDDC, after you upgrade the vSphere Replication appliance, proceed to the Site Recovery Manager system in Region B.

What to do next

- Verify that the vSphere and Disaster Recovery components function flawlessly after the upgrade. See the *VMware Validated Design Operational Verification* documentation.

Upgrade Management Platform Services Controller in Region A

When you upgrade the vSphere components in Region A and Region B, upgrade the Platform Services Controller instance first 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://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 Rename the virtual machine name of the mgmt01psc01.sfo01.rainpole.local appliance.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the mgmt01vc01.sfo01.rainpole.local control tree.
 - c Locate **mgmt01psc01.sfo01**

- d Right-click on the virtual machine and select **Rename**.
- e Update the name from **mgmt01psc01.sfo01** to **mgmt01psc01.sfo01_old** and click **OK**.
- 3 On the Windows host that has access to the data center, mount the vCenter Server Appliance installer .iso file, navigate to the `vcsa-ui-installer\win32` directory, and run the **installer.exe** executable file.
- 4 On the **Home** page, click **Upgrade**.
- 5 Review the **Introduction** page to understand the upgrade process and click **Next**.
- 6 Read and accept the license agreement on the **End user license agreement** page, and click **Next**.
- 7 On the **Connect to source appliance** page, connect to the Management Platform Services Controller appliance and click **Next**.
 - a In the **Source appliance** section, enter the following information about the Platform Services Controller appliance.

Setting	Value
Appliance FQDN or IP address	mgmt01psc01.sfo01.rainpole.local
Appliance HTTPS port	443
SSO user name	administrator@vsphere.local
SSO password	<i>vsphere_admin_password</i>
Appliance (OS) root password	<i>mgmtpsc_root_password</i>

- b In the **ESXi host or vCenter Server that manages the source appliance** section, enter the following settings about the Management vCenter Server instance on which the Platform Services Controller appliance resides.

Setting	Value
ESXi host or vCenter Server name	mgmt01vc01.sfo01.rainpole.local
HTTPS port	443
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 8 In the **Certificate Warning** dialog box that appears, verify that the thumbprints match those used on mgmt01psc01.sfo01.rainpole.local and mgmt01vc01.sfo01.rainpole.local, and click **Yes**.
- 9 On the **Appliance deployment target** page, enter the settings the Management vCenter Server for the deployment and click **Next**.

Setting	Value
ESXi host or vCenter Server name	mgmt01vc01.sfo01.rainpole.local
HTTPS port	443

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_passwrod

- 10 On the **Certificate Warning** dialog box that appears, verify that the thumbprint matches the one that is used on mgmt01vc01.sfo01.rainpole.local, and click **Yes**.
- 11 On the **Select folder** page, navigate to **mgmt01vc01.sfo01.rainpole.local > SFO01 > Discovered virtual machines**, and click **Next**.
- 12 On the **Select compute resource** page, select **SFO01 > SFO01-Mgmt01** and click **Next**.
- 13 On the **Set up target appliance VM** page, enter the information about Management Platform Services Controller and click **Next**.

Setting	Value
VM name	mgmt01psc01
Root password	mgmtpsc_root_password
Confirm root password	mgmtpsc_root_password

- 14 On the **Select datastore** page, locate and select **SFO01A-VSAN01-MGMT01**, and click **Next**.
- 15 On the **Configure network settings** page, enter the temporary networking information to be used by the new Platform Services Controller appliance to perform the upgrade then click **Next**.
 - a From the **Network** drop-down menu, select **vDS-Mgmt-Management**.
 - b In the **Temporary network settings** section, enter the temporary network configurations for the appliance.

Setting	Value
IP version	IPv4
IP assignment	static
Temporary IP address	172.16.11.70
Subnet mask or prefix length	24
Default gateway	172.16.11.1
DNS servers	172.16.11.5,172.16.11.4

- 16 On the **Ready to complete stage 1** page, verify that all of the settings are correct and click **Finish**.
- 17 Allow for the new Management Platform Services Controller to be deployed.
- 18 After a successful deployment of the appliance, click **Continue**.
- 19 On the **Introduction** page, click **Next** and allow for the **Pre-upgrade checks** to automatically be performed.

- 20 On the **Configure CEIP** page, select **Join the VMware's Customer Experience Improvement Program (CEIP)** and click **Next**.
- 21 On the **Ready to complete** page, select **I have backed up the source Platform Services Controller and all the required data from the database** and click **Finish**.
- 22 On the **Shutdown Warning** page, click **OK**.

The vCenter Server Appliance is upgraded. The old vCenter Server Appliance is powered off and the new appliance starts.

Upgrade Management vCenter Server in Region A

When you upgrade the vSphere components in Region A and Region B, after you complete the upgrade to the Platform Services Controller instance first in Region A, you move onto the Management vCenter Server 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://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 Rename the virtual machine name of the mgmt01vc01.sfo01.rainpole.local appliance.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the mgmt01vc01.sfo01.rainpole.local control tree.
 - c Locate **mgmt01vc01.sfo01**.
 - d Right-click the virtual machine and select **Rename**, change the name from mgmt01vc01.sfo01 to **mgmt01vc01.sfo01_old**, and click **OK**.
- 3 Locate the management ESXi host that runs the Management vCenter Server instance.

You use this information to specify the location of the newly-deployed vCenter Server.

 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the mgmt01vc01.sfo01.rainpole.local control tree and click **mgmt01vc01.sfo01_old**.
 - c On the **Summary** tab of the virtual machine, review the **Host** field which contains the ESXi host the vCenter Server virtual machine runs on.
- 4 On the Windows host that has access to the data center, mount the vCenter Server Appliance installer .iso file, navigate to the `vcsa-ui-installer\win32` directory, and run the `installer.exe` executable file.

- 5 On the **Home** page, click **Upgrade**.
- 6 Review the **Introduction** page to understand the upgrade process and click **Next**.
- 7 Read and accept the license agreement on the **End user license agreement** page, and click **Next**.
- 8 On the **Connect to source appliance** page, provide the details for the management vCenter Server appliance and click **Next**.
 - a In the **Source appliance** section, enter the following information about the Management vCenter Server appliance.

Setting	Value
Appliance FQDN or IP address	mgmt01vc01.sfo01.rainpole.local
Appliance HTTPS port	443
SSO user name	administrator@vsphere.local
SSO password	vsphere_admin_password
Appliance (OS) root password	mgmtpsc_root_password

- b In the **ESXi host or vCenter Server that manages the source appliance** section, enter the information about management ESXi host instance on which the vCenter Server appliance resides from [Step 3](#).

Setting	Value
ESXi host or vCenter Server name	mgmt01esx0x.sfo01.rainpole.local
HTTPS port	443
User name	root
Password	esxi_root_password

- 9 On the **Certificate Warning** dialog box that appears, verify that the thumbprints match those used on mgmt01vc01.sfo01.rainpole.local and management ESXi host, and click **Yes**.
- 10 On the **Appliance deployment target** page, enter the connection settings of the management ESXi host from [Step 3](#) and click **Next**.

Setting	Value
ESXi host or vCenter Server name	mgmt01esx01.sfo01.rainpole.local
HTTPS port	443
User name	root
Password	esxi_root_password

- 11 On the **Certificate Warning** dialog box that appears, verify that the thumbprint matches that one used on the management ESXi host, and click **Yes**.

- 12 On the **Set up target appliance VM** page, enter the information about the Management vCenter Server appliance and click **Next**.

Setting	Value
VM name	mgmt01vc01
Root password	<i>mgmtvc_root_password</i>
Confirm root password	<i>mgmtvc_root_password</i>

- 13 On the **Select Deployment Size** page, select **Small vCenter Server** from the **Deployment size** drop-down menu.
- 14 On the **Select datastore** page, locate and select **SFO01A-VSAN01-MGMT01**, and click **Next**.
- 15 On the **Configure network settings** page, enter the temporary networking information to be used by the new vCenter Server appliance to perform the upgrade then click **Next**.
- In the **Network** drop-down menu, select **vDS-Mgmt-Management**.
 - In the **Temporary network settings** section, enter the temporary network configurations for the appliance .

Setting	Value
IP version	IPv4
IP assignment	static
Temporary IP address	172.16.11.70
Subnet mask or prefix length	24
Default gateway	172.16.11.1
DNS servers	172.16.11.5,172.16.11.4

- 16 On the **Ready to complete stage 1** page, verify that all of the settings are correct and click **Finish**.
- 17 Allow for the new Management vCenter Server to be deployed.
- 18 After a successful deployment of the appliance, click **Continue**.
- 19 On the **Introduction** page, click **Next** and allow for the **Pre-upgrade checks** to be performed automatically.

The **Pre-upgrade check result** page will return an expected warning about vCenter External Extensions related to NSX for vSphere, vSphere Replication and Site Recovery Manager. You update vSphere Replication and Site Recovery Manager later in the SDDC upgrade sequence.

- 20 Click **Close** in the pre-upgrade check warning messages that appears.
- 21 On the **Select upgrade data** page, select **Configuration** and click **Next**.
- 22 On the **Ready to complete** page, select **I have backed up the source vCenter Server and all the required data from the database** and click **Finish**.
- 23 On the **Shutdown Warning** dialog box, click **OK** to initiate the upgrade.

- 24 On the **Complete** page, click **Close** button.
- 25 Exclude the new Management vCenter Server from all of your distributed firewall rules to ensure that network access between vCenter Server and NSX is not blocked.
- Open a Web browser and go to **`https://mgmt01vc01.sfo01.rainpole.local/vsphere-client`**.
 - Log in using the following credentials.
- | Setting | Value |
|-----------|-----------------------------|
| User name | administrator@vsphere.local |
| Password | vsphere_admin_password |
- In the **Navigator**, click **Networking & Security**.
 - Click **NSX Managers** and select the **172.16.11.65** instance.
 - On the **Manage** tab, click **Exclusion List** and click **Add**.
 - Add **mgmt01vc01** to the **Selected Objects** list, and click **OK**.
- 26 In the **Navigator**, locate the **mgmt01vc01_old** virtual machine and click the **Delete** button.

Upgrade Management vSphere Replication Appliance in Region A

After you upgrade the Management Platform Services Controller and vCenter Server, upgrade to vSphere Replication appliance in Region A.

Procedure

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

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Take a snapshot of the vSphere Replication appliance in Region A.
 - a In the **Navigator**, click **VMs and Templates** and navigate to the mgmt01vrms01 virtual machine.
 - b Right-click the **mgmt01vrms01** virtual machine and select **Snapshot > Take Snapshot**.
 - c In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	<i>Snapshot name</i>
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

- 3 Mount the upgrade .iso file to the virtual appliance.
- 4 Log in to the Virtual Appliance Management Interface of the vSphere Replication appliance
 - a Open a Web browser and go to **https://mgmt01vrms01.sfo01.rainpole.local:5480**
 - b Log in using the following credentials.

Settings	Value
User name	root
Password	<i>vr_sfo_root_password</i>

- 5 On the **Update** tab, click the **Settings** button.
- 6 Under the **Update Repository** section, select the **Use CDROM Updates** radio button and click **Save Settings**.
- 7 Click **Status** and click **Check Updates** to load the update from the .iso file.
- 8 Validate that **Available Updates** match the version defined by the VMware Validated Design Software Components and click **Install Updates**.
- 9 In the **Install Update** dialog box, click **OK**.
- 10 After the upgrade completes, click the **System** tab and click **Reboot**.
 During the upgrade process, after you have initiated the reboot of the appliance, the appliance will reboot two more times during the upgrade.
- 11 After the vSphere Replication appliance reboots, log in to the Virtual Appliance Management Interface and repeat the steps to register the vSphere Replication appliance with the Platform Services Controller.
 - a Open a Web browser and go **https://mgmt01vrms01.sfo01.rainpole.local:5480**
 - b Log in using the following credentials.

Settings	Value
User name	root
Password	<i>vr_sfo_root_password</i>

- c On the **VR** tab, click the **Configuration** button.
- d Under the **Startup Configuration** section, enter the password for vCenter Single Sign-On and click **Save and Restart Service**.

Setting	Value
Configuration Mode	Configure using the embedded database
LookupService Address	mgmt01psc01.sfo01.rainpole.local
SSO Administrative Account	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>
VRM Host	172.16.11.123
VRM Site Name	mgmt01vc01.sfo01.rainpole.local
vCenter Server Address	mgmt01vc01.sfo01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	<i>vcenter_server_admin_email</i>

- e After the restart is complete, ensure that the **Service Status** section on the **Configuration** tab reports that the VRM service is running.

12 In the vSphere Web Client, unmount the ISO image after the upgrade is complete.

13 Close all browser sessions to vCenter Server and clear the browser's cache.

Upgrade Management Site Recovery Manager in Region A

After you upgrade the vSphere Replication appliance in Region A, proceed to Site Recovery Manager 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 Take a snapshot of the Site Recovery Manager Windows machine.
 - a In the **Navigator**, click **VMs and Templates** and navigate to the mgmt01srm01 virtual machine.
 - b Right-click the **mgmt01srm01** virtual machine and select **Snapshot > Take Snapshot**.
 - c In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	<i>Snapshot name</i>
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

- 3 On the Windows host that has access to the data center, log in to the mgmt01srm01.sfo01.rainpole.local by using a Remote Desktop Protocol (RDP) client.
 - a Open an RDP connection to the virtual machine mgmt01srm01.sfo01.rainpole.local.
 - b Log in using the following credentials.

Setting	Value
User name	Windows administrative user
Password	<i>Windows_administrator_password</i>

- 4 Copy the upgrade .msi file to the Windows virtual machine of Site Recovery Manager.
- 5 Navigate to the folder where you downloaded the VMware Site Recovery Manager upgrade installer, and open the file to start the installation wizard.
- 6 On the **Welcome** page, click **Next**.
- 7 On the **VMware Patents** page, click **Next**.
- 8 On the **End User License Agreement** page, select **I agree to the terms in the license agreement**, and click **Next**.
- 9 On the **vSphere Platform Services Controller** page, verify that the Platform Services Controller settings are accurate , re-enter the following settings and click **Next**.

Setting	Value
Address	mgmt01psc01.sfo01.rainpole.local
HTTPS Port	443
Username	administrator@vsphere.local
Password	sso_password

- 10 On the **VMware vCenter Server** page, validate that the settings for vCenter Server mgmt01vc01.sfo01.rainpole.local is correct, and click **Next**.

- 11 On the **Site Recovery Manager Extension** page, verify that the following settings are intact and click **Next**.

Setting	Value
Administrator E-Mail	<i>srm_admin_sfo_email_address</i>
Local Host:	mgmt01srm01.sfo01.rainpole.local
Listener Port:	9086

- 12 If prompted, in the **VMware vCenter Site Recovery Manager** dialog box, click **Yes**.
- 13 On the **Certificate Type** page, select **Use existing certificate** and click **Next**.
- 14 On the **Embedded Database Configuration** page, re-enter the Site Recovery Manager srm_admin password for the database, validate the following settings and click **Next**.

Setting	Value
Data Source Name	SRM_SITE_SFO
Database User Name	srm_admin
Database Password	<i>srm_admin_sfo_password</i>
Database Port	5678
Connection Count	5
Max. Connections	20

- 15 On the **Ready to Install the Program** page, click **Install**.
- 16 After you upgrade the Site Recovery Manager, restart the vSphere Web Client to trigger the upgrade of the SRM plug-ins.
- Open an SSH connection to the mgmt01vc01.sfo01.rainpole.local vCenter Server Appliance that the SRM is connected to.
 - Log in using the following credentials.

Credential	Value
User name	root
Password	<i>mgmtvc_root_password</i>

- Run the following commands to restart the vSphere Web Client.

```
service-control --stop vsphere-client
service-control --start vsphere-client
```

Upgrade Management Platform Services Controller in Region B

After you complete the upgrade of the management virtual infrastructure layer and disaster recovery layer in Region A, you upgrade the Platform Services Controller for the management cluster 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	vsphere_admin_password

- 2 Rename the virtual machine name of the mgmt01psc51.lax01.rainpole.local appliance.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the mgmt01psc51.lax01.rainpole.local control tree.
 - c Locate **mgmt01psc51.lax01**
 - d Right-click on the virtual machine and select **Rename**.
 - e Update the name from **mgmt01psc51.lax01** to **mgmt01psc51.lax01_old** and click **OK**.
- 3 On the Windows host that has access to the data center, mount the vCenter Server Appliance installer .iso file, navigate to the vcsa-ui-installer\win32 directory, and run the **installer.exe** executable file.
- 4 On the **Home** page, click **Upgrade**.
- 5 Review the **Introduction** page to understand the upgrade process and click **Next**.
- 6 Read and accept the license agreement on the **End user license agreement** page, and click **Next**.

- 7 On the **Connect to source appliance** page, connect to the `mgmt01psc51.lax01.rainpole.local` appliance to begin the upgrade and click **Next**.

- a In the **Source appliance** section, enter the following information about the source `mgmt01psc51.lax01.rainpole.local` appliance.

Setting	Value
Appliance FQDN or IP address	<code>mgmt01psc51.lax01.rainpole.local</code>
Appliance HTTPS port	443
SSO user name	<code>administrator@vsphere.local</code>
SSO password	<code>vsphere_admin_password</code>
Appliance (OS) root password	<code>mgmtpsc_root_password</code>

- b In the **ESXi host or vCenter Server that manages the source appliance** section, enter the information about Management vCenter Server instance on which the Platform Services Controller appliance runs.

Setting	Value
ESXi host or vCenter Server name	<code>mgmt01vc51.lax01.rainpole.local</code>
HTTPS port	443
User name	<code>administrator@vsphere.local</code>
Password	<code>vsphere_admin_password</code>

- 8 On the **Certificate Warning** dialog box that appears, verify that the thumbprints match those used on `mgmt01psc51.lax01.rainpole.local` and `mgmt01vc51.lax01.rainpole.local`, and click **Yes**.

- 9 On the **Appliance deployment target** page, enter the connection settings of the Management vCenter Server and click **Next**.

- a In the **Appliance deployment target** section, enter the connection settings of the Management vCenter Server instance on which the Platform Services Controller appliance resides.

Setting	Value
ESXi host or vCenter Server name	<code>mgmt01vc51.lax01.rainpole.local</code>
HTTPS port	443
User name	<code>administrator@vsphere.local</code>
Password	<code>vsphere_admin_password</code>

- 10 In the **Certificate Warning** dialog box that appears, verify that the thumbprint matches the one used on `mgmt01vc51.lax01.rainpole.local`, and click **Yes**.

- 11 On the **Select folder** page, navigate to the `mgmt01vc51.lax01.rainpole.local > LAX01 > Discovered virtual machines` and click **Next**.

- 12 On the **Select compute resource** page, select `LSX01 > LAX01-Mgmt01` and click **Next**.

- 13 On the **Set up target appliance VM** page, enter the information about Management Platform Services Controller and click **Next**.

Setting	Value
VM name	mgmt01psc51
Root password	<i>mgmtpsc_root_password</i>
Confirm root password	<i>mgmtpsc_root_password</i>

- 14 On the **Select datastore** page, locate and select **LAX01A-VSAN01-MGMT01**, and click **Next**.
- 15 On the **Configure network settings** page, enter the temporary networking information to be used by the new Platform Services Controller appliance to perform the upgrade and click **Next**.
- From the **Network** drop-down menu, select **vDS-Mgmt-Management**.
 - In the **Temporary network settings** section, enter the temporary network configurations for the appliance

Setting	Value
IP version	IPv4
IP assignment	static
Temporary IP address	172.17.11.70
Subnet mask or prefix length	24
Default gateway	172.17.11.1
DNS servers	172.17.11.5,172.17.11.4

- 16 On the **Ready to complete stage 1** page, verify that all of the settings are correct and click **Finish**.
- 17 Allow for the new Management Platform Services Controller to be deployed.
- 18 After the deployment of the appliance, click **Continue**.
- 19 On the **Introduction** page, click **Next** and allow for the **Pre-upgrade checks** to automatically be performed.
- 20 On the **Configure CEIP** page, select **Join the VMware's Customer Experience Improvement Program (CEIP)** and click **Next**.
- 21 On the **Ready to complete** page, select **I have backed up the source Platform Services Controller and all the required data from the database** and click **Finish**.
- 22 On the **Shutdown Warning** page, click **OK**.

The vCenter Server Appliance is upgraded. The old vCenter Server Appliance is powered off and the new appliance starts.

Upgrade Management vCenter Server in Region B

When you upgrade the vSphere components in Region B, after you upgrade the Platform Services Controller instance, you proceed with upgrading the Management vCenter Server 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	vsphere_admin_password

- 2 Rename the virtual machine name of the mgmt01vc51.lax01.rainpole.local appliance
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the mgmt01vc51.lax01.rainpole.local control tree.
 - c Locate **mgmt01vc51.lax01**.
 - d Right-click the virtual machine, select **Rename**, change the name from mgmt01vc51.lax01 to **mgmt01vc51.lax01_old** and click **OK**.
- 3 Locate the management ESXi host that the vCenter Server runs on.

You must provide the address of the host when you deploy the new appliance that runs vCenter Server 6.5.

 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the mgmt01vc51.lax01.rainpole.local control tree and locate **mgmt01vc51.lax01_old**.
 - c On the **Summary** tab of the virtual machine, review the Host field which contains the ESXi host that runs the vCenter Server virtual machine.
- 4 On the Windows host that has access to the data center, mount the vCenter Server Appliance installer .iso file, navigate to the vcsa-ui-installer\win32 directory, and run the **installer.exe** executable file.
- 5 On the **Home** page, click **Upgrade**.
- 6 Review the **Introduction** page to understand the upgrade process and click **Next**.
- 7 Read and accept the license agreement on the **End user license agreement** page, and click **Next**.

- 8 On the **Connect to source appliance** page, connect to the `mgmt01vc51.lax01.rainpole.local` appliance to begin the upgrade and click **Next**.

- a In the **Source appliance** section, enter the following information about the source `mgmt01vc51.lax01.rainpole.local` appliance

Setting	Value
Appliance FQDN or IP address	<code>mgmt01vc51.lax01.rainpole.local</code>
Appliance HTTPS port	443
SSO user name	<code>administrator@vsphere.local</code>
SSO password	<code>vsphere_admin_password</code>
Appliance (OS) root password	<code>mgmtvc_root_password</code>

- b In the **ESXi host or vCenter Server that manages the source appliance** section, enter the information about management ESXi host on which the vCenter Server appliance is running from [Step 3](#).

Setting	Value
ESXi host or vCenter Server name	<code>mgmt01esx51.lax01.rainpole.local</code>
HTTPS port	443
User name	<code>root</code>
Password	<code>esxi_root_password</code>

- 9 On the **Certificate Warning** dialog box that appears, verify that the thumbprints match those used on `mgmt01vc51.lax01.rainpole.local` and management ESXi host, and click **Yes**.
- 10 On the **Appliance deployment target** page, enter the connection settings of the management ESXi host for the deployment and click **Next**.

Setting	Value
ESXi host or vCenter Server name	<code>mgmt01esx51.lax01.rainpole.local</code>
HTTPS port	443
User name	<code>root</code>
Password	<code>esxi_root_password</code>

- 11 On the **Certificate Warning** dialog box that appears, verify that the thumbprint matches that used on the management ESXi host, and click **Yes**.

- 12 On the **Set up target appliance VM** page, enter the information about Management vCenter Server and click **Next**.

Setting	Value
VM name	mgmt01vc51
Root password	mgmtvc_root_password
Confirm root password	mgmtvc_root_password

- 13 If prompted, on the **Select deployment size** page, select **Small vCenter Server** from the **Deployment size** drop-down menu, and click **Next**.
- 14 On the **Select datastore** page, locate and select **LAX01A-VSAN01-MGMT01**, and click **Next**.
- 15 On the **Configure network settings** page, enter the temporary networking information to be used by the new vCenter Server appliance to perform the upgrade, and click **Next**.
- From the **Network** drop-down menu, select **vDS-Mgmt-Management**.
 - In the **Temporary network settings** section, enter the temporary network configurations for the appliance

Setting	Value
IP version	IPv4
IP assignment	static
Temporary IP address	172.17.11.70
Subnet mask or prefix length	24
Default gateway	172.17.11.1
DNS servers	172.17.11.5,172.17.11.4

- 16 On the **Ready to complete stage 1** page, verify that all of the settings are correct and click **Finish**.
- 17 Allow for the new Management vCenter Server to be deployed.
- 18 After a successful deployment of the appliance, click **Continue**.
- 19 On the **Introduction** page, click **Next** and allow for the **Pre-upgrade checks** to automatically be performed.

The **Pre-upgrade check result** page will return an expected warning about vCenter External Extensions related to NSX for vSphere, vSphere Replication and Site Recovery Manager. You update vSphere Replication and Site Recovery Manager later in the SDDC upgrade sequence.

- 20 Click **Close** in the pre-upgrade check warning messages that appears.
- 21 On the **Select upgrade data** page, select **Configuration** and click **Next**.
- 22 On the **Ready to complete** page, select **I have backed up the source vCenter Server and all the required data from the database** and click **Finish**.
- 23 On the **Shutdown Warning** dialog, click **OK** to initiate upgrade.

- 24 On the **Complete** page, click **Close** button.
- 25 Exclude the new Management vCenter Server appliance from all distributed firewall rules to ensure that network access between vCenter Server and NSX is not blocked.
- Open a Web browser and go to **`https://mgmt01vc51.lax01.rainpole.local/vsphere-client`**.
 - Log in using the following credentials.
- | Setting | Value |
|-----------|-----------------------------|
| User name | administrator@vsphere.local |
| Password | vsphere_admin_password |
- In the **Navigator**, click **Networking & Security**.
 - Click **NSX Managers** and select the **172.17.11.65** instance.
 - On the **Manage** tab, click **Exclusion List** and click **Add**.
 - Add **mgmt01vc51** to the **Selected Objects** list, and click **OK**.

Upgrade Management vSphere Replication Appliance in Region B

To continue your upgrade of the vSphere and disaster recovery instances in the SDDC, after you upgrade the Management Platform Services Controller and vCenter Server, proceed to the vSphere Replication appliance in Region B.

Procedure

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

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Take a snapshot of the vSphere Replication appliance in Region B.
 - a In the **Navigator**, click **VMs and Templates** and navigate to the mgmt01vrms51 virtual machine.
 - b Right-click the **mgmt01vrms51** virtual machine and select **Snapshot > Take Snapshot**.
 - c In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	<i>Snapshot name</i>
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

- 3 Mount the upgrade .iso file to the virtual appliance.
- 4 Log in to the Virtual Appliance Management Interface of the vSphere Replication appliance
 - a Open a Web browser and go **https://mgmt01vrms51.lax01.rainpole.local:5480**
 - b Log in using the following credentials.

Settings	Value
User name	root
Password	<i>vr_lax_root_password</i>

- 5 On the **Update** tab, click the **Settings** button.
- 6 Under the **Update Repository** section, select the **Use CDRom Updates** radio button and click **Save Settings**.
- 7 Click **Status** and click **Check Updates** to load the update from the .iso file.
- 8 Validate that **Available Updates** match the version defined by the VMware Validated Design Software Components and click **Install Updates**.
- 9 In the **Install Update** dialog box, click **OK**.
- 10 After the upgrade completes, click the **System** tab and click **Reboot**.

During the upgrade process, after you have initiated the reboot of the appliance, the appliance will reboot two more times during the upgrade.
- 11 After the vSphere Replication appliance reboots, log in to the Virtual Appliance Management Interface and repeat the steps to register the vSphere Replication appliance with the Platform Services Controller.
 - a Open a Web browser and go **https://mgmt01vrms51.lax01.rainpole.local:5480**
 - b Log in using the following credentials.

Settings	Value
User name	root
Password	<i>vr_lax_root_password</i>

- c On **VR** tab, click the **Configuration** button.
- d Under the **Startup Configuration** section, enter the password for vCenter Single Sign-On and click **Save and Restart Service**.

Setting	Value
Configuration Mode	Configure using the embedded database
LookupService Address	mgmt01psc51.lax01.rainpole.local
SSO Administrative Account	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>
VRM Host	172.17.11.123
VRM Site Name	mgmt01vc51.lax01.rainpole.local
vCenter Server Address	mgmt01vc51.lax01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	<i>vcserver_admin_email</i>

- e After the restart is complete, ensure that the **Service Status** section on the **Configuration** tab reports that VRM service is **running**.

12 In the vSphere Web Client, unmount the ISO image after the upgrade has successfully completed.

13 Close all browser sessions to vCenter Server and clear the browser's cache.

Upgrade Management Site Recovery Manager in Region B

To continue your update of the Foundation Layer for Management instances in the SDDC, after you upgrade the vSphere Replication appliance, proceed to the Site Recovery Manager system 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 Take a snapshot of the vSphere Replication appliance in Region A.
 - a In the **Navigator**, click **VMs and Templates** and navigate to the mgmt01srm51 virtual machine.
 - b Right-click the **mgmt01srm51** virtual machine and select **Snapshot > Take Snapshot**.
 - c In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	<i>Snapshot name</i>
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

- 3 On the Windows host that has access to the data center, log in to the mgmt01srm51.lax01.rainpole.local by using a Remote Desktop Protocol (RDP) client.
 - a Open an RDP connection to the virtual machine mgmt01srm51.lax01.rainpole.local.
 - b Log in using the following credentials.

Setting	Value
User name	Windows administrative user
Password	<i>Windows_administrator_password</i>

- 4 Copy the upgrade .msi file to the Windows virtual machine of Site Recovery Manager.
- 5 Navigate to the folder where you downloaded the VMware Site Recovery Manager upgrade installer, and open the file to start the installation wizard.
- 6 On the **Welcome** page, click **Next**.
- 7 On the **VMware Patents** page, click **Next**.
- 8 On the **End User License Agreement** page, select **I agree to the terms in the license agreement**, and click **Next**.
- 9 On the **Installation Prerequisites** page, click **Next**.
- 10 On the **vSphere Platform Services Controller** page, verify that the Platform Services Controller is accurate and re-enter the following settings and click **Next**.

Setting	Value
Address	mgmt01psc51.lax01.rainpole.local
HTTPS Port	443
Username	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 11 On the **VMware vCenter Server** page, validate that the settings for vCenter Server mgmt01vc51.lax01.rainpole.local are correct, and click **Next**.

- 12 On the **Site Recovery Manager Extension** page, verify that the following settings are still intact and click **Next**.

Setting	Value
Administrator E-Mail	<i>srm_admin_lax_email_address</i>
Local Host:	mgmt01srm51.lax01.rainpole.local
Listener Port:	9086

- 13 If prompted, in the **VMware vCenter Site Recovery Manager** dialog box, click **Yes**.
- 14 On the **Certificate Type** page, select **Use existing certificate** and click **Next**.
- 15 On the **Embedded Database Configuration** page, re-enter the srm_admin password for the database, validate the following settings and click **Next**.

Setting	Value
Data Source Name	SRM_SITE_LAX
Database User Name	srm_admin
Database Password	<i>srm_admin_lax_password</i>
Database Port	5678
Connection Count	5
Max. Connections	20

- 16 On the **Site Recovery Manager Service Account** page, leave the checkbox selected and click **Next**.
- 17 On the **Ready to Install the Program** page, click **Install**.
- 18 After you upgrade the Site Recovery Manager, restart the vSphere Web Client to trigger the upgrade of the Site Recovery Manager plug-ins.

- Open an SSH connection to the mgmt01vc51.lax01.rainpole.local vCenter Server Appliance that Site Recovery Manager is connected to.
- Log in using the following credentials.

Setting	Value
User name	root
Password	<i>mgmtvc_root_password</i>

- Run the following commands to restart the vSphere Web Client.

```
service-control --stop vsphere-client
service-control --start vsphere-client
```

Note If the Site Recovery Manager plug-in does not appear in the vSphere Web Client after restarting the service, clear the cache of your browser and log in again.

19 After you restart the vSphere Web Client, reconnect the Site Recovery Manager instances in Region A and Region B.

- 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

- c From the **Home** menu, select **Site Recovery**.
- d On the **Site Recovery** page, click **Sites**
- e On the **Sites** page, right-click **mgmt01vc01.sfo01.rainpole.local** and select **Reconfigure Pairing**.
- f In the **Reconfigure Site Recovery Manager Server Pairing** dialog box, on the **Select site** page, validate the following settings, and click **Next**.

Settings	Value
PSC address	mgmt01psc51.lax01.rainpole.local
Port	443

- g On the **Select vCenter Server** page, enter the password for the administrator@vsphere.local user, validate the following settings and click **Finish**.

Setting	Value
vCenter Servers with matching SRM Extension	mgmt01vc51.lax01.rainpole.local
Username	administrator@vsphere.local
Password	vsphere_admin_password

20 On the **Sites** page in the **Navigator**, click **mgmt01vc01.sfo01.rainpole.local** and verify that the **Client Connection** and **Server Connection** settings on the **Summary** tab appear as **Connected**, and **VR Compatibility** appears as **Compatible**.

Post-Upgrade Configuration of the vSphere Components for the Management Cluster

After you upgrade the vCenter Server and Platform Services Controller instances for the management cluster, configure the environment according to the objectives and deployment guidelines of this validated design.

Procedure

1 [Change Admission Control in the Management Cluster in Region A](#)

After you upgrade vSphere, change the admission control of the management cluster in Region A to use the number of hosts to tolerate setting according to this validated design.

2 [Register Again vRealize Operations Manager with the Management vCenter Server Instances](#)

After you upgrade Management vCenter Server instances, re-register vRealize Operations Manager with each of these instances to use health badges on the inventory objects in vSphere Web Client.

3 [Update Scheduled Backup Jobs for the Management vCenter Server Instance in Region A](#)

After upgrading the vCenter Server and Platform Services Controller to the latest version of vSphere, new virtual machines are deployed. You must update the scheduled backup job in Region A for full image backup of the Management vCenter Server and the connected external Platform Services Controller.

4 [Place Management vCenter Server and Platform Services Controller in a VM and Templates Folder in Region A](#)

Create a folder on the Management vCenter Server in Region A to group vCenter Server and Platform Services Controller instances together for easier management, and move the appliances there.

5 [vSphere Update Manager Download Service Implementation in Region A](#)

Install the vSphere Update Manager Download Service (UMDS) on a Linux virtual machine to download and store binaries and metadata in a shared repository in Region A.

6 [Reconnect vRealize Log Insight to vSphere by Using a Service Account](#)

This version of this validated design uses service accounts for controlled communication between the management components of the SDDC. Connect vRealize Log Insight to vSphere using such a service account to make your environment compliant with this validated design.

7 [Change Admission Control in the Management Cluster in Region B](#)

After you upgrade vSphere, change the admission control of the management cluster in Region B to use the number of hosts to tolerate setting according to this validated design.

8 [Update Scheduled Backup Jobs for the Management vCenter Server Instance in Region B](#)

After upgrading the vCenter Server and Platform Services Controller to the latest version of vSphere, new virtual machines are deployed. You must update the scheduled backup job in Region B for full image backup of the Management vCenter Server and the connected external Platform Services Controller.

9 [Place Management vCenter Server and Platform Services Controller in a VM and Templates Folder in Region B](#)

Create a folder on the Management vCenter Server in Region B to group vCenter Server and Platform Services Controller instances together for easier management, and move the appliances there.

10 vSphere Update Manager Download Service Implementation in Region B

Install the vSphere Update Manager Download Service (UMDS) on a Linux virtual machine to download and store binaries and metadata in a shared repository in Region B.

11 Configure the Management vCenter Server to Forward Log Events to vRealize Log Insight in Region B

You can configure the Management vCenter Server and connected Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster in Region B. You can then view and analyze all syslog information in the vRealize Log Insight web interface.

Change Admission Control in the Management Cluster in Region A

After you upgrade vSphere, change the admission control of the management cluster in Region A to use the number of hosts to tolerate setting according to this validated design.

vSphere 6.5 or later introduces an admission control policy that directly uses a number of host failures to tolerate to adjust the CPU and memory resources for virtual machine availability in the 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 In the Navigator, click **Host and Clusters**.

- a Expand the **mgmt01vc01.sfo01.rainpole.local** inventory.
 - b Select the **SFO01-Mgmt01** cluster under the **SFO01** data center.

- 3 Click the **Configure** tab and click **vSphere Availability**.

- 4 Click **Edit**.

- 5 In the **Edit Cluster Settings** dialog box, click **Admission Control** under **vSphere Availability**, enter the following settings and click **OK**.

Setting	Value
Host failures cluster tolerates	1
Define host failover capacity by	Cluster resource percentage
Override calculated failover capacity	Deselected
Performance degradation VMs tolerate	100%

Register Again vRealize Operations Manager with the Management vCenter Server Instances

After you upgrade Management vCenter Server instances, re-register vRealize Operations Manager with each of these instances to use health badges on the inventory objects in vSphere Web Client.

Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.
- 3 On the **Solutions** page, select **VMware vSphere** from the solution table, and click **Configure**.
- 4 Register again the vCenter Adapters for the Management vCenter Server instances.

- a In the **Manage Solution** dialog box, under **Instance Settings**, select the vCenter Adapter instance.

Region	vCenter Server	Display Name
Region A	mgmt01vc01.sfo01.rainpole.local	mgmt01vc01-sfo01
Region B	mgmt01vc51.lax01.rainpole.local	mgmt01vc51-lax01

- b Click **Manage Registrations**.
 - c Enter a user account with administrator privileges to re-register vRealize Operations Manager with the vCenter Server instance.

Setting	Value
Registration user	administrator@vsphere.local
Registration Password	vsphere_admin_password

- d Click **Register** and click **OK** in the informational dialog box that appears.
 - e Click **Save Settings** and click **OK** in the informational dialog box that appears.
 - f Repeat these steps to re-register vRealize Operations Manager with the Management vCenter Server in Region B.
- 5 In the **Manage Solution - VMware vSphere** dialog box, click **Close**.

Update Scheduled Backup Jobs for the Management vCenter Server Instance in Region A

After upgrading the vCenter Server and Platform Services Controller to the latest version of vSphere, new virtual machines are deployed. You must update the scheduled backup job in Region A for full image backup of the Management vCenter Server and the connected external Platform Services Controller.

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 On the vSphere Web Client **Home** page, click the **VDP** icon.
- 3 On the **Welcome to vSphere Data Protection** page, select **mgmt01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.
- 4 Click the **Backup** tab.
- 5 Locate and update the backup job **Management and Compute vCenter Server Backups** to include the new Management vCenter Server and Platform Services Controller in Region A.
 - a Click on the backup job **Management and Compute vCenter Server Backups**.
 - b From the **Backup job actions** menu, select **Edit** to run the **Edit backup job** wizard.
 - c On the **Data Type** page, select **Full Image**, leave the **Fall back to the non-quieted backup if quiescence fails** check box selected, and click **Next**.
 - d On the **Backup Sources** page, fully expand the **Virtual Machines** tree.

Object	Value
vCenter Server	mgmt01vc01.sfo01.rainpole.local
Data center	SFO01
Cluster	SFO01-Mgmt01

- e Locate the obsolete Management vCenter Server and Platform Services Controller virtual machines and deselect them.

Obsolete Object	VM Name
Management Platform Services Controller	mgmt01psc01.sfo01_old
Management vCenter Server	mgmt01vc01.sfo01_old

- f Select the new virtual appliances for Management vCenter Server and the Platform Services Controller.

Object	VM Name
Management Platform Services Controller	mgmt01psc01
Management vCenter Server	mgmt01vc01

- g Verify that the following the virtual appliances for vCenter Server and the Platform Services Controller in Region A have been selected, and click **Next**.

Object	VM Name
Management Platform Services Controller	mgmt01psc01
Management vCenter Server	mgmt01vc01
Compute Platform Services Controller	comp01psc01.sfo01
Compute vCenter Server	comp01vc01.sfo01

- h On the **Schedule** page, leave **Backup Schedule** to **Daily** and click **Next**.
- i On the **Retention Policy** page, leave **Keep** to **for 3 days** and click **Next**.
- j On the **Job Name** page, leave **Management and Compute vCenter Server Backups** as a name for the backup job and click **Next**.
- k On the **Ready to Complete** page, review the summary information for the backup job and click **Finish**.
- l In the dialog box that shows a confirmation that the job is created, click **OK**.

Place Management vCenter Server and Platform Services Controller in a VM and Templates Folder in Region A

Create a folder on the Management vCenter Server in Region A to group vCenter Server and Platform Services Controller instances together for easier management, and move the appliances there.

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 Create the MGMT01 folder.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **mgmt01vc01.sfo01.rainpole.local** tree.
 - c Right-click the **SFO01** data center, and select **New Folder > New VM and Template Folder**.
 - d In the **New Folder** dialog box enter **MGMT01** as the name to label the folder and click **OK**.
- 3 Move the vCenter Server and Platform Services Controller virtual machines to the MGMT01 folder.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **mgmt01vc01.sfo01.rainpole.local** tree.
 - c Expand the **Discovered virtual machines** folder.
 - d Drag **mgmt01vc01** and **mgmt01psc01** to the MGMT01 folder.

vSphere Update Manager Download Service Implementation in Region A

Install the vSphere Update Manager Download Service (UMDS) on a Linux virtual machine to download and store binaries and metadata in a shared repository in Region A.

Procedure

- 1 [Configure PostgreSQL Database on Your Linux-Based Host Operating System for UMDS in Region A](#)
On a virtual machine with Ubuntu 14.04 Long Term Support (LTS) where you plan to install Update Manager Download Service (UMDS), configure a PostgreSQL database instance.
- 2 [Install UMDS on Ubuntu OS in Region A](#)
After you install the PostgreSQL database on the UMDS virtual machine, install the UMDS software.
- 3 [Set Up the Data to Download with UMDS in Region A](#)
By default UMDS downloads patch binaries, patch metadata, and notifications for hosts. Specify which patch binaries and patch metadata to download with UMDS in Region A.
- 4 [Install and Configure the UMDS Web Server in Region A](#)
The UMDS server in Region A downloads upgrades, patch binaries, patch metadata, and notifications to a directory that you must share to vSphere Update Manager by using a Web server.
- 5 [Use the UMDS Shared Repository as the Download Source in Update Manager in Region A](#)
Configure Update Manager to use the UMDS shared repository as a source for downloading ESXi patches, extensions, and notifications.

Configure PostgreSQL Database on Your Linux-Based Host Operating System for UMDS in Region A

On a virtual machine with Ubuntu 14.04 Long Term Support (LTS) where you plan to install Update Manager Download Service (UMDS), configure a PostgreSQL database instance.

Prerequisites

- Create a virtual machine for UMDs on the management cluster of Region A. See *Virtual Machine Specifications* from the *Planning and Preparation* documentation.
- Verify you have PostgreSQL database user credentials.

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 In the vSphere Web Client, right-click the mgmt01umds01.sfo01.rainpole.local virtual machine and select **Open Console** to open the remote console to the virtual machine.
- 3 At the command prompt, log in as the **svc-umds** user using **`svc-umds_password`**.
- 4 Install VMtools and Secure Shell (SSH) server, and end the session.

```
sudo apt-get update
sudo apt-get -y install SSH
exit
```

- 5 Log back in to the UMDs virtual machine using SSH and the **svc-umds** service account credentials.
- 6 Install and start PostgreSQL and its dependencies:

```
sudo apt-get -y install vim perl tar sed psmisc unixodbc postgresql postgresql-contrib odbc-
postgresql
sudo service postgresql start
```

- 7 Log in as a PostgreSQL user, and create a database instance and a database user, by running the following commands.

When prompted, enter and confirm the **`umds_db_user_password`** password.

```
sudo su - postgres
createdb umds_db
createuser -d -e -r umds_db_user -P
```

8 Enable password authentication for the database user.

- a Navigate to the folder that contains the PostgreSQL configuration file `pg_hba.conf`.

Linux system	Default Location
Ubuntu 14.04	<code>/etc/postgresql/postgres_version/main</code>

```
cd /etc/postgresql/postgres_version/main
```

- b In the PostgreSQL configuration file, enable password authentication for the database user by inserting the following line right above `local all all peer`.

You can use the `vi` editor to make and save the changes.

#TYPE	DATABASE	USER	ADDRESS	METHOD
local	<code>umds_db</code>	<code>umds_db_user</code>		md5

- c Log out as a PostgreSQL user by running the following command.

```
logout
```

9 Configure the PostgreSQL driver and the data source name (DSN) for connection to the UMDS database.

- a Edit the ODBC configuration file.

```
sudo vi /etc/odbcinst.ini
```

- b Replace the file with the following content and save the change using `:wq`.

```
[PostgreSQL]
Description=PostgreSQL ODBC driver (Unicode version)
Driver=/usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so
Debug=0
CommLog=1
UsageCount=1
```

- c Edit the system file `/etc/odbc.ini`.

```
sudo vi /etc/odbc.ini
```

- d Replace the file with the following content and save the change using `:wq`,

```
[UMDS_DSN]
;DB_TYPE = PostgreSQL
;SERVER_NAME = localhost
;SERVER_PORT = 5432
;TNS_SERVICE = <database_name>
;USER_ID = <database_username>
Driver = PostgreSQL
DSN = UMDS_DSN
ServerName = localhost
PortNumber = 5432
Server = localhost
Port = 5432
UserID = umds_db_user
User = umds_db_user
Database = umds_db
```

- 10 Create a symbolic link between the UMDS and the PostgreSQL by running the following command.

```
ln -s /var/run/postgresql/.s.PGSQL.5432 /tmp/.s.PGSQL.543
```

- 11 Restart PostgreSQL.

```
sudo service postgresql restart
```

Install UMDS on Ubuntu OS in Region A

After you install the PostgreSQL database on the UMDS virtual machine, install the UMDS software.

Prerequisites

- Verify you have administrative privileges on the UMDS Ubuntu virtual machine.
- Mount the ISO file of the vCenter Server Appliance to the Linux machine.

Procedure

- 1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.
 - a Open an SSH connection to `mgmt01umds01.sfo01.rainpole.local`.
 - b Log in using the following credentials.

Setting	Value
User name	<code>svc-umds</code>
Password	<code>svc-umds_password</code>

- 2 Mount the vCenter Server Appliance ISO to the UMDS virtual machine.

```
sudo mkdir -p /mnt/cdrom
sudo mount /dev/cdrom /mnt/cdrom
```

- 3 Unarchive the VMware-UMDS-6.5.0.-*build_number*.tar.gz file:

```
tar -xzf /mnt/cdrom/ums/VMware-UMDS-6.5.0-build_number.tar.gz -C /tmp
```

- 4 Run the UMDS installation script.

```
sudo /tmp/vmware-ums-distrib/vmware-install.pl
```

- 5 Read and accept the EULA.
- 6 Press Enter to install UMDS in the default directory /usr/local/vmware-ums and enter **yes** to confirm directory creation.
- 7 Enter the UMDS proxy settings if needed according to the settings of your environment.
- 8 Press Enter to set the patch location to /var/lib/vmware-ums and enter **yes** to confirm directory creation.
- 9 Provide the database details.

Option	Description
Provide the database DSN	UMDS_DSN
Provide the database username	<i>ums_db_user</i>
Provide the database password	<i>ums_db_user_password</i>

- 10 Type **yes** and press Enter to install UMDS.

Set Up the Data to Download with UMDS in Region A

By default UMDS downloads patch binaries, patch metadata, and notifications for hosts. Specify which patch binaries and patch metadata to download with UMDS in Region A.

Procedure

- 1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.
 - a Open an SSH connection to mgmt01ums01.sfo01.rainpole.local.
 - b Log in using the following credentials.

Setting	Value
User name	svc-ums
Password	<i>svc-ums_password</i>

- 2 Navigate to the directory where UMDS is installed.

```
cd /usr/local/vmware-umds/bin
```

- 3 Disable the updates for older hosts and virtual appliances.

```
sudo ./vmware-umds -S -n
sudo ./vmware-umds -S -d embeddedEsx-5.5.0
sudo ./vmware-umds -S -d embeddedEsx-6.0.0
```

- 4 Configure automatic daily downloads by creating a cron job file.

```
cd /etc/cron.daily/
sudo touch umds-download
sudo chmod 755 umds-download
```

- 5 Edit the download command of the cron job.

```
sudo vi umds-download
```

- 6 Add the following lines to the file.

```
#!/bin/sh
/usr/local/vmware-umds/bin/vmware-umds -D
```

- 7 Test the UMDS Download cron job.

```
sudo ./umds-download
```

Install and Configure the UMDS Web Server in Region A

The UMDS server in Region A downloads upgrades, patch binaries, patch metadata, and notifications to a directory that you must share to vSphere Update Manager by using a Web server.

The default folder to which UMDS downloads patch binaries and patch metadata on a Linux machine is `/var/lib/vmware-umds`. You share this folder out to the VUM instances within the region using an Nginx Web server.

Procedure

- 1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.
 - a Open an SSH connection to `mgmt01umds01.sfo01.rainpole.local`.
 - b Log in using the following credentials.

Setting	Value
User name	<code>svc-umds</code>
Password	<code>svc-umds_password</code>

- 2 Install the Nginx Web server with the following command.

```
sudo apt-get -y install nginx
```

- 3 Change the patch repository directory permissions by running the command.

```
sudo chmod -R 755 /var/lib/vmware-umds
```

- 4 Copy the default site configuration for use with the UMDs configuration.

```
sudo cp /etc/nginx/sites-available/default /etc/nginx/sites-available/umds
```

- 5 Edit the new `/etc/nginx/sites-available/umds` site configuration file and replace the `server {}` block with the following text.

```
server {
    listen 80 default_server;
    listen [::]:80 default_server ipv6only=on;

    root /var/lib/vmware-umds;
    index index.html index.htm;

    # Make site accessible from http://localhost/
    server_name localhost mgmt01umds01 mgmt01umds01.sfo01.rainpole.local;

    location / {
        # First attempt to serve request as file, then
        # as directory, then fall back to displaying a 404.
        try_files $uri $uri/ =404;
        # Uncomment to enable naxsi on this location
        # include /etc/nginx/naxsi.rules
        autoindex on;
    }
}
```

- 6 Disable the existing default site.

```
sudo rm /etc/nginx/sites-enabled/default
```

- 7 Enable the new UMDs site.

```
sudo ln -s /etc/nginx/sites-available/umds /etc/nginx/sites-enabled/
```

- 8 Restart the Nginx Web service to apply the new configuration.

```
sudo service nginx restart
```

- 9 Ensure you can browse the files on the UMDs Web server by opening a Web browser to **`http://mgmt01umds01.sfo01.rainpole.local`**.

Use the UMDS Shared Repository as the Download Source in Update Manager in Region A

Configure Update Manager to use the UMDS shared repository as a source for downloading ESXi patches, extensions, and notifications.

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 On the **Home** page of the vSphere Web Client, click the **Update Manager** icon.
- 3 From the **Objects** tab, click the **mgmt01vc01.sfo01.rainpole.local** vCenter Server for Region A.
The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.
- 4 On the **Manage** tab, click **Settings** and select **Download Settings**.
- 5 On the **Download sources** page, click **Edit**.
An **Edit Download Sources** dialog box opens.
- 6 Enter the following setting and click **OK**.

Setting	Value
Use a shared repository	Selected
URL	http://mgmt01umds01.sfo01.rainpole.local

The vSphere Web Client performs validation of the URL.

- 7 In the **Download sources** page, click **Download Now** to run the download patch definitions.
- 8 If you are deploying the management components in Region A, repeat the procedure to configure the **http://mgmt01umds01.sfo01.rainpole.local** repository for the **comp01vc01.sfo01.rainpole.local** vCenter Server.

Skip this step during SDDC upgrade.

Reconnect vRealize Log Insight to vSphere by Using a Service Account

This version of this validated design uses service accounts for controlled communication between the management components of the SDDC. Connect vRealize Log Insight to vSphere using such a service account to make your environment compliant with this validated design.

Configure User Privileges in vSphere for Integration with vRealize Log Insight

Assign global permissions to the operations service account svc-loginsight to access monitoring data from the Management vCenter Server and Compute vCenter Server with vRealize Log Insight.

The svc-loginsight user account is specifically dedicated to collecting log information from vCenter Server and ESXi.

Prerequisites

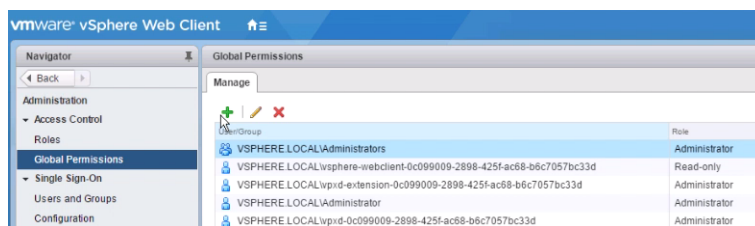
- Verify that the Management vCenter Server and Compute vCenter Server for Region A are connected to the Active Directory domain.
- Verify that the users and groups from the rainpole.local domain are available in the Management vCenter Server and in the Compute vCenter Server for Region A.

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.

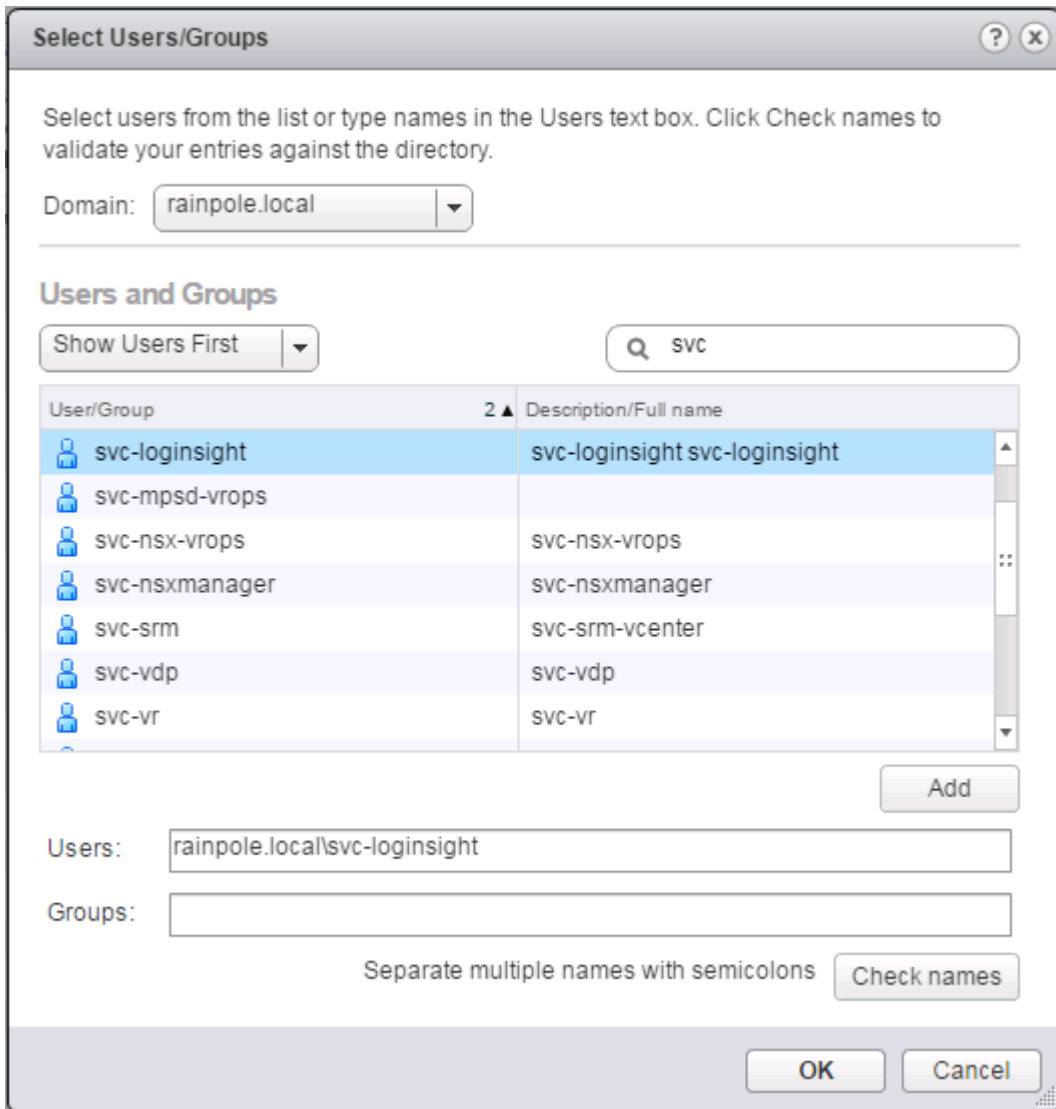
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Administration**.
- 3 Assign global permissions to the svc-loginsight@rainpole.local service account.
 - a In the vSphere Web Client, select **Administration** from the **Home** menu and click **Global Permissions** under **Access Control**.
 - b On the **Manage** tab, click **Add Permission**.



- c In the **Global Permissions Root - Add Permission** dialog box, click **Add** to associate a user or a group with a role.
- d In the **Select Users/Groups** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.

- e From the list of users and groups, select the **svc-loginsight** user, click **Add**, and click **OK**.



- f In the **Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **LogInsight**, select **Propagate to children**, and click **OK**.

The global permissions of the svc-loginsight@rainpole.local user propagate to all vCenter Server instances.

Configure the Management vCenter Server to Forward Log Events to vRealize Log Insight in Region A

You can configure the Management vCenter Server and connected Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster in Region A. You can then view and analyze all syslog information in the vRealize Log Insight Web interface.

In Region A, you configure the following vCenter Server and Platform Services Controller instances:

Region	Appliance Type	Appliance Management Interface URL	vRealize Log Insight Syslog Host
Region A	vCenter Server instances	https://mgmt01vc01.sfo01.rainpole.local:5480	vrli-cluster-01.sfo01.rainpole.local
	Platform Services Controller instances	https://mgmt01psc01.sfo01.rainpole.local:5480	vrli-cluster-01.sfo01.rainpole.local

Procedure

- 1 Redirect the log events from the appliance to vRealize Log Insight.

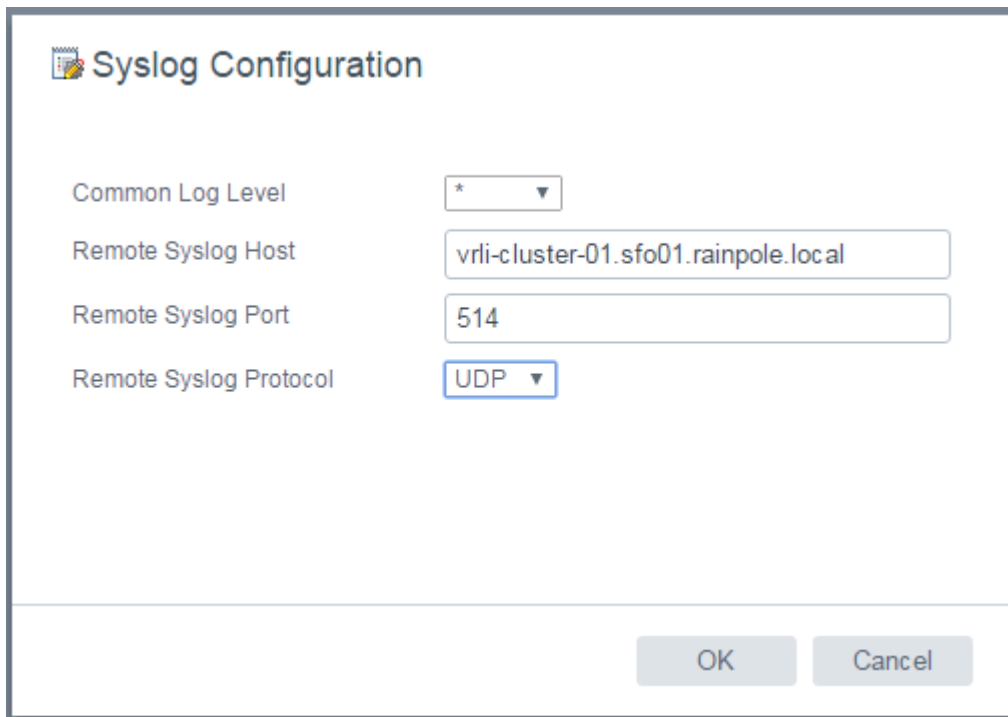
- a Open a Web browser and go to the following URL.
https://mgmt01vc01.sfo01.rainpole.local:5480.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>mgmtvc_root_password</i>

- c In the **Navigator**, click **Syslog Configuration**.

- d On the **Syslog Configuration** page, click **Edit**, configure the following settings, and click **OK**.

Setting	Value
Common Log Level	*
Remote Syslog Host	vrli-cluster-01.sfo01.rainpole.local
Remote Syslog Port	514
Remote Syslog Protocol	UDP



Syslog Configuration

Common Log Level: *

Remote Syslog Host: vrli-cluster-01.sfo01.rainpole.local

Remote Syslog Port: 514

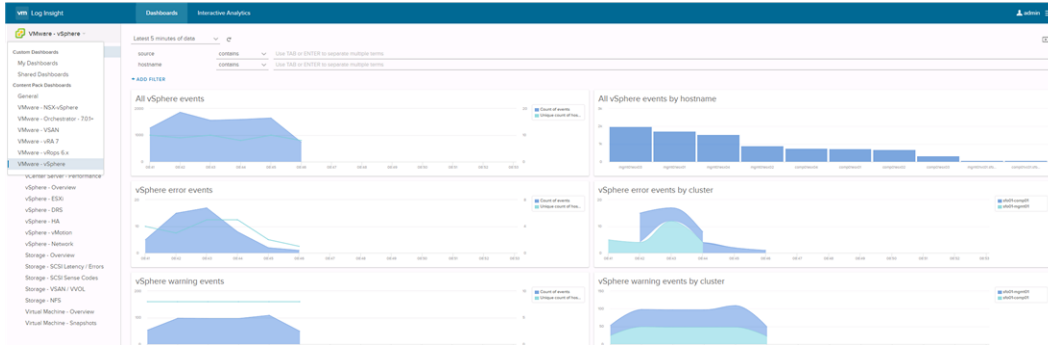
Remote Syslog Protocol: UDP

OK Cancel

- e Repeat the steps for the Platform Services Controller appliance.
- 2 Verify that the appliances are forwarding their syslog traffic to vRealize Log Insight.
- a Open a Web browser and go to **https://vrli-cluster-01.sfo01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- c In the vRealize Log Insight user interface, click **Dashboards** and select **VMware - vSphere** from the content pack dashboard drop-down menu.
- d Verify that the vCenter Server and Platform Services Controller nodes are presented on the **All vSphere events by hostname** widget of the **General Overview** dashboard.



Change Admission Control in the Management Cluster in Region B

After you upgrade vSphere, change the admission control of the management cluster in Region B to use the number of hosts to tolerate setting according to this validated design.

vSphere 6.5 or later introduces an admission control policy that directly uses a number of host failures to tolerate to adjust the CPU and memory resources for virtual machine availability in the 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://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 **Host and Clusters**.
 - a Expand the **mgmt01vc51.lax01.rainpole.local** inventory.
 - b Select the **LAX01-Mgmt01** cluster under the **LAX01** data center.
- 3 Click the **Configure** tab and click **vSphere Availability**.
- 4 Click **Edit**.

- 5 In the **Edit Cluster Settings** dialog box, click **Admission Control** under **vSphere Availability**, enter the following settings and click **OK**.

Setting	Value
Host failures cluster tolerates	1
Define host failover capacity by	Cluster resource percentage
Override calculated failover capacity	Deselected
Performance degradation VMs tolerate	100%

Update Scheduled Backup Jobs for the Management vCenter Server Instance in Region B

After upgrading the vCenter Server and Platform Services Controller to the latest version of vSphere, new virtual machines are deployed. You must update the scheduled backup job in Region B for full image backup of the Management vCenter Server and the connected external Platform Services Controller.

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 On the vSphere Web Client **Home** page, click the **VDP** icon.
- 3 On the **Welcome to vSphere Data Protection** page, select **mgmt01vdp51** from the **VDP Appliance** drop-down menu and click **Connect**.
- 4 Click the **Backup** tab.
- 5 Locate and update the backup job **Management and Compute vCenter Server Backups** to include the new Compute vCenter Server and Platform Services Controller in Region B.
 - a Click on the backup job **Management and Compute vCenter Server Backups**.
 - b From the **Backup job actions** menu, select **Edit** to run the **Edit backup job** wizard.
 - c On the **Data Type** page, select **Full Image**, leave the **Fall back to the non-quieted backup if quiescence fails** check box selected, and click **Next**.

- d On the **Backup Sources** page, fully expand the **Virtual Machines** tree.

Object	Value
vCenter Server	mgmt01vc51.lax01.rainpole.local
Data center	LAX01
Cluster	LAX01-Mgmt01

- e Locate the obsolete Management vCenter Server and Platform Services Controller virtual machines and deselect them.

Obsolete Object	VM Name
Management Platform Services Controller	mgmt01psc51.lax01_old
Management vCenter Server	mgmt01vc51.lax01_old

- f Select the new virtual appliances for Management vCenter Server and the Platform Services Controller.

Object	VM name
Management Platform Services Controller	mgmt01psc51
Management vCenter Server	mgmt01vc51

- g Verify that the following the virtual appliances for vCenter Server and the Platform Services Controller in Region B have been selected, and click **Next**.

Object	VM name
Management Platform Services Controller	mgmt01psc51
Management vCenter Server	mgmt01vc51
Compute Platform Services Controller	comp01psc51.lax01
Compute vCenter Server	comp01vc51.lax01

- h On the **Schedule** page, leave **Backup Schedule** to **Daily** and click **Next**.
- i On the **Retention Policy** page, leave **Keep to for 3 days** and click **Next**.
- j On the **Job Name** page, leave **Management and Compute vCenter Server Backups** as a name for the backup job and click **Next**.
- k On the **Ready to Complete** page, review the summary information for the backup job and click **Finish**.
- l In the dialog box that shows a confirmation that the job is created, click **OK**.

Place Management vCenter Server and Platform Services Controller in a VM and Templates Folder in Region B

Create a folder on the Management vCenter Server in Region B to group vCenter Server and Platform Services Controller instances together for easier management, and move the appliances there.

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 Create the MGMT51 folder.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **mgmt01vc51.lax01.rainpole.local** tree.
 - c Right-click the **LAX01** data center, and select **New Folder > New VM and Template Folder**.
 - d In the **New Folder** dialog box enter **MGMT51** as the name to label the folder and click **OK**.
- 3 Move the vCenter Server and Platform Services Controller virtual machines to the MGMT51 folder.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **mgmt01vc51.lax01.rainpole.local** tree.
 - c Expand the **Discovered virtual machines** folder.
 - d Drag **mgmt01vc51** and **mgmt01psc51** to the MGMT51 folder.

vSphere Update Manager Download Service Implementation in Region B

Install the vSphere Update Manager Download Service (UMDS) on a Linux virtual machine to download and store binaries and metadata in a shared repository in Region B.

Procedure

- 1 [Configure PostgreSQL Database on Your Linux-Based Host Operating System for UMDS in Region B](#)

In Region B, on a virtual machine with Ubuntu 14.04 Long Term Support (LTS) where you plan to install Update Manager Download Service (UMDS), install and configure a PostgreSQL database instance .

- 2 [Install UMDS on Ubuntu OS in Region B](#)

After you install the PostgreSQL database on the UMDS virtual machine in Region B, install the UMDS software.

- 3 [Set Up the Data to Download with UMDS in Region B](#)

By default UMDS downloads patch binaries, patch metadata, and notifications for hosts. Specify which patch binaries and patch metadata to download with UMDS in Region B.

4 Install and Configure the UMDS Web Server in Region B

The UMDS server in Region B downloads upgrades, patch binaries, patch metadata, and notifications to a directory that you must share to vSphere Update Manager by using a Web server.

5 Use the UMDS Shared Repository as the Download Source in Update Manager in Region B

You configure Update Manager to use the UMDS shared repository in Region B as a source for downloading ESXi patches, extensions, and notifications.

Configure PostgreSQL Database on Your Linux-Based Host Operating System for UMDS in Region B

In Region B, on a virtual machine with Ubuntu 14.04 Long Term Support (LTS) where you plan to install Update Manager Download Service (UMDS), install and configure a PostgreSQL database instance .

Prerequisites

- Create a virtual machine for UMDS on the management cluster of Region B. See *Virtual Machine Specifications* from the *Planning and Preparation* documentation.
- Verify you have PostgreSQL database user credentials.

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 vSphere Web Client, right-click the mgmt01umds51.lax01.rainpole.local virtual machine and select **Open Console** to open the remote console to the virtual machine.
- 3 At the command prompt, log in as the **svc-umds** user using **`svc-umds_password`**.
- 4 Install VMtools and Secure Shell (SSH) server, and end the session.

```
sudo apt-get update
sudo apt-get -y install SSH
exit
```

- 5 Log back into the UMDS virtual machine using SSH and the **svc-umds** service account credentials.
- 6 Install and start PostgreSQL and its dependencies:

```
sudo apt-get -y install vim perl tar sed psmisc unixodbc postgresql postgresql-contrib odbc-
postgresql
sudo service postgresql start
```

- 7 Log in as a PostgreSQL user, and create a database instance and a database user, by running the following commands.

When prompted, enter and confirm the `umds_db_user_password` password.

```
sudo su - postgres
createdb umds_db
createuser -d -e -r umds_db_user -P
```

- 8 Enable password authentication for the database user.

- a Navigate to the folder that contains the PostgreSQL configuration file `pg_hba.conf`.

Linux system	Default Location
Ubuntu 14.04	<code>/etc/postgresql/postgres_version/main</code>

```
cd /etc/postgresql/postgres_version/main
```

- b In the PostgreSQL configuration file, enable password authentication for the database user by inserting the following line right above `local all all peer`.

You can use the `vi` editor to make and save the changes.

#TYPE	DATABASE	USER	ADDRESS	METHOD
local	<code>umds_db</code>	<code>umds_db_user</code>		md5

- c Log out as a PostgreSQL user by running the following command.

```
logout
```

- 9 Configure the PostgreSQL driver and the data source name (DSN) for connection to the UMDS database.

- a Edit the ODBC configuration file.

```
sudo vi /etc/odbcinst.ini
```

- b Replace the file with the following content and save the change using `:wq`.

```
[PostgreSQL]
Description=PostgreSQL ODBC driver (Unicode version)
Driver=/usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so
Debug=0
CommLog=1
UsageCount=1
```

- c Edit the system file `/etc/odbc.ini`.

```
sudo vi /etc/odbc.ini
```

- d Replace the file with the following content and save the change using `:wq`,

```
[UMDS_DSN]
;DB_TYPE = PostgreSQL
;SERVER_NAME = localhost
;SERVER_PORT = 5432
;TNS_SERVICE = <database_name>
;USER_ID = <database_username>
Driver = PostgreSQL
DSN = UMDS_DSN
ServerName = localhost
PortNumber = 5432
Server = localhost
Port = 5432
UserID = umds_db_user
User = umds_db_user
Database = umds_db
```

- 10 Create a symbolic link between the UMDS and the PostgreSQL by running the following command.

```
ln -s /var/run/postgresql/.s.PGSQL.5432 /tmp/.s.PGSQL.543
```

- 11 Restart PostgreSQL.

```
sudo service postgresql restart
```

Install UMDS on Ubuntu OS in Region B

After you install the PostgreSQL database on the UMDS virtual machine in Region B, install the UMDS software.

Prerequisites

- Verify you have administrative privileges on the UMDS Ubuntu virtual machine.
- Mount the ISO file of the vCenter Server Appliance to the Linux machine.

Procedure

- 1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.
 - a Open an SSH connection to `mgmt01umds51.lax01.rainpole.local`.
 - b Log in using the following credentials.

Setting	Value
User name	<code>svc-umds</code>
Password	<code>svc-umds_password</code>

- 2 Mount the vCenter Server Appliance ISO to the UMDS virtual machine.

```
sudo mkdir -p /mnt/cdrom
sudo mount /dev/cdrom /mnt/cdrom
```

- 3 Unarchive the VMware-UMDS-6.5.0.-*build_number*.tar.gz file:

```
tar -xzf /mnt/cdrom/ums/VMware-UMDS-6.5.0-build_number.tar.gz -C /tmp
```

- 4 Run the UMDS installation script.

```
sudo /tmp/vmware-ums-distrib/vmware-install.pl
```

- 5 Read and accept the EULA.
- 6 Press Enter to install UMDS in the default directory /usr/local/vmware-ums and enter **yes** to confirm directory creation.
- 7 Enter the UMDS proxy settings if needed according to the settings of your environment.
- 8 Press Enter to set the patch location to /var/lib/vmware-ums and enter **yes** to confirm directory creation.
- 9 Provide the database details.

Option	Description
Provide the database DSN	UMDS_DSN
Provide the database username	<i>ums_db_user</i>
Provide the database password	<i>ums_db_user_password</i>

- 10 Type **yes** and press Enter to install UMDS.

Set Up the Data to Download with UMDS in Region B

By default UMDS downloads patch binaries, patch metadata, and notifications for hosts. Specify which patch binaries and patch metadata to download with UMDS in Region B.

Procedure

- 1 Log in to UMDS virtual machine by using a Secure Shell (SSH) client.
 - a Open an SSH connection to mgmt01ums51.lax01.rainpole.local.
 - b Log in using the following credentials.

Setting	Value
User name	svc-ums
Password	<i>svc-ums_password</i>

- 2 Navigate to the directory where UMDS is installed.

```
cd /usr/local/vmware-umds/bin
```

- 3 Disable the updates for older hosts and virtual appliances.

```
sudo ./vmware-umds -S -n
sudo ./vmware-umds -S -d embeddedEsx-5.5.0
sudo ./vmware-umds -S -d embeddedEsx-6.0.0
```

- 4 Configure automatic daily downloads by creating a cron job file.

```
cd /etc/cron.daily/
sudo touch umds-download
sudo chmod 755 umds-download
```

- 5 Edit the download command to the cron job.

```
sudo vi umds-download
```

- 6 Add the following lines to the file.

```
#!/bin/sh
/usr/local/vmware-umds/bin/vmware-umds -D
```

- 7 Test the UMDS Download cron job.

```
sudo ./umds-download
```

Install and Configure the UMDS Web Server in Region B

The UMDS server in Region B downloads upgrades, patch binaries, patch metadata, and notifications to a directory that you must share to vSphere Update Manager by using a Web server.

The default folder to which UMDS downloads patch binaries and patch metadata on a Linux machine is `/var/lib/vmware-umds`. You share this folder out to the VUM instances within the region using the Nginx Web server.

Procedure

- 1 Log in to UMDS virtual machine by using a Secure Shell (SSH) client.
 - a Open an SSH connection to `mgmt01umds51.lax01.rainpole.local`.
 - b Log in using the following credentials.

Setting	Value
User name	<code>svc-umds</code>
Password	<code>svc-umds_password</code>

- 2 Install the Nginx Web server with the following command.

```
sudo apt-get -y install nginx
```

- 3 Change the patch repository directory permissions by running the command.

```
sudo chmod -R 755 /var/lib/vmware-umds
```

- 4 Copy the default site configuration for use with the UMDs configuration.

```
sudo cp /etc/nginx/sites-available/default /etc/nginx/sites-available/umds
```

- 5 Edit the new `/etc/nginx/sites-available/umds` site configuration file and replace the `server {}` block with the following text.

```
server {
    listen 80 default_server;
    listen [::]:80 default_server ipv6only=on;

    root /var/lib/vmware-umds;
    index index.html index.htm;

    # Make site accessible from http://localhost/
    server_name localhost mgmt01umds51 mgmt01umds51.lax01.rainpole.local;

    location / {
        # First attempt to serve request as file, then
        # as directory, then fall back to displaying a 404.
        try_files $uri $uri/ =404;
        # Uncomment to enable naxsi on this location
        # include /etc/nginx/naxsi.rules
        autoindex on;
    }
}
```

- 6 Disable the existing default site.

```
sudo rm /etc/nginx/sites-enabled/default
```

- 7 Enable the new UMDs site.

```
sudo ln -s /etc/nginx/sites-available/umds /etc/nginx/sites-enabled/
```

- 8 Restart the Nginx Web service to apply the new configuration.

```
sudo service nginx restart
```

- 9 Ensure you can browse the files of the UMDs Web server by opening a web browser to **`http://mgmt01umds51.lax01.rainpole.local`**.

Use the UMDS Shared Repository as the Download Source in Update Manager in Region B

You configure Update Manager to use the UMDS shared repository in Region B as a source for downloading ESXi patches, extensions, and notifications.

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 On the **Home** page of the vSphere Web Client, click the **Update Manager** icon.
- 3 From the **Objects** tab, click the **mgmt01vc51.lax01.rainpole.local** vCenter Server for Region B.
The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.
- 4 On the **Manage** tab, click **Settings** and select **Download Settings**.
- 5 On the **Download sources** page, click **Edit**.
An **Edit Download Sources** dialog box opens.
- 6 Enter the following setting and click **OK**.

Setting	Value
Use a shared repository	Selected
URL	http://mgmt01umds51.lax01.rainpole.local

The vSphere Web Client performs validation of the URL.

- 7 In the **Download Sources** page, click **Download Now** to run the download patch definitions.
- 8 If you are deploying the management components in Region B, repeat the procedure to configure the **http://mgmt01umds51.lax01.rainpole.local** repository for the **comp01vc51.lax01.rainpole.local** vCenter Server.

Skip this step during SDDC upgrade.

Configure the Management vCenter Server to Forward Log Events to vRealize Log Insight in Region B

You can configure the Management vCenter Server and connected Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster in Region B. You can then view and analyze all syslog information in the vRealize Log Insight web interface.

In Region B, you configure the following vCenter Server and Platform Services Controller instances for the management cluster:

Region	Appliance Type	Appliance Management Interface URL	vRealize Log Insight Syslog Host
Region B	vCenter Server instances	https://mgmt01vc51.lax01.rainpole.local:5480	vrli-cluster-51.lax01.rainpole.local
	Platform Services Controller instances	https://mgmt01psc51.lax01.rainpole.local:5480	vrli-cluster-51.lax01.rainpole.local

Procedure

- 1 Redirect the log events from the appliance to vRealize Log Insight.

- a Open a Web browser and go to **https://mgmt01vc51.lax01.rainpole.local:5480**.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	mgmtvc_root_password

- c In the **Navigator**, click **Syslog Configuration**.
- d On the **Syslog Configuration** page, click **Edit**, configure the following settings, and click **OK**.

Setting	Value
Common Log Level	*
Remote Syslog Host	vrli-cluster-51.lax01.rainpole.local
Remote Syslog Port	514
Remote Syslog Protocol	UDP

- e Repeat the steps for the Platform Services Controller Appliance.

- 2 Verify that the appliances are forwarding their syslog traffic to vRealize Log Insight.

- a Open a Web browser and go to **https://vrli-cluster-51.lax01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- c In the vRealize Log Insight user interface, click **Dashboards** and select **VMware - vSphere** from the content pack dashboard drop-down menu.
- d Verify that the vCenter Server and Platform Services Controller nodes are presented on the **All vSphere events by hostname** widget of the **General Overview** dashboard.

Complete vSphere Upgrade for the Management Cluster

After you upgrade the vCenter Server and Platform Services Controller, and vSphere Data Protection and Site Recovery Manager, upgrade the ESXi hosts and Virtual SAN storage.

Procedure

1 Upgrade the ESXi Hosts in the Management Clusters

Complete the upgrade of the management part of the Virtual Infrastructure layer by upgrading the management ESXi hosts in Region A and Region B.

2 Upgrade the ESXi Hosts in the Management Cluster in Region B

Complete the upgrade of the management part of the virtual infrastructure layer by upgrading the management ESXi hosts in Region B.

Upgrade the ESXi Hosts in the Management Clusters

Complete the upgrade of the management part of the Virtual Infrastructure layer by upgrading the management ESXi hosts in Region A and Region B.

Upgrading the management ESXi hosts when using NSX for vSphere is a multi-step operations in which you must download the NSX for vSphere VIBs, slipstream the NSX for vSphere VIBs into the ESXi 6.5 image, and use vSphere Update Manager to automate a cluster-wide upgrade operation on each of the clusters.

Table 4-10. Management ESXi hosts In the SDDC

Region	IP Address	Fully Qualified Domain Name	Cluster Name	Virtual SAN Datastore
Region A	172.16.11.101	mgmt01esx01.sfo01.raipole.local	SFO01-Mgmt01	SFO01A-VSAN01-MGMT01
	172.16.11.102	mgmt01esx02.sfo01.raipole.local		
	172.16.11.103	mgmt01esx03.sfo01.raipole.local		
	172.16.11.104	mgmt01esx04.sfo01.raipole.local		
Region B	172.17.11.101	mgmt01esx51.lax01.raipole.local	LAX01-Mgmt01	LAX01A-VSAN01-MGMT01
	172.17.11.102	mgmt01esx52.lax01.raipole.local		
	172.17.11.103	mgmt01esx53.lax01.raipole.local		
	172.17.11.104	mgmt01esx54.lax01.raipole.local		

Prerequisites

- Make sure that the system hardware complies with ESXi requirements by consulting [VMware Compatibility Guide](#). Check for system compatibility, I/O compatibility with network and host bus adapter (HBA) cards, storage compatibility, and backup software compatibility.
- Ensure the firmware for the network and host bus adapter (HBA) cards have been updated for compatibility.
- Ensure the BIOS for the ESXi hosts are updated for compatibility.
- Ensure that sufficient disk space is available on the host for the upgrade.
- Ensure DRS has been set to Fully Automated for the duration of the upgrade operations to allow for management workloads to be evacuated from hosts as they are upgraded.
- Download the ESXi 6.5 .iso file.

Procedure

1 [Use the Image Builder to Create an ESXi 6.5 Image with NSX for vSphere VIBs in Region A](#)

Using the new Image Builder service included in vSphere 6.5, inject the NSX for vSphere VIBs from the NSX Manager 6.3.x in an ESXi image for Region A.

2 [Use vSphere Update Manager to Remediate the ESXi Management Cluster in Region A](#)

After creating a slipstreamed ESXi 6.5a with NSX 6.3.1 VIBs, upload it to vSphere Update Manager on the Management vCenter Server instances in Region A. You use this image to remediate your shared compute and edge cluster too.

What to do next

- Verify that the management ESXi hosts function flawlessly after the upgrade. See *Validate the ESXi Hosts* in the *VMware Validated Design Operational Verification* documentation.

Use the Image Builder to Create an ESXi 6.5 Image with NSX for vSphere VIBs in Region A

Using the new Image Builder service included in vSphere 6.5, inject the NSX for vSphere VIBs from the NSX Manager 6.3.x in an ESXi image for Region A.

Using the Image Builder service to inject the NSX for vSphere 6.3.x VIBs into an ESXi image allows for a stream-lined operation for upgrading the hosts within a cluster. By using this method, additional preparation via NSX Manager for the ESXi hosts is not needed, which greatly expedites the upgrade time window by allowing vSphere Update Manager to automate a cluster-wide upgrade.

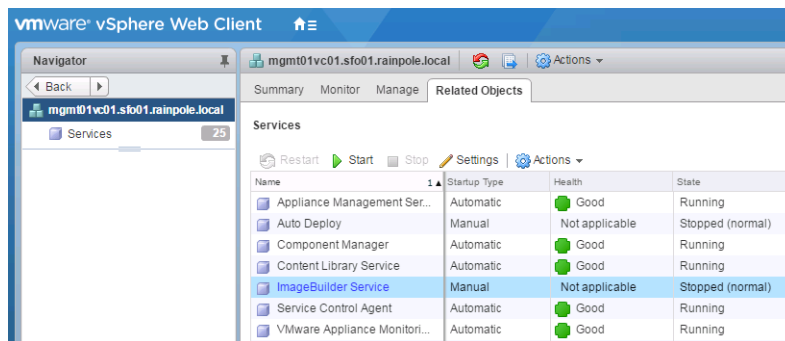
Procedure

- 1 To download the NSX for vSphere VIBs from the NSX Manager in Region A, open a Web browser and go to
<https://mgmt01nsxm01.sfo01.rainpole.local/bin/vdn/vibs-6.3.1/6.5-5124743/vxlan.zip>

- 2 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

- 3 Start the Image Builder service on vCenter Server.
 - a From the **Home** page, under the **Administration** section, click **System Configuration**.
 - b In the **Navigator** pane, click **Nodes**.
 - c Under **Nodes**, click **mgmt01vc01.sfo01.rainpole.local** and click the **Related Objects** tab.
 - d Locate ImageBuilder Service and click **Start**.



- 4 Log out and log back in to the vSphere Web Client to re-load the Image Builder plug-in.
- 5 Create an image depot for the VMware Validated Design ESXi image.
 - a On the **Home** page, click **Auto Deploy**.
 - b In the **Auto Deploy** pane, select **mgmt01vc01.sfo01.rainpole.local** from the **vCenter Server** drop-down menu, and click the **Software Depots** tab.
 - c Click the **Add Software Depot** icon.
 - d In the **Add Software Depot** dialog box, provide the following settings and click **OK**.

Setting	Value
Select the type of depot you want to create:	Custom Depot
Name	VVD ESXi 6.5 Upgrade

6 Upload the NSX for vSphere 6.3.x VIBs to the Image Builder for sharing.

- a On the **Software Depots** tab, click the **Import Software Depot** icon.
- b In the **Import Software Depot** dialog box, click **Browse**, locate `vxlan.zip` from [Step 1](#) and provide the following settings.

Setting	Value
Name	NSX 6.3.1 VIBs
File	<i>path_to_vxlan.zip</i>

- c Click **Upload** and click **Close** after the upload is complete.

7 Upload the ESXi 6.5 image to the Image Builder for sharing.

- a On the **Software Depots** tab, click on the **Import Software Depot** icon.
- b In the **Import Software Depot** dialog box, click **Browser** and locate the ESXi 6.5a offline depot .zip file.

Setting	Value
Name	ESXi 6.5a
File	<i>path_to_ESXi65_Offline_Depot.zip</i>

- c Click **Upload** and click **Close** after the upload is complete.

8 Create a slipstreaming ESXi 6.5 image with the NSX for vSphere VIBs.

- a In the left **Software Depots** pane, click on **ESXi 6.5a**.
- b In the right **Software Depots** pane, click on **ESXi-6.5.0-<Release Date>-standard**, and click the **Clone Image Profile** icon.
- c In the **Clone Image Profile** wizard, on the **1 Name and details** page, provide the following settings and click **Next**.

Setting	Value
Name	VVD ESXi 6.5a with NSX 6.3.1 VIBs
Vendor	VMware Validated Design
Description	VMware Validated Design 4.0 upgrade ISO for ESXi 6.5a with NSX 6.3.1 VIBs
Software depot	VVD ESXi 6.5 Upgrade

- d On the **2 Select software packages** page, enter the following configuration and click **Next**.

Setting	Value
Acceptance Level	VMware certified
Software depot	NSX 6.3.1 VIBs
Available	<i>all vib in the software depot</i>

- e On the **3 Ready to complete** page, click **Finish**.

The VMware ESXi 6.5 Standard ISO with the NSX for vSphere VIBs has 125 software packages. If a vendor-specific ESXi 6.5 image is used, the software package number might vary.

9 Export the ESXi 6.5 image with NSX 6.3.1 VIBs.

- From the **Home** page of the vSphere Web Client, click **Auto Deploy**.
- In the **Auto Deploy** pane, click the **Software Depots** tab.
- In the left **Software Depots** pane, click the **VVD ESXi 6.5 Upgrade** depot.
- In the right **Software Depots** pane, right-click **VVD ESXi 6.5a with NSX 6.3.1 VIBs** and click **Export Image Profile**.
- In the **Export Image Profile** dialog box, select **ISO - Generate a bootable ISO image from the image profile** and click **Generate Image**.
- After the image is generated, click **Download Image**.

An ISO file VVD ESXi 6.5a with NSX6.3.1 VIBs.iso is downloaded to your workstation.

Use vSphere Update Manager to Remediate the ESXi Management Cluster in Region A

After creating a slipstreamed ESXi 6.5a with NSX 6.3.1 VIBs, upload it to vSphere Update Manager on the Management vCenter Server instances in Region A. You use this image to remediate your shared compute and edge cluster too.

Procedure

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

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Upload the slipstreamed ESXi image to the vSphere Update Manager in Region A .
 - a On the **Home** page of the vSphere Web Client, under the **Operations and Policies** section, click **Update Manager**.
 - b In the left **Servers** pane, click **mgmt01vc01.sfo01.rainpole.local**.
 - c In the right pane, click the **Manage** tab, click **ESXi Images** and click **Import ESXi Image**.
 - d In the **Import ESXi Image** dialog box, click **Browse** and locate the VVD ESXi 6.5a with NSX 6.3.1 VIBs.iso .
 - e Click **Open** to upload the image.
 - f After the image has been successfully imported, click **Close**.

- 3 Create a baseline for your VMware Validated Design ESXi image.

- a On the **Manage** tab, select **Host Baselines**.
- b Click the **New Baseline** icon.
- c In the **New Baseline** dialog box, provide the following settings and click **Next**.

Setting	Value
Name	VMware Validated Design ESXi 6.5a Upgrade
Description	--
Baseline type	Host Upgrade

- d In the **ESXi Image** section, click the **VVD ESXi 6.5a with NSX 6.3.1 VIBs** image from the list and click **Next**.
 - e Click **Finish** to complete making the baseline.
- 4 Attach the new VMware Validated Design ESXi 6.5a Upgrade Baseline to your management cluster.
 - a On the **Host Baselines** tab, click **Go to Compliance View** to go to the mgmt01vc01.sfo01.rainpole vCenter Server and to the SFO01-Mgmt01 cluster.
 - b From the **Update Manager** tab, click **Attach Baseline**.
 - c In the **Attach Baseline or Baseline Group** dialog box, under **Upgrade Baselines**, select the **VMware Validated Design ESXi 6.5a Upgrade** baseline and click **OK**.
 - 5 Scan the cluster for updates against the new baseline
 - a On the **Update Manager** tab, click **Scan for Updates** .
 - b In the **Scan for Updates** dialog box, under **Scan hosts for**, select **Upgrades** and click **OK**.
After the scan is complete, the cluster reports back as **Non-Compliant**.

6 Remediate the cluster and upgrade to vSphere 6.5.

- a From the **Update Manager** tab, click **Remediate**.
- b In the **Remediate** wizard, under **Baselines Groups and Types**, select the baseline **VMware Validated Design ESXi 6.5a Upgrade** and click **Next**.
- c On the **Select Target** page, select all of the management hosts in the cluster and click **Next**.
- d On the **End User License Agreement** page, select **I accept the terms and license agreement** and click **Next**.
- e On the **Advanced options** page, click **Next**.
- f On the **Host remediation options** page, deselect **Retry entering maintenance mode in case of failure** and click **Next**.
- g On the **Cluster remediation options** page, select the following options and click **Next**.

Setting	Value
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters	Selected
Disable High Availability admission control if it is enabled for any of the selected clusters	Selected
Enable parallel remediation for the hosts in the cluster > Automatically determine the maximum number of concurrently remediated hosts in a cluster	Selected
Migrate powered off or suspended VMs to other hosts in the cluster, if a host must enter maintenance mode	Selected

- h On the **Ready to complete** page, click **Pre-check Remediation** to generate a pre-upgrade report of any identifiable problems that would prevent a successful upgrade.

Address any items reported in the **Pre-check Remediation** dialog box before proceeding with the upgrade. Click **OK** to close the screen. Ignore the **Disable HA admission control** message from **Recommended Changes**.

- i After you address all pre-check items, click **Finish** to begin the upgrade.

7 Review the NSX for vSphere status of the management clusters.

- a Select **Home > Networking & Security**.
- b Select **Installation** in the **Navigator**.
- c On the **Host Preparation** tab, select **172.16.11.65** from the **NSX Manager** menu and verify that **Installation Status** for all management ESXi hosts is green.

Upgrade the ESXi Hosts in the Management Cluster in Region B

Complete the upgrade of the management part of the virtual infrastructure layer by upgrading the management ESXi hosts in Region B.

Procedure

1 Use the Image Builder to Create an ESXi 6.5 Image with NSX for vSphere VIBs in Region B

Using the new Image Builder service included in vSphere 6.5, inject the NSX for vSphere VIBs from the NSX Manager 6.3.x in an ESXi image for Region B.

2 Use vSphere Update Manager to Remediate the Management Cluster in Region B

After creating a slipstreamed ESXi 6.5a with NSX 6.3.1 VIBs, upload it to vSphere Update Manager on the Management vCenter Server instance in Region B. You use this image to remediate your shared compute and edge cluster in the region too.

Use the Image Builder to Create an ESXi 6.5 Image with NSX for vSphere VIBs in Region B

Using the new Image Builder service included in vSphere 6.5, inject the NSX for vSphere VIBs from the NSX Manager 6.3.x in an ESXi image for Region B.

Using the Image Builder service to inject the NSX for vSphere 6.3.x VIBs into an ESXi image allows for a stream-lined operation for upgrading the hosts within a cluster. By using this method, additional preparation via NSX Manager for the ESXi hosts is not needed, which greatly expedites the upgrade time window by allowing vSphere Update Manager to automate a cluster-wide upgrade.

Procedure

- 1 To download the NSX for vSphere VIBs from the NSX Manager in Region B, open a Web browser and go to
<https://mgmt01nsxm51.lax01.rainpole.local/bin/vdn/vibs-6.3.1/6.5-5124743/vxlan.zip>

- 2 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

- 3 Start the Image Builder service on vCenter Server.
 - a From the **Home** page, under the **Administration** section, click **System Configuration**.
 - b In the **Navigator** pane, click **Nodes**.
 - c Under **Nodes**, click **mgmt01vc51.lax01.rainpole.local** and click the **Related Objects** tab.
 - d Locate ImageBuilder Service and click **Start**.
- 4 Log out and log back in to the vSphere Web Client to re-load the Image Builder plug-in.

5 Create an image depot for the VMware Validated Design ESXi image.

- a On the **Home** page, click **Auto Deploy**.
- b In the **Auto Deploy** pane, select **mgmt01vc51.lax01.rainpole.local** from the **vCenter Server** drop-down menu, and click the **Software Depots** tab.
- c Click the **Add Software Depot** icon.
- d In the **Add Software Depot** dialog box, provide the following settings and click **OK**.

Setting	Value
Select the type of depot you want to create	Custom Depot
Name	VVD ESXi 6.5 Upgrade

6 Upload the NSX for vSphere 6.3.x VIBs to the Image Builder for sharing.

- a On the **Software Depots** tab, click the **Import Software Depot** icon.
- b In the **Import Software Depot** dialog box, click **Browse**, locate **vxlan.zip** from [Step 1](#) and provide the following settings.

Setting	Value
Name	NSX 6.3.1 VIBs
File	<i>path_to_vxlan.zip</i>

- c Click **Upload** and click **Close** after the upload is complete.

7 Upload the ESXi 6.5 image to the Image Builder for sharing.

- a On the **Software Depots** tab, click on the **Import Software Depot** icon.
- b In the **Import Software Depot** dialog box, click **Browser** and locate the ESXi 6.5a offline depot .zip file.

Setting	Value
Name	ESXi 6.5a
File	<i>path_to_ESXi65_Offline_Depot.zip</i>

- c Click **Upload** and click **Close** after the upload is complete.

8 Create a slipstreaming ESXi 6.5 image with the NSX for vSphere VIBs.

- a In the left **Software Depots** pane, click on **ESXi 6.5a**.
- b In the right **Software Depots** pane, click on **ESXi-6.5.0-<Release Date>-standard**, and click the **Clone Image Profile** icon.

- c In the **Clone Image Profile** wizard, on the **1 Name and details** page, provide the following settings and click **Next**.

Setting	Value
Name	VVD ESXi 6.5a with NSX 6.3.1 VIBs
Vendor	VMware Validated Design
Description	VMware Validated Design 4.0 upgrade ISO for ESXi 6.5a with NSX 6.3.1 VIBs
Software depot	VVD ESXi 6.5 Upgrade

- d On the **2 Select software packages** page, enter the following configuration and click **Next**.

Setting	Value
Acceptance Level	VMware certified
Software depot	NSX 6.3.1 VIBs
Available	<ul style="list-style-type: none"> ■ esx-vsip ■ esx-vxlan

- e On the **3 Ready to complete** page, click **Finish**.

The VMware ESXi 6.5 Standard ISO with the NSX for vSphere VIBs has 125 software packages. If a vendor-specific ESXi 6.5 image is used, the software package number might vary.

9 Export the ESXi 6.5 image with NSX 6.3.1 VIBs.

- a From the **Home** page of the vSphere Web Client, click **Auto Deploy**.
- b In the **Auto Deploy** pane, click the **Software Depots** tab.
- c In the left **Software Depots** pane, click the **VVD ESXi 6.5 Upgrade** depot.
- d In the right **Software Depots** pane, right-click **VVD ESXi 6.5a with NSX 6.3.1 VIBs** and click **Export Image Profile**.
- e In the **Export Image Profile** dialog box, select **ISO - Generate a bootable ISO image from the image profile** and click **Generate Image**.
- f After the image is generated, click **Download Image**.

An ISO file VVD ESXi 6.5a with NSX6.3.1 VIBs.iso is downloaded to your workstation.

Use vSphere Update Manager to Remediate the Management Cluster in Region B

After creating a slipstreamed ESXi 6.5a with NSX 6.3.1 VIBs, upload it to vSphere Update Manager on the Management vCenter Server instance in Region B. You use this image to remediate your shared compute and edge cluster in the region too.

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 Upload the slipstreamed ESXi image to the vSphere Update Manager in Region B.

- a On the **Home** page of the vSphere Web Client, under the **Operations and Policies** section, click **Update Manager**.
- b In the left **Servers** pane, click **mgmt01vc51.lax01.rainpole.local**.
- c In the right pane, click the **Manage** tab, click **ESXi Images** and click **Import ESXi Image**.
- d In the **Import ESXi Image** dialog box, click **Browse** and locate the VVD ESXi 6.5a with NSX 6.3.1 VIBs.iso .
- e Click **Open** to upload the image.
- f After the image has been successfully imported, click **Close**.

- 3 Create a baseline for your VMware Validated Design ESXi image.

- a On the **Manage** tab, select **Host Baselines**.
- b Click the **New Baseline** icon.
- c In the **New Baseline** dialog box, provide the following settings and click **Next**.

Setting	Value
Name	VMware Validated Design ESXi 6.5a Upgrade
Description	--
Baseline type	Host Upgrade

- d In the **ESXi Image** section, click the **VVD ESXi 6.5a with NSX 6.3.1 VIBs** image from the list and click **Next**.
- e Click **Finish** to complete making the baseline.

- 4 Attach the new VMware Validated Design ESXi 6.5a Upgrade Baseline to your management cluster.
 - a On the **Host Baselines** tab, click **Go to Compliance View** to go to the mgmt01vc51.lax01.rainpole vCenter Server and to the LAX01-Mgmt01 cluster.
 - b From the **Update Manager** tab, click **Attach Baseline**.
 - c In the **Attach Baseline or Baseline Group** dialog box, under **Upgrade Baselines**, select the **VMware Validated Design ESXi 6.5a Upgrade** baseline and click **OK**.
- 5 Scan the cluster for updates against the new baseline
 - a On the **Update Manager** tab, click **Scan for Updates**.
 - b In the **Scan for Updates** dialog box, under **Scan hosts for**, select **Upgrades** and click **OK**.
After the scan is complete, the cluster reports back as **Non-Compliant**.
- 6 Remediate the cluster and upgrade to vSphere 6.5.
 - a From the **Update Manager** tab, click **Remediate**.
 - b In the **Remediate** wizard, under **Baselines Groups and Types**, select the baseline **VMware Validated Design ESXi 6.5a Upgrade** and click **Next**.
 - c On the **Select Target** page, select all of the management hosts in the cluster and click **Next**.
 - d On the **End User License Agreement** page, select **I accept the terms and license agreement** and click **Next**.
 - e On the **Advanced options** page, click **Next**.
 - f On the **Host remediation options** page, deselect **Retry entering maintenance mode in case of failure** and click **Next**.
 - g On the **Cluster remediation options** page, select the following options and click **Next**.

Setting	Value
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters	Selected
Disable High Availability admission control if it is enabled for any of the selected clusters	Selected
Enable parallel remediation for the hosts in the cluster > Automatically determine the maximum number of concurrently remediated hosts in a cluster	Selected
Migrate powered off or suspended VMs to other hosts in the cluster, if a host must enter maintenance mode	Selected

- h On the **Ready to complete** page, click **Pre-check Remediation** to generate a pre-upgrade report of any identifiable problems that would prevent a successful upgrade.

Address any items reported in the **Pre-check Remediation** dialog box before proceeding with the upgrade. Click **OK** to close the screen. Ignore the Disable HA admission control message from Recommended Changes.

- i After you address all pre-check items, click **Finish** to begin the upgrade.
- 7 Review the NSX for vSphere status of the management clusters.
 - a Select **Home > Networking & Security**.
 - b Select **Installation** in the **Navigator**.
 - c On the **Host Preparation** tab, select **172.17.11.65** from the **NSX Manager** menu and verify that **Installation Status** for all management ESXi hosts is green.

Post-Upgrade Configuration of the Management ESXi Hosts and vSAN Storage

After you complete the upgrade of the vSphere management components, perform a final update of the configuration of vCenter Server and ESXi according to the objectives and deployment guidelines of this validated design.

Procedure

1 Upgrade the vSphere Distributed Switch in the Management Cluster in Region A

After you upgrade vCenter Server and ESXi in the management cluster in Region A, upgrade the vSphere Distributed Switch to use the new features of the switch in the latest release of the environment.

2 Place the VMkernel Adapter for vSphere vMotion Traffic on a Separate TCP/IP Stack on the Management Hosts in Region A

To comply with the objective and deployment guidelines of this validated design, configure a template management host with a separate network for vSphere vMotion in Region A.

3 Configure VM Swap Files as Sparse Objects on the vSAN Datastore in Region A

After you upgrade vCenter Server and the management ESXi hosts in the SDDC, turn on the vSAN Sparse Swap feature in Region A to save storage space by allocating space for VM swap files only when virtual machines are running.

4 Create and Apply the Host Profile for the Management Cluster in Region A

After you upgrade the vSphere components, use a host profile for the ESXi management hosts in Region A to ensure that they have the same configuration.

5 Upgrade the vSphere Distributed Switch in the Management Cluster in Region B

After you upgrade vCenter Server and ESXi in the management cluster in Region B, upgrade the vSphere Distributed Switch to use the new features of the switch in the latest release in the environment.

6 Place the VMkernel Adapter for vSphere vMotion Traffic on a Separate TCP/IP Stack on the Management Hosts in Region B

To comply with the objective and deployment guidelines of this validated design, configure a template management host with a separate network for vSphere vMotion in Region B.

7 Configure the VM Swap Files as Sparse Objects on the vSAN Datastore in Region B

After you upgrade vCenter Server and the management ESXi hosts in the SDDC, turn on the vSAN Sparse Swap feature in Region B to save storage space by allocating space for VM swap files only when virtual machines are running.

8 Create and Apply the Host Profile for the Management Cluster in Region B

After you upgrade the vSphere components, apply a host profile on the ESXi management hosts in Region B to ensure that they have the same configuration.

What to do next

After you enable Sparse Swap on vSAN, power off and then power on all management virtual machines to enforce the new, thin-provisioned swap file creation.

Power cycle the virtual machines in groups per layer during separate maintenance windows. For more information about powering off and powering on the VMware Validated Design SDDC management components, see *SDDC Startup and Shutdown* in the *VMware Validated Design Backup and Restore* documentation.

Upgrade the vSphere Distributed Switch in the Management Cluster in Region A

After you upgrade vCenter Server and ESXi in the management cluster in Region A, upgrade the vSphere Distributed Switch to use the new features of the switch in the latest release of the environment.

Prerequisites

Back up the configuration of the distributed switch. See the *VMware Validated Design Backup and Restore* documentation.

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 In the **Navigator**, click **Networking** and expand the **mgmt01vc01.sfo01.rainpole.local** tree.

- 3 Right-click the **vDS-Mgmt** distributed switch and select **Upgrade > Upgrade Distributed Switch**.
The **Upgrade Distributed Switch** wizard appears.
- 4 On the **Configure upgrade page**, select **Version 6.5.0** and click **Next**.
- 5 On the **Check compatibility** page, review host compatibility and click **Next**.
- 6 Review the upgrade configuration and click **Finish**.

Place the VMkernel Adapter for vSphere vMotion Traffic on a Separate TCP/IP Stack on the Management Hosts in Region A

To comply with the objective and deployment guidelines of this validated design, configure a template management host with a separate network for vSphere vMotion in Region A.

You create a VMkernel adapter for vSphere vMotion traffic on a management host in each region. You configure the VMkernel adapter with a static IP address and route the traffic to a network that is different from the network for the ESXi management. You transfer the vMotion networking configuration of the host to the management host profile in the region.

Table 4-11. vMotion Network Configuration of a Template Host After vSphere Upgrade

Region	Template Management Host	vMotion IP Address	vMotion Gateway
Region A	mgmt01esx01.sfo01.rainpole.local	172.16.12.101	172.16.12.253

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 Delete the legacy VMkernel adapter for vSphere vMotion.

- a On the **Configure** tab, select **VMkernel adapters** again.
- b Locate the VMkernel adapter with the following settings and click the **Remove selected network adapter** icon.
- c On the Remove VMkernel Adapter dialog, click **OK**.

Setting	Value
Network Label	vDS-Mgmt-vMotion
IP Address	172.16.12.101
TCP/IP Stack	Default
vMotion	Enabled

3 Create a new vMotion VMkernel adapter on the vMotion TCP/IP stack on the mgmt01esx01.sfo01.rainpole.local host.

- a In the **Navigator**, click **Host and Clusters** and expand the **mgmt01vc01.sfo01.rainpole.local** tree.
- b Click on **mgmt01esx01.sfo01.rainpole.local**.
- c Click the **Configure** tab, select **VMkernel adapters** under **Networking** and click the **Add host networking** icon.

The **Add Networking** wizard appears.

- d On the **Select connection type** page, select **VMkernel Network Adapter** and click **Next**.
- e On the **Select target device** page, select **Select an existing network**, browse to select the **vDS-Mgmt-vMotion** port group, click **OK**, and click **Next**.
- f On the **Port properties** page, select **vMotion** from the **TCP/IP stack** drop-down menu and click **Next**.
- g On the **IPv4 settings** page, select **Use static IPv4 settings** enter IP address **172.16.12.101** and subnet mask **255.255.255.0**, and click **Next**.
- h Click **Finish**.

4 Configure the vMotion TCP/IP stack on the host.

- a On the **Configure** tab of the host object, click **TCP/IP configuration**.
- b Select **vMotion** and click the **Edit TCP/IP Stack Configuration** icon.
- c In the **Edit TCP/IP Stack Configuration** dialog box, click **Routing**, enter **172.16.12.253** in the **VMkernel gateway** text box, and click **OK**.

Configure VM Swap Files as Sparse Objects on the vSAN Datastore in Region A

After you upgrade vCenter Server and the management ESXi hosts in the SDDC, turn on the vSAN Sparse Swap feature in Region A to save storage space by allocating space for VM swap files only when virtual machines are running.

You configure vSAN Sparse Swap only on the first host in the management cluster of the region. The configuration is applied to the other hosts in the cluster when you apply the host profiles that are extracted from the first host.

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 In the **Navigator**, click **Hosts and Clusters**.
- 3 Expand the entire **mgmt01vc01.sfo01.rainpole.local** vCenter Server tree, and select the **mgmt01esx01.sfo01.rainpole.local** host.
- 4 Click the **Configure** tab, click **System > Advanced System Settings**.
- 5 Click the **Edit** button.
- 6 In the **filter** box, enter **vsan.swap** and wait for the search results.
- 7 Change the value of **VSAN.SwapThickProvisionDisabled** to **1** and click **OK**.

Create and Apply the Host Profile for the Management Cluster in Region A

After you upgrade the vSphere components, use a host profile for the ESXi management hosts in Region A to ensure that they have the same 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 Create a host profile from the mgmt01esx01.sfo01.rainpole.local host.

- a In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc01.sfo01.rainpole.local** tree.
- b Right-click **mgmt01esx01.sfo01.rainpole.local** and select **Host Profiles > Extract Host Profile**.
- c In the **Extract Host Profile** window, enter **SFO01-Mgmt01** as the name of the host profile and click **Next**.
- d On the **Ready to complete** page, click **Finish**.

- 3 Attach the host profile to the management cluster.

- a In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc01.sfo01.rainpole.local** tree.
- b Right-click the **SFO01-Mgmt01** cluster, and select **Host Profiles > Attach Host Profile**.
- c In the **Attach Host Profile** dialog box, click **SFO01-Mgmt01**, select the **Skip Host Customization** check box, and click **Finish**.

- 4 Export a host customizations file for the hosts in the management cluster.

- a Select **Home > Policies and Profiles** in the vSphere Web Client.
- b In the **Navigator**, click **Host Profiles**.
- c Right-click **SFO01-Mgmt01**, select **Export Host Customizations** and click **Save**.
- d Navigate to a file location to store the **SFO01-Mgmt01_host_customizations.csv** Excel file that is generated and click **Save**.

- e Edit the Excel file to include the following values.

ESXi Host	Active Directory Configuration Password	Active Directory Configuration Username	NetStack Instance defaultTcpipStack->DNS configuration Name for this host
mgmt01esx01.sfo01.rainpole.local	ad_admin_password	ad_admin_acct@sfo01.rainpole.local	mgmt01esx01
mgmt01esx02.sfo01.rainpole.local	ad_admin_password	ad_admin_acct@sfo01.rainpole.local	mgmt01esx02
mgmt01esx03.sfo01.rainpole.local	ad_admin_password	ad_admin_acct@sfo01.rainpole.local	mgmt01esx03
mgmt01esx04.sfo01.rainpole.local	ad_admin_password	ad_admin_acct@sfo01.rainpole.local	mgmt01esx04

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-Management:management->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-Management:management->IP address settings Subnet Mask
mgmt01esx01.sfo01.rainpole.local	172.16.11.101	255.255.255.0
mgmt01esx02.sfo01.rainpole.local	172.16.11.102	255.255.255.0
mgmt01esx03.sfo01.rainpole.local	172.16.11.103	255.255.255.0
mgmt01esx04.sfo01.rainpole.local	172.16.11.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-NFS:<UNRESOLVED>->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-NFS:<UNRESOLVED>->IP address settings Subnet Mask
mgmt01esx01.sfo01.rainpole.local	172.16.15.101	255.255.255.0
mgmt01esx02.sfo01.rainpole.local	172.16.15.102	255.255.255.0
mgmt01esx03.sfo01.rainpole.local	172.16.15.103	255.255.255.0
mgmt01esx04.sfo01.rainpole.local	172.16.15.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VR:vSphereReplication,vSphereReplicationNFC->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VR:vSphereReplication,vSphereReplication->IP address settings Subnet Mask
mgmt01esx01.sfo01.rainpole.local	172.16.16.101	255.255.255.0
mgmt01esx02.sfo01.rainpole.local	172.16.16.102	255.255.255.0
mgmt01esx03.sfo01.rainpole.local	172.16.16.103	255.255.255.0
mgmt01esx04.sfo01.rainpole.local	172.16.16.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VSAN:vsan->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VSAN:vsan->IP address settings Subnet Mask
mgmt01esx01.sfo01.rainpole.local	172.16.13.101	255.255.255.0
mgmt01esx02.sfo01.rainpole.local	172.16.13.102	255.255.255.0
mgmt01esx03.sfo01.rainpole.local	172.16.13.103	255.255.255.0
mgmt01esx04.sfo01.rainpole.local	172.16.13.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-vMotion:vmotion->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-vMotion:vmotion->IP address settings Subnet Mask
mgmt01esx01.sfo01.rainpole.local	172.16.12.101	255.255.255.0
mgmt01esx02.sfo01.rainpole.local	172.16.12.102	255.255.255.0
mgmt01esx03.sfo01.rainpole.local	172.16.12.103	255.255.255.0
mgmt01esx04.sfo01.rainpole.local	172.16.12.104	255.255.255.0

- f In the vSphere Web Client, on the **Host Profiles** page, click **SFO01-Mgmt01**, click the **Configure** tab and click the **Edit Host Customizations** button.
 - g On the **Select hosts** page, select all hosts and click **Next**.
 - h On the **Customize hosts** page, click the **Browse** button, locate the SF001-Mgmt01_host_customizations.csv file, click **Open** and click **Finish**.
- 5** Remediate the hosts in the management cluster.
- a On the **SFO01-Mgmt01** page, click the **Monitor** tab and click the **Compliance** tab.
 - b Click **SFO01-Mgmt01** in the **Host/Cluster** column and click **Check Host Profile Compliance**.
This compliance test shows that the first host is compliant, but the other hosts are not compliant.
 - c Click each of the non-compliant hosts, click **Remediate Hosts Based on its Host Profile**, and click **Finish** in the wizard that appears.
All hosts must have a **Compliant** status in the **Host Compliance** column.
- 6** Schedule nightly compliance checks.
- a On the **SFO01-Mgmt01** page, click the **Monitor** tab, and click the **Scheduled Tasks** tab.
 - b Select **Schedule a New Task > Check Host Profile Compliance**.
 - c In the **Check Host Profile Compliance (scheduled)** dialog box, click **Scheduling Options**.
 - d Enter **SFO01-Mgmt01 Compliance Check** in the **Task Name** text box.
 - e Click the **Change** button next to **Configured Scheduler**.

- f In the **Configure Scheduler** dialog box, select **Setup a recurring schedule for this action**, change the **Start time** to **10:00 PM**, and click **OK**.
- g Click **OK** in the **Check Host Profile Compliance (scheduled)** dialog box.

Upgrade the vSphere Distributed Switch in the Management Cluster in Region B

After you upgrade vCenter Server and ESXi in the management cluster in Region B, upgrade the vSphere Distributed Switch to use the new features of the switch in the latest release in the environment.

Prerequisites

Back up the configuration of the distributed switch. See the *VMware Validated Design Backup and Restore* documentation.

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 **Networking** and expand the **mgmt01vc51.lax01.rainpole.local** tree.
- 3 Right-click the **vDS-Mgmt** distributed switch and select **Upgrade > Upgrade Distributed Switch**. The **Upgrade Distributed Switch** wizard appears.
- 4 On the **Configure upgrade page**, select **Version 6.5.0** and click **Next**.
- 5 On the **Check compatibility** page, review host compatibility and click **Next**.
- 6 Review the upgrade configuration and click **Finish**.

Place the VMkernel Adapter for vSphere vMotion Traffic on a Separate TCP/IP Stack on the Management Hosts in Region B

To comply with the objective and deployment guidelines of this validated design, configure a template management host with a separate network for vSphere vMotion in Region B.

You create a VMkernel adapter for vSphere vMotion traffic on a management host in each region. You configure the VMkernel adapter with a static IP address and route the traffic to a network that is different from the network for the ESXi management. You transfer the vMotion networking configuration of the host to the management host profile in the region.

Table 4-12. vMotion Network Configuration of a Template Host After vSphere Upgrade

Region	Template Management Host	vMotion IP Address	vMotion Gateway
Region B	mgmt01esx51.lax01.rainpole.local	172.17.12.101	172.17.12.253

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 Delete the legacy VMkernel adapter for vSphere vMotion.

- a On the **Configure** tab, select **VMkernel adapters** again.
 - b Locate the VMkernel adapter with the following settings and click the **Remove selected network adapter** icon.
 - c On the Remove VMkernel Adapter dialog, click **OK**.

Setting	Value
Network Label	vDS-Mgmt-vMotion
IP Address	172.17.12.101
TCP/IP Stack	Default
vMotion	Enabled

- 3 Create a new vMotion VMkernel adapter on the vMotion TCP/IP stack on the mgmt01esx51.lax01.rainpole.local host.

- a In the **Navigator**, click **Host and Clusters** and expand the **mgmt01vc51.lax01.rainpole.local** tree.
 - b Click on **mgmt01esx51.lax01.rainpole.local**.
 - c Click the **Configure** tab, select **VMkernel adapters** under **Networking** and click the **Add host networking** icon.

The **Add Networking** wizard appears.

- d On the **Select connection type** page, select **VMkernel Network Adapter** and click **Next**.
 - e On the **Select target device** page, select **Select an existing network**, browse to select the **vDS-Mgmt-vMotion** port group, click **OK**, and click **Next**.

- f On the **Port properties** page, select **vMotion** from the **TCP/IP stack** drop-down menu and click **Next**.
 - g On the **IPv4 settings** page, select **Use static IPv4 settings** enter IP address **172.17.12.101** and subnet mask **255.255.255.0**, and click **Next**.
 - h Click **Finish**.
- 4 Configure the vMotion TCP/IP stack on the host.
- a On the **Configure** tab of the host object, click **TCP/IP configuration**.
 - b Select **vMotion** and click the **Edit TCP/IP Stack Configuration** icon.
 - c In the **Edit TCP/IP Stack Configuration** dialog box, click **Routing**, enter **172.17.12.253** in the **VMkernel gateway** text box, and click **OK**.

Configure the VM Swap Files as Sparse Objects on the vSAN Datastore in Region B

After you upgrade vCenter Server and the management ESXi hosts in the SDDC, turn on the vSAN Sparse Swap feature in Region B to save storage space by allocating space for VM swap files only when virtual machines are running.

You configure vSAN Sparse Swap only on the first host in the management cluster of the region. The configuration is applied to the other hosts in the cluster when you apply the host profiles that are extracted from the first host.

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 Expand the entire **mgmt01vc51.lax01.rainpole.local** vCenter Server tree, and select the **mgmt01esx51.lax01.rainpole.local** host.
- 4 Click the **Configure** tab, click **System > Advanced System Settings**.
- 5 Click the **Edit** button.
- 6 In the **filter** box, enter **vsan.swap** and wait for the search results.
- 7 Change the value of **VSAN.SwapThickProvisionDisabled** to **1** and click **OK**.

Create and Apply the Host Profile for the Management Cluster in Region B

After you upgrade the vSphere components, apply a host profile on the ESXi management hosts in Region B to ensure that they have the same 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 Create a host profile from the mgmt01esx51.lax01.rainpole.local host.

- a In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc51.lax01.rainpole.local** tree.
- b Right-click the ESXi host **mgmt01esx51.lax01.rainpole.local** and choose **Host Profiles > Extract Host Profile**.
- c In the **Extract Host Profile** window, enter **LAX01-Mgmt01** for the **Name** and click **Next**.
- d In the **Ready to complete** page, click **Finish**.

- 3 Attach the Host Profile to the management cluster.

- a In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc51.lax01.rainpole.local** tree.
- b Right-click on the **LAX01-Mgmt01** cluster and select **Host Profiles > Attach Host Profile**.
- c In the **Attach Host Profile** dialog box, click the **LAX01-Mgmt01** host profile, select the **Skip Host Customization** check box, and click **Finish**.

- 4 Export a host customizations file for the hosts in the management cluster.

- a Select **Home > Policies and Profiles** in the vSphere Web Client.
- b In the **Navigator**, click **Host Profiles**.
- c Right-click **LAX01-Mgmt01**, select **Export Host Customizations** and click **Save**.
- d Navigate to a file location to save the **LAX01-Mgmt01_host_customizations.csv** Excel file that is generated and click **Save**.

- e Edit the Excel file to include the following values.

ESXi Host	Active Directory Configuration Password	Active Directory Configuration Username	NetStack Instance defaultTcpipStack->DNS configuration Name for this host
mgmt01esx51.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	mgmt01esx51
mgmt01esx52.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	mgmt01esx52
mgmt01esx53.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	mgmt01esx53
mgmt01esx54.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	mgmt01esx54

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-Management:management->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-Management:management->IP address settings SubnetMask
mgmt01esx51.lax01.rainpole.local	172.17.11.101	255.255.255.0
mgmt01esx52.lax01.rainpole.local	172.17.11.102	255.255.255.0
mgmt01esx53.lax01.rainpole.local	172.17.11.103	255.255.255.0
mgmt01esx54.lax01.rainpole.local	172.17.11.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-NFS:<UNRESOLVED>->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-NFS:<UNRESOLVED>->IP address settings SubnetMask
mgmt01esx51.lax01.rainpole.local	172.17.15.101	255.255.255.0
mgmt01esx52.lax01.rainpole.local	172.17.15.102	255.255.255.0
mgmt01esx53.lax01.rainpole.local	172.17.15.103	255.255.255.0
mgmt01esx54.lax01.rainpole.local	172.17.15.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VR:vSphereReplication,vSphereReplicationNFC->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VR:vSphereReplication,vSphereReplication->IP address settings SubnetMask
mgmt01esx51.lax01.rainpole.local	172.17.16.101	255.255.255.0
mgmt01esx52.lax01.rainpole.local	172.17.16.102	255.255.255.0
mgmt01esx53.lax01.rainpole.local	172.17.16.103	255.255.255.0
mgmt01esx54.lax01.rainpole.local	172.17.16.104	255.255.255.0

	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VSAN:vsan->IP address settings	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VSAN:vsan->IP address settings
ESXi Host	Host IPv4 address	SubnetMask
mgmt01esx51.lax01.rainpole.local	172.17.13.101	255.255.255.0
mgmt01esx52.lax01.rainpole.local	172.17.13.102	255.255.255.0
mgmt01esx53.lax01.rainpole.local	172.17.13.103	255.255.255.0
mgmt01esx54.lax01.rainpole.local	172.17.13.104	255.255.255.0

	Host virtual NIC vDS-Mgmt:vDS-Mgmt-vMotion:vmotion->IP address settings	Host virtual NIC vDS-Mgmt:vDS-Mgmt-vMotion:vmotion->IP address settings
ESXi Host	Host IPv4 address	SubnetMask
mgmt01esx51.lax01.rainpole.local	172.17.12.101	255.255.255.0
mgmt01esx52.lax01.rainpole.local	172.17.12.102	255.255.255.0
mgmt01esx53.lax01.rainpole.local	172.17.12.103	255.255.255.0
mgmt01esx54.lax01.rainpole.local	172.17.12.104	255.255.255.0

- f In the vSphere Web Client, on the **Host Profiles** page, click **LAX01-Mgmt01**, click the **Configure** tab and click the **Edit Host Customizations** button.
- g On the **Select hosts** page, select all hosts and click **Next**.
- h On the **Customize hosts** page, click the **Browse** button, locate the LAX01-Mgmt01_host_customizations.csv file, click **Open**, and click **Finish**.

5 Remediate the hosts in the management cluster

- a On the **LAX01-Mgmt01** page, click the **Monitor** tab and click **Compliance** tab.
- b Click **LAX01-Mgmt01** in the **Host/Cluster** column and click the **Check Host Profile Compliance** button.

This compliance test shows that the first host is compliant, but the other hosts are not compliant.

- c Click each of the non-compliant hosts, click **Remediate Hosts Based on its Host Profile**, and click **Finish** in the wizard that appears.

All hosts must have a **Compliant** status in the **Host Compliance** column.

6 Schedule nightly compliance checks.

- a On the **LAX01-Mgmt01** page, click the **Monitor** tab, and click the **Scheduled Tasks** tab.
- b Select **Schedule a New Task > Check Host Profile Compliance**.
- c In the **Check Host Profile Compliance (scheduled)** dialog box, click **Scheduling Options**.
- d Enter **LAX01-Mgmt01 Compliance Check** in the **Task Name** text box.
- e Click the **Change** button next to **Configured Scheduler**.

- f In the **Configure Scheduler** dialog box, select **Setup a recurring schedule for this action**, change the **Start time** to **10:00 PM** and click **OK**.
- g Click **OK** in the **Check Host Profile Compliance (scheduled)** dialog box.

Upgrade the Components for the Shared Edge and Compute Cluster

After you upgrade the components that support the management cluster, you upgrade the components for the shared edge and compute cluster to complete the upgrade of the SDDC virtual infrastructure layer.

Procedure

1 Upgrade vSphere for the Shared Edge and Compute Cluster

When you upgrade the components that support the management cluster in the SDDC , you upgrade Compute Platform Services Controller and Compute vCenter Server in Region A and repeat this operation in Region B.

2 Post-Upgrade Configuration of the vCenter Server Components for the Shared Edge and Compute Cluster

After you upgrade the vCenter Server and Platform Services Controller instances for the shared edge and compute cluster, configure the environment according to the objectives and deployment guidelines of this validated design.

3 Upgrade the ESXi Hosts in the Shared Edge and Compute Cluster

To complete your upgrade of the shared edge and compute pod in the SDDC, update the shared edge and compute ESXi hosts in Region A and Region B.

4 Post-Upgrade Configuration of the Shared Edge and Compute ESXi Hosts

After you complete the upgrade of the vSphere shared edge and compute components, perform a final update of the configuration of vCenter Server and ESXi according to the objectives and deployment guidelines of this validated design

Upgrade vSphere for the Shared Edge and Compute Cluster

When you upgrade the components that support the management cluster in the SDDC , you upgrade Compute Platform Services Controller and Compute vCenter Server in Region A and repeat this operation in Region B.

Upgrading the VMware Validated Design vSphere layer for the shared edge and compute cluster is a multi-step operations in which you must upgrade the Compute Platform Services Controller and Compute vCenter Server in Region A before repeating this operation in Region B. This sequence ensures minimal compromise to your ability to provision within the SDDC.

Table 4-13. Compute vSphere and Disaster Recovery Nodes In the SDDC

Region	Role	IP Address	Fully Qualified Domain Name
Region A	Compute Platform Services Controller	172.16.11.63	comp01psc01.sfo01.rainpole.local
	Compute vCenter Server	172.16.11.64	comp01vc01.sfo01.rainpole.local
Region B	Compute Platform Services Controller	172.17.11.63	comp01psc51.lax01.rainpole.local
	Compute vCenter Server	172.17.11.64	comp01vc51.lax01.rainpole.local

Prerequisites

- Download the vCenter Server Appliance .iso file.
- Verify that vSphere DRS is set to Partially Automated for the duration of the upgrade operations.
- Verify that the static IP addresses 172.16.11.70 and 172.17.11.70 are available for use as the temporary network settings of the appliances.
- Ensure that any integration with the Compute vCenter Servers within environment has been quiesced of all activities, including but not limited to, users ordering new virtual machines with or without virtual wires via the vRealize Automation Cloud Management Platform (CMP), third-party integration that may automate the ordering or deployment of new virtual machines as well as administrators manually creating new virtual objects within the Compute vCenter Servers. Without quiescing the environment, rollback operations may be disrupted by generated orphaned objects. You might also have to extend the time of the maintenance windows.
- Create a snapshot of all Platform Services Controller appliances that you want to upgrade as a precaution in case of failure during the upgrade process.
- Create a snapshot of the Compute vCenter Server appliances that you want to upgrade as a precaution in case of failure during the upgrade process.
- Create a backup copy of all Platform Services Controllers and Compute vCenter Servers.
- See the *Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance* section of the *vSphere 6.5 Upgrade Guide* for additional guidance.

Procedure

- 1 [Upgrade the Shared Edge and Compute Platform Services Controller in Region A](#)
- 2 [Upgrade the Compute vCenter Server in Region A](#)
- 3 [Upgrade Shared Edge and Compute Platform Services Controller in Region B](#)
- 4 [Upgrade the Compute vCenter Server in Region B](#)

What to do next

- Verify that vCenter Server and Platform Services Controller function flawlessly after the upgrade. See *Validate Platform Services Controller and vCenter Server Instances* in the *VMware Validated Design Operational Verification* documentation.

Upgrade the Shared Edge and Compute Platform Services Controller in Region A

When you upgrade the vSphere components for the shared edge and compute pods in Region A and Region B, upgrade the Platform Services Controller instance first 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://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 Rename the virtual machine name of the comp01psc01.sfo01.rainpole.local appliance.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the mgmt01vc01.sfo01.rainpole.local control tree.
 - c Locate **comp01psc01.sfo01**
 - d Right-click on the virtual machine and select **Rename**.
 - e Update the name from **comp01psc01.sfo01** to **comp01psc01.sfo01_old** and click **OK**.
- 3 On the Windows host that has access to the data center, mount the vCenter Server Appliance installer .iso file, navigate to the vcsa-ui-installer\win32 directory, and run the **installer.exe** executable file.
- 4 On the **Home** page, click **Upgrade**.
- 5 Review the **Introduction** page to understand the upgrade process and click **Next**.
- 6 Read and accept the license agreement on the **End user license agreement** page, and click **Next**.

- 7 On the **Connect to source appliance** page, connect to the comp01psc01.sfo01.rainpole.local appliance to begin the upgrade and click **Next**.

- a In the **Source appliance** section, enter the following information about the source comp01psc01.sfo01.rainpole.local appliance

Setting	Value
Appliance FQDN or IP address	comp01psc01.sfo01.rainpole.local
Appliance HTTPS port	443
SSO user name	administrator@vsphere.local
SSO password	<i>vsphere_admin_password</i>
Appliance (OS) root password	<i>comppsc_root_password</i>

- b In the **ESXi host or vCenter Server that manages the source appliance** section, enter the information about Management vCenter Server instance on which the Platform Services Controller appliance resides.

Setting	Value
ESXi host or vCenter Server name	mgmt01vc01.sfo01.rainpole.local
HTTPS port	443
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 8 In the **Certificate Warning** dialog box, verify that the thumbprints match those used on comp01psc01.sfo01.rainpole.local and mgmt01vc01.sfo01.rainpole.local, and click **Yes**.
- 9 In the **Appliance deployment target** section, enter the connection settings of the Management vCenter Server for the deployment and click **Next**.

Setting	Value
ESXi host or vCenter Server name	mgmt01vc01.sfo01.rainpole.local
HTTPS port	443
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 10 In the **Certificate Warning** dialog box, click **Yes**.
- 11 On the **Select folder** page, navigate to **mgmt01vc01.sfo01.rainpole.local > SFO01 > Discovered virtual machines**, and click **Next**.
- 12 On the **Select compute resource** page, expand **SFO01 > SFO01-Mgmt01**, and click **Next**.

- 13 On the **Set up target appliance VM** page, enter the information about the Compute Platform Services Controller .

Setting	Value
VM name	comp01psc01
Root password	<i>comppsc_root_password</i>
Confirm root password	<i>comppsc_root_password</i>

- 14 On the **Select datastore** page, locate and select **SFO01A-VSAN01-MGMT01**, and click **Next**.
- 15 On the **Configure network settings** page, enter the temporary networking information to be used by the new Platform Services Controller appliance to perform the upgrade and click **Next**.
- From the **Network** drop-down menu, select **vDS-Mgmt-Management**.
 - In the **Temporary network settings** section, enter the temporary network configurations for the appliance.

Setting	Value
IP version	IPv4
IP assignment	static
Temporary IP address	172.16.11.70
Subnet mask or prefix length	24
Default gateway	172.16.11.1
DNS servers	172.16.11.5,172.16.11.4

- 16 On the **Ready to complete stage 1** page, verify that all of the settings are correct and click **Finish**.
- 17 Allow for the new Compute Platform Services Controller to be deployed.
- 18 After a successful deployment of the appliance, click **Continue**.
- 19 On the **Introduction** page, click **Next** and allow for the **Pre-upgrade checks** to automatically be performed.
- 20 On the **Configure CEIP** page, click the checkbox next to **Join the VMware's Customer Experience Improvement Program (CEIP)** and click **Next**.
- 21 On the **Ready to complete** page, click the checkbox next to **I have backed up the source Platform Services Controller and all the required data from the database** and click **Finish**.
- 22 On the **Shutdown Warning** page, click **OK** to initiate upgrade.
- 23 On the **Complete** page, click **Close**.
- 24 Allow for the Compute Platform Services Controller to be configured.

Upgrade the Compute vCenter Server in Region A

When you upgrade the vSphere components in Region A and Region B, after you complete the upgrade of the Compute Platform Services Controller instance in Region A, you upgrade the Compute vCenter Server 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://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 Rename the virtual machine name of the comp01vc01.sfo01.rainpole.local appliance
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the mgmt01vc01.sfo01.rainpole.local control tree.
 - c Locate **comp01vc01.sfo01**
 - d Right-click on the virtual machine and select **Rename**.
 - e Update the name from comp01vc01.sfo01 to **comp01vc01.sfo01_old** and click **OK**.
- 3 On the Windows host that has access to the data center, mount the vCenter Server Appliance installer .iso file, navigate to the vcsa-ui-installer\win32 directory, and run the **installer.exe** executable file.
- 4 On the **Home** page, click **Upgrade**.
- 5 Review the **Introduction** page to understand the upgrade process and click **Next**.
- 6 Read and accept the license agreement on the **End user license agreement** page, and click **Next**.

- 7 On the **Connect to source appliance** page, connect to the `comp01vc01.sfo01.rainpole.local` appliance to begin the upgrade and click **Next**.

- a In the **Source appliance** section, enter the following information about the source `comp01vc01.sfo01.rainpole.local` appliance

Setting	Value
Appliance FQDN or IP address	<code>comp01vc01.sfo01.rainpole.local</code>
Appliance HTTPS port	443
SSO user name	<code>administrator@vsphere.local</code>
SSO password	<code>vsphere_admin_password</code>
Appliance (OS) root password	<code>compvc_root_password</code>

- b In the **ESXi host or vCenter Server that manages the source appliance** section, enter the information about Management vCenter Server instance on which the Compute vCenter Server appliance resides.

Setting	Value
ESXi host or vCenter Server name	<code>mgmt01vc01.sfo01.rainpole.local</code>
HTTPS port	443
User name	<code>administrator@vsphere.local</code>
Password	<code>vsphere_admin_password</code>

- 8 In the **Certificate Warning** dialog box that appears, verify that the thumbprints match those used on `comp01vc01.sfo01.rainpole.local` and `mgmt01vc01.sfo01.rainpole.local`, and click **Yes**.

- 9 On the **Appliance deployment target** page, enter the connection settings of the Management vCenter Server for the deployment and click **Next**.

Setting	Value
ESXi host or vCenter Server name	<code>mgmt01vc01.sfo01.rainpole.local</code>
HTTPS port	443
User name	<code>administrator@vsphere.local</code>
Password	<code>vsphere_admin_password</code>

- 10 In the **Certificate Warning** dialog box, click **Yes**.
- 11 On the **Select folder** page, expand the **mgmt01vc01.sfo01.rainpole.local** control tree, expand **SFO01**, select **Discovered virtual machines**, and click **Next**.
- 12 On the **Select compute resource** page, expand **SFO01**, select **SFO01-Mgmt01**, and click **Next**.

- 13 On the **Set up target appliance VM** page, enter the following information about Compute vCenter Server and click **Next**.

Setting	Value
VM name	comp01vc01
Root password	<i>compvc_root_password</i>
Confirm root password	<i>compvc_root_password</i>

- 14 On the **Select Deployment Size** page, from the **Deployment size** drop-down menu, select **Large vCenter Server**.
- 15 On the **Select datastore** page, locate and select **SFO01A-VSAN01-MGMT01**, and click **Next**.
- 16 On the **Configure network settings** page, enter the temporary networking information for the new vCenter Server appliance during upgrade and click **Next**.
- From the **Network** drop-down menu, select **vDS-Mgmt-Management**.
 - In the **Temporary network settings** section, enter the temporary network configurations for the appliance

Setting	Value
IP version	IPv4
IP assignment	static
Temporary IP address	172.16.11.70
Subnet mask or prefix length	24
Default gateway	172.16.11.1
DNS servers	172.16.11.5,172.16.11.4

- 17 On the **Ready to complete stage 1** page, verify that all of the settings are correct and follow the information provided in the above steps and click **Finish**.
- 18 Allow for the new Compute vCenter Server to be deployed.
- 19 After a successful deployment of the appliance, click **Continue**.
- 20 On the **Introduction** page, click **Next** and allow for the **Pre-upgrade checks** to automatically be performed.

Note The **Pre-upgrade check result** page will return an expected warning about vCenter External Extensions related to NSX for vSphere and vRealize Operations Manager. Click **Close** in this dialog box.

- 21 On the **Select upgrade data** page, select **Configuration** and click **Next**.
- 22 On the **Ready to complete** page, select **I have backed up the source vCenter Server and all the required data from the database** and click **Finish**.
- 23 On the **Shutdown Warning** dialog box, click **OK** to initiate upgrade.

- 24 On the **Complete** page, click **Close**.
- 25 Allow for the Compute vCenter Server Appliance to be configured.
- 26 Exclude the new Compute vCenter Server from all distributed firewall rules to ensure that network access between vCenter Server and NSX is not blocked.
 - 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

 - c In the **Navigator**, click **Networking & Security**.
 - d Click **NSX Managers** and select the **172.16.11.65** instance.
 - e On the **Manage** tab, click **Exclusion List** and click **Add**.
 - f Add **comp01vc01** to the **Selected Objects** list, and click **OK**.

Upgrade Shared Edge and Compute Platform Services Controller in Region B

After you complete the upgrade of the vCenter Server and Platform Services Controller for the shared edge and compute in Region A, continue your upgrade of the VMware Validated Design vSphere layer by upgrading the Platform Services Controller instance 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	vsphere_admin_password
- 2 Rename the virtual machine name of the comp01psc51.lax01.rainpole.local appliance.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the mgmt01vc51.lax01.rainpole.local control tree.
 - c Locate **comp01psc51.lax01**.
 - d Right-click on the virtual machine and select **Rename**.
 - e Update the name from comp01psc51.lax01 to **comp01psc51.lax01_01d** and click **OK**.

- 3 On the Windows host that has access to the data center, mount the vCenter Server Appliance installer .iso file, navigate to the `vc5a-ui-installer\win32` directory, and run the **installer.exe** executable file.
- 4 On the **Home** page, click **Upgrade**.
- 5 Review the **Introduction** page to understand the upgrade process and click **Next**.
- 6 Read and accept the license agreement on the **End user license agreement** page, and click **Next**.
- 7 On the **Connect to source appliance** page, connect to the `comp01psc51.lax01.rainpole.local` appliance to begin the upgrade and click **Next**.

- a In the **Source appliance** section, enter the following information about the source `comp01psc51.lax01.rainpole.local` appliance

Setting	Value
Appliance FQDN or IP address	<code>comp01psc51.lax01.rainpole.local</code>
Appliance HTTPS port	443
SSO user name	<code>administrator@vsphere.local</code>
SSO password	<code>vsphere_admin_password</code>
Appliance (OS) root password	<code>comppsc_root_password</code>

- b In the **ESXi host or vCenter Server that manages the source appliance** section, enter the information about Management vCenter Server instance on which the Platform Services Controller appliance resides.

Setting	Value
ESXi host or vCenter Server name	<code>mgmt01vc51.lax01.rainpole.local</code>
HTTPS port	443
User name	<code>administrator@vsphere.local</code>
Password	<code>vsphere_admin_password</code>

- 8 In the **Certificate Warning** dialog box that appears, verify that the thumbprints match those used on `comp01psc51.lax01.rainpole.local` and `mgmt01vc51.lax01.rainpole.local`, and click **Yes**.
- 9 On the **Appliance deployment target** page, enter the connection settings to the Management vCenter Server and click **Next**.

Setting	Value
ESXi host or vCenter Server name	<code>mgmt01vc51.lax01.rainpole.local</code>
HTTPS port	443
User name	<code>administrator@vsphere.local</code>
Password	<code>vsphere_admin_password</code>

- 10 In the **Certificate Warning** dialog box, click **Yes**.

- 11 On the **Select folder** page, expand the **mgmt01vc51.lax01.rainpole.local** control tree, expand **LAX01**, select **Discovered virtual machines**, and click **Next**.
- 12 On the **Select compute resource** page, expand **LAX01**, select **LAX01-Mgmt01**, and click **Next**.
- 13 On the **Set up target appliance VM** page, enter the information about the Compute Platform Services Controller.

Setting	Value
VM name	comp01psc51
Root password	<i>comppsc_root_password</i>
Confirm root password	<i>comppsc_root_password</i>

- 14 On the **Select datastore** page, locate and select **LAX01A-VSAN01-MGMT01**, and click **Next**.
- 15 On the **Configure network settings** page, enter the temporary networking information to be used by the new Platform Services Controller appliance to perform the upgrade and click **Next**.
 - a From the **Network** drop-down menu, select **vDS-Mgmt-Management**.
 - b In the **Temporary network settings** section, enter the temporary network configurations for the appliance.

Setting	Value
IP version	IPv4
IP assignment	static
Temporary IP address	172.17.11.70
Subnet mask or prefix length	24
Default gateway	172.17.11.1
DNS servers	172.17.11.5,172.17.11.4

- 16 On the **Ready to complete stage 1** page, verify that all of the settings are correct and follow the information provided in the above steps and click **Finish**.
- 17 Allow for the new Compute Platform Services Controller to be deployed.
- 18 After a successful deployment of the appliance, click **Continue**.
- 19 On the **Introduction** page, click **Next** and allow for the **Pre-upgrade checks** to automatically be performed.
- 20 On the **Configure CEIP** page, select **Join the VMware's Customer Experience Improvement Program (CEIP)** and click **Next**.
- 21 On the **Ready to complete** page, select **I have backed up the source Platform Services Controller and all the required data from the database** and click **Finish**.
- 22 On the **Shutdown Warning** page, click **OK** to initiate upgrade.
- 23 On the **Complete** page, click **Close**.

- 24 Allow for the Compute Platform Services Controller Appliance to be configured.

Upgrade the Compute vCenter Server in Region B

When you upgrade the vSphere components in Region B, after you upgrade the Platform Services Controller instance, you upgrade the Compute vCenter Server 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	vsphere_admin_password

- 2 Rename the virtual machine name of the comp01vc51.lax01.rainpole.local appliance.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the mgmt01vc51.lax01.rainpole.local control tree.
 - c Locate **comp01vc51.lax01**
 - d Right-click the virtual machine and select **Rename**.
 - e Update the name from comp01vc51.lax01 to **comp01vc51.lax01_old** and click **OK**.
- 3 On the Windows host that has access to the data center, mount the vCenter Server Appliance installer .iso file, navigate to the vcsa-ui-installer\win32 directory, and run the **installer.exe** executable file.
- 4 On the **Home** page, click **Upgrade**.
- 5 Review the **Introduction** page to understand the upgrade process and click **Next**.
- 6 Read and accept the license agreement on the **End user license agreement** page, and click **Next**.

- 7 On the **Connect to source appliance** page, connect to the comp01vc51.lax01.rainpole.local appliance to begin the upgrade and click **Next**.

- a In the **Source appliance** section, enter the following information about the source comp01vc51.lax01.rainpole.local appliance

Setting	Value
Appliance FQDN or IP address	comp01vc51.lax01.rainpole.local
Appliance HTTPS port	443
SSO user name	administrator@vsphere.local
SSO password	vsphere_admin_password
Appliance (OS) root password	compvc_root_password

- b In the **ESXi host or vCenter Server that manages the source appliance** section, enter the information about Management vCenter Server instance on which the Compute vCenter Server appliance resides.

Setting	Value
ESXi host or vCenter Server name	mgmt01vc51.lax01.rainpole.local
HTTPS port	443
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 8 In the **Certificate Warning** dialog box that appears, verify that the thumbprints match those used on comp01vc51.lax01.rainpole.local and mgmt01vc51.lax01.rainpole.local, and click **Yes**.

- 9 On the **Appliance deployment target** page, enter the connection settings of the Management vCenter Server for the deployment and click **Next**.

Setting	Value
ESXi host or vCenter Server name	mgmt01vc51.lax01.rainpole.local
HTTPS port	443
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 10 On the **Certificate Warning** dialog, click **Yes**.
- 11 On the **Select folder** page, expand the **mgmt01vc51.lax01.rainpole.local** control tree, expand **LAX01**, select **Discovered virtual machines**, and click **Next**.
- 12 On the **Select compute resource** page, expand **LAX01**, select **LAX01-Mgmt01**, and click **Next**.

- 13 On the **Set up target appliance VM** page, enter the information about Compute vCenter Server and click **Next**.

Setting	Value
VM name	comp01vc51
Root password	<i>compvc_root_password</i>
Confirm root password	<i>compvc_root_password</i>

- 14 On the **Select Deployment Size** page, from the **Deployment size** drop-down menu, select **Large vCenter Server**.
- 15 On the **Select datastore** page, locate and select **LAX01A-VSAN01-MGMT01**, and click **Next**.
- 16 On the **Configure network settings** page, enter the temporary networking information to be used by the new vCenter Server appliance to perform the upgrade and click **Next**.
- From the **Network** drop-down menu, select **vDS-Mgmt-Management**.
 - In the **Temporary network settings** section, enter the temporary network configurations for the appliance

Setting	Value
IP version	IPv4
IP assignment	static
Temporary IP address	172.17.11.70
Subnet mask or prefix length	24
Default gateway	172.17.11.1
DNS servers	172.17.11.5,172.17.11.4

- 17 On the **Ready to complete stage 1** page, verify that all of the settings are correct and follow the information provided in the above steps and click **Finish**.
- 18 Allow for the new Compute vCenter Server to be deployed.
- 19 After a successful deployment of the appliance, click **Continue**.
- 20 On the **Introduction** page, click **Next** and allow for the **Pre-upgrade checks** to automatically be performed.

Note The **Pre-upgrade check result** page will return an expected warning about vCenter External Extensions related to NSX for vSphere and vRealize Operations Manager. Click **Close** in this message.

- 21 On the **Select upgrade data** page, select **Configuration** and click **Next**.
- 22 On the **Ready to complete** page, select **I have backed up the source vCenter Server and all the required data from the database** and click **Finish**.
- 23 In the **Shutdown Warning** dialog box, click **OK** to initiate upgrade.

24 On the **Complete** page, click **Close**.

25 Allow for the Compute vCenter Server Appliance to be configured.

Now, exclude the new compute vCenter Server from all of your distributed firewall rules. This ensures that network access between vCenter Server and NSX is not blocked.

26 Exclude the new Compute vCenter Server from all distributed firewall rules to ensure that network access between vCenter Server and NSX is not blocked.

- 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

- c In the **Navigator**, click **Networking & Security**.
- d Click **NSX Managers** and select the **172.17.11.65** instance.
- e On the **Manage** tab, click **Exclusion List** and click **Add**.
- f Add **comp01vc51** to the **Selected Objects** list, and click **OK**.

Post-Upgrade Configuration of the vCenter Server Components for the Shared Edge and Compute Cluster

After you upgrade the vCenter Server and Platform Services Controller instances for the shared edge and compute cluster, configure the environment according to the objectives and deployment guidelines of this validated design.

Procedure

1 Change Admission Control in the Shared Edge and Compute Cluster in Region A

After you upgrade vSphere, change the admission control of the shared edge and compute cluster in Region A to use the number of hosts to tolerate setting according to this validated design.

2 Change the Memory Reservation of the NSX Resource Pools in the Shared Edge and Compute Cluster in Region A

After you complete the upgrade of the vSphere management components, increase the memory reservation of the NSX Edge resource pools in the shared edge and compute clusters in Region A according to the objectives and design guidelines of this validated design.

3 Register Again vRealize Operations Manager with the Compute vCenter Server Instances

After you upgrade the Compute vCenter Server instances, re-register vRealize Operations Manager with each vCenter Server instances to use health badges on inventory objects in vSphere Web Client.

4 [Update Scheduled Backup Jobs for the Compute vCenter Server Instance in Region A](#)

After upgrading the vCenter Server and Platform Services Controller to the latest version of vSphere, new virtual machines are deployed. You must update the scheduled backup job in Region A for full image backup of the Compute vCenter Server and the connected external Platform Services Controller.

5 [Place Compute vCenter Server and Platform Services Controller in a VM and Templates Folder in Region A](#)

In Region A, place the Compute vCenter Server and the connected Platform Services Controller in a virtual machine folder that is dedicated to the vCenter Server and Platform Services Controller virtual machines.

6 [Use the UMDS Shared Repository as the Download Source in Update Manager for the Shared Edge and Compute Cluster in Region A](#)

After you upgrade vCenter Server and Platform Services Controller instances for the shared edge and compute cluster, configure Update Manager in Region A to use the UMDS shared repository as a source for downloading ESXi patches, extensions, and notifications on the hosts in the shared edge and compute cluster.

7 [Configure the Compute vCenter Server to Forward Log Events to vRealize Log Insight in Region A](#)

You can configure the Compute vCenter Server and connected Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster in Region A. You can then view and analyze all syslog information in the vRealize Log Insight Web interface.

8 [Change Admission Control in the Shared Edge and Compute Cluster in Region B](#)

After you upgrade vSphere, change the admission control of the shared edge and compute cluster in Region B to use the number of hosts to tolerate setting according to this validated design.

9 [Change the Memory Reservation of the NSX Resource Pool in the Shared Edge and Compute Cluster in Region B](#)

After you complete the upgrade of the vSphere management components, increase the memory reservation of the NSX Edge resource pools in the shared edge and compute cluster in Region B according to the objectives and design guidelines of this validated design.

10 [Update Scheduled Backup Jobs for the Compute vCenter Server Instance in Region B](#)

After upgrading the vCenter Server and Platform Services Controller to the latest version of vSphere, new virtual machines are deployed. You must update the scheduled backup job in Region B for full image backup of the Compute vCenter Server and the connected external Platform Services Controller.

11 [Place Compute vCenter Server and Platform Services Controller in a VM and Templates Folder in Region B](#)

In Region B, place the Compute vCenter Server and the connected Platform Services Controller in a virtual machine folder that is dedicated to the vCenter Server and Platform Services Controller virtual machines.

12 Use the UMDS Shared Repository as the Download Source in Update Manager for the Shared Edge and Compute Cluster in Region B

After you upgrade vCenter Server and Platform Services Controller instances for the shared edge and compute cluster, configure Update Manager in Region B to use the UMDS shared repository as a source for downloading ESXi patches, extensions, and notifications on the hosts in the shared edge and compute cluster.

13 Configure the Compute vCenter Server to Forward Log Events to vRealize Log Insight in Region B

You can configure the Compute vCenter Server and connected Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster in Region B. You can then view and analyze all syslog information in the vRealize Log Insight web interface.

Change Admission Control in the Shared Edge and Compute Cluster in Region A

After you upgrade vSphere, change the admission control of the shared edge and compute cluster in Region A to use the number of hosts to tolerate setting according to this validated design.

vSphere 6.5 or later introduces an admission control policy that directly uses a number of host failures to tolerate to adjust the CPU and memory resources for virtual machine availability in the cluster.

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://comp01vc01.sfo01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator, click **Host and Clusters**.
 - a Expand the **comp01vc01.sfo01.rainpole.local** inventory.
 - b Select the **SFO01-Comp01** cluster under the **SFO01** data center.
- 3 Click the **Configure** tab and click **vSphere Availability**.
- 4 Click **Edit**.
- 5 In the **Edit Cluster Settings** dialog box, click **Admission Control** under **vSphere Availability**, enter the following settings and click **OK**.

Setting	Value
Host failures cluster tolerates	1
Define host failover capacity by	Cluster resource percentage

Setting	Value
Override calculated failover capacity	Deselected
Performance degradation VMs tolerate	100%

Change the Memory Reservation of the NSX Resource Pools in the Shared Edge and Compute Cluster in Region A

After you complete the upgrade of the vSphere management components, increase the memory reservation of the NSX Edge resource pools in the shared edge and compute clusters in Region A according to the objectives and design guidelines of this validated design.

Table 4-14. NSX Edge Resource Pools That You Update After Upgrade

Region	vCenter Server Cluster Pool
Region A	comp01vc01.sfo01.rainpole.local > SFO01 > SFO01-Comp01 > SDDC-EdgeRP01

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to <https://comp01vc01.sfo01.rainpole.local/vsphere-client>.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Hosts and Clusters** and expand the entire **comp01vc01.sfo01.rainpole.local** tree.
- 3 Right-click the **SDDC-EdgeRP01** resource pool and select **Edit Resource Settings**.
- 4 In the **Edit Resource Settings** dialog box, change the memory reservation from 15 GB to 16 GB and click **OK**.

Setting	Value
Name	SDDC-EdgeRP01
CPU-Shares	High
CPU-Reservation	0
CPU-Reservation Type	Expandable selected
CPU-Limit	Unlimited
Memory-Shares	Normal
Memory-Reservation	16 GB

Setting	Value
Memory-Reservation type	Expandable selected
Memory-Limit	Unlimited

Register Again vRealize Operations Manager with the Compute vCenter Server Instances

After you upgrade the Compute vCenter Server instances, re-register vRealize Operations Manager with each vCenter Server instances to use health badges on inventory objects in vSphere Web Client.

Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.
- 3 On the **Solutions** page, select **VMware vSphere** from the solution table, and click **Configure**.
- 4 Register again the vCenter Adapters for the Compute vCenter Server instances.
 - a In the **Manage Solution** dialog box, under **Instance Settings**, select the vCenter Adapter instance.

Region	vCenter Server	Display Name
Region A	comp01vc01.sfo01.rainpole.local	comp01vc01-sfo01
Region B	comp01vc51.lax01.rainpole.local	comp01vc51-lax01

- b Click **Manage Registrations**.
 - c Specify a user account with administrator privileges to re-register vRealize Operations Manager with the vCenter Server instance.

Setting	Value
Registration user	administrator@vsphere.local
Registration Password	vsphere_admin_password

- d Click **Register** and click **OK** in the informational dialog box that appears.
 - e Click **Save Settings** and click **OK** in the informational dialog box that appears.
 - f Repeat these steps to re-register vRealize Operations Manager with the Compute vCenter Server in Region B.

- 5 In the **Manage Solution - VMware vSphere** dialog box, click **Close**.

Update Scheduled Backup Jobs for the Compute vCenter Server Instance in Region A

After upgrading the vCenter Server and Platform Services Controller to the latest version of vSphere, new virtual machines are deployed. You must update the scheduled backup job in Region A for full image backup of the Compute vCenter Server and the connected external Platform Services Controller.

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 On the vSphere Web Client **Home** page, click the **VDP** icon.
- 3 On the **Welcome to vSphere Data Protection** page, select **mgmt01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.
- 4 Click the **Backup** tab.
- 5 Locate and update the backup job **Management and Compute vCenter Server Backups** to include the new Compute vCenter Server and Platform Services Controller instances in Region A.
 - a Click on the backup job **Management and Compute vCenter Server Backups**
 - b From the **Backup job actions** menu, select **Edit** to run the **Edit backup job** wizard.
 - c On the **Data Type** page, select **Full Image**, leave the **Fall back to the non-quiesced backup if quiescence fails** check box selected, and click **Next**.
 - d On the **Backup Sources** page, fully expand the **Virtual Machines** tree.

Object	Value
vCenter Server	mgmt01vc01.sfo01.rainpole.local
Data center	SFO01
Cluster	SFO01-Mgmt01

- e Locate the obsolete Compute vCenter Server and Platform Services Controller virtual machines, and deselect them.

Obsolete Object	VM Name
Compute Platform Services Controller	comp01psc01.sfo01_old
Compute vCenter Server	comp01vc01.sfo01_old

- f Select the new virtual appliances for Compute vCenter Server and the Platform Services Controller.

Object	VM Name
Compute Platform Services Controller	comp01psc01
Compute vCenter Server	comp01vc01

- g Verify the following the virtual appliances for vCenter Server and the Platform Services Controller in Region A have been selected, and click **Next**.

Object	VM Name
Management Platform Services Controller	mgmt01psc01
Management vCenter Server	mgmt01vc01
Compute Platform Services Controller	comp01psc01
Compute vCenter Server	comp01vc01

- h On the **Schedule** page, leave **Backup Schedule** to **Daily** and click **Next**.
- i On the **Retention Policy** page, leave **Keep** to **for 3 days** and click **Next**.
- j On the **Job Name** page, leave **Management and Compute vCenter Server Backups** as a name for the backup job and click **Next**.
- k On the **Ready to Complete** page, review the summary information for the backup job and click **Finish**.
- l In the dialog box that shows a confirmation that the job is created, click **OK**.

Place Compute vCenter Server and Platform Services Controller in a VM and Templates Folder in Region A

In Region A, place the Compute vCenter Server and the connected Platform Services Controller in a virtual machine folder that is dedicated to the vCenter Server and Platform Services Controller virtual machines.

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 Move the vCenter Server and Platform Services Controller virtual machines to the MGMT01 folder.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **mgmt01vc01.sfo01.rainpole.local** tree.
 - c Expand the **Discovered virtual machines** folder.
 - d Drag the **comp01vc01** and **comp01psc01** virtual machines and drop them in the MGMT01 folder.

Use the UMDS Shared Repository as the Download Source in Update Manager for the Shared Edge and Compute Cluster in Region A

After you upgrade vCenter Server and Platform Services Controller instances for the shared edge and compute cluster, configure Update Manager in Region A to use the UMDS shared repository as a source for downloading ESXi patches, extensions, and notifications on the hosts in the shared edge and compute cluster.

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://comp01vc01.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 **Home** page of the vSphere Web Client, click the **Update Manager** icon.
- 3 From the **Objects** tab, click the **comp01vc01.sfo01.rainpole.local** vCenter Server for Region A.
The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.
- 4 On the **Manage** tab, click **Settings** and select **Download Settings**.

- 5 On the **Download sources** page, click **Edit**.

An **Edit Download Sources** dialog box opens.

- 6 Enter the following setting and click **OK**.

Setting	Value
Use a shared repository	Selected
URL	http://mgmt01umds01.sfo01.rainpole.local

The vSphere Web Client performs validation of the URL.

- 7 On the **Download sources** page, click **Download Now** to run the download patch definitions.

Configure the Compute vCenter Server to Forward Log Events to vRealize Log Insight in Region A

You can configure the Compute vCenter Server and connected Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster in Region A. You can then view and analyze all syslog information in the vRealize Log Insight Web interface.

In Region A, you configure the following vCenter Server and Platform Services Controller instances:

Region	Appliance Type	Appliance Management Interface URL	vRealize Log Insight Syslog Host
Region A	vCenter Server instances	https://comp01vc01.sfo01.rainpole.local:5480	vrli-cluster-01.sfo01.rainpole.local
	Platform Services Controller instances	https://comp01psc01.sfo01.rainpole.local:5480	vrli-cluster-01.sfo01.rainpole.local

Procedure

- 1 Redirect the log events from the appliance to vRealize Log Insight.
 - a Open a Web browser and go to **https://comp01vc01.sfo01.rainpole.local:5480**.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	compvc_root_password

- c In the **Navigator**, click **Syslog Configuration**.

- d On the **Syslog Configuration** page, click **Edit**, configure the following settings, and click **OK**.

Setting	Value
Common Log Level	*
Remote Syslog Host	vrli-cluster-01.sfo01.rainpole.local
Remote Syslog Port	514
Remote Syslog Protocol	UDP

- e Repeat the steps for the Platform Services Controller appliance.
- 2 Verify that the appliances are forwarding their syslog traffic to vRealize Log Insight.
- a Open a Web browser and go to **`https://vrli-cluster-01.sfo01.rainpole.local`**.
- b Log in using the following credentials.

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

- c In the vRealize Log Insight user interface, click **Dashboards** and select **VMware - vSphere** from the content pack dashboard drop-down menu.
- d Verify that the vCenter Server and Platform Services Controller nodes are presented on the **All vSphere events by hostname** widget of the **General Overview** dashboard.

Change Admission Control in the Shared Edge and Compute Cluster in Region B

After you upgrade vSphere, change the admission control of the shared edge and compute cluster in Region B to use the number of hosts to tolerate setting according to this validated design.

vSphere 6.5 or later introduces an admission control policy that directly uses a number of host failures to tolerate to adjust the CPU and memory resources for virtual machine availability in the cluster.

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://comp01vc51.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 **Host and Clusters**.
 - a Expand the **comp01vc51.lax01.rainpole.local** inventory.
 - b Select the **LAX01-Comp01** cluster under the **LAX01** data center.
- 3 Click the **Configure** tab and click **vSphere Availability**.
- 4 Click **Edit**.
- 5 In the **Edit Cluster Settings** dialog box, click **Admission Control** under **vSphere Availability**, enter the following settings and click **OK**.

Setting	Value
Host failures cluster tolerates	1
Define host failover capacity by	Cluster resource percentage
Override calculated failover capacity	Deselected
Performance degradation VMs tolerate	100%

Change the Memory Reservation of the NSX Resource Pool in the Shared Edge and Compute Cluster in Region B

After you complete the upgrade of the vSphere management components, increase the memory reservation of the NSX Edge resource pools in the shared edge and compute cluster in Region B according to the objectives and design guidelines of this validated design.

Table 4-15. NSX Edge Resource Pools That You Update After Upgrade

Region	vCenter Server Cluster Pool
Region B	comp01vc51.lax01.rainpole.local > LAX01 > LAX01-Comp01 > SDDC-EdgeRP01

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://comp01vc51.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 expand the entire **comp01vc51.lax01.rainpole.local** tree.
- 3 Right-click the **SDDC-EdgeRP01** resource pool and select **Edit Resource Settings**.
- 4 In the **Edit Resource Settings** dialog box, change the memory reservation from 15 GB to 16 GB and click **OK**.

Setting	Value
Name	SDDC-EdgeRP01
CPU-Shares	High
CPU-Reservation	0
CPU-Reservation Type	Expandable selected
CPU-Limit	Unlimited
Memory-Shares	Normal
Memory-Reservation	16 GB
Memory-Reservation type	Expandable selected
Memory-Limit	Unlimited

Update Scheduled Backup Jobs for the Compute vCenter Server Instance in Region B

After upgrading the vCenter Server and Platform Services Controller to the latest version of vSphere, new virtual machines are deployed. You must update the scheduled backup job in Region B for full image backup of the Compute vCenter Server and the connected external Platform Services Controller.

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 On the vSphere Web Client **Home** page, click the **VDP** icon.
- 3 On the **Welcome to vSphere Data Protection** page, select **mgmt01vdp51** from the **VDP Appliance** drop-down menu and click **Connect**.
- 4 Click the **Backup** tab.
- 5 Locate and update the backup job **Management and Compute vCenter Server Backups** to include the new Compute vCenter Server and Platform Services Controller instances in Region B.
 - a Click on the backup job **Management and Compute vCenter Server Backups**.
 - b From the **Backup job actions** menu, select **Edit** to run the **Edit backup job** wizard.
 - c On the **Data Type** page, select **Full Image**, leave the **Fall back to the non-quieted backup if quiescence fails** check box selected, and click **Next**.
 - d On the **Backup Sources** page, fully expand the **Virtual Machines** tree.

Object	Value
vCenter Server	mgmt01vc51.lax01.rainpole.local
Data center	LAX01
Cluster	LAX01-Mgmt01

- e Locate the obsolete Compute vCenter Server and Platform Services Controller virtual machines, and deselect them.

Obsolete Object	VM Name
Compute Platform Services Controller	comp01psc51.lax01_old
Compute vCenter Server	comp01vc51.lax01_old

- f Select the new virtual appliances for Compute vCenter Server and the Platform Services Controller.

Object	VM Name
Compute Platform Services Controller	comp01psc51
Compute vCenter Server	comp01vc51

- g Verify the following the virtual appliances for vCenter Server and the Platform Services Controller in Region B have been selected, and click **Next**.

Object	VM Name
Management Platform Services Controller	mgmt01psc51
Management vCenter Server	mgmt01vc51
Compute Platform Services Controller	comp01psc51
Compute vCenter Server	comp01vc51

- h On the **Schedule** page, leave **Backup Schedule** to **Daily** and click **Next**.
- i On the **Retention Policy** page, leave **Keep** to **for 3 days** and click **Next**.
- j On the **Job Name** page, leave **Management and Compute vCenter Server Backups** as a name for the backup job and click **Next**.
- k On the **Ready to Complete** page, review the summary information for the backup job and click **Finish**.
- l In the dialog box that shows a confirmation that the job is created, click **OK**.

Place Compute vCenter Server and Platform Services Controller in a VM and Templates Folder in Region B

In Region B, place the Compute vCenter Server and the connected Platform Services Controller in a virtual machine folder that is dedicated to the vCenter Server and Platform Services Controller virtual machines.

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 Move the vCenter Server and Platform Services Controller virtual machines to the MGMT51 folder.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **mgmt01vc51.lax01.rainpole.local** tree.
 - c Expand the **Discovered virtual machines** folder.
 - d Drag the **comp01vc51** and **comp01psc51** virtual machines and drop them in the MGMT51 folder.

Use the UMDS Shared Repository as the Download Source in Update Manager for the Shared Edge and Compute Cluster in Region B

After you upgrade vCenter Server and Platform Services Controller instances for the shared edge and compute cluster, configure Update Manager in Region B to use the UMDS shared repository as a source for downloading ESXi patches, extensions, and notifications on the hosts in the shared edge and compute cluster.

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://comp01vc51.lax01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 On the **Home** page of the vSphere Web Client, click the **Update Manager** icon.
- 3 From the **Objects** tab, click the **comp01vc51.lax01.rainpole.local** vCenter Server for Region B.
The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.
- 4 On the **Manage** tab, click **Settings** and select **Download Settings**.
- 5 On the **Download sources** page, click **Edit**.
An **Edit Download Sources** dialog box opens.
- 6 Enter the following setting and click **OK**.

Setting	Value
Use a shared repository	Selected
URL	<code>http://mgmt01umds51.lax01.rainpole.local</code>

The vSphere Web Client performs validation of the URL.

- 7 On the **Download sources** page, click **Download Now** to run the download patch definitions.

Configure the Compute vCenter Server to Forward Log Events to vRealize Log Insight in Region B

You can configure the Compute vCenter Server and connected Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster in Region B. You can then view and analyze all syslog information in the vRealize Log Insight web interface.

In Region B, you configure the following vCenter Server and Platform Services Controller instances:

Region	Appliance Type	Appliance Management Interface URL	vRealize Log Insight Syslog Host
Region B	vCenter Server instances	https://comp01vc51.lax01.rainpole.local:5480	vrli-cluster-51.lax01.rainpole.local
	Platform Services Controller instances	https://comp01psc51.lax01.rainpole.local:5480	vrli-cluster-51.lax01.rainpole.local

Procedure

- 1 Redirect the log events from the appliance to vRealize Log Insight.

- a Open a Web browser and go to the following URI.
https://comp01vc51.lax01.rainpole.local:5480.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	compvc_root_password

- c In the **Navigator**, click **Syslog Configuration**.
- d On the **Syslog Configuration** page, click **Edit**, configure the following settings, and click **OK**.

Setting	Value
Common Log Level	*
Remote Syslog Host	vrli-cluster-51.lax01.rainpole.local
Remote Syslog Port	514
Remote Syslog Protocol	UDP

- e Repeat the steps for the Platform Services Controller appliance.

- 2 Verify that the appliances are forwarding their syslog traffic to vRealize Log Insight.

- a Open a Web browser and go to **https://vrli-cluster-51.lax01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- c In the vRealize Log Insight user interface, click **Dashboards** and select **VMware - vSphere** from the content pack dashboard drop-down menu.
- d Verify that the vCenter Server and Platform Services Controller nodes are presented on the **All vSphere events by hostname** widget of the **General Overview** dashboard.

Upgrade the ESXi Hosts in the Shared Edge and Compute Cluster

To complete your upgrade of the shared edge and compute pod in the SDDC, update the shared edge and compute ESXi hosts in Region A and Region B.

Upgrading the Compute ESXi hosts when using NSX for vSphere is a multi-step operations in which you must download the NSX for vSphere VIBs, slipstream the NSX for vSphere VIBs into the ESXi 6.5 image, and use vSphere Update Manager to automate a cluster-wide upgrade operation on each of the clusters.

Table 4-16. Compute ESXi hosts In the SDDC

Region	Cluster Name	IP Address	Fully Qualified Domain Name
Region A	SFO01-Comp01	172.16.31.101	comp01esx01.sfo01.rainpole.local
		172.16.31.102	comp01esx02.sfo01.rainpole.local
		172.16.31.103	comp01esx03.sfo01.rainpole.local
		172.16.31.104	comp01esx04.sfo01.rainpole.local
Region B	LAX01-Comp01	172.17.31.101	comp01esx51.lax01.rainpole.local
		172.17.31.102	comp01esx52.lax01.rainpole.local
		172.17.31.103	comp01esx53.lax01.rainpole.local
		172.17.31.104	comp01esx54.lax01.rainpole.local

Prerequisites

- Make sure that the system hardware complies with ESXi requirements by consulting [VMware Compatibility Guide](#). Check for system compatibility, I/O compatibility with network and host bus adapter (HBA) cards, storage compatibility, and backup software compatibility.
- Ensure the firmware for the network and host bus adapter (HBA) cards have been updated for compatibility.
- Ensure the BIOS for the ESXi hosts are updated for compatibility.
- Ensure that sufficient disk space is available on the host for the upgrade.
- Ensure that vSphere DRS is set to Fully Automated for the duration of the upgrade operations to allow for compute workloads to be evacuated from hosts as the are upgraded.
- Download the ESXi 6.5 .iso file

What to do next

- Verify that the shared edge and compute ESXi host function flawlessly after the upgrade. See *Validate ESXi Hosts* in the *VMware Validated Design Operational Verification* documentation.

Use Image Builder to Create an ESXi 6.5 Image with NSX for vSphere VIBs for the Shared Edge and Compute Cluster in Region A

Using the new Image Builder service included in vSphere 6.5, insert the NSX for vSphere VIBs from the NSX Manager 6.3.x in an ESXi image for Region A.

Using the Image Builder service to insert the NSX for vSphere 6.3.x VIBs in to an ESXi image allows for a stream-lined operation for upgrading the hosts within a cluster. By using this method, additional preparation via NSX Manager for the ESXi hosts is not needed, which greatly expedites the upgrade time window by allowing vSphere Update Manager to automate a cluster-wide upgrade.

Procedure

- 1 Download the NSX for vSphere VIBs from the Region A NSX Manager.

- a Open a Web browser and go to **`https://comp01nsxm01.sfo01.rainpole.local/bin/vdn/nwfabric.properties`**
- b Locate the vSphere 6.5 section.

```
...
# 6.5 VDN EAM Info
VDN_VIB_PATH.3=/bin/vdn/vibs-6.3.1/6.5-5124743/vxlan.zip
VDN_VIB_VERSION.3=5124743
VDN_HOST_PRODUCT_LINE.3=embeddedEsx
VDN_HOST_VERSION.3=6.5.*
...
```

- c Append the VDN_VIB_PATH.3 line to the URL in your browser to download the NSX for vSphere VIBs from **`https://comp01nsxm01.sfo01.rainpole.local/bin/vdn/vibs-6.3.1/6.5-5124743/vxlan.zip`**

- 2 Log in to the Compute vCenter Server by using the vSphere Web Client.

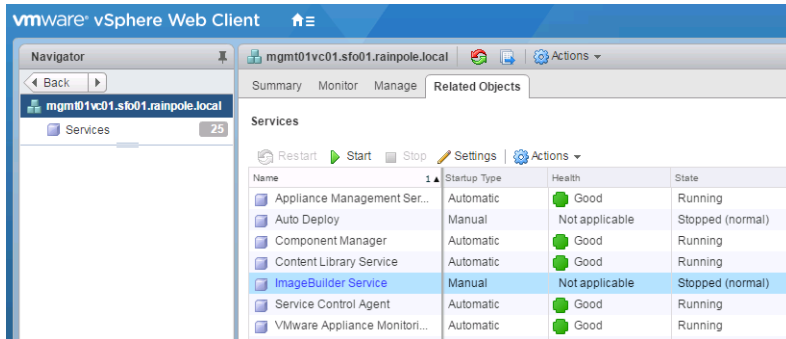
- a Open a Web browser and go to **`https://comp01vc01.sfo01.rainpole.local/vsphere-client`**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 3 Start the Image Builder service on vCenter Server.

- a From the **Home** page, under the **Administration** section, click **System Configuration**.
- b In the **Navigator** pane, click **Nodes**.

- c Under **Nodes**, click **comp01vc01.sfo01.rainpole.local** and click **Related Objects**.
- d Locate ImageBuilder Service and click **Start**.



- 4 Log out and then log back in to the vSphere Web Client to re-load the Image Builder plug-in.
- 5 Create an image depot for the VMware Validated Design ESXi Image .
 - a From the **Home** page, click **Auto Deploy**.
 - b Select **comp01vc01.sfo01.rainpole.local** from the **vCenter Server** drop-down menu.
 - c In the **Auto Deploy** pane, click the **Software Depots** tab and click **Add Software Depot**.
 - d In the **Add Software Depot** dialog box, provide the following settings.

Setting	Value
Select the type of depot you want to create:	Custom Depot
Name	VVD ESXi 6.5 Upgrade

- 6 Upload the NSX for vSphere 6.3.x VIBs to Image Builder for slipstreaming.
 - a From the **Home** page, click **Auto Deploy**.
 - b In the **Auto Deploy** pane, click the **Software Depots** tab and click **Import Software Depot**.
 - c In the **Import Software Depot** dialog box, click **Browse**, locate the vxlan.zip file from [Step 1](#) and provide the following settings.

Setting	Value
Name	NSX 6.3.1 VIBs
File	<i>path_to_vxlan.zip</i>

- d Click **Upload**.
- 7 Upload the ESXi 6.5 image to Image Builder for slipstreaming.
 - a From the **Home** page, click **Auto Deploy**.
 - b In the **Auto Deploy** pane, click the **Software Depots** tab and click **Import Software Depot**.

- c In the **Import Software Depot** dialog box, click **Browser**, locate the ESXi 6.5a offline depot .zip file and provide the following configuration.

Setting	Value
Name	ESXi 6.5a
File	<i>path_to_ESXi65_Offline_Depot.zip</i>

- d Click **Upload**.

- 8 Create a slipstreaming ESXi 6.5 image with the NSX for vSphere VIBs.

- a From the **Home** page, click **Auto Deploy**.
- b In the **Auto Deploy** pane, click the **Software Depots** tab.
- c In the left **Software Depots** pane, click **ESXi 6.5a**.
- d In the right **Software Depots** pane, click **ESXi-6.5.0-<Release Date>-standard**, and click the **Clone.** icon.
- e On the **Name and details** page of the **Clone Image Profile** wizard, provide the following and click **Next**.

Setting	Value
Name	VVD ESXi 6.5a with NSX 6.3.1 VIBs
Vendor	VMware Validated Design
Description	VMware Validated Design 4.0 upgrade ISO for ESXi 6.5a with NSX 6.3.1 VIBs
Software depot	VVD ESXi 6.5 Upgrade

- f On the **2 Select software packages** page, enter the following configuration and click **Next**.

Setting	Value
Acceptance Level	VMware certified
Software depot	NSX 6.3.1 VIBs
Available	<i>all vibs in the software depot</i>

- g On the **Ready to complete** page, review the settings and click **Finish**.

The VMware ESXi 6.5 Standard ISO with the NSX for vSphere VIBs has 125 software packages. If you use a vendor-specific ESXi 6.5 image, the software package number might vary.

- 9 Export the ESXi 6.5 image with NSX 6.3.1 VIBs.

- a From the **Home** page, click **Auto Deploy**.
- b In the **Auto Deploy** pane, click the **Software Depots** tab
- c In the left **Software Depots** pane, click the **VVD ESXi 6.5 Upgrade** depot.
- d In the right **Software Depots** pane, click **VVD ESXi 6.5a with NSX 6.3.1 VIBs** and click **Export Image Profile**.

- e In the **Export Image Profile** dialog box, select **ISO - Generate a bootable ISO image from the image profile** and click **Generate Image**.
- f After the image has been generated, click **Download Image**.

An ISO file named VVD ESXi 6.5a with NSX 6.3.1 VIBs.iso will be downloaded to your workstation.

Use vSphere Update Manager to Remediate ESXi Shared Edge and Compute Cluster in Region A

After creating a slipstreamed ESXi 6.5a with NSX 6.3.1 VIBs, upload the image to vSphere Update Manager on the Compute vCenter Servers in Region A. Then use this image to remediate the shared edge and compute clusters.

Procedure

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

- a Open a Web browser and go to **https://comp01vc01.sfo01.rainpole.local/vsphere-client**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Upload the slipstreamed ESXi image to the vSphere Update Manager.
 - a From the **Home** page of the vSphere Web Client, under the **Operations and Policies** section, click **Update Manager**.
 - b In **Servers** pane, click **comp01vc01.sfo01.rainpole.local**.
 - c In the right pane, click the **Manage** tab, select **ESXi Images** and click **Import ESXi Image**.
 - d In the **Import ESXi Image** dialog box, click **Browse** and locate the VVD ESXi 6.5a with NSX 6.3.1 VIBs.iso.
 - e Once the image has been successfully imported, click **Close**.
- 3 Create a baseline for your VMware Validated Design ESXi image.
 - a On the **Manage** tab, select **Host Baselines** and click the **New Baseline** icon.
 - b In the **New Baseline** dialog box, provide the following settings and click **Next**.

Setting	Value
Name	VMware Validated Design ESXi 6.5a Upgrade
Description	--
Baseline type	Host Upgrade

- c In the **ESXi Image** section, click the **VVD ESXi 6.5a with NSX 6.3.1 VIBs** image from the list and click **Next**.
 - d In the **Ready to complete** section, click **Finish** to complete making the baseline.
- 4 Attaching the new VMware Validated Design ESXi 6.5a upgrade baseline to your compute cluster.
- a On the **Host Baseline** tab, click the **Go to compliance view** button to go to the comp01vc01.sfo01.rainpole.local vCenter Server and to SFO01-Comp01 cluster.
 - b On the **Update Manager** tab, click **Attach Baseline**.
 - c In the **Attach Baseline or Baseline Group** dialog box, under **Upgrade Baselines**, select **VMware Validated Design ESXi 6.5a Upgrade** baseline.
 - d Click **OK** to set the baseline.
- 5 Scan the cluster for updates against the new baseline.
- a On the **Update Manager** tab, click **Scan for Updates**.
 - b In the **Scan for Updates** dialog box, under the **Scan hosts for** section, select only the **Upgrades** check box and click **OK**.
- After the scan is complete, the cluster reports back as Non-Compliant.
- 6 Remediate the cluster and upgrade to vSphere 6.5.
- a On the **Update Manager** tab, click **Remediate**.
 - b In the **Remediate** dialog box, under **Baseline Groups and Types**, select the baseline **VMware Validated Design ESXi 6.5a Upgrade** and click **Next**.
 - c On the **Select target objects** section, select all of the compute hosts in the cluster and click **Next**.
 - d On the **EULA** section, select **I accept the terms and license agreement** and click **Next**.
 - e On the **Advanced options** section, click **Next**.
 - f On the **Host remediation options** section, deselect **Retry entering maintenance mode in case of failure** and click **Next**.
 - g On the **Cluster remediation options** section, select the following options and click **Next**.

Options	
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters	Selected
Disable High Availability admission control if it is enabled for any of the selected clusters	Selected
Enable parallel remediation for the hosts in the selected clusters > Automatically determine the maximum number of concurrently remediated hosts in a cluster	Selected
Migrate powered off and suspended VMs to other hosts in the cluster, if a host must enter maintenance mode	Selected

- h In the **Ready to complete** section, click **Pre-check Remediation** to generate a pre-upgrade report of any identifiable problems that would prevent a successful upgrade.

Note Address any items reported in the **Pre-check Remediation** dialog box before proceeding with the upgrade. Click **OK** to close the screen. Ignore Disable HA admission control message from the recommended changes.

- i After you address all pre-check items, click **Finish** to begin the upgrade.
- 7 Review the NSX for vSphere status of the management clusters.
- a Select **Home > Networking & Security**.
 - b Select Installation in the **Navigator**.
 - c On the **Host Preparation** tab, select **172.16.11.66** from the **NSX Manager** drop-down menu and verify that **Installation Status** for all shared edge and compute ESXi hosts is green.

Use the Image Builder to Create an ESXi 6.5 Image with NSX for vSphere VIBs for the Shared Edge and Compute Cluster in Region B

Using the new Image Builder service included in vSphere 6.5, insert the NSX for vSphere VIBs from the NSX Manager 6.3.x in an ESXi image for Region B.

Using the Image Builder service to insert the NSX for vSphere 6.3.x VIBs in to an ESXi image allows for a stream-lined operation for upgrading the hosts within a cluster. By using this method, additional preparation via NSX Manager for the ESXi hosts is not needed, which greatly expedites the upgrade time window by allowing vSphere Update Manager to automate a cluster-wide upgrade.

Procedure

- 1 Download the NSX for vSphere VIBs from the Region B NSX Manager.
 - a Open a Web browser and go to
`https://comp01nsxm51.lax01.rainpole.local/bin/vdn/nwfabric.properties`
 - b Locate the vSphere 6.5 section.

```
...
# 6.5 VDN EAM Info
VDN_VIB_PATH.3=/bin/vdn/vibs-6.3.1/6.5-5124743/vxlan.zip
VDN_VIB_VERSION.3=5124743
VDN_HOST_PRODUCT_LINE.3=embeddedEsx
VDN_HOST_VERSION.3=6.5.*
...
```

- c Append the VDN_VIB_PATH.3 line to the URL in your browser to download the NSX for vSphere VIBs from
`https://comp01nsxm51.lax01.rainpole.local/bin/vdn/vibs-6.3.1/6.5-5124743/vxlan.zip`

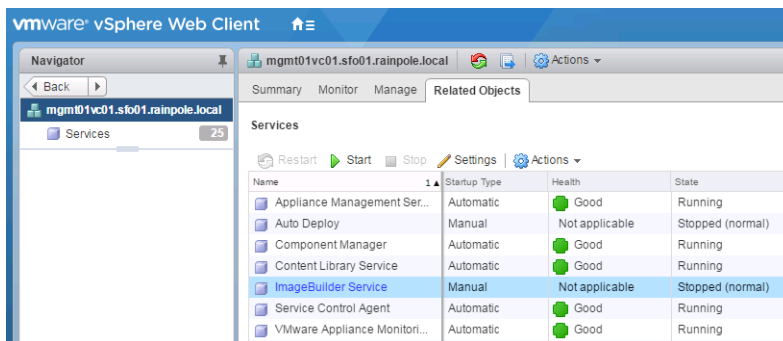
- 2 Log in to the Compute vCenter Server by using the vSphere Web Client.

- a Open a Web browser and go to **https://comp01vc51.lax01.rainpole.local/vsphere-client**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 3 Start the Image Builder service on vCenter Server.

- a From the **Home** page, under the **Administration** section, click **System Configuration**.
- b In the **Navigator** pane, click **Nodes**.
- c Under **Nodes**, click **comp01vc51.lax01.rainpole.local** and click **Related Objects**.
- d Locate ImageBuilder Service and click **Start**.



- 4 Log out and log back in to the vSphere Web Client to re-load the Image Builder plug-in.
- 5 Create an image depot for the VMware Validated Design ESXi Image .
 - a From the **Home** page, click **Auto Deploy**.
 - b Select **comp01vc51.lax01.rainpole.local** from the **vCenter Server** drop-down menu.
 - c In the **Auto Deploy** pane, click the **Software Depots** tab and click **Add Software Depot**.
 - d In the **Add Software Depot** dialog box, provide the following settings.

Setting	Value
Select the type of depot you want to create:	Custom Depot
Name	VVD ESXi 6.5 Upgrade

- 6 Upload the NSX for vSphere 6.3.x VIBs to Image Builder for slipstreaming.
 - a From the **Home** page, click **Auto Deploy**.
 - b In the **Auto Deploy** pane, click the **Software Depots** tab and click **Import Software Depot**.

- c In the **Import Software Depot** dialog box, click **Browse**, locate the `vxlan.zip` file from [Step 1](#) and provide the following settings.

Setting	Value
Name	NSX 6.3.1 VIBs
File	<i>path_to_vxlan.zip</i>

- d Click **Upload**.

7 Upload the ESXi 6.5 image to the Image Builder for slipstreaming.

- a From the **Home** page, click **Auto Deploy**.
- b In the **Auto Deploy** pane, click the **Software Depots** tab and click **Import Software Depot**.
- c In the **Import Software Depot** dialog box, click **Browse**, locate the ESXi 6.5a offline depot .zip file and provide the following configuration.

Setting	Value
Name	ESXi 6.5a
File	<i>path_to_ESXi65_Offline_Depot.zip</i>

- d Click **Upload**.

8 Create a slipstreaming ESXi 6.5 image with the NSX for vSphere VIBs.

- a From the **Home** page, click **Auto Deploy**.
- b In the **Auto Deploy** pane, click the **Software Depots** tab.
- c In the left **Software Depots** pane, click **ESXi 6.5a**.
- d In the right **Software Depots** pane, click **ESXi-6.5.0-<Release Date>-standard**, and click the **Clone** icon.
- e On the **Name and details** page of the **Clone Image Profile** wizard, provide the following and click **Next**.

Setting	Value
Name	VVD ESXi 6.5a with NSX 6.3.1 VIBs
Vendor	VMware Validated Design
Description	VMware Validated Design 4.0 upgrade ISO for ESXi 6.5a with NSX 6.3.1 VIBs
Software depot	VVD ESXi 6.5 Upgrade

- f On the **2 Select software packages** page, enter the following configuration and click **Next**.

Setting	Value
Acceptance Level	VMware certified
Software depot	NSX 6.3.1 VIBs
Available	<input type="checkbox"/> esx-vsip <input type="checkbox"/> esx-vxlan

- g On the **Ready to complete** page, review the settings and click **Finish**.

The VMware ESXi 6.5 Standard ISO with the NSX for vSphere VIBs has 125 software packages. If you use a vendor-specific ESXi 6.5 image, the software package number might vary.

- 9 Export the ESXi 6.5 image with NSX 6.3.1 VIBs.

- a From the **Home** page, click **Auto Deploy**.
- b In the **Auto Deploy** pane, click the **Software Depots** tab
- c In the left **Software Depots** pane, click the **VVD ESXi 6.5 Upgrade** depot.
- d In the right **Software Depots** pane, click **VVD ESXi 6.5a with NSX 6.3.1 VIBs** and click **Export Image Profile**.
- e In the **Export Image Profile** dialog box, select **ISO - Generate a bootable ISO image from the image profile** and click **Generate Image**.
- f After the image has been generated, click **Download Image**.

An ISO file named VVD ESXi 6.5a with NSX 6.3.1 VIBs.iso will be downloaded to your workstation.

Use vSphere Update Manager to Remediate the ESXi Hosts in the Shared Edge and Compute Cluster in Region B

After creating a slipstreamed ESXi 6.5a with NSX 6.3.1 VIBs, upload the image to vSphere Update Manager on the Compute vCenter Server in Region B. Then use this image to remediate the shared edge and compute clusters.

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://comp01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Upload the slipstreamed ESXi image to the vSphere Update Manager.
 - a From the **Home** page of the vSphere Web Client, under the **Operations and Policies** section, click **Update Manager**.
 - b In **Servers** pane, click **comp01vc51.lax01.rainpole.local**.
 - c In the right pane, click the **Manage** tab, select **ESXi Images** and click **Import ESXi Image**.
 - d In the **Import ESXi Image** dialog box, click **Browse** and locate the VVD ESXi 6.5a with NSX 6.3.1 VIBs.iso.
 - e Once the image has been successfully imported, click **Close**.

- 3 Create a baseline for your VMware Validated Design ESXi image.

- a On the **Manage** tab, select **Host Baselines** and click the **New Baseline** icon.
- b In the **New Baseline** dialog box, provide the following settings and click **Next**.

Setting	Value
Name	VMware Validated Design ESXi 6.5a Upgrade
Description	--
Baseline type	Host Upgrade

- c In the **ESXi Image** section, click the **VVD ESXi 6.5a with NSX 6.3.1 VIBs** image from the list and click **Next**.
 - d In the **Ready to complete** section, click **Finish** to complete making the baseline.
- 4 Attaching the new VMware Validated Design ESXi 6.5a Upgrade Baseline to your compute cluster.
 - a On the **Host Baseline** tab, click the **Go to compliance view** button to go to the comp01vc51.lax01.rainpole.local vCenter Server and to LAX01-Comp01 cluster.
 - b On the **Update Manager** tab, click **Attach Baseline**.
 - c In the **Attach Baseline or Baseline Group** dialog box, under **Upgrade Baselines**, select **VMware Validated Design ESXi 6.5a Upgrade** baseline.
 - d Click **OK** to set the baseline.
 - 5 Scan the cluster for updates against the new baseline.
 - a On the **Update Manager** tab, click **Scan for Updates**.
 - b In the **Scan for Updates** dialog box, under the **Scan hosts for** section, select only the **Upgrades** checkbox and click **OK**.

After the scan is complete, the cluster reports back as Non-Compliant.

6 Remediate the cluster and upgrade to vSphere 6.5.

- a On the **Update Manager** tab, click **Remediate**.
- b In the **Remediate** dialog box, under **Baseline Groups and Types**, select the baseline **VMware Validated Design ESXi 6.5a Upgrade** and click **Next**.
- c On the **Select target objects** section, select all of the compute hosts in the cluster and click **Next**.
- d On the **EULA** section, select **I accept the terms and license agreement** and click **Next**.
- e On the **Advanced options** section, click **Next**.
- f On the **Host remediation options** section, deselect **Retry entering maintenance mode in case of failure** and click **Next**.
- g On the **Cluster remediation options** section, select the following options and click **Next**.

Options	
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters	Selected
Disable High Availability admission control if it is enabled for any of the selected clusters	Selected
Enable parallel remediation for the hosts in the selected clusters > Automatically determine the maximum number of concurrently remediated hosts in a cluster	Selected
Migrate powered off and suspended VMs to other hosts in the cluster, if a host must enter maintenance mode	Selected

- h In the **Ready to complete** section, click **Pre-check Remediation** to generate a pre-upgrade report of any identifiable problems that would prevent a successful upgrade.

Note Address any items reported in the **Pre-check Remediation** dialog box before proceeding with the upgrade. Click **OK** to close the screen. Ignore Disable HA admission control message from the recommended changes.

- i After you address all pre-check items, click **Finish** to begin the upgrade.

7 Review the NSX for vSphere status of the management clusters.

- a Select **Home > Networking & Security**.
- b Select **Installation** in the **Navigator**.
- c On the **Host Preparation** tab, select **172.17.11.66** from the **NSX Manager** drop-down menu and verify that **Installation Status** for all shared edge and compute ESXi hosts is green.

Post-Upgrade Configuration of the Shared Edge and Compute ESXi Hosts

After you complete the upgrade of the vSphere shared edge and compute components, perform a final update of the configuration of vCenter Server and ESXi according to the objectives and deployment guidelines of this validated design

Procedure

1 Upgrade the vSphere Distributed Switch in the Shared Edge and Compute Cluster in Region A

After you upgrade vCenter Server and ESXi in the shared edge and compute clusters in Region A and Region B, upgrade the vSphere Distributed Switch in Region A to install the new features of switch in the latest release in the environment.

2 Place the VMkernel Adapter for vSphere vMotion Traffic on a Separate TCP/IP Stack on the Compute Hosts in Region A

To comply with the objective and deployment guidelines of this validated design, configure a template compute host with a separate network for vSphere vMotion in Region A.

3 Create and Apply the Host Profile for the Shared Edge and Compute Cluster in Region A

After you upgrade the vSphere components in the shared edge and compute cluster, use a host profile for the ESXi hosts in Region A to ensure that they have the same configuration.

4 Upgrade the vSphere Distributed Switch in the Shared Edge and Compute Cluster in Region B

After you upgrade vCenter Server and ESXi in the shared edge and compute clusters in Region A and Region B, upgrade the vSphere Distributed Switch in Region B to install the new features of switch in the latest release in the environment.

5 Place the VMkernel Adapter for vSphere vMotion Traffic on a Separate TCP/IP Stack on the Compute Hosts in Region B

To comply with the objective and deployment guidelines of this validated design, configure a template compute host with a separate network for vSphere vMotion in Region B.

6 Create and Apply the Host Profile for the Shared Edge and Compute Cluster in Region B

After you upgrade the vSphere components in the shared edge and compute cluster, use a host profile for the ESXi hosts in Region B to ensure that they have the same configuration.

Upgrade the vSphere Distributed Switch in the Shared Edge and Compute Cluster in Region A

After you upgrade vCenter Server and ESXi in the shared edge and compute clusters in Region A and Region B, upgrade the vSphere Distributed Switch in Region A to install the new features of switch in the latest release in the environment.

Prerequisites

Back up the configuration of the distributed switch. See the *VMware Validated Design Backup and Restore* documentation.

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://comp01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Networking** and expand the **comp01vc01.sfo01.rainpole.local** tree.
- 3 Right-click the **vDS-Comp01** distributed switch and select **Upgrade > Upgrade Distributed Switch**.
The **Upgrade Distributed Switch** wizard appears.
- 4 On the **Configure upgrade page**, click **Next**.
- 5 On the **Check compatibility** page, review host compatibility and click **Next**.
- 6 Review the upgrade configuration and click **Finish**.

Place the VMkernel Adapter for vSphere vMotion Traffic on a Separate TCP/IP Stack on the Compute Hosts in Region A

To comply with the objective and deployment guidelines of this validated design, configure a template compute host with a separate network for vSphere vMotion in Region A.

You create a VMkernel adapter for vSphere vMotion traffic on a compute host in each region. You configure the VMkernel adapter with a static IP address and route the traffic to a network that is different from the network for ESXi management. You transfer the vMotion networking configuration of the host to the compute host profile in the region.

Table 4-17. vMotion Network Configuration of a Template Host After vSphere Upgrade

Region	Template Compute Host	vMotion IP Address	vMotion Gateway
Region A	comp01esx01.sfo01.rainpole.local	172.16.32.101	172.16.32.253

Procedure

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

- a Open a Web browser and go to **https://comp01vc01.sfo01.rainpole.local/vsphere-client**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Delete the legacy VMkernel adapter for vSphere vMotion.

- a In the **Navigator**, click **Host and Clusters** and expand the **comp01vc01.sfo01.rainpole.local** tree.
- b Click on **comp01esx01.sfo01.rainpole.local**.
- c On the **Configure** tab, select **VMkernel adapters** under **Networking**.
- d Locate the VMkernel adapter with the following settings and click the **Remove selected network adapter** icon.

Setting	Value
Network Label	vDS-Comp01-vMotion
IP Address	172.16.32.101
TCP/IP Stack	Default
vMotion	Enabled

- e On the **Remove VMkernel Adapter** dialog, click **OK**.

- 3 Create a new vMotion VMkernel adapter on the vMotion TCP/IP stack on the comp01esx01.sfo01.rainpole.local host.

- a On the **Configure** tab, select **VMkernel adapters** under **Networking** and click the **Add host networking** icon.

The **Add Networking** wizard appears.

- b On the **Select connection type** page, select **VMkernel Network Adapter** and click **Next**.
- c On the **Select target device** page, select **Select an existing network**, browse to select the **vDS-Comp01-vMotion** port group, click **OK**, and click **Next**.
- d On the **Port properties** page, select **vMotion** from the **TCP/IP stack** drop-down menu and click **Next**.
- e On the **IPv4 settings** page, select **Use static IPv4 settings** enter IP address **172.16.32.101** and subnet mask **255.255.255.0**, and click **Next**.
- f Click **Finish**.

- 4 Configure the vMotion TCP/IP stack on the host.
 - a On the **Configure** tab of the host object, click **TCP/IP configuration**.
 - b Select **vMotion** and click the **Edit TCP/IP Stack Configuration** icon.
 - c In the **Edit TCP/IP Stack Configuration** dialog box, click **Routing**, enter **172.16.32.253** in the **VMkernel gateway** text box, and click **OK**.

Create and Apply the Host Profile for the Shared Edge and Compute Cluster in Region A

After you upgrade the vSphere components in the shared edge and compute cluster, use a host profile for the ESXi hosts in Region A to ensure that they have the same configuration.

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://comp01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password
- 2 Create the host profile from the comp01esx01.sfo01.rainpole.local host.
 - a In the **Navigator**, select **Hosts and Clusters** and expand the **comp01vc01.sfo01.rainpole.local** tree.
 - b Right-click the ESXi host **comp01esx01.sfo01.rainpole.local** and select **Host Profiles > Extract Host Profile...**
 - c In the **Extract Host Profile** window, enter **SFO01-Comp01** as the name of the host profile and click **Next**.
 - d In the **Ready to complete** window, click **Finish**.
- 3 Attach the host profile to the shared edge and compute cluster.
 - a In the **Navigator**, select **Hosts and Clusters** and expand the **comp01vc01.sfo01.rainpole.local** tree.
 - b Right-click on the **SFO01-Comp01** cluster and select **Host Profiles > Attach Host Profile...**
 - c In the **Attach Host Profile** dialog box, select the **SFO01-Comp01** host profile, select the **Skip Host Customization** checkbox, and click **Finish**.
- 4 Export a host customizations file for the hosts in the shared edge and compute cluster.
 - a Select **Home > Policies and Profiles** in the vSphere Web Client.
 - b In the **Navigator**, click **Host Profiles**.

- c Right-click **SF001-Comp01**, select **Export Host Customizations** and click **Save**.
- d Navigate to a file location to store the SF001-Comp01_host_customizations.csv Excel file that is generated and click **Save**.

- e Edit the Excel file to include the following values.

ESXi Host	Active Directory Configuration Password	Active Directory Configuration Username	NetStack Instance defaultTcpipStack->DNS configuration Name for this host
comp01esx01.sfo01.rainpole.local	ad_admin_password	ad_admin_acct@sfo01.rainpole.local	comp01esx01
comp01esx02.sfo01.rainpole.local	ad_admin_password	ad_admin_acct@sfo01.rainpole.local	comp01esx02
comp01esx03.sfo01.rainpole.local	ad_admin_password	ad_admin_acct@sfo01.rainpole.local	comp01esx03
comp01esx04.sfo01.rainpole.local	ad_admin_password	ad_admin_acct@sfo01.rainpole.local	comp01esx04

ESXi Host	Host virtual NIC vDS-Comp01:vDS-Comp01-Management:management->IP address settings IPv4 address	Host virtual NIC vDS-Comp01:vDS-Comp01-Management:management->IP address settings Subnet Mask
comp01esx01.sfo01.rainpole.local	172.16.31.101	255.255.255.0
comp01esx02.sfo01.rainpole.local	172.16.31.102	255.255.255.0
comp01esx03.sfo01.rainpole.local	172.16.31.103	255.255.255.0
comp01esx04.sfo01.rainpole.local	172.16.31.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Comp01:vDS-Comp01-NFS:<UNRESOLVED>->IP address settings IPv4 address	Host virtual NIC vDS-Comp01:vDS-Comp01-Management:management->IP address settings Subnet Mask
comp01esx01.sfo01.rainpole.local	172.16.25.101	255.255.255.0
comp01esx02.sfo01.rainpole.local	172.16.25.102	255.255.255.0
comp01esx03.sfo01.rainpole.local	172.16.25.103	255.255.255.0
comp01esx04.sfo01.rainpole.local	172.16.25.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Comp01:vDS-Comp01-vMotion:vmotion->IP address settings IPv4 address	Host virtual NIC vDS-Comp01:vDS-Comp01-vMotion:vmotion->IP address settings Subnet Mask
comp01esx01.sfo01.rainpole.local	172.16.32.101	255.255.255.0
comp01esx02.sfo01.rainpole.local	172.16.32.102	255.255.255.0
comp01esx03.sfo01.rainpole.local	172.16.32.103	255.255.255.0
comp01esx04.sfo01.rainpole.local	172.16.32.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Comp01:vDS-Comp01-VSAN:vsan->IP address settings	Host virtual NIC vDS-Comp01:vDS-Comp01-VSAN:vsan->IP address settings
	IPv4 address	Subnet Mask
comp01esx01.sfo01.rainpole.local	172.16.33.101	255.255.255.0
comp01esx02.sfo01.rainpole.local	172.16.33.102	255.255.255.0
comp01esx03.sfo01.rainpole.local	172.16.33.103	255.255.255.0
comp01esx04.sfo01.rainpole.local	172.16.33.104	255.255.255.0

ESXi Host	NetStack Instance vmotion->DNS configuration	NetStack Instance vxlan->DNS configuration
	Name for this host	Name for this host
comp01esx01.sfo01.rainpole.local	comp01esx01	comp01esx01
comp01esx02.sfo01.rainpole.local	comp01esx02	comp01esx02
comp01esx03.sfo01.rainpole.local	comp01esx03	comp01esx03
comp01esx04.sfo01.rainpole.local	comp01esx04	comp01esx04

- f In the vSphere Web Client, on the **Host Profiles** page, click **SFO01-Comp01**, click the **Configure** tab and click the **Edit Host Customizations** button.
 - g On the **Select hosts** page, select all hosts and click **Next**.
 - h On the **Customize hosts** page, click the **Browse** button, locate the SF001-Comp01_host_customizations.csv file, click **Open** and click **Finish**.
- 5** Remediate the hosts in the shared edge and compute cluster.
- a On the **SFO01-Comp01** page, click the **Monitor** tab and click **Compliance** tab.
 - b Click **SFO01-Comp01** in the **Host/Cluster** column and click **Check Host Profile Compliance** icon.
- This compliance test shows that the first host is compliant, but the other hosts are not compliant.
- c Click each of the non-compliant hosts, click **Remediate host based on its host profile** icon and click **Finish** in the wizard that appears.
- All hosts must have a **Compliant** status in the **Host Compliance** column.
- 6** Schedule nightly compliance checks.
- a On the **SFO01-Comp01** page, click the **Monitor** tab, and click the **Scheduled Tasks** tab.
 - b Select **Schedule a New Task > Check Host Profile Compliance**.
 - c In the **Check Host Profile Compliance (scheduled)** dialog box, click **Scheduling Options**.
 - d Enter **SFO01-Comp01 Compliance Check** in the **Task name** text box.
 - e Click the **Change** button next to **Configured Scheduler**.

- f In the **Configure Scheduler** dialog box, select **Setup a recurring schedule for this action**, change the **Start time** to **10:00 PM**, and click **OK**.
- g Click **OK** in the **Check Host Profile Compliance (scheduled)** dialog box.

Upgrade the vSphere Distributed Switch in the Shared Edge and Compute Cluster in Region B

After you upgrade vCenter Server and ESXi in the shared edge and compute clusters in Region A and Region B, upgrade the vSphere Distributed Switch in Region B to install the new features of switch in the latest release in the environment.

Prerequisites

Back up the configuration of the distributed switch. See the *VMware Validated Design Backup and Restore* documentation.

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://comp01vc51.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 **Networking** and expand the **comp01vc51.lax01.rainpole.local** tree.
- 3 Right-click the **vDS-Comp01** distributed switch and select **Upgrade > Upgrade Distributed Switch**. The **Upgrade Distributed Switch** wizard appears.
- 4 On the **Configure upgrade page**, click **Next**.
- 5 On the **Check compatibility** page, review host compatibility and click **Next**.
- 6 Review the upgrade configuration and click **Finish**.

Place the VMkernel Adapter for vSphere vMotion Traffic on a Separate TCP/IP Stack on the Compute Hosts in Region B

To comply with the objective and deployment guidelines of this validated design, configure a template compute host with a separate network for vSphere vMotion in Region B.

You create a VMkernel adapter for vSphere vMotion traffic on a compute host in each region. You configure the VMkernel adapter with a static IP address and route the traffic to a network that is different from the network for ESXi management. You transfer the vMotion networking configuration of the host to the compute host profile in the region.

Table 4-18. vMotion Network Configuration of a Template Host After vSphere Upgrade

Region	Template Compute Host	vMotion IP Address	vMotion Gateway
Region B	comp01esx51.lax01.rainpole.local	172.17.32.101	172.17.32.253

Procedure

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

- a Open a Web browser and go to **https://comp01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Delete the legacy VMkernel adapter for vSphere vMotion.

- a In the **Navigator**, click **Host and Clusters** and expand the **comp01vc51.lax01.rainpole.local** tree.
 - b Click on **comp01esx51.lax01.rainpole.local**.
 - c On the **Configure** tab, select **VMkernel adapters** under **Networking**.
 - d Locate the VMkernel adapter with the following settings and click the **Remove selected network adapter** icon.

Setting	Value
Network Label	vDS-Comp01-vMotion
IP Address	172.17.32.101
TCP/IP Stack	Default
vMotion	Enabled

- e On the **Remove VMkernel Adapter** dialog, click **OK**.

- 3 Create a new vMotion VMkernel adapter on the vMotion TCP/IP stack on the comp01esx51.lax01.rainpole.local host.

- a On the **Configure** tab, select **VMkernel adapters** under **Networking** and click the **Add host networking** icon.

The **Add Networking** wizard appears.

- b On the **Select connection type** page, select **VMkernel Network Adapter** and click **Next**.
 - c On the **Select target device** page, select **Select an existing network**, browse to select the **vDS-Comp01-vMotion** port group, click **OK**, and click **Next**.

- d On the **Port properties** page, select **vMotion** from the **TCP/IP stack** drop-down menu and click **Next**.
 - e On the **IPv4 settings** page, select **Use static IPv4 settings** enter IP address **172.17.32.101** and subnet mask **255.255.255.0**, and click **Next**.
 - f Click **Finish**.
- 4 Configure the vMotion TCP/IP stack on the host.
- a On the **Configure** tab of the host object, click **TCP/IP configuration**.
 - b Select **vMotion** and click the **Edit TCP/IP Stack Configuration** icon.
 - c In the **Edit TCP/IP Stack Configuration** dialog box, click **Routing**, enter **172.17.32.253** in the **VMkernel gateway** text box, and click **OK**.

Create and Apply the Host Profile for the Shared Edge and Compute Cluster in Region B

After you upgrade the vSphere components in the shared edge and compute cluster, use a host profile for the ESXi hosts in Region B to ensure that they have the same configuration.

Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://comp01vc51.lax01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a host profile from the comp01esx51.lax01.rainpole.local host.
 - a In the **Navigator**, select **Hosts and Clusters** and expand the **comp01vc51.lax01.rainpole.local** tree.
 - b Right-click **comp01esx51.lax01.rainpole.local** and select **Host Profiles > Extract Host Profile**.
 - c In the **Extract Host Profile** window, enter **LAX01-Comp01** as the name of the host profile and click **Next**.
 - d On the **Ready to complete** page, click **Finish**.

- 3 Attach the host profile to the shared edge and compute cluster.
 - a In the **Navigator**, select **Hosts and Clusters** and expand the **comp01vc51.lax01.rainpole.local** tree.
 - b Right-click the **LAX01-Comp01** cluster, and select **Host Profiles > Attach Host Profile**.
 - c In the **Attach Host Profile** dialog box, click **LAX01-Comp01**, select the **Skip Host Customization** check box, and click **Finish**.
- 4 Export a host customizations file for the hosts in the shared edge and compute cluster.
 - a Select **Home > Policies and Profiles** in the vSphere Web Client.
 - b In the **Navigator**, click **Host Profiles**.
 - c Right-click **LAX01-Comp01**, select **Export Host Customizations** and click **Save**.
 - d Navigate to a file location to store the LAX01-Comp01_host_customizations.csv Excel file that is generated and click **Save**.

- e Edit the Excel file to include the following values.

ESXi Host	Active Directory Configuration Password	Active Directory Configuration Username	NetStack Instance defaultTcpipStack->DNS configuration Name for this host
comp01esx51.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	comp01esx51
comp01esx52.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	comp01esx52
comp01esx53.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	comp01esx53
comp01esx54.lax01.rainpole.local	ad_admin_password	ad_admin_acct@lax01.rainpole.local	comp01esx54

ESXi Host	Host virtual NIC vDS-Comp01:vDS-Comp01-Management:management->IP address settings IPv4 address	Host virtual NIC vDS-Comp01:vDS-Comp01-Management:management->IP address settings Subnet Mask
comp01esx51.lax01.rainpole.local	172.17.31.101	255.255.255.0
comp01esx52.lax01.rainpole.local	172.17.31.102	255.255.255.0
comp01esx53.lax01.rainpole.local	172.17.31.103	255.255.255.0
comp01esx54.lax01.rainpole.local	172.17.31.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Comp01:vDS-Comp01-NFS:<UNRESOLVED>->IP address settings IPv4 address	Host virtual NIC vDS-Comp01:vDS-Comp01-Management:management->IP address settings Subnet Mask
comp01esx51.lax01.rainpole.local	172.17.25.101	255.255.255.0
comp01esx52.lax01.rainpole.local	172.17.25.102	255.255.255.0
comp01esx53.lax01.rainpole.local	172.17.25.103	255.255.255.0
comp01esx54.lax01.rainpole.local	172.17.25.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Comp01:vDS-Comp01-vMotion:vmotion->IP address settings IPv4 address	Host virtual NIC vDS-Comp01:vDS-Comp01-vMotion:vmotion->IP address settings Subnet Mask
comp01esx51.lax01.rainpole.local	172.17.32.101	255.255.255.0
comp01esx52.lax01.rainpole.local	172.17.32.102	255.255.255.0
comp01esx53.lax01.rainpole.local	172.17.32.103	255.255.255.0
comp01esx54.lax01.rainpole.local	172.17.32.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Comp01:vDS-Comp01-VSAN:vsan->IP address settings	Host virtual NIC vDS-Comp01:vDS-Comp01-VSAN:vsan->IP address settings
	IPv4 address	Subnet Mask
comp01esx51.lax01.rainpole.local	172.17.33.101	255.255.255.0
comp01esx52.lax01.rainpole.local	172.17.33.102	255.255.255.0
comp01esx53.lax01.rainpole.local	172.17.33.103	255.255.255.0
comp01esx54.lax01.rainpole.local	172.17.33.104	255.255.255.0

ESXi Host	NetStack Instance vmotion->DNS configuration	NetStack Instance vxlan->DNS configuration
	Name for this host	Name for this host
comp01esx51.lax01.rainpole.local	comp01esx51	comp01esx51
comp01esx52.lax01.rainpole.local	comp01esx52	comp01esx52
comp01esx53.lax01.rainpole.local	comp01esx53	comp01esx53
comp01esx54.lax01.rainpole.local	comp01esx54	comp01esx54

- f In the vSphere Web Client, on the **Host Profiles** page, click **LAX01-Comp01**, click the **Configure** tab and click the **Edit Host Customizations** button.
- g On the **Select hosts** page, select all hosts and click **Next**.
- h On the **Customize hosts** page, click the **Browse** button, locate the LAX01-Comp01_host_customizations.csv file, click **Open** and click **Finish**.

5 Remediate the hosts in the shared edge and compute cluster

- a On the **LAX01-Comp01** page, click the **Monitor** tab and click the **Compliance** tab.
- b Click **LAX01-Comp01** in the **Host/Cluster** column and click **Check Host Profile Compliance**.

Host/Cluster	Host Compliance	Last Checked
▼ LAX01-Comp01	3 Not Compliant 1 Compliant	10/31/2016 10:06 AM
comp01esx51.lax01.rainpole...	✓ Compliant	10/31/2016 10:06 AM
comp01esx52.lax01.rainpole...	✗ Not Compliant	10/31/2016 10:06 AM
comp01esx53.lax01.rainpole...	✗ Not Compliant	10/31/2016 10:06 AM
comp01esx54.lax01.rainpole...	✗ Not Compliant	10/31/2016 10:06 AM

This compliance test shows that the first host is compliant, but the other hosts are not compliant.

- c Click each of the non-compliant hosts, click **Remediate Hosts Based on its Host Profile**, and click **Finish** in the wizard that appears.

All hosts must have a Compliant status in the **Host Compliance** column.

Host/Cluster	Host Compliance	Last Checked
▼ LAX01-Comp01	4 Compliant	11/8/2016 10:00 PM
comp01esx51.lax01.rainpole...	✓ Compliant	11/8/2016 10:00 PM
comp01esx52.lax01.rainpole...	✓ Compliant	11/8/2016 10:00 PM
comp01esx53.lax01.rainpole...	✓ Compliant	11/8/2016 10:00 PM
comp01esx54.lax01.rainpole...	✓ Compliant	11/8/2016 10:00 PM

6 Schedule nightly compliance checks.

- a On the **LAX01-Comp01** page, click the **Monitor** tab, and click the **Scheduled Tasks** tab.
- b Select **Schedule a New Task > Check Host Profile Compliance**.
- c In the **Check Host Profile Compliance (scheduled)** dialog box, click **Scheduling Options**.
- d Enter **LAX01-Comp01 Compliance Check** in the **Task Name** text box.
- e Click the **Change** button next to **Configured Scheduler**.

- f In the **Configure Scheduler** dialog box select **Setup a recurring schedule for this action**, change the **Start time** to **10:00 PM**, and click **OK**.
- g Click **OK** in the **Check Host Profile Compliance (scheduled)** dialog box.

Global Post-Upgrade Configuration of the Virtual Infrastructure Components

After you upgrade all virtual infrastructure components, perform global post-upgrade configuration according to the dependencies between these components.

Procedure

1 [Configure the Anti-Affinity Rules for the Platform Services Controller Instances in Region A](#)

After you upgrade the vCenter Server and Platform Services Controller instances, create the anti-affinity rules for the Platform Services Controllers in Region A in vSphere DRS to implement a configuration that matches the deployment guidelines in this VMware Validated Design.

2 [Create Virtual Machine Groups to Define Startup Order in the Management Cluster in Region A](#)

After you upgrade vSphere, the virtual machine groups allow you to define the startup order of virtual machines in Region A. Startup orders are used during vSphere HA events such that vSphere HA powers on virtual machines in a defined order.

3 [Deploy the Platform Services Controllers Load Balancer in Region A](#)

After you upgrade vCenter Server and Platform Services Controllers in Region A, you deploy load balancing for all services and components related to Platform Services Controllers (PSC) using an NSX Edge load balancer.

4 [Repoint the vCenter Server Instances to the Platform Services Controller Load Balancer in Region A](#)

After you configure the NSX load balancer to distribute the traffic between the Management vCenter Server and Compute vCenter Server in Region A, repoint the vCenter Server instances in the region from the individual Platform Services Controller instances to the load balancer.

5 [Connect the NSX Managers to the Platform Services Controller Load Balancer in Region A](#)

After you upgrade NSX and vSphere components, and deploy the Platform Services Controller load balancers in the two regions, in each region, you must connect the NSX Manager instances in each region to the load balancer for vCenter Single Sign-On communication.

6 [Reconnect vSphere Replication to vCenter Server in Region A](#)

Assign vCenter Single Sign-On administrative, global permissions to the operations service account svc-vr so that you can manage and configure virtual machine replication for disaster recovery operations between the management vCenter Server instances by using vSphere Replication. After you configure the rights of the svc-vr account, reconnect the vSphere Replication instance to the Platform Services Controller in Region A using the secure account and the Platform Services Controller load balancer address.

7 [Reconnect Site Recovery Manager to vCenter Server and Platform Services Controller Instances in Region A](#)

After you upgrade the management vCenter Server and Platform Services Controller, and Site Recovery Manager, in Region A you must reconnect Site Recovery Manager to vSphere using the svc-srm service account and the load-balanced address of the Platform Services Controller pair.

8 [Register vSphere Data Protection with the Management vCenter Server in Region A](#)

After you upgrade the virtual appliances of vSphere Data Protection, in Region A register the appliance with the Management vCenter Server using vSphere Data Protection Service Account and NSX Load Balancer for Platform Services Controller.

9 [Configure Point in Time in vSphere Replication](#)

After you upgrade Management vCenter Server and Platform Services Controller, and Site Recovery Manager and vSphere Replication, enable point-in-time support to be able to recover virtual machines at specific points in time.

10 [Clean Up Obsolete Appliances and Snapshots in Region A](#)

After you complete the upgrade and operational verification of the virtual infrastructure components in Region A, clean up the environment from appliances that run old software versions and from snapshots of upgraded nodes.

11 [Configure the Anti-Affinity Rules for the Platform Services Controller Instances in Region B](#)

After you upgrade the vCenter Server and Platform Services Controller instances, create the anti-affinity rules for the Platform Services Controllers in Region B in vSphere DRS to implement a configuration that matches the deployment guidelines in this VMware Validated Design.

12 [Create Virtual Machine Groups to Define Startup Order in the Management Cluster in Region B](#)

After you upgrade vSphere, the virtual machine groups allow you to define the startup order of virtual machines in Region B. Startup orders are used during vSphere HA events such that vSphere HA powers on virtual machines in a defined order.

13 [Deploy the Platform Services Controllers Load Balancer in Region B](#)

After you upgrade vCenter Server and Platform Services Controllers in Region B, you deploy load balancing for all services and components related to Platform Services Controllers (PSC) using an NSX Edge load balancer.

14 [Repoint the vCenter Server Instances to the Platform Services Controller Load Balancer in Region B](#)

After you configure the NSX load balancer to distribute the traffic between the Management vCenter Server and Compute vCenter Server in Region B, repoint the vCenter Server instances in the region from the individual Platform Services Controller instances to the load balancer.

15 [Connect the NSX Managers to the Platform Services Controller Load Balancer in Region B](#)

After you upgrade NSX and vSphere components in the management cluster, and deploy the Platform Services Controller load balancers in the two regions, in each region, you connect the NSX Manager for the management cluster to the load balancer for vCenter Single Sign-On communication.

16 Reconnect vSphere Replication to vCenter Server in Region B

Reconnect the vSphere Replication instance to the Platform Services Controller in Region B using the secure account svc-vr and the Platform Services Controller load balancer address.

17 Reconnect Site Recovery Manager to vCenter Server and Platform Services Controller Instances in Region B

After you upgrade vCenter Server and Site Recovery Manager, redirect Site Recovery Manager to the load balancer of the two Platform Services Controller instances in Region B using the svc-srm service account.

18 Register vSphere Data Protection with the Management vCenter Server in Region B

After you upgrade the virtual appliances for vSphere Data Protection, in Region B register the appliance with the Management vCenter Server using vSphere Data Protection Service Account and NSX Load Balancer for Platform Services Controller.

19 Clean Up Obsolete Appliances and Snapshots in Region B

After you complete the upgrade and operational verification of the virtual infrastructure components in Region B, clean up the environment from appliances that run old software versions and from snapshots of upgraded nodes.

Configure the Anti-Affinity Rules for the Platform Services Controller Instances in Region A

After you upgrade the vCenter Server and Platform Services Controller instances, create the anti-affinity rules for the Platform Services Controllers in Region A in vSphere DRS to implement a configuration that matches the deployment guidelines in this VMware Validated Design.

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 In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc01.sfo01.rainpole.local** control tree.
- 3 Select the **SFO01-Mgmt01** cluster and click the **Configure** tab.
- 4 On the **Configure** page, click **VM/Host Rules**.
- 5 On the **VM/Host Rules** page, click **Add**.

- 6 In the **Create VM/Host Rule** dialog, enter **anti-affinity-rule-psc** in the **Name** field, ensure the **Enable rule** checkbox is selected, select **Separate Virtual Machines** from the **Type** drop down menu, and click the **Add**.
- 7 In the **Add Rule Member** dialog, select **mgmt01psc01** and **comp01psc01** and click **OK**.
- 8 In the **Create VM/Host Rule** dialog, click **OK** to create the rule.

Create Virtual Machine Groups to Define Startup Order in the Management Cluster in Region A

After you upgrade vSphere, the virtual machine groups allow you to define the startup order of virtual machines in Region A. Startup orders are used during vSphere HA events such that vSphere HA powers on virtual machines in a defined order.

Create virtual machine groups for the two Platform Services Controller instances and one for the Management vCenter Server, and include the groups in a startup order rule.

Table 4-19. VM Groups and Startup Rules for the Management vCenter Server and Platform Services Controller Instances

Region	vCenter Server Cluster	VM Group	Group Members	Rule
Region A	mgmt01vc01.sfo01.rainpole.local > SFO01 > SFO01-Mgmt01	Platform Services Controllers	mgmt01psc01,comp01psc01	SDDC Management Virtual Machines
		vCenter Servers	mgmt01vc01	

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 In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc01.sfo01.rainpole.local** tree.
- 3 Create a virtual machine DRS group for the Platform Services Controller instances.
 - a Select the **SFO01-Mgmt01** cluster and click the **Configure** tab.
 - b On the **Configure** page, click **VM/Host Groups**.
 - c On the **VM/Host Groups** page, click the **Add** button.

- d In the **Create VM/Host Group** dialog box, enter **Platform Services Controllers** in the **Name** text box, select **VM Group** from the **Type** drop-down menu, and click the **Add** button.
 - e In the **Add VM/Host Group Member** dialog box, select **mgmt01psc01** and **comp01psc01**, and click **OK**.
- 4 Create a virtual machine DRS group for the vCenter Server virtual machine.
- a Select the **SFO01-Mgmt01** cluster and click the **Configure** tab.
 - b On the **Configure** page, click **VM/Host Groups**.
 - c On the **VM/Host Groups** page, click the **Add** button.
 - d In the **Create VM/Host Group** dialog, enter **vCenter Servers** in the **Name** text box, select **VM Group** from the **Type** drop-down menu.
 - e Click the **Add** button, select **mgmt01vc01** in the **Add VM/Host Group Member** dialog box, and click **OK**.
 - f Click **OK**.
- 5 Create a DRS rule to power on the Platform Services Controller instances first and then the Management vCenter Server.
- a Select the **SFO01-Mgmt01** cluster and click the **Configure** tab.
 - b On the **Configure** page, click **VM/Host Rules**.
 - c On the **VM/Host Rules** page, click the **Add** button.
 - d In the **Create VM/Host Rule** dialog, enter the following settings and click **OK**.

Setting	Value
Name	SDDC Management Virtual Machines
Enable rule	Selected
Type	Virtual Machines to Virtual Machines
First restart VMs in VM group	Platform Services Controllers
Then restart VMs in VM group	vCenter Servers

Deploy the Platform Services Controllers Load Balancer in Region A

After you upgrade vCenter Server and Platform Services Controllers in Region A, you deploy load balancing for all services and components related to Platform Services Controllers (PSC) using an NSX Edge load balancer.

Procedure

1 [Deploy the Platform Services Controller NSX Load Balancer in Region A](#)

The first step in deploying load balancing for the Platform Services Controller is to deploy the edge services gateway.

2 Replace the Platform Services Controller Certificates in Region A

After you upgrade the virtual infrastructure and deploy the load balancer for the Platform Services Controller in Region A, you replace the machine SSL certificate on each Platform Services Controller instance with a custom certificate that is signed by the certificate authority (CA) available on the parent Active Directory (AD) server.

3 Update the Single Sign-On Configuration of the Platform Services Controllers in Region A

After you upgrade the virtual infrastructure layer to VMware Validated Design 4.0 in Region A, after you deploy the load balancer for the Platform Services Controllers, update the vCenter Single Sign-On endpoints to reflect the name of the load balancers virtual IP.

4 Create Platform Services Controller Application Profiles in Region A

Create an application profile to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

5 Create Platform Services Controller Server Pools in Region A Post-Upgrade

A server pool consists of backend server members. After you create a server pool, you associate a service monitor with the pool to manage and share the backend servers flexibly and efficiently.

6 Create Virtual Servers in Region A

After load balancing is set up, the NSX load balancer distributes network traffic across multiple servers. When a virtual server receives a request, it chooses the appropriate pool to send traffic to. Each pool consists of one or more members. You create virtual servers for all of the configured server pools.

7 Update the DNS Record for the Platform Services Controller Load Balancer in Region A

You must modify the sfo01psc01 DNS A record to point to the load balancer VIP after you configure the load balancer for the Platform Services Controller instances in Region A.

Deploy the Platform Services Controller NSX Load Balancer in Region A

The first step in deploying load balancing for the Platform Services Controller is to deploy the edge services gateway.

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 Click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.16.11.65** from the NSX Manager drop-down menu.
- 5 Click the **Add** icon tab to create an NSX Edge.

The **New NSX Edge** wizard appears.

- 6 On the **Name and description** page, enter the following settings and click **Next**.

Setting	Value
Install Type	Edge Services Gateway
Name	SFO01PSC01
Hostname	sfo01psc01.sfo01.rainpole.local
Deploy NSX EDGE	Selected
Enable High Availability	Selected

New NSX Edge

1 **Name and description**

2 **Settings**

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Firewall and HA

7 Ready to complete

Name and description

Install Type: ☒ Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

☐ Logical (Distributed) Router
Provides Distributed Routing and Bridging capabilities.

☐ Universal Logical (Distributed) Router
Provides Distributed Routing capabilities for Universal Logical Switches.

Name:

Hostname:

Description:

Tenant:

☒ Deploy NSX Edge
Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.

☒ Enable High Availability
Enable HA, for enabling and configuring High Availability.

Back Next Finish Cancel

- 7 On the **Settings** page, enter the following settings and click **Next**.

Setting	Value
User Name	admin
Password	edge_admin_password
Enable SSH access	Selected
Enable FIPS mode	Deselected

Setting	Value
Enable auto rule generation	Selected
Edge Control Level logging	INFO

8 On the **Configure deployment** page, perform the following configuration steps and click **Next**.

- Select **SF001**, from the **Datacenter** drop-down menu.
- Click **Large** to specify the **Appliance Size**.
- Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Resource pool	SFO01-Mgmt01
Datastore	SFO01A-VSAN01-MGMT01
Folder	NSX01

- To create a second appliance, click the **Add** icon again, make the same selections in the **New NSX Appliance** dialog box, and click **OK**.

9 On the **Configure Interfaces** page, click the **Add** icon to configure the PSCLB interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	PSCLB
Type	Internal

Setting	Value
Connected To	vDS-Mgmt-Management
Connectivity Status	Connected
Primary IP Address	172.16.11.71
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- 10 On the **Default gateway** settings page, enter the following settings and click **Next**.

Setting	Value
Gateway IP	172.16.11.1
MTU	9000

New NSX Edge

1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete

Default gateway settings

☒ Configure Default Gateway

vNIC: PSC LB

Gateway IP: 172.16.11.1

MTU: 9000

Admin Distance: 1

Back Next Finish Cancel

- 11 On the **Firewall and HA** page, select the following settings and click **Next**.

Setting	Value
Configure Firewall default policy	Selected
Default Traffic Policy	Accept
Logging	Disable
vNIC	any
Declare Dead Time	15

New NSX Edge

1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete

Firewall and HA

☒ Configure Firewall default policy

Default Traffic Policy: ☒ Accept ☐ Deny

Logging: ☐ Enable ☒ Disable

Configure HA parameters
Configuring HA parameters is mandatory for HA to work.

vNIC: (seconds)

Declare Dead Time: (seconds)

Management IPs:

Management IPs must be in CIDR format with /30 subnet and must not overlap with any vnic subnets.

Back Next Finish Cancel

12 On the **Ready to complete** page, review the configuration settings you entered and click **Finish**.

New NSX Edge

1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete

Ready to complete

Name and description

Name: SFO01PSC01
Install Type: Edge Services Gateway
Tenant: Large
HA: Enabled
Automatic Rule Generation: Enabled

NSX Edge Appliances

Resource Pool	Host
SFO01-Mgmt01	
SFO01-Mgmt01	

Interfaces

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
0	PSC LB	172.16.11.71*	24	vDS-Mgmt-Ma...

Back Next Finish Cancel

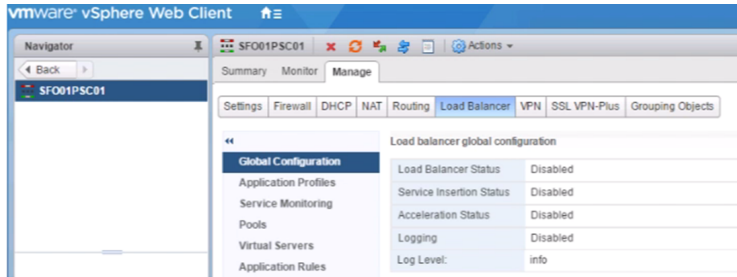
13 Enable HA logging.

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

- c Double-click the **SFO01PSC01** device.
- d On the **Manage** tab, click the **Settings** tab.
- e Click **Change** in the **HA Configuration** window.
- f Select the **Enable Logging** checkbox and click **OK**.

14 Enable the Load Balancer service.

- a On the **Manage** tab, click the **Load Balancer** tab, click **Global Configuration**, and click **Edit**.
The **Edit load balancer global configuration** dialog box appears.



- 15** In the **Edit load balancer global configuration** dialog box, select **Enable Load Balancer** and click **OK**.

Replace the Platform Services Controller Certificates in Region A

After you upgrade the virtual infrastructure and deploy the load balancer for the Platform Services Controller in Region A, you replace the machine SSL certificate on each Platform Services Controller instance with a custom certificate that is signed by the certificate authority (CA) available on the parent Active Directory (AD) server.

You must repeat this procedure twice: first on the Platform Services Controller for the Management vCenter Server (mgmt01psc01.sfo01.rainpole.local), and then on the Platform Services Controller for the Compute vCenter Server (comp01psc01.sfo01.rainpole.local).

Table 4-20. Certificate-Related Files on Platform Services Controllers

Platform Services Controller	Certificate File Name	Replacement Order
mgmt01psc01.sfo01.rainpole.local	■ sfo01psc01.sfo01.1.cer	First
	■ sfo01psc01.sfo01.key	
	■ root64.cer	
comp01psc01.sfo01.rainpole.local	■ sfo01psc01.sfo01.1.cer	Second
	■ sfo01psc01.sfo01.key	
	■ root64.cer	

Procedure

- 1 Change the Platform Services Controller command shell to the Bash shell to allow secure copy (scp) connections.

- a SSH to `mgmt01psc01.sfo01.rainpole.local` and login using the following credentials.

Setting	Value
Username	root
Password	<i>mgmtpsc_root_password</i>

- b Run the command `shell`
 - c Run the command `chsh -s /bin/bash root`.
- 2 Copy the generated certificates to the Platform Services Controller.
 - a Use the `scp` command to copy the contents of the folder `C:\CertGenVVD\SignedByMCSACerts\sfo01psc01.sfo01` to the folder `/tmp/certs`.
 - b Use the `scp` command to copy the `Root64.cer` file from the folder `C:\CertGenVVD\SignedByMCSACerts\RootCA` to the folder `/tmp/certs`.

- 3 Replace the certificate on the Platform Services Controller.

- a Start the vSphere Certificate Manager utility on the Platform Services Controller.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

- b Select **Option 1 (Replace Machine SSL certificate with Custom Certificate)**.
 - c Enter the default vCenter Single Sign-On user name `administrator@vsphere.local` and the `vsphere_admin` password.
 - d Select **Option 2 (Import custom certificate(s) and key(s) to replace existing Machine SSL certificate)**.
 - e When prompted for the custom certificate enter `/tmp/certs/sfo01psc01.sfo01.1.cer`.
 - f When prompted for the custom key enter `/tmp/certs/sfo01psc01.sfo01.key`.
 - g When prompted for the signing certificate enter `/tmp/certs/Root64.cer`.
 - h When prompted to Continue operation enter `Y`.
 - i The Platform Services Controller services will restart automatically.
- 4 Repeat the procedure to replace the certificate on `comp01psc01.sfo01.rainpole.local`.

Update the Single Sign-On Configuration of the Platform Services Controllers in Region A

After you upgrade the virtual infrastructure layer to VMware Validated Design 4.0 in Region A, after you deploy the load balancer for the Platform Services Controllers, update the vCenter Single Sign-On endpoints to reflect the name of the load balancers virtual IP.

Prerequisites

Before completing this procedure a DNS A record must be created. This A record is the FQDN of the load balancer with the IP address of mgmt01psc01.sfo01.rainpole.local. After the load balancer is setup this DNS record is changed to the virtual IP of the load balancer.

Procedure

- 1 Create a DNS record for the load balancer FQDN. Create a DNS A record using the values listed below.

- a Open a remote desktop connection to your DNS server.
- b Create a DNS A record with the values below:

FQDN	IP
sfo01psc01.sfo01.rainpole.com	172.16.11.61

Note After the load balancer is configured the IP address will be updated to reflect the load balancer's VIP instead of the IP address of mgmt01psc01.sfo01.rainpole.local

- 2 Update the vCenter Single Sign-On configuration on mgmt01psc01.sfo01.rainpole.local.

- a Open an SSH connection to **mgmt01psc01.sfo01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>mgmtpsc_root_password</i>

- c Enter **cd /usr/lib/vmware-sso/bin/** and press **Enter**.
- d Enter **python updateSSOConfig.py --lb-fqdn=sfo01psc01.sfo01.rainpole.local** and press **Enter**.

- 3 Update the vCenter Single Sign-On configuration on comp01psc01.sfo01.rainpole.local.

- a Open an SSH connection to **comp01psc01.sfo01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>comppsc_root_password</i>

- c Enter **cd /usr/lib/vmware-sso/bin/** and press **Enter**.
- d Enter **python updateSSOConfig.py --lb-fqdn=sfo01psc01.sfo01.rainpole.local** and press **Enter**.

4 Update the Platform Services Controller endpoints.

Only perform this procedure on one of the Platform Services Controllers.

- a Open an SSH connection to **mgmt01psc01.sfo01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>mgmtpsc_root_password</i>

- c Enter **cd /usr/lib/vmware-ssobin/** and press **Enter**.
- d Enter
**python UpdateLsEndpoint.py -lb-fqdn=sfo01psc01.sfo01.rainpole.local --
user=Administrator@vsphere.local** and press **Enter**.
- e Enter the *vsphere_admin_password* when prompted.

Create Platform Services Controller Application Profiles in Region A

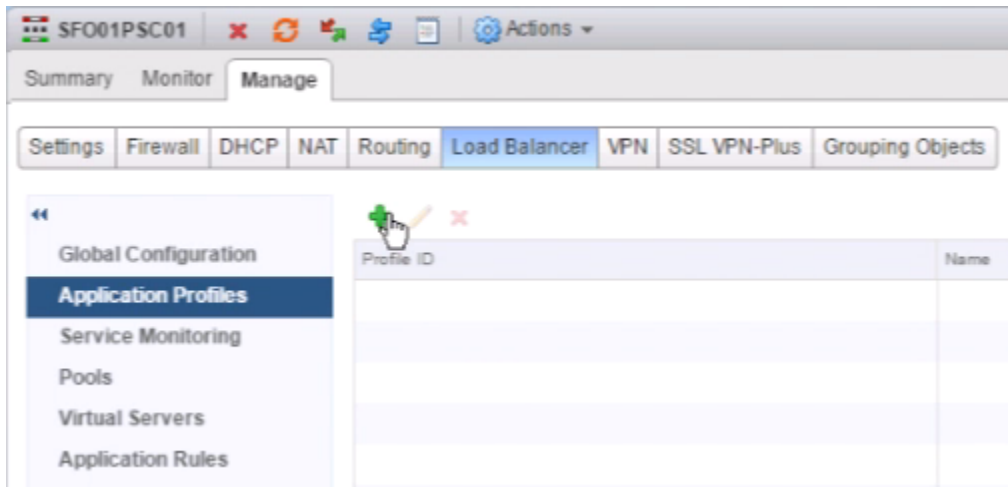
Create an application profile to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

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 Click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **SFO01PSC01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Application Profiles**.



- 6 Click the **Add** icon, and in the **New Profile** dialog box, enter the following values.

Setting	Value	Value
Name	PSC-TCP	PSC-HTTPS
Type	TCP	HTTPS
Enable SSL Passthrough	Deselected	Selected
Persistence	Source IP	Source IP
Expires in (Seconds)	60	60

New Profile

Name:

Type:

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence:

Cookie Name:

Mode:

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certific... Pool Certificates

Service Certificates CA Certificates CRL

☐ Configure Service Certificate

	Common Name	Issuer	Validity
<input type="radio"/>	sfo01psc01.sfo01.rainp	rainpole-DC01RPL-CA	Mon Oct 24 2016 - Wed O
<input type="radio"/>	VSM_SOLUTION_c511	VSM_SOLUTION_c511	Tue Oct 25 2016 - Thu Oct
<input type="radio"/>	VSM_SOLUTION_a6ce	VSM_SOLUTION_a6ce	Tue Oct 25 2016 - Thu Oct
<input type="radio"/>	VSM_SOLUTION_c511	VSM_SOLUTION_c511	Tue Oct 25 2016 - Thu Oct
<input type="radio"/>	VSM_SOLUTION_a6ce	VSM_SOLUTION_a6ce	Tue Oct 25 2016 - Thu Oct

Cipher:

Client Authentication:

OK Cancel

7 Click **OK** to save the configuration.

Create Platform Services Controller Server Pools in Region A Post-Upgrade

A server pool consists of backend server members. After you create a server pool, you associate a service monitor with the pool to manage and share the backend servers flexibly and efficiently.

Repeat this procedure to create two server pools.

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 Click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **SFO01PSC01** NSX Edge to manage its network settings.
- 5 On the **Manage** tab, click **Load Balancer** and click **Pools**.
- 6 Click the **Add** icon, and in the **New Pool** dialog box, enter the following values.

Setting	Value
Name	PSC-HTTPS
Algorithm	ROUND-ROBIN
Monitors	default-tcp-monitor

New Pool

Name: * PSC-HTTPS

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_tcp_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection

☐ Transparent

OK Cancel

- 7 **New Members** dialog box, click the **Add** icon to add the first pool member.
- 8 In the **New Member** dialog box, enter the following values, and click **OK**.

Setting	Values for First Server Pool	Values for Second Server Pool
Name	mgmt01psc01	mgmt01psc01
IP Address/VC Container	mgmt01psc01	mgmt01psc01
State	Enable	Enable
Port		

Setting	Values for First Server Pool	Values for Second Server Pool
Monitor Port	443	389
Weight	1	1

9 Under **Members**, click the **Add** icon to add the second pool member.

10 In the **New Member** dialog box, enter the following values, click **OK** and click **OK**.

Setting	Values for First Server Pool	Values for Second Server Pool
Name	comp01psc01	comp01psc01
IP Address/VC Container	comp01psc01	comp01psc01
State	Enable	Enable
Port		
Monitor Port	443	389
Weight	1	1

New Pool

Name: * PSC-HTTPS

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_tcp_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	mgmt01...	mgmt01p...	1	443		0	0
✓	comp01...	comp01p...	1	443		0	0

☐ Transparent

OK Cancel

11 Repeat the procedure to create the second server pool PSC-TCP.

Create Virtual Servers in Region A

After load balancing is set up, the NSX load balancer distributes network traffic across multiple servers. When a virtual server receives a request, it chooses the appropriate pool to send traffic to. Each pool consists of one or more members. You create virtual servers for all of the configured server pools.

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 Click **Networking & Security**.

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

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **SFO01PSC01** NSX Edge to manage its network settings.

5 On the **Manage** tab, click **Load Balancer**, and select **Virtual Servers**.

6 Click the **Add** icon, and in the **New Virtual Server** dialog box configure the values for the virtual server you are adding, and click **OK**.

Setting	Value	Value
Enable Virtual server	Selected	Selected
Application Profile	PSC-TCP	PSC-HTTPS
Name	PSC-TCP	PSC-HTTPS
Description	389-LDAP,2012-Control Interface,2014-RPC Port,2020-Authentication,636-SSL LDAP	Data from the vSphere Web Client
IP Address	172.16.11.71	172.16.11.71
Protocol	TCP	HTTPS
Port	389,636,2012,2014,2020	443
Default Pool	PSC-TCP	PSC-HTTPS

New Virtual Server

General | Advanced

☒ Enable Virtual Server
☐ Enable Acceleration

Application Profile: * psc-tcp

Name: * PSC-TCP

Description: 389-LDAP,2012-Control Interface,2014-RPC,Port 2020

IP Address: * 172.16.11.71 [Select IP Address](#)

Protocol: TCP

Port / Port Range: * 389,636,2012,2014,2020

Default Pool: PSC-TCP

Connection Limit:

Connection Rate Limit: (CPS)

OK Cancel

- 7 Repeat the steps to create a virtual server for each component.

Update the DNS Record for the Platform Services Controller Load Balancer in Region A

You must modify the sfo01psc01 DNS A record to point to the load balancer VIP after you configure the load balancer for the Platform Services Controller instances in Region A.

Procedure

- 1 Open an RDP connection to the AD server dc01sfo.sfo01.rainpole.local and log in as administrator.
- 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 and locate the **sfo01psc01** record on the right.

- 4 Double-click the **sfo01psc01** record, enter the following values and click **OK**.

Setting	Value
Fully Qualified domain name (FQDN)	sfo01psc01.sfo01.rainpole.local
IP Address	172.16.11.71
Update Associated Pointer (PTR) record	Selected

The screenshot shows a Windows-style dialog box titled "sfo01psc01 Properties". It has two tabs: "Host (A)" and "Security". The "Security" tab is active. Inside the dialog, there are three text input fields: "Host (uses parent domain if left blank):" with the value "sfo01psc01", "Fully qualified domain name (FQDN):" with the value "sfo01psc01.sfo01.rainpole.local", and "IP address:" with the value "172.16.11.71". Below these fields is a checkbox labeled "Update associated pointer (PTR) record" which is checked. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

Repoint the vCenter Server Instances to the Platform Services Controller Load Balancer in Region A

After you configure the NSX load balancer to distribute the traffic between the Management vCenter Server and Compute vCenter Server in Region A, repoint the vCenter Server instances in the region from the individual Platform Services Controller instances to the load balancer.

Procedure

- 1 Log in to mgmt01vc01.sfo01.rainpole.local by using Secure Shell (SSH) client.
 - a Open an SSH connection to the virtual machine mgmt01vc01.sfo01.rainpole.local.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	vcenter_server_root_password

- 2 To repoint vCenter Server to the load balancer for the Platform Services Controller instances, run the following command.

```
cmsso-util repoint --repoint-psc sfo01psc01.sfo01.rainpole.local
```

- 3 Verify that vCenter Server directs its requests to the load balancer. run the following commands.

- a Run the following command and verify that it returns sfo01psc01.sfo01.rainpole.local for the Platform Services Controller Load Balancer in Region A.

```
/usr/lib/vmware-vmafd/bin/vmafd-cli get-dc-name --server-name localhost
```

- b Run the following command and verify that it returns the https://sfo01psc01.sfo01.rainpole.local:443/lookupservice/sdk Lookup Service of the Platform Services Controller Load Balancer in Region A.

```
/usr/lib/vmware-vmafd/bin/vmafd-cli get-ls-location --server-name localhost
```

- 4 Verify that all vCenter Server services are running.

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

- 5 Repeat the procedure on the Compute vCenter Server comp01vc01.sfo01.rainpole.local.

Connect the NSX Managers to the Platform Services Controller Load Balancer in Region A

After you upgrade NSX and vSphere components, and deploy the Platform Services Controller load balancers in the two regions, in each region, you must connect the NSX Manager instances in each region to the load balancer for vCenter Single Sign-On communication.

Table 4-21. Lookup Service URL for the NSX Managers for the Shared Edge and Compute Clusters

NSX Manager URL	Lookup Service FQDN
https://mgmt01nsxm01.sfo01.rainpole.local	sfo01psc01.sfo01.rainpole.local
https://comp01nsxm01.sfo01.rainpole.local	sfo01psc01.sfo01.rainpole.local

Procedure

- 1 Log in to the Compute NSX Manager appliance user interface.
 - a Open a Web browser and go to **https://mgmt01nsxm01.sfo01.rainpole.local**.
 - b Log in using the following credentials.

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

- 2 Click **Manage vCenter Registration**.
- 3 Under **Lookup Service**, click **Edit**.
- 4 In the **Lookup Service** dialog box, change the address in the Lookup Service IP text box to **sfo01psc01.sfo01.rainpole.local** and click **OK**.

Setting	Value
Lookup Service IP	sfo01psc01.sfo01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 5 In the **Trust Certificate?** dialog box, click **Yes**.
- 6 Wait for the **Status** indicators for the Lookup Service to change to the Connected status.
- 7 Repeat the procedure to connect the NSX Manager for the shared edge and compute cluster in Region A, comp01nsxm01.sfo01.rainpole.local, to the Platform Services Controller load balancer in the region.

Reconnect vSphere Replication to vCenter Server in Region A

Assign vCenter Single Sign-On administrative, global permissions to the operations service account svc-vr so that you can manage and configure virtual machine replication for disaster recovery operations between the management vCenter Server instances by using vSphere Replication. After you configure the rights of the svc-vr account, reconnect the vSphere Replication instance to the Platform Services Controller in Region A using the secure account and the Platform Services Controller load balancer address.

Table 4-22. Configuration Changes on vSphere Replication after Upgrade

Region	vSphere Replication Management Interface URL	Old Single Sign-On Account	New Single Sign-On Account	Old Lookup Service URL	New Lookup Service URL
Region A	https://mgmt01vrms01.sfo01.rainpole.local:5480	administrator@vsphere.local	svc-vr@rainpole.local	mgmt01psc01.sfo01.rainpole.local	sfo01psc01.sfo01.rainpole.local

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, select **Administration**.
- 3 Assign the service account **`svc-vr@rainpole.local`** to the Single Sign-On Administrators group
 - a In the vSphere Web Client, navigate to **Administration** and click **Users and Groups**.
 - b On the **Groups** tab, click the **Administrators** group and click the **Add Member** icon under **Group Members**.

- c In the **Add Principals** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.
- d From the list of users and groups, select the **svc-vr** user, click **Add**, and click **OK**.

Add Principals

Select users from the list or type names in the Users text box. Click Check names to validate your entries against the directory.

Domain:

Users and Groups

Show Users First

User/Group	Description/Full name
svc-nsxmanager	svc-nsxmanager
svc-srm	svc-srm-vcenter
svc-vdp	svc-vdp
svc-vr	svc-vr
svc-vRA	svc-vRA svc-vRA
svc-vra-vrops	svc-vra-vrops
svc-vrli-vrops	svc-vrli-vrops

Add

Users:

Groups:

Separate multiple names with semicolons **Check names**

OK **Cancel**

The global vCenter Single Sign-On administrative permissions of the svc-vr account propagates to all other linked vCenter Server instances.

- 4 Change the connection settings of the vSphere Replication appliance and reconnect it to the Platform Services Controller pair and Management vCenter Server.

- a Open a Web browser and go to **https://mgmt01vrms01.sfo01.rainpole.local:5480**.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vr_sfo_root_password</i>

The virtual appliance management interface of the vSphere Replication instance opens.

- c On the **VR** tab, click **Configuration**, enter the following settings, and click **Save and Restart Service**.

You change the administrator vCenter Single Sign-On account to the svc-vr service account and the lookup service address mgmt01psc01.sfo01.rainpole.local to the address of the Platform Services Controller load balancer sfo01psc01.sfo01.rainpole.local.

Setting	Value
Configuration Mode	Configure using the embedded database
LookupService Address	sfo01psc01.sfo01.rainpole.local
SSO Administrative Account	svc-vr@rainpole.local
Password	svc-vr_password
VRM Host	172.16.11.123
VRM Site Name	mgmt01vc01.sfo01.rainpole.local
vCenter Server Address	mgmt01vc01.sfo01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	<i>vcserver_admin_email</i>

- d In the **Confirm SSL Certificate** dialog box, click **Accept**.

Reconnect Site Recovery Manager to vCenter Server and Platform Services Controller Instances in Region A

After you upgrade the management vCenter Server and Platform Services Controller, and Site Recovery Manager, in Region A you must reconnect Site Recovery Manager to vSphere using the svc-srm service account and the load-balanced address of the Platform Services Controller pair.

Configure Service Account in vSphere for Site Recovery Manager

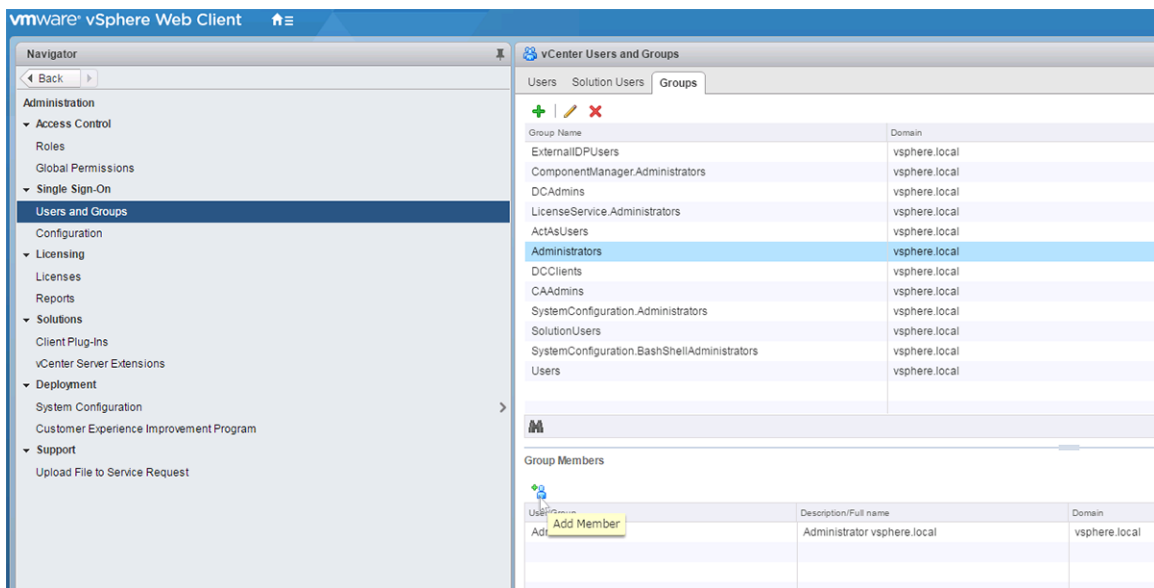
Assign vCenter Single Sign-On administrative global permissions to the operations service account svc-srm so that you can manage, pair and perform orchestrated disaster recovery operations between the management vCenter Server instances by using Site Recovery Manager in a safe way.

Procedure

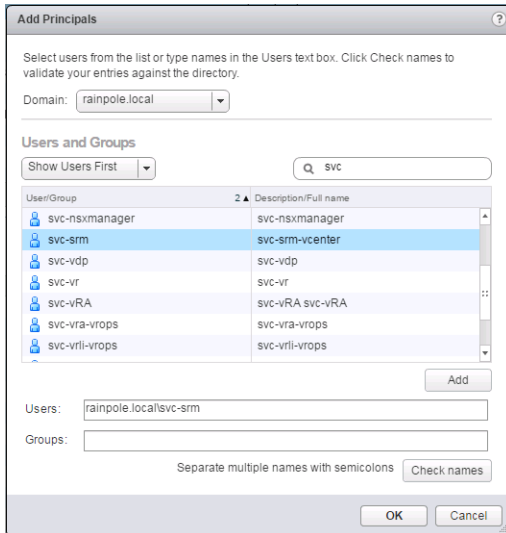
- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://mgmt01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Administration**.
- 3 Add the service account svc-srm@rainpole.local to the Single Sign-On administrators group
 - a In the vSphere Web Client, select **Administration** from the **Home** menu and click **Users and Groups** under **Users and Groups**.
 - b On the **Groups** tab, click the **Administrators** group and click the **Add Member** icon under **Group Members**.



- c In the **Add Principals** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.
- d From the list of users and groups, select the **svc-srm** user, click **Add**, and click **OK**.



The global vCenter Single Sign-On administrative permissions of the svc-srm account propagate to all other linked vCenter Server instances.

Modify the Site Recovery Manager Server Installation in Region A

After you upgrade vCenter Server and Site Recovery Manager, redirect Site Recovery Manager to the load balancer of the two Platform Services Controller instances in Region A using the svc-srm service account.

Procedure

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

Region	Site Recovery Manager FQDN
Region A	mgmt01srm01.sfo01.rainpole.local

- a Open an RDP connection to the virtual machine mgmt01srm01.sfo01.rainpole.local.
- b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	windows_administrator_password

- 2 Open **Programs and Features** from the Windows Control Panel.
- 3 Select the entry for the **VMware vCenter Site Recovery Manager** and click **Change**.

The VMware Site Recovery Manager installation wizard appears.

- 4 On the Welcome page, click **Next**.
- 5 Select **Modify** and click **Next**.
- 6 On the **vSphere Platform Services Controller** page, change the Platform Services Controller address, enter the svc-srm account settings, and click **Next**.

Setting	Value
Address	<code>sfo01psc01.sfo01.rainpole.local</code>
HTTPS Port	443
Username	<code>svc-srm@rainpole.local</code>
Password	<code>svc-srm_password</code>

- 7 If prompted to accept the certificate of the Platform Services Controller in the **Platform Services Controller Certificate** dialog box, click **Accept**.
- 8 On the **VMware vCenter Server** page, click **Next**.
- 9 If prompted, in the **vCenter Server Certificate** dialog box, click **Accept**.
- 10 On the **Site Recovery Manager Extension** page, leave the existing settings, and click **Next**.

Setting	Value
Administrator E-mail	<code>srm_admin_sfo_email_address</code>
Local Host	172.16.11.124
Listener Port	9086

- 11 On the **Certificate Type** page, select **Use existing certificate** and click **Next**.
- 12 On the **Database Server Selection** page, select **Use the embedded database server** and click **Next**.
- 13 On the **Embedded Database Configuration** page, enter the following settings and click **Next**.

Setting	Value
Data Source Name	<code>SRM_SITE_SFO</code>
Database User Name	<code>srm_admin</code>
Database Password	<code>srm_admin_sfo_password</code>
Database Port	5678
Connection Count	5
Max. Connections	20

- 14 On the **Site Recovery Manager Service Account** page, enter the following credentials, and click **Next**.

Setting	Value
Use Local System account	Deselected
Username	MGMT01SRM01\Administrator
Password	<i>mgmt01srm01_admin_password</i>

- 15 On the **Ready to Install the Program** page, click **Install**.

- 16 Click **Finish** to complete the installation.

- 17 Reconnect the Site Recovery Manager instance in Region A.

- Open a Web browser and go to **<https://mgmt01vc01.sfo01.rainpole.local/vsphere-client/>**.
- Log in using the following credentials.

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

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

- 19 On the **Site Recovery** page, click **Sites**.

- 20 On the **Sites** page, right-click **mgmt01vc01.sfo01.rainpole.local** and select **Reconfigure Pairing**.

The **Reconfigure Site Recovery Manager Server Pairing** wizard appears.

- 21 On the **Select Site** page, validate the following settings and click **Next**.

Settings	Value
PSC address	lax01psc51.lax01.rainpole.local
Port	443

- 22 On the **Select vCenter Server** page, enter the administrator@vsphere.local password, validate the following settings, and click **Finish**.

Settings	Value
vCenter Servers with matching SRM Extension	mgmt01vc51.lax01.rainpole.local
Username	svc-srm@rainpole.local
Password	<i>svc-srm_password</i>

Register vSphere Data Protection with the Management vCenter Server in Region A

After you upgrade the virtual appliances of vSphere Data Protection, in Region A register the appliance with the Management vCenter Server using vSphere Data Protection Service Account and NSX Load Balancer for Platform Services Controller.

Procedure

- 1 Log in to the vSphere Data Protection Configuration Utility.

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

Region	URL
Region A	https://mgmt01vdp01.sfo01.rainpole.local:8543/vdp-configure/

- b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vdp_root_password</i>

- 2 On the **Configuration** tab, click the wheel icon next to **VDP Appliance** and select **vCenter Registration**.

The **vCenter Registration** wizard appears.

- 3 On the **vCenter Registration** page, select **I have reviewed the information. I want to reconfigure vCenter** and click **Next**.
- 4 On the **vCenter Configuration** page, change the **vCenter username** setting to use the svc-vdp service account for authentication to vCenter Server and the **SSO FQDN or IP** setting to connect vSphere Data Protection to the NSX load balancer for the Platform Services Controllers, and click **Next**.

vCenter Server Setting	Value
vCenter username	rainpole.local\svc-vdp
vCenter password	<i>svc-vdp_password</i>
vCenter FQDN or IP	mgmt01vc01.sfo01.rainpole.local
vCenter HTTP port	80
vCenter HTTPS port	443
Verify vCenter certificate	Deselected

Single Sign-On Setting	Value
Use vCenter for SSO authentication	Deselected
SSO FQDN or IP	sfo01psc01.sfo01.rainpole.local
SSO port	443

- 5 On the **Ready to Complete** page review the configuration changes and click **Finish**.
- 6 If you are unable to proceed because of a false status like `One or more jobs are running` although you are not running any backup jobs, run this command to restart the Tomcat Web server and try again.

```
emwebapp.sh --restart
```

- 7 Verify that the vSphere Data Protection is accessible in the vSphere Web Client after you complete the initial configuration of vSphere Data Protection.
 - 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>

- c On the vSphere Web Client Home page, verify that the **VDP** icon is available and that you can connect to each appliance.

Configure Point in Time in vSphere Replication

After you upgrade Management vCenter Server and Platform Services Controller, and Site Recovery Manager and vSphere Replication, enable point-in-time support to be able to recover virtual machines at specific points in time.

You reconfigure the individual replications of the vRealize Operations Manager analytics nodes and the Cloud Management Platform components that are failed over 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	<i>vsphere_admin_password</i>

- 2 From the **Home** menu of the vSphere Web Client, select **Hosts and Clusters**.
- 3 Select the mgmt01vc01.sfo01.rainpole.local vCenter Server, click the **Monitor** tab, click the **vSphere Replication** tab and click **Outgoing Replications**.
- 4 Configure point in time instances for the replications of the vRealize Operations Manager analytics cluster.
 - a Right-click a virtual machine of the analytics cluster and select **Reconfigure**.

Virtual Machine Name	Role
vrops-mstrn-01	Master node
vrops-repln-02	Master replica node
vrops-datan-03	Data node 1
vrops-datan-04	Data node 2

- b In the **Reconfigure Replication** wizard, click **Next** until you reach **Recovery Settings**.
 - c On the **Recovery Settings** page, select **Enable** under **Point in time instances** and keep **3** instances per day for the last **1** days.
 - d Click **Finish**.
 - e Repeat the steps for the other virtual machines in the analytics cluster.
- 5 Repeat [Step 4](#) to configure point in time instances for the replications of the Cloud Management Platform.

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

Clean Up Obsolete Appliances and Snapshots in Region A

After you complete the upgrade and operational verification of the virtual infrastructure components in Region A, clean up the environment from appliances that run old software versions and from snapshots of upgraded nodes.

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 Delete the virtual machines that contain the old version of vCenter Server and Platform Services Controller.

Role	Obsolete Virtual Machine	vCenter Server
Management Platform Services Controller	mgmt01psc01.sfo01_old	mgmt01vc01.sfo01.rainpole.local
Management vCenter Server	mgmt01vc01.sfo01_old	mgmt01vc01.sfo01.rainpole.local
Compute Platform Services Controller	comp01psc01.sfo01_old	comp01vc01.sfo01.rainpole.local
Compute vCenter Server	comp01vc01.sfo01_old	comp01vc01.sfo01.rainpole.local

- a In the **Navigator**, click **VMs and Templates**, expand the mgmt01vc01.sfo01.rainpole.local and navigate to the **mgmt01psc01.sfo01_old** virtual machine.
 - b Right-click the virtual machine and select **Delete from Disk**.
 - c Repeat the steps on the other obsolete virtual machines in Region A.
- 3 Delete the snapshots of upgraded management components in the vSphere Web Client.
 - a In the **Navigator**, click **VMs and Templates**, expand mgmt01vc01.sfo01.rainpole.local and navigate to the mgmt01vrms01 virtual machine.
 - b Right-click the **mgmt01vrms01** virtual machine and select **Manage Snapshots**.
 - c In the **Snapshot Manager** dialog box, click the snapshot that you created before the vSphere Replication update and select **Delete**.
 - d Click **Yes** in the confirmation dialog box and click **Close** in **Snapshot Manager**.
 - e Repeat the steps on the mgmt01srm01 virtual machine.

Configure the Anti-Affinity Rules for the Platform Services Controller Instances in Region B

After you upgrade the vCenter Server and Platform Services Controller instances, create the anti-affinity rules for the Platform Services Controllers in Region B in vSphere DRS to implement a configuration that matches the deployment guidelines in this VMware Validated Design.

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**, select **Hosts and Clusters** and expand the **mgmt01vc51.lax01.rainpole.local** control tree.
- 3 Select the **LAX01-Mgmt01** cluster and click the **Configure** tab.
- 4 On the **Configure** page, click **VM/Host Rules**.
- 5 On the **VM/Host Rules** page, click **Add**.
- 6 In the **Create VM/Host Rule** dialog, enter **anti-affinity-rule-psc** in the **Name** field, ensure the **Enable rule** checkbox is selected, select **Separate Virtual Machines** from the **Type** drop down menu, and click the **Add**.
- 7 In the **Add Rule Member** dialog, select **mgmt01psc51** and **comp01psc51**, and click **OK**.
- 8 In the **Create VM/Host Rule** dialog, click **OK** to create the rule.

Create Virtual Machine Groups to Define Startup Order in the Management Cluster in Region B

After you upgrade vSphere, the virtual machine groups allow you to define the startup order of virtual machines in Region B. Startup orders are used during vSphere HA events such that vSphere HA powers on virtual machines in a defined order.

Create virtual machine groups for the two Platform Services Controller instances and one for the Management vCenter Server, and include the groups in a startup order rule.

Table 4-23. VM Groups and Startup Rules for the Management vCenter Server and Platform Services Controller Instances

Region	vCenter Server Cluster	VM Group	Group Members	Rule
Region B	mgmt01vc51.lax01.rainpole.local > LAX01 > LAX01-Mgmt01	Platform Services Controllers	mgmt01psc51,comp01psc51	SDDC Management Virtual Machines
		vCenter Servers	mgmt01vc51	

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**, select **Hosts and Clusters** and expand the **mgmt01vc51.lax01.rainpole.local** tree.
- 3 Create a virtual machine DRS group for the Platform Services Controller instances.
 - a Select the **LAX01-Mgmt01** cluster and click the **Configure** tab.
 - b On the **Configure** page, click **VM/Host Groups**.
 - c On the **VM/Host Groups** page, click the **Add** button.
 - d In the **Create VM/Host Group** dialog box, enter **Platform Services Controllers** in the **Name** text box, select **VM Group** from the **Type** drop-down menu, and click the **Add** button.
 - e In the **Add VM/Host Group Member** dialog box, select **mgmt01psc51** and **comp01psc51**, and click **OK**.
- 4 Create a virtual machine DRS group for the vCenter Server virtual machine.
 - a Select the **LAX01-Mgmt01** cluster and click the **Configure** tab.
 - b On the **Configure** page, click **VM/Host Groups**.
 - c On the **VM/Host Groups** page, click the **Add** button.
 - d In the **Create VM/Host Group** dialog, enter **vCenter Servers** in the **Name** text box, select **VM Group** from the **Type** drop-down menu.
 - e Click the **Add** button, select **mgmt01vc51** in the **Add VM/Host Group Member** dialog box, and click **OK**.
 - f Click **OK**.

- 5 Create a DRS rule to power on the Platform Services Controller instances first and then the Management vCenter Server.
 - a Select the **LAX01-Mgmt01** cluster and click the **Configure** tab.
 - b On the **Configure** page, click **VM/Host Rules**.
 - c On the **VM/Host Rules** page, click the **Add** button.
 - d In the **Create VM/Host Rule** dialog, enter the following settings and click **OK**.

Setting	Value
Name	SDDC Management Virtual Machines
Enable rule	Selected
Type	Virtual Machines to Virtual Machines
First restart VMs in VM group	Platform Services Controllers
Then restart VMs in VM group	vCenter Servers

Deploy the Platform Services Controllers Load Balancer in Region B

After you upgrade vCenter Server and Platform Services Controllers in Region B, you deploy load balancing for all services and components related to Platform Services Controllers (PSC) using an NSX Edge load balancer.

Procedure

1 [Deploy the Platform Services Controller NSX Load Balancer in Region B](#)

The first step in deploying load balancing for the Platform Services Controller is to deploy the edge services gateway.

2 [Replace the Platform Services Controller Certificates in Region B](#)

After you deploy the load balancer for the Platform Services Controller instances in Region B, replace the machine SSL certificate on each Platform Services Controller instance with a custom certificate that is signed by the certificate authority (CA) on the child Active Directory (AD) server.

3 [Update the Single Sign-On Configuration on the Platform Services Controllers in Region B](#)

After you upgrade vCenter Server and Platform Services Controller, you must update the endpoints to reflect the name of the load balancer FQDN.

4 [Create Platform Services Controller Application Profiles in Region B](#)

Create application profiles for the TCP and HTTPS traffic on the Platform Services Controller load balancer.

5 [Create Platform Services Controller Server Pools in Region B](#)

Create server pools on the Platform Services Controller load balancer to direct TCP and HTTPS traffic from the load balancer to the two Platform Services Controller instances in Region B .

6 Create Virtual Servers in Region B

After you configure the application profiles and server pools on the load balancer, the NSX load balancer can start distributing network traffic across multiple servers. When a virtual server receives a TCP or HTTPS request, it selects the dedicated pool to send traffic to. You create virtual servers for the two configured server pools.

7 Update the DNS Record for the Platform Services Controller Load Balancer in Region B

You must modify the lax01psc51 DNS A record to point to the load balancer VIP after you configure the load balancer for the Platform Services Controller instances in Region B.

Deploy the Platform Services Controller NSX Load Balancer in Region B

The first step in deploying load balancing for the Platform Services Controller is to deploy the edge services gateway.

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 Click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.17.11.65** from the NSX Manager drop-down menu.
- 5 Click the **Add** icon tab to create an NSX Edge.

The **New NSX Edge** wizard appears.
- 6 On the **Name and description** page, enter the following settings and click **Next**.

Setting	Value
Install Type	Edge Services Gateway
Name	LAX01PSC51
Deploy NSX EDGE	Selected
Enable High Availability	Selected

New NSX Edge

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Firewall and HA

7 Ready to complete

Name and description

Install Type: ☒ **Edge Services Gateway**
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

☐ **Logical (Distributed) Router**
Provides Distributed Routing and Bridging capabilities.

Name: * LAX01PSC51

Hostname: lax01psc51.lax01.rainpole.local

Description:

Tenant:

☒ **Deploy NSX Edge**
Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.

☒ **Enable High Availability**
Enable HA, for enabling and configuring High Availability.

Back Next Finish Cancel

- 7 On the **Settings** page, enter the following settings and click **Next**.

Setting	Value
User Name	admin
Password	edge_admin_password
Enable SSH access	Selected
Enable auto rule generation	Selected
Edge Control Level logging	INFO

- 8 On the **Configure deployment** page, perform the following configuration steps and click **Next**.
- Select **LAX01**, from the **Datacenter** drop-down menu.
 - Click **Large** to specify the **Appliance Size**.

- c Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Resource pool	LAX01-Mgmt01
Datastore	LAX01A-VSAN01-MGMT01
Folder	NSX51

- d To create a second appliance, click the **Add** icon again, make the same selections in the **New NSX Appliance** dialog box, and click **OK**.

New NSX Edge

1 Name and description
2 Settings
3 **Configure deployment**
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete

Configure deployment

Datacenter: LAX01

Appliance Size: ☐ Compact ☒ Large ☐ X-Large ☐ Quad Large

NSX Edge Appliances

Resource Pool	Host	Datastore	Folder
LAX01-Mgmt01		LAX01A-VSAN...	NSX51
LAX01-Mgmt01		LAX01A-VSAN...	NSX51

Specifying a resource pool and datastore is mandatory for configuring the NSX Edge appliance.

Both the Edge Appliances are currently deployed on the same resources. It is recommended to deploy them on different resource pools, hosts and datastores.

Back Next Finish Cancel

- 9 On the **Configure Interfaces** page, click the **Add** icon to configure the PSCLB interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	PSCLB
Type	Internal
Connected To	vDS-Mgmt-Management
Connectivity Status	Connected
Primary IP Address	172.17.11.71
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- 10 On the **Default gateway** settings page, enter the following settings and click **Next**.

Setting	Value
Gateway IP	172.17.11.1
MTU	9000

New NSX Edge

1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete

Default gateway settings

☒ Configure Default Gateway

vNIC: * PSCLB

Gateway IP: * 172.17.11.1

MTU: 9000

Admin Distance: 1

Back Next Finish Cancel

- 11 On the **Firewall and HA** page, select the following settings and click **Next**.

Setting	Value
Configure Firewall default policy	Selected
Default Traffic Policy	Accept
Logging	Disable
vNIC	any
Declare Dead Time	15

New NSX Edge

1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete

Firewall and HA

☒ Configure Firewall default policy

Default Traffic Policy: ☒ Accept ☐ Deny

Logging: ☐ Enable ☒ Disable

Configure HA parameters
Configuring HA parameters is mandatory for HA to work.

vNIC: (seconds)

Declare Dead Time: (seconds)

Management IPs:

Management IPs must be in CIDR format with /30 subnet and must not overlap with any vnic subnets.

Back Next Finish Cancel

12 On the **Ready to complete** page, review the configuration settings you entered and click **Finish**.

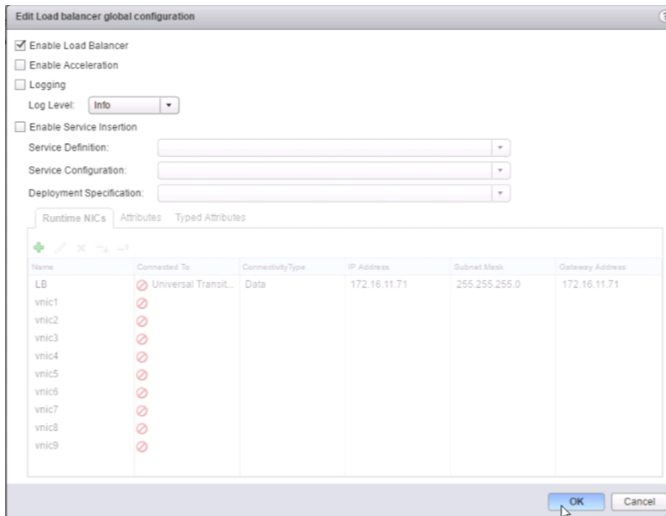
13 Enable HA logging.

- a In the **Navigator**, click **NSX Edges**.
- b Select **172.17.11.65** from the **NSX Manager** drop-down menu.
- c Double-click the device labeled **LAX01PSC51**.
- d Click the **Manage** tab and click the **Settings** tab.
- e Click **Configuration** and click **Change** in the **HA Configuration** window.
- f Select the **Enable Logging** check box and click **OK**.

14 Enable the Load Balancer service.

- a In the **Navigator**, click **NSX Edges**.
- b Select **172.17.11.65** from the **NSX Manager** drop-down menu.
- c Double-click the device labeled **LAX01PSC51**.
- d Click the **Manage** tab and click the **Load Balancer** tab.

- e Click **Global Configuration** and click **Edit**.
- f In the **Edit load balancer global configuration** dialog box, select **Enable Load Balancer** and click **OK**.



Replace the Platform Services Controller Certificates in Region B

After you deploy the load balancer for the Platform Services Controller instances in Region B, replace the machine SSL certificate on each Platform Services Controller instance with a custom certificate that is signed by the certificate authority (CA) on the child Active Directory (AD) server.

Since the Platform Services Controllers will be load balanced the machine certificate on both must be the same. The certificate must have a common name of the load-balanced Fully Qualified Domain Name (FQDN) and each Platform Service Controllers FQDN and short name along with the load balanced FQDN and short name must be in the Subject Alternate Name (SAN) of the generated certificate.

You replace certificates twice: on the Platform Services Controller for the Management vCenter Server `mgmt01psc51.lax01.rainpole.local` and on the Platform Services Controller for the Compute vCenter Server `comp01psc51.lax01.rainpole.local`. You start replacing certificates on Platform Services Controller `mgmt01psc51.lax01.rainpole.local` first.

Table 4-24. Certificate-Related Files on Platform Services Controllers

Platform Services Controller	Certificate File Name	Replacement Order
<code>mgmt01psc51.lax01.rainpole.local</code>	<code>lax01psc51.lax01.1.cer</code>	First
<code>comp01psc51.lax01.rainpole.local</code>	<code>lax01psc51.lax01.1.cer</code>	Second

Procedure

- 1 Log in to a Windows host that has access to both the AD server and the Platform Services Controllers as an administrator.

2 Generate the certificate for the Platform Services Controllers.

- a Download the VMware Validated Design Certificate Generation Utility from VMware Knowledge Base article [2146215](#).
- b Extract the contents of the zip file to the C:\ drive.
- c Open a Windows PowerShell prompt as an administrator and navigate to the C:\CertGenVVD-*version* folder.
- d Run Set-ExecutionPolicy RemoteSigned.
- e Run the following command to generate the certificate for the Platform Services Controller.

For example, you use the following command if you have downloaded version 2.1 of the utility.

```
.\CertGenVVD-2.1.ps1 -MSCASigned -attrib 'CertificateTemplate:VMware'
```

- f The certificate and supporting files are saved to the C:\CertGenVVD\SignedByMSCACerts folder.

3 Change the appliance shell to Bash shell to enable copying files to the appliance using the Secure Copy Protocol (SCP).

- a Open an SSH connection to mgmt01psc51.lax01.rainpole.local and log in with the following credentials.

Setting	Value
Username	root
Password	mgmtpsc_root_password

- b Run the following commands.

```
shell
chsh -s /bin/bash root
```

4 Copy the generated certificates from the Windows host to the Platform Services Controller appliance.

Use scp, WinSCP or FileZilla.

- a Copy the contents of the C:\CertGenVVD\SignedByMSCACerts\lax01psc51.lax01 folder to /tmp/certs.
- b Copy the Root64.cer file from C:\CertGenVVD\SignedByMSCACerts\RootCA folder to /tmp/certs.

5 Replace the certificate on the Platform Services Controller.

- a Start the vSphere Certificate Manager utility on the Platform Services Controller.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

- b Select **Option 1 (Replace Machine SSL certificate with Custom Certificate)**

- c Enter default vCenter Single Sign-On user name **administrator@vsphere.local** and the **vsphere_admin** password.
- d Select **Option 2 (Import custom certificate(s) and key(s) to replace existing Machine SSL certificate)**.
- e When prompted for the custom certificate, enter **/tmp/certs/lax01psc51.lax01.1.cer**.
- f When prompted for the custom key, enter **/tmp/certs/lax01psc51.lax01.key**.
- g When prompted for the signing certificate, enter **/tmp/certs/Root64.cer**.
- h When prompted to Continue operation, enter **Y**.

```
Note : Use Ctrl-D to exit.
Option [1 to 5]: 1

Please provide valid SSO and VC privileged user credential to perform certificate operations.
Enter username [Administrator@vsphere.local]:
Enter password:
  1. Generate Certificate Signing Request(s) and Key(s) for Machine SSL certificate
  2. Import custom certificate(s) and key(s) to replace existing Machine SSL certificate
Option [1 or 2]: 2

Please provide valid custom certificate for Machine SSL.
File : /tmp/certs/lax01psc51.lax01.1.cer

Please provide valid custom key for Machine SSL.
File : /tmp/certs/lax01psc51.lax01.key

Please provide the signing certificate of the Machine SSL certificate
File : /tmp/certs/Root64.cer

You are going to replace Machine SSL cert using custom cert
Continue operation : Option[Y/N] ? : Y
Get site nameCompleted [Replacing Machine SSL Cert...]
lax01
Lookup all services
Get service lax01:0ac7cf31-d7d0-44a1-9866-f7f9728e9aad
Update service lax01:0ac7cf31-d7d0-44a1-9866-f7f9728e9aad: spec: /tmp/avcspec_Q2Tvw
Get service lax01:ac42ca63-dec7-46fc-a27f-0ce2e3922ada
Update service lax01:ac42ca63-dec7-46fc-a27f-0ce2e3922ada: spec: /tmp/avcspec_C3PS1R
```

- i The Platform Services Controller services restart automatically.
- 6 Repeat [Step 3](#) to [Step 5](#) to replace the certificate on the Compute Platform Services Controller, comp01psc51.lax01.rainpole.local, in Region B.

Update the Single Sign-On Configuration on the Platform Services Controllers in Region B

After you upgrade vCenter Server and Platform Services Controller, you must update the endpoints to reflect the name of the load balancer FQDN.

Prerequisites

You create a DNS A record for the FQDN of the load balancer and the IP address of mgmt01psc51.lax01.rainpole.local. After you configure the load balancer is setup this DNS record is changed to the virtual IP of the load balancer.

Procedure

- 1 Create a DNS record for the load balancer FQDN.
 - a Open a remote desktop connection to your DNS server.
 - b Create a DNS A record with the following values.

FQDN	IP
lax01psc51.lax01.rainpole.com	172.17.11.61

Note After you configure the Platform Services Controller load balancer, you are going to is configured the IP address will be updated to reflect the load balancer's VIP instead of the IP address of mgmt01psc51.lax01.rainpole.local

- 2 Update the vCenter Single Sign-On configuration on mgmt01psc51.lax01.rainpole.local.
 - a Open an SSH connection to mgmt01psc51.lax01.rainpole.local.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	mgmtpsc_root_password

- c Run the following commands.

```
cd /usr/lib/vmware-sso/bin/
python updateSSOConfig.py --lb-fqdn=lax01psc51.lax01.rainpole.local
```

```
root@mgmt01psc51 [ ~ ]# cd /usr/lib/vmware-sso/bin/
root@mgmt01psc51 [ /usr/lib/vmware-sso/bin ]# python updateSSOConfig.py --lb-fqdn=lax01psc51.lax01.rainpole.local
script version:1.0.0
executing vmafd-cli command
modifying hostname.txt
modifying server.xml
Executing StopService --all
Executing StartService --all
```


3 Update the vCenter Single Sign-On configuration on comp01psc51.lax01.rainpole.local.

- a Open an SSH connection to comp01psc51.lax01.rainpole.local.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	comppsc_root_password

- c Run the following commands.

```
cd /usr/lib/vmware-sso/bin/
python updateSSOConfig.py --lb-fqdn=lax01psc51.lax01.rainpole.local
```

```
root@comp01psc51 [ ~ ]# cd /usr/lib/vmware-sso/bin/
root@comp01psc51 [ /usr/lib/vmware-sso/bin ]# python updateSSOConfig.py --lb-fqdn=lax01psc51.lax01.rainpole.local
script version:1.0.0
executing vmafd-cli command
Modifying hostname.txt
modifying server.xml
Executing StopService --all
Executing StartService --all
root@comp01psc51 [ /usr/lib/vmware-sso/bin ]#
```

4 Update the Platform Services Controller endpoints.

You update the endpoints only on one of the Platform Services Controller instances.

- a Open an SSH connection to mgmt01psc51.lax01.rainpole.local.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	mgmtpsc_root_password

- c Run the following commands.

```
cd /usr/lib/vmware-sso/bin/
python UpdateLsEndpoint.py --lb-fqdn=lax01psc51.lax01.rainpole.local --
user=Administrator@vsphere.local
```

- d Enter the *vsphere_admin_password* when prompted.

```
root@mgmt01psc51 [ /usr/lib/vmware-sso/bin ]# python UpdateLsEndpoint.py --lb-fqdn=lax01psc51.lax01.rainpole.local --user=ad
ministrator@vsphere.local
Password:
```

Create Platform Services Controller Application Profiles in Region B

Create application profiles for the TCP and HTTPS traffic on the Platform Services Controller load balancer.

After you configure a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

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 Click **Networking & Security**.

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

- 4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **LAX01PSC51** NSX Edge to manage its network settings.

- 5 Click the **Manage** tab, click **Load Balancer**, and select **Application Profiles**.

- 6 Click the **Add** icon, in the **New Profile** dialog box, enter the following values, and click **OK**.

Setting	Value for TCP Traffic	Value for HTTPS Traffic
Name	PSC-TCP	PSC-HTTPS
Type	TCP	HTTPS
Enable SSL Passthrough	Deselected	Selected
Persistence	Source IP	Source IP
Expires in (Seconds)	60	60

New Profile

Name:

Type:

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence:

Cookie Name:

Mode:

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certificate **Pool Certificates**

Service Certificates **CA Certificates** **CRL**

☐ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	lax01psc51.lax01.rainp	rainpole-DC01RPL-CA	Mon Mar 20 2017 - Wed M
<input type="radio"/>	VSM_SOLUTION_ca88:	VSM_SOLUTION_ca88:	Mon Mar 20 2017 - Wed Fi
<input type="radio"/>	VSM_SOLUTION_ca88:	VSM_SOLUTION_ca88:	Mon Mar 20 2017 - Wed Fi
<input type="radio"/>	VSM_SOLUTION_19e1:	VSM_SOLUTION_19e1:	Sun Feb 26 2017 - Tue Fe
<input type="radio"/>	VSM_SOLUTION_19e1:	VSM_SOLUTION_19e1:	Sun Feb 26 2017 - Tue Fe

Cipher:

Client Authentication:

OK **Cancel**

7 Repeat the step to create an application profile for HTTPS.

Create Platform Services Controller Server Pools in Region B

Create server pools on the Platform Services Controller load balancer to direct TCP and HTTPS traffic from the load balancer to the two Platform Services Controller instances in Region B .

A server pool consists of backend server members. After you create a server pool, you associate a service monitor with the pool to manage and share the backend servers flexibly and efficiently.

Repeat this procedure to create two server pools. Use the values indicated in the procedure to create the first and second server pools.

Procedure

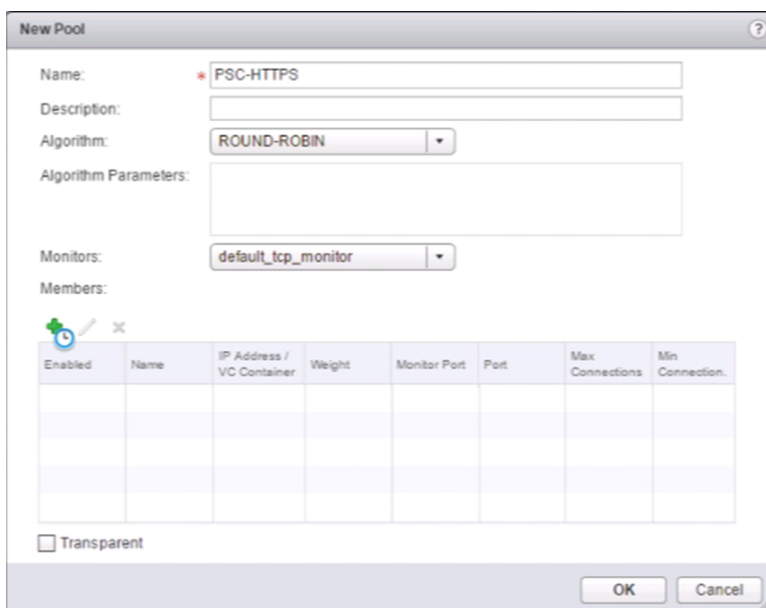
- 1 Log in to the Management vCenter Server by using the vSphere Web Client.

- 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 Click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager, and double-click the **LAX01PSC51** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.
- 6 Click the **Add** icon and in the **New Pool** dialog box, enter the following values.

Setting	Value
Name	PSC-HTTPS
Algorithm	ROUND-ROBIN
Monitors	default-tcp-monitor



The 'New Pool' dialog box is shown with the following fields and values:

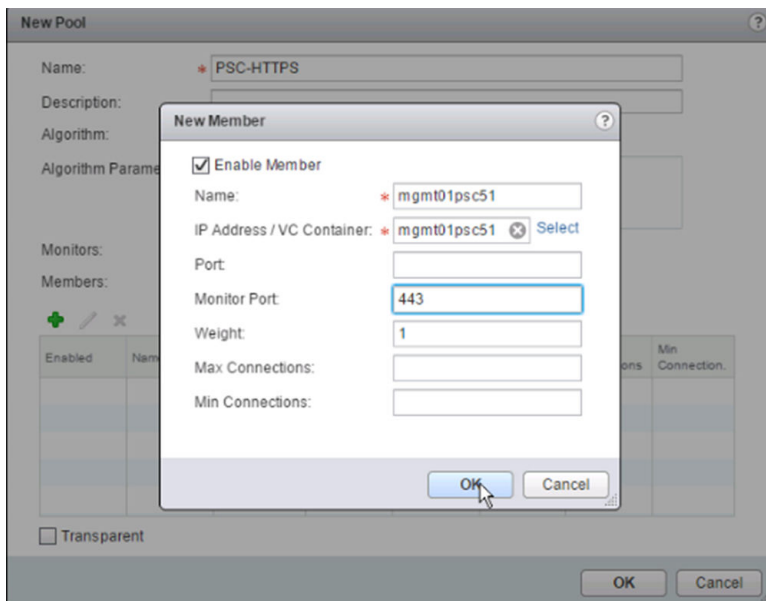
- Name: * PSC-HTTPS
- Description: (empty)
- Algorithm: ROUND-ROBIN
- Algorithm Parameters: (empty)
- Monitors: default_tcp_monitor
- Members: (empty table)
- Transparent: ☐

Buttons: OK, Cancel

7 In **New Members** dialog box, click the **Add** icon to add the first pool member.

8 In the **New Member** dialog box, enter the following values, and click **OK**.

Setting	Value for HTTPS Server Pool	Value for TCP Server Pool
Name	mgmt01psc51	mgmt01psc51
IP Address/VC Container	mgmt01psc51	mgmt01psc51
State	Enable	Enable
Monitor Port	443	389
Weight	1	1



The 'New Member' dialog box is shown with the following fields and values:

- Enable Member: ☒
- Name: * mgmt01psc51
- IP Address / VC Container: * mgmt01psc51 (with a 'Select' button)
- Port: (empty)
- Monitor Port: 443
- Weight: 1
- Max Connections: (empty)
- Min Connections: (empty)

Buttons: OK, Cancel

- 9 Under **Members**, click the **Add** icon to add the second pool member.
- 10 In the **New Member** dialog box, enter the following values, click **OK** and click **OK** to save the Platform Services Controller server pool.

Setting	Value for HTTPS Server Pool	Value for TCP Server Pool
Name	comp01psc51	comp01psc51
IP Address/VC Container	comp01psc51	comp01psc51
State	Enable	Enable
Port		
Monitor Port	443	389
Weight	1	1

New Pool

Name: * PSC-HTTPS

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_tcp_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	mgmt01...	mgmt01p...	1	443		0	0
✓	comp01...	comp01p...	1	443		0	0

☐ Transparent

OK Cancel

- 11 Repeat the procedure to create the second server pool PSC-TCP and add the two Platform Services Controller instances to it.

Create Virtual Servers in Region B

After you configure the application profiles and server pools on the load balancer, the NSX load balancer can start distributing network traffic across multiple servers. When a virtual server receives a TCP or HTTPS request, it selects the dedicated pool to send traffic to. You create virtual servers for the two configured server pools.

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 Click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.17.11.65** as the NSX Manager and double-click the **LAX01PSC51** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Virtual Servers**.
- 6 Click the **Add** icon, and in the **New Virtual Server** dialog box configure the values for the virtual server you are adding, and click **OK**.

Setting	Value for TCP Traffic	Value for HTTPS Traffic
Enable Virtual server	Selected	Selected
Application Profile	PSC-TCP	PSC-HTTPS
Name	PSC-TCP	PSC-HTTPS
Description	389-LDAP,2012-Control Interface,2014-RPC Port,2020-Authentication,636-SSL LDAP	Data from the vSphere Web Client
IP Address	172.17.11.71	172.17.11.71
Protocol	TCP	HTTPS
Port	389,636,2012,2014,2020	443
Default Pool	PSC-TCP	PSC-HTTPS

New Virtual Server

General | Advanced

☒ Enable Virtual Server

☐ Enable Acceleration

Application Profile: * PSC-TCP

Name: * PSC-TCP

Description:

IP Address: * 172.17.11.71 [Select IP Address](#)

Protocol: TCP

Port / Port Range: * 389,636,2012,2014,2020

Default Pool: PSC-TCP

Connection Limit:

Connection Rate Limit: (CPS)

OK Cancel

- 7 Repeat the steps to create a virtual server for the other virtual server.

Update the DNS Record for the Platform Services Controller Load Balancer in Region B

You must modify the `lax01psc51` DNS A record to point to the load balancer VIP after you configure the load balancer for the Platform Services Controller instances in Region B.

Procedure

- 1 Open an RDP connection to the AD server `dc01lax.lax01.rainpole.local` that resides in the `lax01.rainpole.local` domain as administrator.
- 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 `lax01psc51` record on the right.
- 4 Double-click the `lax01psc51` record, change the IP address to the VIP of the load balancer and click **OK**.

Setting	Value
Fully Qualified domain name (FQDN)	<code>lax01psc51.lax01.rainpole.local</code>

Setting	Value
IP Address	172.17.11.71
Update Associated Pointer (PTR) record	Selected

Repoint the vCenter Server Instances to the Platform Services Controller Load Balancer in Region B

After you configure the NSX load balancer to distribute the traffic between the Management vCenter Server and Compute vCenter Server in Region B, repoint the vCenter Server instances in the region from the individual Platform Services Controller instances to the load balancer.

Procedure

- 1 Log in to `mgmt01vc51.lax01.rainpole.local` by using Secure Shell (SSH) client.
 - a Open an SSH connection to the virtual machine `mgmt01vc51.lax01.rainpole.local`.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vcenter_server_root_password</i>

- 2 To repoint vCenter Server to the load balancer for the Platform Services Controller instances, run the following command.

```
cmsso-util repoint --repoint-psc lax01psc51.lax01.rainpole.local
```

- 3 Verify that vCenter Server directs its requests to the load balancer. run the following commands.
 - a Run the following command and verify that it returns `lax01psc51.lax01.rainpole.local` Platform Services Controller Load Balancer in Region B.

```
/usr/lib/vmware-vmafd/bin/vmafd-cli get-dc-name --server-name localhost
```

- b Run the following command and verify that it returns the `https://lax01psc51.lax01.rainpole.local:443/lookupservice/sdk` Lookup Service of the Platform Services Controller Load Balancer in Region B.

```
/usr/lib/vmware-vmafd/bin/vmafd-cli get-ls-location --server-name localhost
```

- 4 Verify that all vCenter Server services are running.

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

- 5 Repeat the procedure on the Compute vCenter Server `comp01vc51.lax01.rainpole.local`.

Connect the NSX Managers to the Platform Services Controller Load Balancer in Region B

After you upgrade NSX and vSphere components in the management cluster, and deploy the Platform Services Controller load balancers in the two regions, in each region, you connect the NSX Manager for the management cluster to the load balancer for vCenter Single Sign-On communication.

Table 4-25. Lookup Service URLs for the NSX Managers for the Management Clusters

NSX Manager URL	Lookup Service FQDN
https://mgmt01nsxm51.lax01.rainpole.local	lax01psc51.lax01.rainpole.local
https://comp01nsxm51.lax01.rainpole.local	lax01psc51.lax01.rainpole.local

Procedure

- 1 Log in to the appliance user interface of the Management NSX Manager.
 - a Open a Web browser and go to **https://mgmt01nsxm51.lax01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	nsx_manager_admin

- 2 Click **Manage vCenter Registration**.
- 3 Under **Lookup Service**, click **Edit**.
- 4 In the **Lookup Service** dialog box, change the address in the **Lookup Service IP** text box to **lax01psc51.lax01.rainpole.local** and click **OK**.

Setting	Value
Lookup Service IP	lax01psc51.lax01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	vsphere_admin_password

- 5 In the **Trust Certificate?** dialog box, click **Yes**.
- 6 Wait for the **Status** indicators for the Lookup Service to change to the Connected status.
- 7 Repeat the procedure to connect the NSX Manager for the shared edge and compute cluster in Region B comp01nsxm51.lax01.rainpole.local to the newly-deployed Platform Services Controller load balancer in the region.

Reconnect vSphere Replication to vCenter Server in Region B

Reconnect the vSphere Replication instance to the Platform Services Controller in Region B using the secure account svc-vr and the Platform Services Controller load balancer address.

Table 4-26. Configuration Changes on vSphere Replication after Upgrade

Region	vSphere Replication Management Interface URL	Old Single Sign-On Account	New Single Sign-On Account	Old Lookup Service URL	New Lookup Service URL
Region B	https://mgmt01vrms51.lax01.rainpole.local:5480	administrator@vsphere.local	svc-vr@rainpole.local	mgmt01psc51.lax01.rainpole.local	lax01psc51.lax01.rainpole.local

Procedure

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

- a Open a Web browser and go to **https://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 **Administration**.

- 3 Change the connection settings of the vSphere Replication appliance and reconnect it to the Platform Services Controller pair and Management vCenter Server.

- a Open a Web browser and go to **https://mgmt01vrms51.lax01.rainpole.local:5480**.
- b Log in using the following credentials.

Setting	Value
User name	root
Password	vr_lax_root_password

The virtual appliance management interface of the vSphere Replication instance opens.

- c On the **VR** tab, click **Configuration**, enter the following settings, and click **Save and Restart Service**.

You change the administrator vCenter Single Sign-On account to the svc-vr service account and the lookup service address mgmt01psc51.lax01.rainpole.local to the address of the Platform Services Controller load balancer lax01psc51.lax01.rainpole.local.

Setting	Value
Configuration Mode	Configure using the embedded database
LookupService Address	<code>lax01psc51.lax01.rainpole.local</code>
SSO Administrative Account	<code>svc-vr@rainpole.local</code>
Password	<code>svc-vr_password</code>
VRM Host	172.17.11.123
VRM Site Name	mgmt01vc51.lax01.rainpole.local
vCenter Server Address	mgmt01vc51.lax01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	<code>vcenter_server_admin_email</code>

- d In the **Confirm SSL Certificate** dialog box, click **Accept**.

Reconnect Site Recovery Manager to vCenter Server and Platform Services Controller Instances in Region B

After you upgrade vCenter Server and Site Recovery Manager, redirect Site Recovery Manager to the load balancer of the two Platform Services Controller instances in Region B using the svc-srm service account.

Procedure

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

Region	Site Recovery Manager FQDN
Region B	mgmt01srm51.lax01.rainpole.local

- a Open an RDP connection to the virtual machine mgmt01srm51.lax01.rainpole.local.
- b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	<code>windows_administrator_password</code>

- 2 Open **Programs and Features** from the Windows Control Panel.
- 3 Select the entry for the **VMware vCenter Site Recovery Manager** and click **Change**.

The VMware Site Recovery Manager installation wizard appears.

- 4 On the Welcome page, click **Next**.
- 5 Select **Modify** and click **Next**.
- 6 On the **vSphere Platform Services Controller** page, change the Platform Services Controller address, enter the svc-srm account settings, and click **Next**.

Setting	Value
Address	<code>lax01psc51.lax01.rainpole.local</code>
HTTPS Port	443
Username	<code>svc-srm@rainpole.local</code>
Password	<code>svc-srm_password</code>

- 7 If prompted to accept the certificate of the Platform Services Controller in the **Platform Services Controller Certificate** dialog box, click **Accept**.
- 8 On the **VMware vCenter Server** page, click **Next**.
- 9 If prompted, in the **vCenter Server Certificate** dialog box, click **Accept**.
- 10 On the **Site Recovery Manager Extension** page, leave the existing settings, and click **Next**.

Setting	Value
Administrator E-mail	<code>srm_admin_lax_email_address</code>
Local Host	172.17.11.124
Listener Port	9086

- 11 On the **Certificate Type** page, select **Use existing certificate** and click **Next**.
- 12 On the **Database Server Selection** page, select **Use the embedded database server** and click **Next**.
- 13 On the **Embedded Database Configuration** page, enter the following settings and click **Next**.

Setting	Value
Data Source Name	<code>SRM_SITE_LAX</code>
Database User Name	<code>srm_admin</code>
Database Password	<code>srm_admin_lax_password</code>
Database Port	5678
Connection Count	5
Max. Connections	20

- 14 On the **Site Recovery Manager Service Account** page, enter the following credentials, and click **Next**.

Setting	Value
Use Local System account	Deselected
Username	MGMT01SRM51\Administrator
Password	<i>mgmt01srm51_admin_password</i>

- 15 On the **Ready to Install the Program** page, click **Install**.

- 16 Click **Finish** to complete the installation.

- 17 Reconnect the Site Recovery Manager instance in Region B.

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

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

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

- 19 On the **Site Recovery** page, click **Sites**.

- 20 On the **Sites** page, right-click **mgmt01vc51.lax01.rainpole.local** and select **Reconfigure Pairing**.

The **Reconfigure Site Recovery Manager Server Pairing** wizard appears.

- 21 On the **Select Site** page, validate the following settings and click **Next**.

Settings	Value
PSC address	sfo01psc01.sfo01.rainpole.local
Port	443

- 22 On the **Select vCenter Server** page, enter the administrator@vsphere.local password, validate the following settings, and click **Finish**.

Settings	Value
vCenter Servers with matching SRM Extension	mgmt01vc01.sfo01.rainpole.local
Username	svc-srm@rainpole.local
Password	<i>svc-srm_password</i>

Register vSphere Data Protection with the Management vCenter Server in Region B

After you upgrade the virtual appliances for vSphere Data Protection, in Region B register the appliance with the Management vCenter Server using vSphere Data Protection Service Account and NSX Load Balancer for Platform Services Controller.

Procedure

- 1 Log in to the vSphere Data Protection Configuration Utility.

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

Region	URL
Region B	https://mgmt01vdp51.lax01.rainpole.local:8543/vdp-configure/

- b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vdp_root_password</i>

- 2 On the **Configuration** tab, click the wheel icon next to **VDP Appliance** and select **vCenter Registration**.

The **vCenter Registration** wizard appears.

- 3 On the **vCenter Registration** page, select **I have reviewed the information. I want to reconfigure vCenter** and click **Next**.
- 4 On the **vCenter Configuration** page, change the **vCenter username** setting to use the svc-vdp service account for authentication to vCenter Server and the **SSO FQDN or IP** setting to connect vSphere Data Protection to the NSX load balancer for the Platform Services Controllers, and click **Next**.

vCenter Server Setting	Value
vCenter username	rainpole.local\svc-vdp
vCenter password	<i>svc-vdp_password</i>
vCenter FQDN or IP	mgmt01vc51.lax01.rainpole.local
vCenter HTTP port	80
vCenter HTTPS port	443
Verify vCenter certificate	Deselected

Single Sign-On Setting	Value
Use vCenter for SSO authentication	Deselected
SSO FQDN or IP	lax01psc51.lax01.rainpole.local
SSO port	443

- 5 On the **Ready to Complete** page review the configuration changes and click **Finish**.
- 6 If you are unable to proceed further because of a false status like `One or more jobs are running` although you are not running any backup jobs, run this command to restart the Tomcat Web server and try again.

```
emwebapp.sh --restart
```

- 7 Verify that the vSphere Data Protection is accessible in the vSphere Web Client after you complete the initial configuration of vSphere Data Protection.
 - 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	admininistrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- c On the vSphere Web Client Home page, verify that the **VDP** icon is available and that you can connect to each appliance.

Clean Up Obsolete Appliances and Snapshots in Region B

After you complete the upgrade and operational verification of the virtual infrastructure components in Region B, clean up the environment from appliances that run old software versions and from snapshots of upgraded nodes.

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 Delete the virtual machines that contain the old version of vCenter Server and Platform Services Controller.

Role	Obsolete Virtual Machine	vCenter Server
Management Platform Services Controller	mgmt01psc51.lax01_old	mgmt01vc51.lax01.rainpole.local
Management vCenter Server	mgmt01vc51.lax01_old	mgmt01vc51.lax01.rainpole.local
Compute Platform Services Controller	comp01psc51.lax01_old	comp01vc51.lax01.rainpole.local
Compute vCenter Server	comp01vc51.lax01_old	comp01vc51.lax01.rainpole.local

- a In the **Navigator**, click **VMs and Templates**, expand the mgmt01vc51.lax01.rainpole.local tree and navigate to the **mgmt01psc51.lax01_old** virtual machine.
 - b Right-click the virtual machine and select **Delete from Disk**.
 - c Repeat the steps on the other obsolete virtual machines in Region B.
- 3 Delete the snapshots of upgraded management components in the vSphere Web Client.
 - a In the **Navigator**, click **VMs and Templates**, expand the mgmt01vc51.lax01.rainpole.local tree and navigate to the mgmt01vrms51 virtual machine.
 - b Right-click the **mgmt01vrms51** virtual machine and select **Manage Snapshots**.
 - c In the **Snapshot Manager** dialog box, click the snapshot that you created before the vSphere Replication update and select **Delete**.
 - d Click **Yes** in the confirmation dialog box and click **Close** in **Snapshot Manager**.
 - e Repeat the steps on the mgmt01srm51 virtual machine.